



**UNIVERSITY OF PIRAEUS  
SCHOOL OF INFORMATION AND COMMUNICATION TECHNOLOGIES  
DEPARTMENT OF INFORMATICS**

**PHD THESIS**

|                                |                                                                                                                                                                                                                                                            |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Thesis Title:</b>           | <p>(English)<br/><b>CyberICT: A hybrid evaluation framework<br/>for products and supply chain services</b></p> <p>(Greek)<br/><b>ΚyberICT: Υβριδικό πλαίσιο αξιολόγησης<br/>κυβερνοασφάλειας προϊόντων και<br/>υπηρεσιών εφοδιαστικών αλυσίδων ΤΠΕ</b></p> |
| <b>Student's name-surname:</b> | Eleni Maria Kalogeraki                                                                                                                                                                                                                                     |
| <b>Father's name:</b>          | Nikolaos                                                                                                                                                                                                                                                   |
| <b>Student's ID No:</b>        | ΠΛΔ/1216                                                                                                                                                                                                                                                   |
| <b>Supervisor:</b>             | Despina Polemi, Professor                                                                                                                                                                                                                                  |

**July, 2026**

---

**PhD Thesis**  
**was prepared during the Programme of Doctoral Studies**  
**of the Department of Informatics**  
**of the School of Information and Communication Technologies**  
**of the University of Piraeus**  
**for the degree of Doctor of Philosophy**

**3-Member Counseling Committee**

|                                                                                                                                                                     |                                                                                                                                                                       |                                                                                                                                                                      |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Despina Polemi</b><br>Professor<br>University of Piraeus<br>School of Information and<br>Communication Technologies<br>Department of Informatics<br>(Supervisor) | <b>Georgios Tsihrintzis</b><br>Professor<br>University of Piraeus<br>School of Information and<br>Communication Technologies<br>Department of Informatics<br>(Member) | <b>Dimitrios Apostolou</b><br>Professor<br>University of Piraeus<br>School of Information and<br>Communication Technologies<br>Department of Informatics<br>(Member) |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|

**PhD Thesis**  
**was presented before the 7-Member Examination Committee**  
**and approved on 21/07/2026**

**7-Member Examination Committee**

|                                                                                                                                                     |                                                                                                                                                                           |                                                                                                                                                          |
|-----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Despina Polemi</b><br>Professor<br>University of Piraeus<br>School of Information and<br>Communication Technologies<br>Department of Informatics | <b>Georgios Tsihrintzis</b><br>Professor<br>University of Piraeus<br>School of Information and<br>Communication Technologies<br>Department of Informatics                 | <b>Dimitrios Apostolou</b><br>Professor<br>University of Piraeus<br>School of Information and<br>Communication Technologies<br>Department of Informatics |
| <b>Sotirios Ioannidis</b><br>Professor<br>Technical University of Crete<br>School of Electrical and<br>Computer Engineering                         | <b>Panayiotis Kotzanikolaou</b><br>Professor<br>University of Piraeus<br>School of Information and<br>Communication Technologies<br>Department of Informatics             | <b>Maria Lamprou</b><br>Professor<br>University of the Aegean<br>School of Business Studies<br><br>Department of Shipping,<br>Trade and Transport        |
|                                                                                                                                                     | <b>Ioannis Stamatiou</b><br>Professor<br>University of Patras<br>School of Economics and<br>Business Administration<br>Department of Management<br>Science and Technology |                                                                                                                                                          |

## *In Memoriam*

*This dissertation is dedicated to the memory of my former supervisor, Professor Themis Panayiotopoulos. His wisdom, academic rigour, generosity, and kindness profoundly influenced my decision to embark on this academic journey and laid the foundation for this doctoral research. Together, we started exploring the intersection between the business and information technology domains. It was when he inspired me to conduct interdisciplinary research and bridge diverse scientific domains through semantic technologies.*

*His vision, guidance, and trust in my abilities strengthened my resolve and sustained me throughout my research journey. I feel very privileged to have learned from him not only how to evolve as a researcher but also how to improve myself. I will always cherish his mentorship and the example he set as a scholar and as a person.*

*I would also like to dedicate this dissertation to the memory of my beloved uncle, Nikos Tsaldaris, whose intellect, unwavering optimism, enduring love, and remarkable sense of humour profoundly shaped my character and outlook on life. He stood by me through every challenge and every success, instilling in me the value of perseverance in pursuing my goals and inspiring me to face life's challenges with confidence, resilience, and creativity.*

*Although neither had the opportunity to see the completion of this dissertation, their influence is reflected throughout these pages. Their memory will always remain with me.*

## Acknowledgements

First and foremost, I would like to express my deepest appreciation and gratitude to my supervisor, Professor Nineta Polemi, whose continuous guidance, unwavering support, and patience have played a pivotal role in my scientific and professional development throughout my doctoral journey. She has been a dedicated mentor whose insight, encouragement, and confidence in my abilities guided and motivated me throughout this research, broadening my horizons and allowing me to explore cybersecurity and certification research directions that inspired me to undertake this dissertation. It has been both a privilege and a pleasure to work with her.

I would also like to extend my sincere gratitude to the members of my Counseling Committee, Professor George Tsihrintzis and Professor Dimitris Apostolou, for their insightful comments, valuable suggestions, and continuous support throughout my doctoral research.

Moreover, I am very grateful for the invaluable collaboration with Dr. Spyros Papastergiou, whose dedication and persistent efforts have greatly enriched this research. Working together on common research projects, exchanging ideas through stimulating discussions, and co-authoring several scientific publications have been a truly rewarding experience. His encouragement and steadfast support, especially during challenging periods, has been sincerely appreciated.

Last but not least, I would like to especially thank Dr. Thanos Karantjias and the rest of the research team for providing me with the opportunity to contribute to the design of cybersecurity risk management and certification services within the framework of Horizon Europe research projects.

Piraeus, 15 June 2026



## Περίληψη

Η επιταχυνόμενη ψηφιοποίηση των σύγχρονων οικονομιών έχει αναδείξει την ασφάλεια των προϊόντων και των αλυσίδων εφοδιασμού Τεχνολογιών Πληροφορικής και Επικοινωνιών (ΤΠΕ) σε ζήτημα ρυθμιστικής και επιχειρησιακής επείγουσας ανάγκης. Παρότι ο Κανονισμός για την Κυβερνοανθεκτικότητα -Κανονισμός (ΕΕ) 2024/2847-, η Πράξη για την Κυβερνοασφάλεια -Κανονισμός (ΕΕ) 2019/881- και η Οδηγία NIS 2 -Οδηγία (ΕΕ) 2022/2555- της Ευρωπαϊκής Ένωσης προωθούν την ενοποίηση διαδικασιών εκτίμησης κινδύνου και αξιολόγησης συμμόρφωσης, οι υφιστάμενες ερευνητικές προσεγγίσεις υστερούν σε εναρμόνιση, αφήνοντας τους ενδιαφερόμενους φορείς χωρίς δομημένη καθοδήγηση. Το κενό αυτό επιτείνεται από τον κατακερματισμό προτύπων, την τεχνική πολυπλοκότητα των σύνθετων προϊόντων ΤΠΕ και την ανεπάρκεια των διαθέσιμων μεθόδων ανάλυσης κινδύνου.

Η παρούσα διδακτορική διατριβή προτείνει ένα **υβριδικό πλαίσιο αξιολόγησης προϊόντων και υπηρεσιών εφοδιαστικής αλυσίδας ΤΠΕ (CyberICT hybrid evaluation framework for products and supply chain services)** που ενοποιεί την αξιολόγηση κινδύνου κυβερνοασφάλειας και την αξιολόγηση της συμμόρφωσης σε ένα ενιαίο πλαίσιο για σύνθετα προϊόντα ΤΠΕ και των υπηρεσιών των εφοδιαστικών αλυσίδων τους. Θεμελιωμένη στη μεθοδολογία Design Science Research, η εργασία παράγει ένα συνεκτικό σύνολο αλληλένδετων τεχνουργημάτων: τη μεθοδολογία διαχείρισης κινδύνων κυβερνοασφάλειας με αντίστοιχη οντολογία κινδύνου, την προσέγγιση για την προετοιμασία του Προφίλ Προστασίας σύνθετων προϊόντων ΤΠΕ με αντίστοιχη ταξινόμια και την οντολογία προτύπων κυβερνοασφάλειας.

Η **Μεθοδολογία Διαχείρισης Κινδύνων CyberICT** υποστηρίζει τη σταδιακή διαδικασία αξιολόγησης ευπαθειών, απειλών και κινδύνων, καθώς και των διαδοχικών επιπτώσεών τους, ενώ παράλληλα διερευνά τα αντίστοιχα κλιμακωτά φαινόμενα σε σύνθετα περιβάλλοντα ΤΠΕ. Τα περιβάλλοντα αυτά περιλαμβάνουν σύνθετα προϊόντα ΤΠΕ που δύνανται να αναλυθούν στα πρωτεύοντα συστατικά τους στοιχεία —λογισμικό (software), υλικολογισμικό (firmware) και υλικό (hardware)— καθώς και τις υποστηρικτικές εφοδιαστικές αλυσίδες ετερογενών δικτύων πολυτροπικών υποδομών ΤΠΕ. Προκειμένου να καλυφθούν οι διαφορετικές ανάγκες αξιολόγησης των ενδιαφερόμενων μερών ΤΠΕ, όπως αυτές προέκυψαν από τη βιβλιογραφική ανασκόπηση, η μεθοδολογία παρέχει τρεις διακριτές προοπτικές αξιολόγησης για την ανάλυση υπηρεσιών εφοδιαστικής αλυσίδας ΤΠΕ: την επιχειρηματική, την ολιστική-τεχνική και την εξειδικευμένη ανά τομέα, καθεμία από τις οποίες αποτυπώνει διαφορετική διάσταση του περιβάλλοντος της εφοδιαστικής αλυσίδας. Αναφορικά με την επιχειρηματική ανάλυση, χρησιμοποιούνται τεχνικές μοντελοποίησης διεργασιών για την ενίσχυση της κατανόησης των υπηρεσιών εφοδιαστικής αλυσίδας ΤΠΕ. Μέσω της αναγνώρισης κυβερνοεξαρτήσεων μεταξύ των αλληλοσυνδεδεμένων στοιχείων ΤΠΕ, η μεθοδολογία αντιμετωπίζει την τεχνική πολυπλοκότητα αυτών των περιβάλλοντων, με την αξιολόγηση των αλυσιδωτών επιπτώσεων και της διάδοσης των εντοπισθέντων ευπαθειών και κινδύνων. Η εκμεταλλευσιμότητα των ευπαθειών αξιολογείται μέσω ενός σταθμισμένου μοντέλου βαθμολόγησης, το οποίο λαμβάνει υπ' όψιν συμπληρωματικές πτυχές των εγγενών χαρακτηριστικών της ευπαθείας και των χαρακτηριστικών των φορέων κυβερνοαπειλών. Ο ορισμός ενός συνόλου κανόνων κρισιμότητας για υπηρεσίες, διαδικασίες και περιουσιακά στοιχεία της εφοδιαστικής αλυσίδας ΤΠΕ, με τους οποίους προσδιορίζεται η λειτουργική σημασία, η εξάρτηση των διαδικασιών, η επιχειρησιακή συνέχεια, τα χαρακτηριστικά ανθεκτικότητας και η στρατηγική θέση των περιουσιακών στοιχείων ΤΠΕ στοχεύει στη διεύρυνση της εκτίμησης των επιπτώσεων των ευπαθειών. Επιπλέον, αναπτύχθηκε ένα **μοντέλο Προσομοίωσης Επίθεσης και Δημιουργίας Αλυσίδας Πειστηρίων (Attack Simulation and Evidence Chain Generation —ASECG)** για τον υπολογισμό όλων των αξιόπιστων διαδρομών επίθεσης που

αποτυπώνουν την κίνηση ενός εισβολέα εντός του δικτύου ΤΠΕ στο πλαίσιο ενός επιβεβαιωμένου συμβάντος ασφαλείας. Οι ανωτέρω τεχνικές υπολογισμού αποσκοπούν στην υποστήριξη μιας πολυπαραγοντικής ανάλυσης κινδύνου που λαμβάνει υπόψη τις τεχνικές ιδιαιτερότητες των ευρείας κλίμακας δικτύων ΤΠΕ και στοχεύει στη διεύρυνση των τεχνικών μοντελοποίησης επιθέσεων, αποτυπώνοντας τον τρόπο με τον οποίο συμπεριφέρονται τα διασυνδεδεμένα συστήματα και τον τρόπο με τον οποίο οι αποτυχίες ή οι επιθέσεις μπορούν να διαδοθούν σε εξαρτώμενα στοιχεία βάσει εμπειρικών πειστηρίων. Η μεθοδολογία αυτή υλοποιείται μέσω μιας ειδικά σχεδιασμένης ταξινομίας για το Προφίλ Προστασίας, στηριζόμενης σε ένα ιεραρχικό μοντέλο δεδομένων που καθορίζει τις δομικές σχέσεις μεταξύ των συνιστωσών του Προφίλ Προστασίας, συμπεριλαμβανομένου του Σύνθετου Στόχου Αξιολόγησης (Composite Target of Evaluation).

Το **CyberICT Protection Profile** υποστηρίζεται από ένα σταδιακό πλαίσιο καθοδήγησης (και μια συμπληρωματική ταξινομία) των εμπλεκόμενων φορέων των ΤΠΕ για: i) την προετοιμασία του Προφίλ Προστασίας των σύνθετων προϊόντων τους, και ii) τη συστηματική αξιολόγηση των ισχυρισμών αυτού του Προφίλ Προστασίας στο πλαίσιο του Ευρωπαϊκού Σχήματος Πιστοποίησης της Κυβερνοασφάλειας βάσει Κοινών Κριτηρίων (EUCC). Το CyberICT Protection Profile αξιοποιεί την ανωτέρω Μεθοδολογία Διαχείρισης Κινδύνων (CyberICT Risk Management Methodology) για την αξιολόγηση του επιπέδου προστασίας σύνθετων προϊόντων ΤΠΕ. Η προσέγγιση αυτή υλοποιείται μέσω μιας ειδικά σχεδιασμένης ταξινομίας για το Προφίλ Προστασίας, στηριζόμενης σε ένα ιεραρχικό μοντέλο δεδομένων που καθορίζει τις δομικές σχέσεις μεταξύ των συνιστωσών του Προφίλ Προστασίας, συμπεριλαμβανομένου του Σύνθετου Στόχου Αξιολόγησης (Composite Target of Evaluation). Επιπλέον, η ταξινομία ενσωματώνει δομημένες ταξινομήσεις συνιστωσών του Προφίλ Προστασίας: οι κατηγορίες απειλών (threat categories) αντιστοιχίζονται με στόχους ασφαλείας (security objectives), οι οποίοι με τη σειρά τους αντιστοιχίζονται με λειτουργικές απαιτήσεις ασφαλείας (security functional requirements) και αυτές με συναφή αντίμετρα ασφαλείας (security controls). Αυτή η ταξινόμηση επιτρέπει στους εμπλεκόμενους φορείς των ΤΠΕ να συναγάγουν μετρήσιμα και εφαρμόσιμα σύνολα απαιτήσεων και αντίστοιχων αντιμέτρων ασφαλείας. Το προτεινόμενο υβριδικό πλαίσιο αξιολόγησης στοχεύει να υποστηρίξει τους εμπλεκόμενους φορείς των ΤΠΕ στην ενίσχυση της ετοιμότητας των ΤΠΕ προϊόντων τους για την Ευρωπαϊκή Πιστοποίηση Κυβερνοασφάλειας σύμφωνα με την Πράξη για την Κυβερνοασφάλεια. Επιπλέον, παρέχει έναν μηχανισμό αξιολόγησης που μπορεί να χρησιμοποιηθεί από τις επιχειρήσεις για τη συμμόρφωση προϊόντων με ψηφιακά στοιχεία (products with digital elements) σύμφωνα με τον Κανονισμό για την Κυβερνοανθεκτικότητα, ιδίως για τις κατηγορίες προϊόντων που αναφέρεται ότι απαιτείται αυστηρή και σχολαστική αξιολόγηση της ασφάλειας. Επιπροσθέτως, η ενσωματωμένη μεθοδολογία διαχείρισης κινδύνων της εφοδιαστικής αλυσίδας ΤΠΕ, συμβάλλει στην ανάγκη για ενίσχυση της ασφάλειας και ανθεκτικότητας των εφοδιαστικών αλυσίδων ΤΠΕ, σύμφωνα με τις συστάσεις της Οδηγίας NIS 2.

Στο πλαίσιο της παρούσας διατριβής δημιουργήθηκαν **δύο οντολογίες (οντολογία κινδύνου και οντολογία προτύπων κυβερνοασφάλειας)** για την ενίσχυση της οργανωσιακής μάθησης των σύνθετων περιβάλλοντων ΤΠΕ και την ενίσχυση της γνώσης για τα πρότυπα κυβερνοασφάλειας σχετικά με τον σκοπό και τη χρήση τους, αντιστοίχα. Οι οντολογίες αναπτύχθηκαν χρησιμοποιώντας πρακτικές διαχείρισης γνώσης και τεχνολογίες Σημασιολογικού Ιστού (Semantic Web) για την εξωτερίκευση άρρητης γνώσης του πεδίου και τη δημιουργία αναπαραστάσεων γνώσης σε μηχαναγνώσιμη μορφή.

Η επικύρωση των τεχνουργημάτων του CyberICT υβριδικού πλαισίου αξιολόγησης πραγματοποιήθηκε μέσω της επίδειξης και εφαρμογής ρεαλιστικών σεναρίων κρίσιμων υπηρεσιών

που υπάγονται στη Ναυτική και Εφοδιαστική Αλυσίδα μεταφορών. Το υβριδικό πλαίσιο αξιολόγησης CyberICT έχει υλοποιηθεί σταδιακά σε διάφορες ψηφιακές πλατφόρμες διαχείρισης ασφάλειας και πιστοποίησης στο πλαίσιο ευρωπαϊκών έργων με την παράλληλη συμβολή της παρούσας υποψήφια διδάκτορος στη φάση σχεδίασης, πιλοτικών ελέγχων, εκπαίδευσης και αξιολόγησης. Τα CyberICT τεχνουργήματα επαληθεύτηκαν εξετάζοντας το βαθμό ικανοποίησης των απαιτήσεων που ορίστηκαν για τη δημιουργία τους. Οι οντολογίες επαληθεύτηκαν μέσω μηχανισμών εξαγωγής συμπερασμάτων.

Τα αποτελέσματα επιβεβαιώνουν την εφαρμοσιμότητα, συνέπεια και χρησιμότητα της προτεινόμενης προσέγγισης στην αξιολόγηση της ασφάλειας σύνθετων προϊόντων και των υπηρεσιών εφοδιαστικών τους αλυσίδων ΤΠΕ, την ενίσχυση της ετοιμότητάς τους ως προς το Ευρωπαϊκό Πλαίσιο Πιστοποίησης της Κυβερνοασφάλειας και τη συμμόρφωση με την αντίστοιχη ισχύουσα νομοθεσία της ΕΕ.

## **Λέξεις – Κλειδιά**

Υβριδικό πλαίσιο αξιολόγησης κυβερνοασφάλειας, διαχείριση κινδύνων προϊόντων και υπηρεσιών εφοδιαστικών αλυσίδων ΤΠΕ, αξιολόγηση κινδύνων και συμμόρφωσης σύνθετων προϊόντων ΤΠΕ, Προφίλ Προστασίας ΤΠΕ, μοντέλο Προσομοίωσης Επίθεσης και Δημιουργίας Αλυσίδας Πειστηρίων, οντολογία προτύπων τυποποίησης κυβερνοασφάλειας, Ναυτική και Εφοδιαστική Αλυσίδα Μεταφορών, οντολογία κινδύνου.

## Abstract

The accelerating digitalisation of modern economies has made the security of Information and Communication Technology (ICT) products and their ICT supply chains a matter of regulatory and operational urgency. While the European Union's Cyber Resilience Act -Regulation (EU) 2024/2847-, Cybersecurity Act -Regulation (EU) 2019/881-, and NIS 2 Directive -Regulation (EU) 2022/2555- collectively promote the integration of risk and conformity assessment procedures, existing approaches lack harmonisation between these processes, leaving ICT stakeholders without structured guidance for achieving measurable, holistic security assurance. This gap is further compounded by the fragmentation of cybersecurity and certification standards, the technical complexity of composite ICT products, and the insufficient depth of risk analysis methods available for large-scale, heterogeneous ICT supply chain environments.

This dissertation proposes a hybrid evaluation framework that integrates **Cybersecurity** risk and conformity assessment into a unified framework for composite **ICT** products and their supply chain services (**CyberICT hybrid evaluation framework**). Grounded in the Design Science Research methodology, the work produces a coherent set of interrelated artefacts: a cybersecurity risk management methodology along with a corresponding risk ontology; a Protection Profile preparatory framework for composite ICT products along with a corresponding taxonomy, and a cybersecurity standards ontology.

The **CyberICT Risk Management Methodology** supports a stepwise assessment process that estimates vulnerabilities, threats, and risks and their impact and explores corresponding cascading effects across complex ICT environments. Such environments encompass composite ICT products that can be decomposed into primary elements of software, firmware, and hardware and their supporting ICT supply chain services, constituted by heterogeneous networks of multimodal ICT infrastructures. To support the diverse evaluation needs of ICT stakeholders, derived from the literature review, the methodology provides three distinct evaluation perspectives for ICT supply chain service analysis, i.e., business, holistic-technical, and sector-specific, each capturing a different dimension of the supply chain environment. Concerning the business analysis, process modelling techniques are used to enhance comprehension of the ICT supply chain service. Through the identification of cyberdependencies among interconnected ICT elements, the methodology addresses the technical complexity of these environments, enabling impact, cascading effects, and propagation assessments of the identified vulnerabilities and risks. Vulnerability exploitability is assessed through a weighted scoring model that considers complementary aspects of intrinsic vulnerability characteristics and threat actor attributes. A set of criticality rules is defined for ICT supply chain services, processes, and assets, identifying operational importance, process dependency, business continuity, resilience characteristics, and the strategic position of ICT assets within the supply chain network, thereby enhancing vulnerability impact estimation. Furthermore, an Attack Simulation and Evidence Chain Generation (ASECG) model is developed to calculate all credible attack paths that illustrate how an attacker has moved inside the ICT network in view of a confirmed security event. The above calculation techniques aim to support a multi-factor risk analysis that considers the technical specificities of large-scale ICT networks and enhances attack modelling techniques by capturing how interconnected systems behave and how failures or attacks can propagate across dependent components, based on empirical evidence.

The **CyberICT Protection Profile** establishes a **stepwise approach and a complementary taxonomy** designed to guide ICT stakeholders: i) for the preparation of Protection Profiles for composite ICT products and ii) for the systematic assessment of their security claims upon specified assurance levels within the framework of the Common Criteria-based European Cybersecurity Certification Scheme (EUCC). The

approach utilises the CyberICT Risk Management Methodology mentioned above to evaluate the security posture of composite ICT products. It is operationalised through a purpose-built Protection Profile taxonomy, grounded in a structured data model that defines the structural relationships among Protection Profile components, including the Composite Target of Evaluation (CToE). The taxonomy further incorporates structured security classifications that establish explicit mappings between Protection Profile elements: threat categories are mapped with corresponding security objectives, which in turn inform security requirements and their associated security controls. This hierarchical mapping enables ICT stakeholders to derive measurable and actionable sets of security requirements and recommendations of controls.

The CyberICT hybrid evaluation framework aims to support ICT stakeholders in advancing the readiness of their products for EU cybersecurity certification, in accordance with the Cybersecurity Act. In addition, it provides a rigorous evaluation pathway for demonstrating compliance with the Cyber Resilience Act, particularly for products with digital elements that necessitate a stringent and in-depth security assessment. Moreover, the CyberICT supply chain risk management contributes to enhancing the security and resilience of ICT supply chains, according to NIS 2 Directive recommendation.

Two ontology models were created, i.e., a **risk ontology** and a **cybersecurity standards ontology**, to enhance organisational learning in complex ICT environments and raise ICT stakeholders' awareness of cybersecurity standards in terms of their purpose and use. The ontologies were developed using knowledge management practices and Semantic Web techniques, which were employed to externalise tacit domain knowledge and produce formal, machine-readable knowledge representations.

The artefacts of the CyberICT hybrid evaluation framework were validated against real-life scenarios from the Maritime and Logistics Supply Chain. The framework has been progressively implemented across various digital security management and certification platforms within the context of European projects. In this context, the current doctoral candidate contributed to the design, pilot testing, training, and evaluation phases. The artefacts of the CyberICT hybrid evaluation approach were verified by assessing whether the requirements, identified for their development, are satisfied. Furthermore, the ontologies were verified via reasoning mechanisms.

The evaluation confirms the applicability, consistency, and utility of the proposed approach in assessing the security of composite ICT products and their supply chain services and supporting cybersecurity certification readiness under the current EU regulatory framework.

## Keywords

CyberICT hybrid evaluation framework, cybersecurity risk management of ICT products and supply chain services, risk and conformity assessment of composite ICT products, ICT Protection Profile, Attack Simulation and Evidence Chain Generation model, cybersecurity standards ontology, Maritime and Logistics Supply Chain, risk ontology.

## Table of Contents

|                                                                                  |    |
|----------------------------------------------------------------------------------|----|
| List of Figures.....                                                             | 15 |
| List of Tables.....                                                              | 18 |
| <b>PART I:</b> .....                                                             | 23 |
| <b>INTRODUCTION</b> .....                                                        | 23 |
| 1. Introduction .....                                                            | 24 |
| 1.1 Motivation of the research .....                                             | 24 |
| 1.2 Structure of the Doctoral Thesis.....                                        | 27 |
| 1.3 The Design Science Research approach .....                                   | 28 |
| <b>PART II:</b> .....                                                            | 32 |
| <b>LITERATURE REVIEW AND OPEN ISSUES</b> .....                                   | 32 |
| 2. The interplay of Cybersecurity Risk and Conformity Assessment.....            | 33 |
| 2.1 Digitalisation of products and security challenges .....                     | 33 |
| 2.1.1 Dependencies of digitalisation.....                                        | 33 |
| 2.1.2 The rising demand for enhanced security and continuous security monitoring | 34 |
| 2.2 Security evaluation and compliance.....                                      | 36 |
| 2.2.1 Subjects of evaluation and legal instruments interrelations .....          | 36 |
| 2.2.2 The enhanced security model.....                                           | 40 |
| 3. The ICT ecosystem .....                                                       | 44 |
| 3.1 ICT structures and concepts .....                                            | 44 |
| 3.2 ICT Supply Chains.....                                                       | 46 |
| 3.2.1 Introducing the ICT Supply Chains .....                                    | 46 |
| 3.2.2 ICT Supply Chain Driving Forces.....                                       | 46 |
| 3.2.3 ICT supply chain classification .....                                      | 48 |
| 3.3 Critical Information Infrastructures and services within the EU .....        | 52 |
| 3.3.1 Definition of criticality on infrastructures and services .....            | 52 |
| 3.3.2 The Maritime and Logistics Supply Chain.....                               | 53 |
| 3.4 Knowledge management, semantics and ontologies in the ICT ecosystem .....    | 58 |
| 3.4.1 Business process management.....                                           | 58 |

|       |                                                                                  |     |
|-------|----------------------------------------------------------------------------------|-----|
| 3.4.2 | Knowledge management and semantics .....                                         | 61  |
| 3.5   | Challenges and remarks for the ICT ecosystem .....                               | 68  |
| 4.    | Security concepts and approaches.....                                            | 70  |
| 4.1   | Security concepts definition, dimensions and interrelations .....                | 70  |
| 4.2   | Legal Framework, standards, guidelines and best practices in cybersecurity ..... | 74  |
| 4.2.1 | Cybersecurity regulation.....                                                    | 74  |
| 4.2.2 | Challenges in cybersecurity standards .....                                      | 81  |
| 4.2.3 | Cybersecurity as standardisation priority in policymaking .....                  | 82  |
| 4.2.4 | Critical cybersecurity standards, guidelines and best practices.....             | 83  |
| 4.2.5 | Relations of EU legislation with international standardisation.....              | 87  |
| 4.2.6 | The need for cybersecurity standardisation classification .....                  | 90  |
| 4.3   | Risk assessment approaches and tools.....                                        | 91  |
| 4.4   | Risk Metrics and Prediction Measurements.....                                    | 93  |
| 4.4.1 | The risk metric variance .....                                                   | 93  |
| 4.4.2 | Threat Taxonomies, threat measurements and vulnerability labelling.....          | 95  |
| 4.4.3 | Attack modelling and attack prediction .....                                     | 97  |
| 4.4.4 | Cascading effects and limitations .....                                          | 101 |
| 4.4.5 | Knowledge Risk Management and ontology models.....                               | 103 |
| 4.5   | Disruptions and security challenges in ICT supply chains.....                    | 104 |
| 4.5.1 | Causes leveraging ICT supply chain discontinuity .....                           | 104 |
| 4.5.2 | ICT Supply Chain Risk Management.....                                            | 108 |
| 4.5.3 | Security in the Maritime and Logistics Supply Chain .....                        | 110 |
| 4.5.4 | ICT Supply Chain Requirements .....                                              | 118 |
| 4.6   | Cybersecurity certification and conformity assessment concepts.....              | 120 |
| 4.6.1 | Cybersecurity Certification.....                                                 | 120 |
| 4.6.2 | The conformity assessment process .....                                          | 120 |
| 4.6.3 | The European Cybersecurity Certification scheme (EUCC) .....                     | 121 |
| 4.6.4 | Cybersecurity Certification flows .....                                          | 121 |
| 4.6.5 | Cybersecurity certification process.....                                         | 122 |
| 4.6.6 | Protection Profile elements .....                                                | 124 |

|                                                                                             |                                                                                         |     |
|---------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|-----|
| 4.6.7                                                                                       | Challenges and issues in cybersecurity certification.....                               | 125 |
| 4.7                                                                                         | Challenges and remarks for securing the ICT ecosystem .....                             | 125 |
| <b>PART III:</b>                                                                            | .....                                                                                   | 129 |
| <b>RESEARCH UNDERPINNINGS</b>                                                               | .....                                                                                   | 129 |
| 5.                                                                                          | Research Problem, Requirements, and Conceptual Foundation.....                          | 130 |
| 5.1                                                                                         | Research problem and dissertation objectives .....                                      | 130 |
| 5.1.1                                                                                       | Challenge #1: An integrated framework of Risk Management and Conformity Assessment..... | 131 |
| 5.1.2                                                                                       | Challenge #2: Harmonisation of cybersecurity standards.....                             | 132 |
| 5.1.3                                                                                       | Challenge #3: Address the complex nature of large-scale environments .....              | 132 |
| 5.1.4                                                                                       | Challenge #4: Lack of security typology .....                                           | 133 |
| 5.1.5                                                                                       | Challenge #5: Siloed risk measurements lacking holistic view .....                      | 134 |
| 5.2                                                                                         | CyberICT hybrid evaluation framework overview .....                                     | 135 |
| 5.3                                                                                         | CyberICT standards ontology .....                                                       | 137 |
| 5.3.1                                                                                       | Ontology building blocks.....                                                           | 137 |
| 5.3.2                                                                                       | Structure and Main Pillars .....                                                        | 137 |
| 5.3.3                                                                                       | Semantic Relations .....                                                                | 140 |
| 5.3.4                                                                                       | Ontology application .....                                                              | 144 |
| <b>PART IV:</b>                                                                             | .....                                                                                   | 150 |
| <b>Cybersecurity risk management methodology for ICT products and supply chain services</b> | .....                                                                                   | 150 |
| 6.                                                                                          | CyberICT Risk Management Methodology .....                                              | 151 |
| 6.1                                                                                         | Building Blocks.....                                                                    | 151 |
| 6.1.1                                                                                       | Scope and Objectives .....                                                              | 151 |
| 6.1.2                                                                                       | Regulatory background, related security standards and best practices .....              | 152 |
| 6.1.3                                                                                       | Business Process Models.....                                                            | 153 |
| 6.1.4                                                                                       | Ontology-based Models .....                                                             | 153 |
| 6.1.5                                                                                       | Attack Simulation, cumulative and propagation assessments .....                         | 154 |
| 6.1.6                                                                                       | Additional related work.....                                                            | 155 |
| 6.1.7                                                                                       | Users of CyberICT Risk Management methodology .....                                     | 155 |
| 6.2                                                                                         | Design and development of the CyberICT Risk Management methodology .....                | 156 |
| 6.2.1                                                                                       | Methodology Overview .....                                                              | 156 |



|                                            |                                                                                           |     |
|--------------------------------------------|-------------------------------------------------------------------------------------------|-----|
| 6.2.2                                      | Methodology analysis .....                                                                | 159 |
| 6.2.3                                      | CyberICT Risk Ontology .....                                                              | 214 |
| 6.2.4                                      | Evaluation approach.....                                                                  | 222 |
| 6.3                                        | Practical adoption in system.....                                                         | 224 |
| 6.3.1                                      | Design integration.....                                                                   | 225 |
| 6.3.2                                      | Visualisation of services in the risk management platforms .....                          | 227 |
| 6.4                                        | Demonstration and Applicability .....                                                     | 233 |
| 6.4.1                                      | The Vehicle Transport Service.....                                                        | 234 |
| 6.4.2                                      | The LNG Transport Service .....                                                           | 242 |
| 6.4.3                                      | The Container Cargo Management Service.....                                               | 248 |
| 6.5                                        | Evaluation of the CyberICT Risk Management and risk ontology .....                        | 262 |
| 6.5.1                                      | Questionnaire survey .....                                                                | 262 |
| 6.5.2                                      | CyberICT Risk Management Methodology against domain-specific issues .....                 | 269 |
| 6.5.3                                      | Analysis of CyberICT Risk Management Methodology calculation models ....                  | 271 |
| <b>PART V:</b>                             | .....                                                                                     | 272 |
| <b>PROTECTION PROFILE FOR ICT PRODUCTS</b> | .....                                                                                     | 272 |
| 7.                                         | CyberICT Protection Profile .....                                                         | 273 |
| 7.1                                        | CyberICT Protection Profile preparation of composite ICT products.....                    | 273 |
| 7.1.1                                      | Building Blocks.....                                                                      | 273 |
| 7.1.2                                      | CyberICT Protection Profile preparation of composite ICT products.....                    | 275 |
| 7.2                                        | CyberICT Protection Profile Taxonomy for Composite Product .....                          | 283 |
| 7.2.1                                      | Composite Target of Evaluation structure .....                                            | 283 |
| 7.2.2                                      | Protection Profile Taxonomy of Composite ICT Product.....                                 | 285 |
| 7.3                                        | Practical Adoption in System .....                                                        | 290 |
| 7.3.1                                      | Design integration.....                                                                   | 290 |
| 7.3.2                                      | Visualisation of service in the cybersecurity certification platform.....                 | 290 |
| 7.4                                        | Demonstration and Applicability of CyberICT Protection Profile preparatory framework..... | 293 |
| 7.4.1                                      | Step 0: Define the CToE and Evaluation Conditions .....                                   | 293 |
| 7.4.2                                      | Step 1: Conduct Cybersecurity Risk Assessment on CToE's asset.....                        | 294 |
| 7.4.3                                      | Step 2: Security Problem Definition.....                                                  | 295 |

|                                                                           |                                                                                                                    |            |
|---------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|------------|
| 7.4.4                                                                     | Step 3: Identify Security Objectives and Security Requirements .....                                               | 295        |
| 7.4.5                                                                     | Step 4: Define Security Controls .....                                                                             | 295        |
| 7.4.6                                                                     | Step 5: Capture Evidence and Documentation .....                                                                   | 296        |
| 7.4.7                                                                     | Step 6: Review Protection Profile.....                                                                             | 296        |
| 7.4.1                                                                     | Step 7: Request Conformity Assessment .....                                                                        | 296        |
| 7.5                                                                       | Evaluation of CyberICT Protection Profile.....                                                                     | 296        |
| 7.5.1                                                                     | Evaluation approach.....                                                                                           | 296        |
| 7.5.2                                                                     | Proof of concept demonstration.....                                                                                | 296        |
| 7.5.3                                                                     | Practical adoption .....                                                                                           | 297        |
| 7.5.4                                                                     | Comparative analysis of the CyberICT Protection Profile with respect to the Common Criteria and EUCC.....          | 297        |
| <b>PART VI:</b>                                                           | .....                                                                                                              | <b>299</b> |
| <b>EVALUATION OUTCOMES, CONCLUSIONS, AND CONTRIBUTION TO SCIENCE.....</b> |                                                                                                                    | <b>299</b> |
| 8.                                                                        | Overall Evaluation .....                                                                                           | 300        |
| 8.1                                                                       | Ontologies evaluation.....                                                                                         | 300        |
| 8.2                                                                       | CyberICT Risk Management Methodology evaluation.....                                                               | 301        |
| 8.3                                                                       | CyberICT Protection Profile evaluation.....                                                                        | 302        |
| 8.4                                                                       | Contribution to identified challenges and requirements coverage from the CyberICT hybrid evaluation approach. .... | 302        |
| 9.                                                                        | Conclusions and contribution to science .....                                                                      | 308        |
| 9.1                                                                       | Conclusions and future work.....                                                                                   | 308        |
| 9.2                                                                       | Novelty and Contribution to Science .....                                                                          | 311        |
| 9.2.1                                                                     | Contribution to cybersecurity certification.....                                                                   | 311        |
| 9.2.2                                                                     | Contribution to cybersecurity standardisation .....                                                                | 312        |
| 9.2.3                                                                     | Contribution to Supply Chain security .....                                                                        | 313        |
| 9.2.4                                                                     | Contribution to Cybersecurity Risk Management .....                                                                | 313        |
| 9.2.5                                                                     | Contribution to Knowledge Management and Ontology Engineering.....                                                 | 313        |
| 9.2.6                                                                     | Contribution to Maritime and Logistics Supply Chain security and Critical Infrastructure Protection.....           | 314        |
| 9.2.7                                                                     | Design Science Research .....                                                                                      | 314        |
| References                                                                | .....                                                                                                              | 315        |

|                                                                      |     |
|----------------------------------------------------------------------|-----|
| Appendices .....                                                     | 343 |
| Appendix A: Glossary .....                                           | 343 |
| Appendix B: Acronyms and Abbreviations .....                         | 367 |
| Appendix C: Documents and Forms .....                                | 378 |
| Appendix D: Assessment scales.....                                   | 380 |
| D1. CyberICT Probability Scale.....                                  | 380 |
| D2. NIS 2 Directive Essential and Important services .....           | 380 |
| D3. Threat scale of ICT assets .....                                 | 380 |
| D4. Exploitability and impact related metrics .....                  | 381 |
| D5. Attacker’s Profile.....                                          | 383 |
| D6. Results of the Evidence Chain Generation real-life scenario..... | 384 |
| D7. Assurance Details mappings .....                                 | 389 |
| D8. Protection Profile classifications .....                         | 390 |

## List of Figures

|                                                                                                                                                                                   |     |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| Figure 1. Design Science Research model of the CyberICT hybrid evaluation framework.....                                                                                          | 31  |
| Figure 2. Enhanced security model [60] depicting relations of risk and conformity assessment concepts.....                                                                        | 43  |
| Figure 3. The ICT supply chain model.....                                                                                                                                         | 52  |
| Figure 4. Satellite (SAT) communications and Automatic Identification Systems (AIS) interacting within the Maritime and Logistics Supply Chain for the transport of vehicles..... | 55  |
| Figure 5. Class hierarchy and object and data properties of the BPMN semantic model [92].....                                                                                     | 66  |
| Figure 6. The BPMN semantic model.....                                                                                                                                            | 67  |
| Figure 7: Major Standards and frameworks of Security Management. ....                                                                                                             | 87  |
| Figure 8. Assessment flows of the EUCC. ....                                                                                                                                      | 122 |
| Figure 9. The Common Criteria Protection Profile and its elements.....                                                                                                            | 124 |
| Figure 10. The CyberICT hybrid evaluation framework.....                                                                                                                          | 136 |
| Figure 11. Overall view of the proposed standards-based taxonomy of security management.....                                                                                      | 140 |
| Figure 12. A snapshot of the Cybersecurity Standards ontology structure illustrating the Stakeholder’s profile and relations between classes.....                                 | 143 |

|                                                                                                                                                                                                                                            |     |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| Figure 13. Cybersecurity Standards indicative instances depicting their semantic relations expressed via RDF semantic object and data properties in Protégé. ....                                                                          | 144 |
| Figure 14. Quad selection of stakeholders on the conceptual pillars of the taxonomy to identify relevant Standards/Frameworks/Best practices for the ToE security management. ....                                                         | 145 |
| Figure 15. A combination of cybersecurity standards, frameworks and best practices related to security evaluation of AI/ML-based infrastructures together with sectoral cybersecurity guidelines for maritime transport. ....              | 149 |
| Figure 16. The CyberICT Risk Management Methodology. ....                                                                                                                                                                                  | 158 |
| Figure 17. ICT model-centric cartography. ....                                                                                                                                                                                             | 163 |
| Figure 18. ICT process representation in a business process model. ....                                                                                                                                                                    | 170 |
| Figure 19. Example of an individual vulnerability chain. ....                                                                                                                                                                              | 190 |
| Figure 20. Example of an entry's vulnerability chains. ....                                                                                                                                                                                | 190 |
| Figure 21. Example of cumulative vulnerability chains. ....                                                                                                                                                                                | 190 |
| Figure 22. The Attack Simulation and Evidence Chains Generation (ASECG) model. ....                                                                                                                                                        | 197 |
| Figure 23: The CyberICT Risk Ontology. ....                                                                                                                                                                                                | 216 |
| Figure 24. CyberICT Risk Ontology superclasses. ....                                                                                                                                                                                       | 219 |
| Figure 25. An example of identifying Knowledge Management flows to provide cyber asset characteristics. ....                                                                                                                               | 219 |
| Figure 26. Examples of the semantic assertions usage: i) left window extracts tacit knowledge while reasoning, ii) right window uses semantic axioms. ....                                                                                 | 220 |
| Figure 27. Outcomes from complex SPARQL queries: i) on the left window the results from extracting assets with specific characteristics, ii) on the right window security threat result for FTP Server and Application Server assets. .... | 220 |
| Figure 28. An ontology visualisation of the Port Community System's cyber assets of the Server Network showing semantic relations among them. ....                                                                                         | 221 |
| Figure 29. The reasoning for consistency checking of the CyberICT ontology. No logical errors were found. In the property assertions browser, the implicit information is highlighted. ....                                                | 222 |
| Figure 30. Creation of Supply Chain Service. ....                                                                                                                                                                                          | 227 |
| Figure 31. List of created Supply Chain Services. ....                                                                                                                                                                                     | 228 |
| Figure 32. Create an ICT process in an ICT Supply Chain Service (ICT SCS). ....                                                                                                                                                            | 228 |
| Figure 33. ICT asset technical details. ....                                                                                                                                                                                               | 229 |
| Figure 34. Visualisation of asset dependency graphs. ....                                                                                                                                                                                  | 229 |

|                                                                                                                                                                                          |     |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| Figure 35. Identification of confirmed vulnerabilities in the ICT assets of an ICT process of an ICT SCS. ....                                                                           | 230 |
| Figure 36. Interrelations between assets, vulnerabilities and threats in an threat scenario. ....                                                                                        | 230 |
| Figure 37. Threat scenario management. ....                                                                                                                                              | 231 |
| Figure 38. Threat level estimation. ....                                                                                                                                                 | 231 |
| Figure 39. Risk Assessment results in an ICT process. ....                                                                                                                               | 232 |
| Figure 40. Credible vulnerability chains. ....                                                                                                                                           | 232 |
| Figure 41. Credible vulnerability Attack graphs illustrate the potential attack paths between interdependent asset nodes upon specific query. ....                                       | 233 |
| Figure 42. Port's Services Requested. ....                                                                                                                                               | 237 |
| Figure 43. Vehicles Unloading process. ....                                                                                                                                              | 237 |
| Figure 44. Interdependencies between Port's Community System and Custom's infrastructure. ....                                                                                           | 238 |
| Figure 45. SCADA system for stevedoring; loading/unloading vehicles from vessels and their transportation to car terminals. ....                                                         | 240 |
| Figure 46. Visualisation of vehicles robbery attack during vessels unloading. ....                                                                                                       | 242 |
| Figure 47. Cyberdependency graph of Port Authority assets. ....                                                                                                                          | 251 |
| Figure 48. Combinations of assets and vulnerabilities developed, according to the current scenario. ....                                                                                 | 254 |
| Figure 49. The Individual Vulnerability Level is calculated on asset/vulnerability combinations. ....                                                                                    | 255 |
| Figure 50. Potential attack paths related to the compromised PCS Database Server (A <sub>5</sub> ) given the specific PoC <sub>1</sub> derived from the analysed IoC <sub>1</sub> . .... | 256 |
| Figure 51. The Credible Evidence Chains of the General Cargo Transportation scenario. ....                                                                                               | 261 |
| Figure 52. Sample question of the second survey. ....                                                                                                                                    | 264 |
| Figure 53. ICT process analysis capacity. ....                                                                                                                                           | 265 |
| Figure 54. Business partners and participants' identification (left image) and business partners' infrastructure (right image). ....                                                     | 265 |
| Figure 55. Analysis and vulnerabilities identification (left image) and assets' interdependencies declaration (right image). ....                                                        | 266 |
| Figure 56. Threats' identification cyber assets. ....                                                                                                                                    | 266 |
| Figure 57. Overall evaluation results of the methodology. ....                                                                                                                           | 267 |

|                                                                                                                                                                                |     |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| Figure 58. Overall impression of the respondents regarding the benefits of the MITIGATE security assessment services.....                                                      | 268 |
| Figure 59. Overall impression of the respondents concerning the utilization of the MITIGATE system services. ....                                                              | 268 |
| Figure 60. The impressions of the overall respondents for the system. ....                                                                                                     | 268 |
| Figure 61. The CyberICT hybrid valuation framework embedding the Risk Management Methodology and the Protection Profile preparatory framework.....                             | 277 |
| Figure 62. CyberICT Protection Profile for Composite Products.....                                                                                                             | 285 |
| Figure 63. Service related to the CToE creation. ....                                                                                                                          | 291 |
| Figure 64. Security controls applied to the identified security functional requirements. ....                                                                                  | 291 |
| Figure 65. Evaluation criteria details.....                                                                                                                                    | 291 |
| Figure 66. Use of Protection Profile's security classification to identify threat categories, relevant security objectives and security requirements of product's assets. .... | 292 |
| Figure 67. Assumptions and Organisational Security Policies for the Security Problem Definition. ....                                                                          | 292 |
| Figure 68. Threat categories for the Security Problem Definition.....                                                                                                          | 292 |
| Figure 69. Security Functional Requirements and Extended Requirements visualisation deriving from the security classification.....                                             | 293 |

## List of Tables

|                                                                                                                 |     |
|-----------------------------------------------------------------------------------------------------------------|-----|
| Table 1. Comparative overview of CRA, CSA and NIS 2 Directive. ....                                             | 38  |
| Table 2. Maritime and Logistics Supply Chain critical actors and elements. ....                                 | 56  |
| Table 3. Security Standards relations with EU regulation. ....                                                  | 89  |
| Table 4. Mapping of Challenges with Requirements and Dissertation Objectives. ....                              | 130 |
| Table 5. Mapping of Requirements, Objectives and Artefacts of the CyberICT hybrid evaluation framework.....     | 136 |
| Table 6. Conceptual questions and pillars to identify relevant standards.....                                   | 138 |
| Table 7. Security management standards classification towards their purpose of use. ....                        | 139 |
| Table 8. Template of standard attributes. ....                                                                  | 141 |
| Table 9. Ontology's semantic relations. ....                                                                    | 141 |
| Table 10. Standards/Frameworks/Best practices delivered results towards stakeholder's pre-defined criteria..... | 146 |

|                                                                                                                                             |     |
|---------------------------------------------------------------------------------------------------------------------------------------------|-----|
| Table 11. Methodology structural template. ....                                                                                             | 157 |
| Table 12. Set the boundaries of the Cybersecurity Risk Assessment. ....                                                                     | 159 |
| Table 13. Modelling-based cartography. ....                                                                                                 | 162 |
| Table 14. ICT Supply Chain Service criticality scale based on NIS 2 Directive [12] aspects. ....                                            | 165 |
| Table 15. ICT process analysis template. ....                                                                                               | 167 |
| Table 16. High level ICT infrastructure analysis template. ....                                                                             | 167 |
| Table 17. ICT asset technical specifications template. ....                                                                                 | 168 |
| Table 18. ICT asset matrix. ....                                                                                                            | 168 |
| Table 19. Identification of ICT supply chain elements. ....                                                                                 | 169 |
| Table 20. Analysis of “Ship Formalities Arrangement” ICT process. ....                                                                      | 169 |
| Table 21. High level ICT infrastructure analysis. ....                                                                                      | 170 |
| Table 22. ICT asset technical specifications template. ....                                                                                 | 171 |
| Table 23. ICT asset matrix. ....                                                                                                            | 171 |
| Table 24. Identify and estimate cyber threats. ....                                                                                         | 175 |
| Table 25. Vulnerability and Impact Analysis. ....                                                                                           | 178 |
| Table 26. Individual Vulnerability Level (IVL) scale. ....                                                                                  | 181 |
| Table 27. Exploitability Level - example 1. ....                                                                                            | 183 |
| Table 28. Exploitability Level - example 2. ....                                                                                            | 183 |
| Table 29. Exploitability Level - example 3. ....                                                                                            | 184 |
| Table 30. Individual Impact Level scale. ....                                                                                               | 187 |
| Table 31. Example of Vulnerability metrics of CVSS 3.1 Environmental Group. ....                                                            | 187 |
| Table 32. Environmental group metric values mapped to ICT asset criticality. ....                                                           | 188 |
| Table 33. Tasks to perform the cumulative vulnerability analysis. ....                                                                      | 191 |
| Table 34. Propagation rules ([276],[370]). ....                                                                                             | 192 |
| Table 35. Attack Simulation and Evidence Chains Generation. ....                                                                            | 195 |
| Table 36. Mapping of the attacker’s capability and the attack path exploitability to identify the attacker’s exploitability potential. .... | 202 |
| Table 37. Mapping of the attacker’s capability and the attack path exploitability to identify the attacker’s exploitability potential. .... | 203 |
| Table 38. Risk Estimation. ....                                                                                                             | 204 |
| Table 39. Short scenario for estimating the risk propagation. ....                                                                          | 209 |

|                                                                                                                                                |     |
|------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| Table 40. Management and treatment of risks.....                                                                                               | 210 |
| Table 41. Vehicle Transport Service processes.....                                                                                             | 236 |
| Table 42. Analysis of Vehicle Transport Service infrastructure in ICT processes.....                                                           | 237 |
| Table 43. Asset dependencies in the Port Community System. ....                                                                                | 238 |
| Table 44. Threat scenario for the Port Community System. ....                                                                                  | 239 |
| Table 45. Analysis of “LNG Monitoring Service” ICT process. ....                                                                               | 244 |
| Table 46. High level LNG SCADA infrastructure analysis.....                                                                                    | 244 |
| Table 47. LNG Monitoring asset matrix.....                                                                                                     | 245 |
| Table 48. Threat scenario for PLC Software. ....                                                                                               | 245 |
| Table 49. Attack path scenarios in LNG Transport Service. ....                                                                                 | 248 |
| Table 50. Assets and their cyberdependencies of the current scenario. ....                                                                     | 251 |
| Table 51. Vulnerabilities identified on assets and corresponding CVSS 3.1 metrics.....                                                         | 252 |
| Table 52. Estimation of the Individual Vulnerability Level (IVL) for each identified asset/<br>vulnerability combination.....                  | 254 |
| Table 53. Assets cyberdependencies linked to the detected compromised asset A <sub>5</sub> . ....                                              | 256 |
| Table 54. Attack paths are reconstructed according to the confirmed security event and potential<br>evidence chains.....                       | 257 |
| Table 55. Exploitation Level (EL) calculation for each asset/vulnerability combination, according<br>to the attacker’s profile identified..... | 259 |
| Table 56. The exploitability levels of the 11 potential attack paths is estimated according to the<br>detected IoC <sub>1</sub> . ....         | 260 |
| Table 57. Attack Path prioritisation from highest to lowest exploitability.....                                                                | 260 |
| Table 58. Credible Evidence Chains of the current Port Authority scenario.....                                                                 | 261 |
| Table 59. Questionnaire utilised in the survey. ....                                                                                           | 263 |
| Table 60. Define the CToE and Evaluation Conditions. ....                                                                                      | 278 |
| Table 61. Evaluation Assurance Assessment Scale. ....                                                                                          | 279 |
| Table 62. Conduct Cybersecurity Risk Assessment on CToE’s assets and review the results....                                                    | 280 |
| Table 63. Define the Security Problem. ....                                                                                                    | 281 |
| Table 64. Security objectives and security Requirements identification. ....                                                                   | 281 |
| Table 65. Define Security Controls. ....                                                                                                       | 281 |
| Table 66. Capture Evidence and Documentation. ....                                                                                             | 282 |



|                                                                                                                                           |     |
|-------------------------------------------------------------------------------------------------------------------------------------------|-----|
| Table 67. Review Protection Profile and Security Controls. ....                                                                           | 282 |
| Table 68. Request Conformity Assessment. ....                                                                                             | 283 |
| Table 69. Composite Target of Evaluation (CToE). ....                                                                                     | 283 |
| Table 70. Indicative relations between threats, security objectives, security requirements and security controls in diverse devices. .... | 286 |
| Table 71. CyberICT Protection Profile (PP) Taxonomy. ....                                                                                 | 287 |
| Table 72. CToE assets. ....                                                                                                               | 293 |
| Table 73. CToE details ....                                                                                                               | 294 |
| Table 74. Risk Assessment results ....                                                                                                    | 294 |
| Table 75. Security Problem Definition. ....                                                                                               | 295 |
| Table 76. Security objectives and security requirements. ....                                                                             | 295 |
| Table 77. Security Controls definition. ....                                                                                              | 295 |
| Table 78. Evidence and documentation. ....                                                                                                | 296 |
| Table 79. Protection Profile templates analysis. ....                                                                                     | 298 |
| Table 80. An integrated framework of Risk Management and Conformity Assessment. ....                                                      | 303 |
| Table 81. Harmonisation of cybersecurity standards. ....                                                                                  | 304 |
| Table 82. Address the complex nature of large-scale environments. ....                                                                    | 304 |
| Table 83. Lack of security typology. ....                                                                                                 | 305 |
| Table 84. Siloed risk measurements lacking holistic view. ....                                                                            | 306 |
| Table 85. Glossary of definitions and terms utilized in the current dissertation. ....                                                    | 343 |
| Table 86. Acronyms and Abbreviations. ....                                                                                                | 367 |
| Table 87. CyberICT generic assessment scale. ....                                                                                         | 380 |
| Table 88. CyberICT SCS criticality scale. ....                                                                                            | 380 |
| Table 89. Threat Scale. ....                                                                                                              | 381 |
| Table 90. CVSS 3.1 Modified Attack Vector (MAV defining how a vulnerability can be technically reached. ....                              | 382 |
| Table 91. CVSS 3.1 Modified Attack Complexity (MAC). ....                                                                                 | 382 |
| Table 92. CVSS 3.1 Modified Privileges Required (MPR). ....                                                                               | 382 |
| Table 93. CVSS 3.1 Modified User Interaction (MUI). ....                                                                                  | 383 |
| Table 94. CVSS 3.1 Environmental group metrics. ....                                                                                      | 383 |
| Table 95. CVSS 3.1 MISS sub-score and Scope metric. ....                                                                                  | 383 |

|                                                                                                                                                                                                |     |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| Table 96. The ranking of Attacker’s capability. ....                                                                                                                                           | 384 |
| Table 97. The ranking of Attacker’s location showing from where an attacker currently operates.<br>.....                                                                                       | 384 |
| Table 98. Mapping Attacker’s location with CVSS 3.1 Attack Vector metric. ....                                                                                                                 | 384 |
| Table 99. Depiction of all vulnerability chains of all cyberdependent assets combinations of the<br>Port Authority scenario, presented in Section 6.4.3.2. ....                                | 385 |
| Table 100. The Individual Vulnerability Level (IVL) analysis for each vulnerability of each asset<br>of interest, according to the Port Authority scenario, presented in Section 6.4.3.2. .... | 388 |
| Table 101. The Exploitability Level (EL) estimation analysis for each vulnerability of each asset of<br>interest, according to the Port Authority scenario, presented in Section 6.4.3.2.....  | 388 |
| Table 102. Assurance details mapping of Common Criteria and EUCC [44] to set the CToE<br>evaluation boundaries.....                                                                            | 389 |
| Table 103. Classification of Security Functional Requirements with security and privacy controls.<br>.....                                                                                     | 390 |
| Table 104. Classification of Security objectives with Security Fuctional Requirements. ....                                                                                                    | 392 |
| Table 105. Classification of STRIDE threat categories with security objectives. ....                                                                                                           | 396 |

# PART I:

## INTRODUCTION

---

# 1. Introduction

This chapter is an introduction to the doctoral thesis. It first outlines the motivation underlying the research, then presents an overview of the thesis structure, and finally describes the Design Science Research (DSR) model which drives the current dissertation.

## 1.1 Motivation of the research

The rapid digitalisation of modern societies has fundamentally reshaped the design, deployment, and consumption of Information and Communication Technology (ICT) products and services. Critical Information Infrastructure (CII) operators across industry sectors and entities of diverse types and sizes, such as Microenterprises (MEs), Small and Medium-sized Enterprises (SMEs), large enterprises, public administrations, governmental and national security entities, research and non-profit organisations, are now deeply dependent upon complex, interconnected ICT ecosystems [1]-[2]. This dependency, while driving unprecedented levels of efficiency and innovation, has simultaneously exposed organisations to an expanding and increasingly sophisticated threat landscape, as documented in the recent ENISA Threat Landscape report [3]. In this vein, ransomware attacks, supply chain compromises, Advanced Persistent Threats (APTs) [2],[4],[5], and large-scale data breaches [6]–[8] have become defining features of the contemporary digital environment, with their frequency and severity continuing to escalate year on year [9]. *This constitutes the technically dependent and evolving threat pillar that motivated the current dissertation research.*

In response to this evolving threat landscape, the European Union (EU) has embarked upon an ambitious legislative programme aimed at establishing a harmonised and robust cybersecurity framework for the EU Digital Single Market (see EU Cybersecurity Strategy [10]). Landmark instruments, such as the EU Cyber Resilience Act (CRA) [11], NIS 2 Directive [12], and Cybersecurity Act (CSA) [13] mutually mandate ICT stakeholders to implement security-by-design and maintain cybersecurity throughout ICT products and their ICT supply chain lifecycle. These security mandates imply the following requirements:

- Integration of DevSecOps practices into Continuous Integration/ Continuous Delivery (CI/CD) pipelines for secure software product development (CRA).
- Definition of a set of actionable and measurable security requirements, and implementation of robust security controls alongside continuous security monitoring on ICT products and ICT services to maintain security at specified assurance levels (CRA, CSA).
- Integration of security throughout the entire ICT supply chain of products.
- Systematic risk assessments on ICT products and their corresponding ICT supply chain services.
- Systematic conformity assessment to assess the compliance of products and services to cybersecurity legal requirements.

In this regard, the Common Criteria-based European Cybersecurity Certification Scheme (EUCC) [14] provides a structured mechanism for the conformity assessment and certification of ICT products. Together, these evaluation mechanisms signal a decisive shift towards the security-by-design approach, in which cybersecurity assurance is no longer treated as an afterthought but as a fundamental requirement embedded in the development and procurement of digital products and services.

Despite this significant legislative driving force, a critical gap persists between the theoretical ambitions of the regulatory framework and the practical capacity of ICT stakeholders to meet its requirements [15]-[16]. Risk assessment and conformity assessment have historically been treated as separate disciplines [17]; (cf. Chapter 4.3), addressed by distinct communities of practice and guided by different sets of standards and methodologies (cf. Sections 4.2.4.1 and 4.2.4.3). As a result, ICT product owners, manufacturers, and supply chain operators are frequently left without coherent, integrated guidance on how to assess the security of their products, identify appropriate security controls [16], and prepare for the conformity assessment procedures required under the CRA [11] and CSA [13]. This fragmentation is further compounded by the proliferation of cybersecurity standards, which, even if they may be individually valuable, are often difficult to navigate and apply in a coordinated manner [18]. State-of-the-art approaches reflect the absence of a unified, standards-harmonised approach that integrates risk and conformity assessment into a single, end-to-end evaluation framework, which constitutes a significant obstacle to the realisation of the EU's cybersecurity objectives [18]. *The prevailing cybersecurity legal and standardisation background serves the second motivation pillar of this current dissertation research.*

The 6<sup>th</sup> edition of the ENISA NIS 2 Investments report (2025) [19] reveals the following business issues in cybersecurity investment:

- Shift from people to technology. The focus is directed toward technology solutions and outsourcing, rather than expanding in-house cybersecurity teams.
- Talent crisis. Organisations struggle to attract and retain cybersecurity professionals due to a shrinking talent pool and strong competition, while high turnover further increases risk and drives changes in staffing strategies.
- NIS 2 Directive implementation difficulties are genuinely challenging. Key problem areas include patching management, business continuity planning, and supply chain risk management demanding significant organisational effort and resources.
- Supply chain vulnerability. Organisations are becoming increasingly dependent on third-party ICT and security service providers, many of which are resource-constrained. This deepening dependency is creating new vulnerabilities, particularly when suppliers themselves have weak security postures.
- Inadequate security testing and patching. Many organisations lack regular cybersecurity assessments, with critical vulnerabilities frequently remaining unpatched for prolonged periods. This represents a serious and persistent business risk, particularly as vulnerability exploitation remains a primary intrusion vector.

- The cyber threat evolving landscape, specifically related to ransomware and supply chain attacks, is considered an existential business risk, where threats may cause severe operational, financial, and reputational damage.
- SMEs are impacted by all the above challenges with considerably fewer resources, reporting the lowest confidence in handling and recovering from cyber incidents and lacking access to affordable tooling, skilled personnel, and practical guidance, being the weakest link in the ICT supply chain ecosystem.

The overarching business message relies on the regulatory pressure as a cybersecurity investment driving force. Nevertheless, the gap between compliance intent and operational capability remains dangerously wide, particularly for SMEs and entities heavily dependent on third-party providers [19]. *The need for supply chain and organisational cybersecurity readiness instantiated the third pillar which motivated the current dissertation research.*

Stemming from these three main pillars presented above: i) technical dependencies leading to evolving threats, ii) the prevailing cybersecurity legal and standardisation background, and iii) the supply chain and organisational cybersecurity readiness dimension, an extensive review of the academic literature (see Chapters 3 and 4), standards, regulations, best practices, and relevant reports identifies the following key challenges (analysed in Section 5.1).

First, there is a demonstrable need for measurable and verifiable end-to-end cybersecurity assurance that integrates risk and conformity assessment procedures in a coherent manner.

Second, the fragmentation of cybersecurity standards creates significant barriers to harmonised security assessment, leaving ICT stakeholders uncertain as to which standards are applicable to their specific context and how these standards interrelate with EU legislative requirements.

Third, existing risk assessment methodologies frequently fail to account for the complex, large-scale nature of modern ICT environments and, in particular, the heterogeneous, multi-modal supply chain networks upon which critical infrastructure sectors such as maritime transport and energy are dependent.

Fourth, security awareness across the ICT ecosystem remains insufficient, with tacit and implicit security knowledge often remaining unexternalised and therefore unavailable to inform risk management decisions.

Fifth, the level of risk analysis supported by existing approaches is frequently inadequate, with limited capacity to estimate cascading effects, risk propagation, and the exploitation of asset interdependencies within complex ICT networks.

These challenges collectively define the research problem addressed by the present dissertation. The overarching objective is to develop a hybrid evaluation approach that integrates cybersecurity risk management with conformity assessment procedures, thereby providing ICT stakeholders with a unified, standards-grounded framework for assessing the security of composite ICT products and their associated supply chain services. By bridging the gap between risk assessment and conformity assessment, the proposed hybrid evaluation approach aims to support ICT stakeholders, such as product owners, manufacturers, and supply chain operators,

in achieving a measurable, actionable, and verifiable security assurance framework for their ICT products, raising their readiness for cybersecurity certification under the EUCC scheme and enhance their compliance with CRA requirements for critical and important products.

A further motivation lies in the domain-specific context of supply chain service security, exploring critical industry sectors, according to the NIS 2 Directive, such as the combined industries of Maritime and Logistics Supply Chain (MLoSC) [20]. The MLoSC serves in the current dissertation as the primary application domain for the research. Maritime transport underpins the global economy, accounting for the vast majority of international trade by volume [21]. The increasing digitalisation of maritime operations, encompassing Automatic Identification Systems (AIS), satellite communications, SCADA infrastructures, and port community systems, has introduced significant cybersecurity vulnerabilities into a sector where disruptions can have severe economic, environmental, and safety consequences. Therefore, the MLoSC provides both a compelling and practically significant testbed for the evaluation of the proposed CyberICT approach.

## **1.2 Structure of the Doctoral Thesis**

The current section presents the overall structure of the doctoral thesis. It consists of four (4) main parts, including a group of relevant chapters and sections:

### **PART I – Introduction**

- **Chapter 1** provides an introduction explaining the motivation of research that triggered this dissertation. It continues with the Design Science Research (DSR) model, which establishes the fundamental structure of the current dissertation.

### **PART II – Literature Review and Open Issues**

- **Chapter 2** introduces the main topic of this research, i.e., the interplay of risk and conformity assessment and the underlying regulatory instruments, and presents an enhanced security model that unifies these concepts.
- **Chapter 3** presents the ICT ecosystem, analyses the ICT supply chains and develops a conceptual ICT supply chain model.
- **Chapter 4** analyses security concepts and the legal background and provides state-of-the-art risk management approaches and domain-specific security topics, including the conformity assessment.

### **PART III – Research Underpinnings**

- **Chapter 5** identifies the challenges the current dissertation aims to contribute to based on the literature analysis provided in the previous chapters. It elicits a set of requirements from the identified challenges and identifies corresponding Dissertation Objectives to be addressed. It highlights all the artefacts produced in the context of the current dissertation

that constitute the CyberICT hybrid evaluation framework and the relations among them. In addition, it presents the developed cybersecurity standards ontology.

#### **PART IV – Cybersecurity risk management for ICT products and supply chain services**

- **Chapter 6** presents the CyberICT Risk Management methodology and the respective risk ontology. Their demonstration, applicability, practical adoption and evaluation is also provided.

#### **PART V – Protection Profile for ICT Products**

- **Chapter 7** presents the CyberICT Protection Profile which comprises a Protection Profile preparatory framework for composite ICT products and analyses the structure of its accompanying taxonomy. In addition, the framework guides ICT stakeholders on how to assess the claims of the Protection Profile. Their demonstration, applicability, practical adoption and evaluation is provided.

#### **PART VI – Evaluation Outcomes, Conclusions and Contribution to Science**

- **Chapter 8** summarises the overall evaluation outcomes of the created artefacts
- **Chapter 9** draws the conclusion of the current dissertation and describes the novelties and contribution to science.

### **1.3 The Design Science Research approach**

Design Science Research (DSR) is a problem-solving research paradigm that supports the design and evaluation of innovative artifacts to address complex real-world challenges. Through the generation of prescriptive knowledge, DSR bridges the gap between theory and practice by focusing not only on understanding existing phenomena but also on determining how they should be improved [22]–[23].

DSR is structured around a continuous interplay of three complementary cycles [22],[24]:

- **Relevance Cycle.** Links the research to its application environment by identifying the research problem from identified challenges, deriving requirements, and evaluating the developed artifact within its intended context.
- **Design Cycle.** Constitutes the core of the DSR process, involving the iterative development and evaluation of the artefact to ensure that it effectively contributes to the identified research problem.
- **Rigor Cycle.** Anchors the research in existing scientific knowledge and theoretical foundations, ensuring the design relies on established theories, rigorous methodologies, and proper evaluation techniques

The highly adopted, six-phase DSR Methodology (DSRM) [22]–[24], originally developed by Peffers et al. [24] includes:



- **Problem Identification and Motivation.** Defining the specific research problem and justifying the value of the produced artefacts.
- **Objectives Definition.** Specifying how the proposed artefacts are expected to contribute to the resolution of existing gaps and identified challenges.
- **Design and Development.** Creating the artefacts itself (e.g., business model, methodology, ontology model, structured taxonomy).
- **Demonstration.** Using the artefacts that contribute to the research problem in a specific instance, such as a case study, to verify its applicability, efficacy and efficiency to support the research problem.
- **Evaluation.** Evaluating how well the artefacts meet the identified objectives using empirical evidence or expert feedback.
- **Communication.** Sharing the problem, the artefact, its utility, and the research knowledge obtained with researchers and practitioners.

In DSR, an "artefact" may usually fall into the following categories:

- **Constructs.** The vocabulary and symbols used to define and describe a problem space (e.g., data models, terminology, a taxonomy).
- **Models:** The combinations of constructs that represent real-world situations, design spaces, or arguments (e.g., process model, ontology model, knowledge management model).
- **Methods:** Methodologies, algorithms and practices that guide how to perform a task (e.g., step-wised processes, calculation formulas).
- **Instantiations:** The realised, working implementations of constructs, models, or methods through a use case (e.g., application of a methodology through a real-life example, adoption in a system design).

This dissertation research is based on the DSR practice to develop a composite approach, i.e., the CyberICT evaluation framework, that incorporates interconnected cybersecurity artefacts supporting cybersecurity risk assessment for composite ICT products and their ICT supply chain services. Moreover, it guides ICT stakeholders on how to prepare the Protection Profile of their composite ICT products.

The developed artefacts include:

- **Methods**
  - a cybersecurity risk management methodology for ICT products and ICT supply chain services (CyberICT Risk Management Methodology)
  - a Protection Profile framework which prepares ICT stakeholders to construct the Protection Profile of composite ICT products (part of the CyberICT Protection Profile)

- Models
  - a risk ontology (CyberICT Risk Ontology)
  - an ontology for cybersecurity certification standards (CyberICT Standards Ontology)
- Constructs
  - a data model of a structured taxonomy that accompanies the Protection Profile of composite ICT products (part of the CyberICT Protection Profile)
  - a detailed glossary analysing risk and conformity assessment concepts
  - a list of acronyms and abbreviations
  - assessment scales for the calculations of the risk management methodology and the Protection Profile preparation approach of composite ICT products

The DSRM, described previously, is applied to the current dissertation research, as presented below:

- **Problem Identification and Motivation** (Chapters 1-4). Existing cybersecurity risk assessment approaches inadequately address the complexity of composite ICT products and their supply chain services dependencies. Standards fragmentation and lack of structured guidance hinders the integration of risk and conformity assessment to achieve measurable and verifiable holistic security assurance and develop the Protection Profiles of composite ICT products.
- **Dissertation Objectives Definition** (Sections 5.1-5.2). The proposed artefacts rely on:
  - Developing an ontology that classifies cybersecurity standards based on their objective, usage, and sector, aiming to guide ICT stakeholders on which to adopt to meet their needs
  - Developing a cybersecurity risk management methodology that considers interdependencies and technical complexity of composite ICT products and ICT supply chain services and a corresponding ontology that raises the organisational learning.
  - Developing a risk and conformity assessment approach that guides ICT stakeholders how to prepare the Protection Profile of a composite ICT product and assess their claims, accompanied by a respective taxonomy that enhances the security knowledge of ICT stakeholders.
- **Design and Development.**
  - CyberICT standards ontology (Section 5.3)
  - The CyberICT Risk Management Methodology (Section 6.1–6.2)
  - CyberICT Risk Ontology (Section 6.2.3)
  - CyberICT Protection Profile preparation of composite ICT products (Section 7.1)
  - CyberICT Protection Profile taxonomy (data model) (Section 7.2)

- **Demonstration.** Using the artefacts that contribute to the research problem in a specific instance, such as a case study, to verify its applicability, efficacy and efficiency to support the research problem. It includes the practical adoption in system design – progressively implemented across various security management and certification digital platforms (Sections 6.3- 6.4, 7.3-7.4).
- **Evaluation.** Proof of concept demonstration, scenario-based validation, evidence of utility (qualitative, quantitative), questionnaire survey in the context of CyberICT Risk Management methodology implementation in a digital platform, and reasoning-based validation ontology (Sections 6.5, 7.5, 8)
- **Communication.** The research outcomes are documented through the current doctoral thesis, scientific publications, and methodological models. Contribution to science, innovative aspects. (Chapter 9).

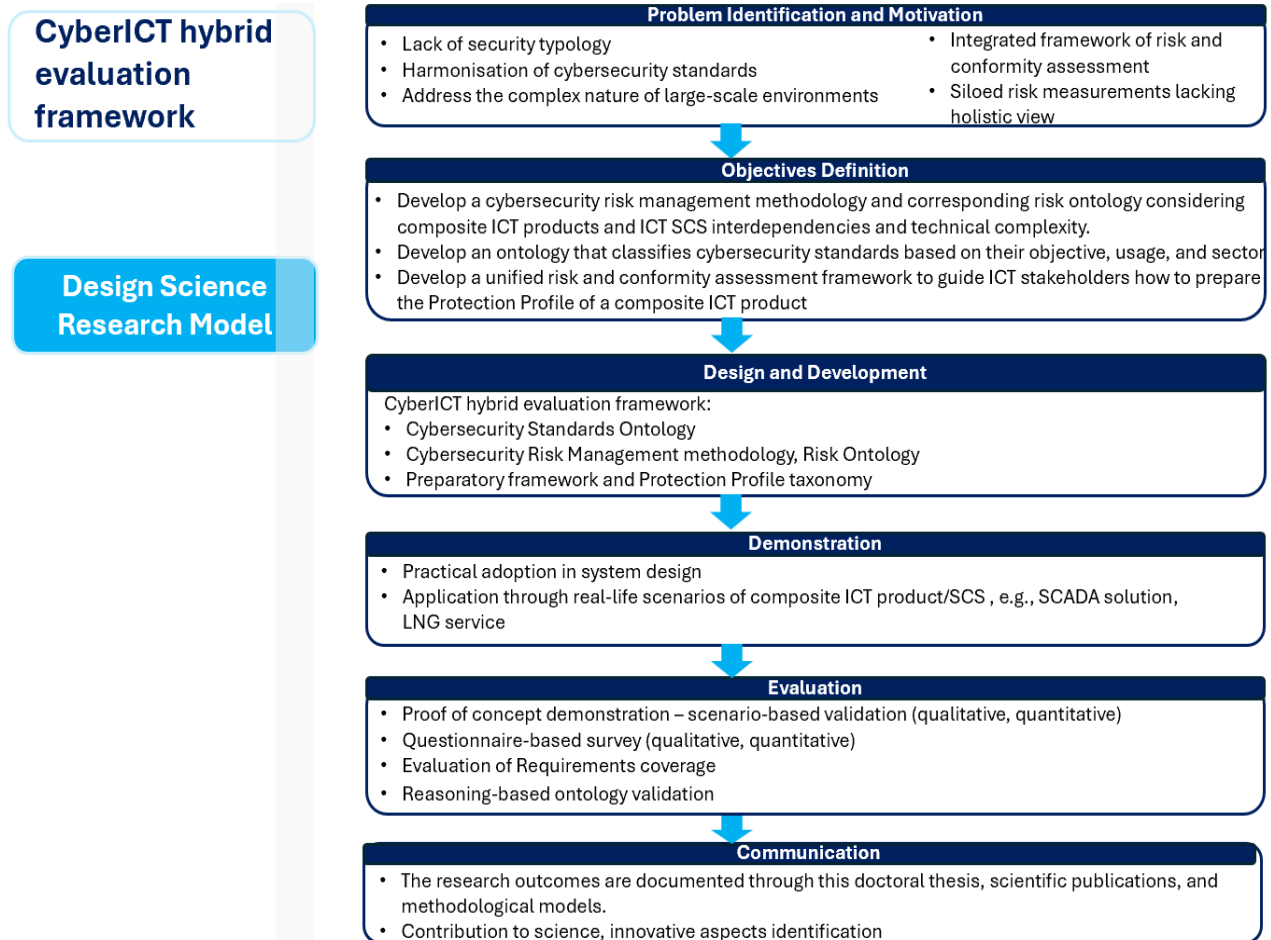


Figure 1. Design Science Research model of the CyberICT hybrid evaluation framework.

# PART II:

## LITERATURE REVIEW AND OPEN ISSUES

---

## 2. The interplay of Cybersecurity Risk and Conformity Assessment

The chapter underlines the importance of cybersecurity and the compelling need for its maintenance in today's digital world. It presents interrelations between the CRA[10] [11], NIS 2 Directive [12] and CSA [13] and highlights generic concepts of risk assessment and conformity assessment and their interplay

### 2.1 Digitalisation of products and security challenges

Factors that are influenced by the digitalisation and factors that trigger the demand for enhanced security and continuous security monitoring are presented in this section.

#### 2.1.1 Dependencies of digitalisation

P. Kotler in [25] describes a product as anything that can be placed on a market for attention, acquisition, use or consumption, providing value to customers to satisfy a want or need, which has become a widely accepted definition from a business perspective. Over the past few decades, the rapid evolution of digital technologies across products deriving from diverse industries and markets [9] has fostered investment in remote work and digital communication. This shift is fueled by a range of *socioeconomic, political, environmental, and technical factors*.

Unexpected crises with serious consequences and socioeconomic impact can trigger digitalisation. For instance, the COVID-19 pandemic was an immediate catalyst for Remote work [26], prompted by employees' demands for flexibility and the potential of organisational cost savings (*socioeconomic factor*) (see Section 4.5).

War conditions and geopolitical uncertainties of recent years (e.g. Iran-Israel and Russia-Ukraine conflicts) are influenced by digital dependencies (cyberdependencies) across states, firms, and infrastructures [27] (*political factor*). For instance, digital war reporting broadens accessibility and intensifies diplomatic efforts in real-time during geopolitical conflicts (cf. Section 4.5).

Climate change stimulates the application of digital and automated technologies. They can be used to address environmental challenges and support environmental goals, such as integrating sustainability principles [28] in green economies. For example, digital tools can monitor cargo emissions, support circular economy and waste management, promote eco-friendly consumer behaviour, and enhance environmental monitoring for conservation and disaster resilience (*environmental factor*) (cf. Section 3.2.2).

Technological advancements<sup>1</sup> and technical innovations<sup>2</sup> reinforce the integration of digitalisation in modern societies and economies [29]–[30] (*technical factor*) (cf. Section 3.3).

Furthermore, they promote networking and interconnectivity across national, regional and global supply chains, infrastructures, systems, services (see Section 3.1), such as maritime transport, container ports, Industrial Control Systems (ICSs) and cloud computing services. The growing need for digitalisation accelerates the productivity of Smart Objects — such as wearable devices, advanced sensor networks, and 5G-enabled autonomous agents — further driving investment in machine-to-machine (M2M) communication [31].

Internet of Everything (IoE), defined as the networked connection of people, processes, data, and things via the Internet, is the norm for complete digitalization [32]–[33]. Nevertheless, the growing addiction to digitalisation of products and services makes them inherently susceptible to security vulnerabilities and weaknesses, exposing them to a great variety of threats (cf. Section 4.5.1.2).

Existing European regulations, such as the Cyber Resilience Act [11], NIS 2 Directive [12] and Cybersecurity Act [13], stress that cybersecurity is no longer a nice-to-have, but a top priority, essential to modern economies.

### **2.1.2 The rising demand for enhanced security and continuous security monitoring**

The Cyber Resilience Act, Regulation (EU) 2024/2847, [11], emphasises the need of cyberdependent products and services to be *secure* and *resilient* not only when they are placed on the market but through their entire development lifecycle. Confidentiality, Integrity, and Availability (CIA triad) are foundational cybersecurity enablers that shall be commonly applied across products and services to safeguard their security and resilience (cf. Section 4.1). They shall be continuously supervised and maintained to ensure data remains secure, accurate, and accessible. This can be achieved by identifying an appropriate set for security requirements on products and services. According to NIST [34], security requirements are requirements levied on products and/or services and/or organisations originated from a set of applicable laws, directives, regulations, policies, standards, procedures, practices or mission/business cases to ensure that the confidentiality, integrity, and availability of information is being processed, stored, or transmitted. For example, an IoT platform requires an appropriate access control mechanism.

In the new digital era, the high interconnectivity of products and services dictates increasingly demanding security requirements due to several factors:

- *To respond to the dynamic dimension of the emerging threat landscape and the growing malicious capacity of adversaries.*

---

<sup>1</sup> Indicative examples are efficient web communication tools and channels, devices including Information and Communication Technologies (ICTs) like Unmanned Aerial Vehicles (UAV) -commonly known as drones-, or autonomous vehicles.

<sup>2</sup> Indicative examples are high-fidelity superconducting chips of great efficiency, intuitive interfaces for seamless human-AI collaboration, or Edge Computing enabling rapid real-time data processing.

Nowadays, adversaries possess high skills and have easy access to open-source malware, such as Next-Generation malware toolkits found on the Deep and Dark Web, which enables them to employ far more advanced techniques than were possible a decade ago, when attacks demanded much greater effort and resources. In this regard, adversaries can launch sophisticated attacks (e.g., in-memory malware that conceals its presence, code obfuscation, injection methods, detection evasion techniques, etc.) on complex cyberphysical interdependent systems (e.g., supply chain attacks like botnet DDoS attacks [35], locker ransomware or crypto-ransomware intrusions [36], etc). In recent years, the evolving threat landscape has driven a significant increase in cyberattacks with substantial impacts on digital privacy and market stability across Europe [37] and globally [38]. Indicative security incidents within the past few years are presented below.

- In 2020, the hack of Uganda's largest mobile money networks resulted in a four-day disruption of service transactions, causing a catastrophe in the country's telecom and banking sectors [7].
- The COVID-19-related cyberattacks in Healthcare generated data breaches of significant impact (e.g., exposing sensitive patient data) [7].
- In 2022, coordinated cyber intrusions, such as the RapperBot brute-force attacks, infected several IoT devices using over 3,500 unique IPs worldwide, indicating the importance of ensuring the security of digital devices [35].
- In 2024, the UK's Ministry of Defence (MoD) suffered from a serious data breach on its payroll system, caused by a cyber intrusion. As a result, sensitive information (e.g. personal data and bank details) was leaked affecting in some cases over 270,000 current and former UK military personnel, approximately (home addresses were exposed) [8].
- In March 2026, a cyberattack hit the cloud infrastructure which hosts the Commission's web presence on the European platform. The Commission promptly responded that immediate mitigation actions were applied and the incident was encountered without disrupting the Europa website services [39].

- ***For product technical modifications.***

Technical modifications (e.g., updates, configurations, enhancements, change of artifacts appearance, etc) introduced in products of evolving nature (e.g., sensory and adaptive systems, dynamic economic services, etc) underscore continuous monitoring of security requirements with enhancements wherever deemed necessary.

- ***To address security risks arising from unintended use of products.***

According to the Cyber Resilience Act (CRA) [11], products may be intended by the product manufacturer to be utilised for specific purposes and under specific conditions, as indicated in corresponding instructions and documentation. Nevertheless, a product can have a reasonably foreseeable use, which may not be intended by the manufacturer (e.g., installing a third-party application on a smart TV, neglecting software updates, etc). In such cases, the security requirements of the product may have changed.

- ***To manage risks associated with changes in the EU regulatory framework.***

Security requirements on products should be monitored for potential enhancements and/or adjustments in view of regulatory changes. For instance, ad hoc (formerly) identified security requirements for product should be reviewed in view of a (new) compliance obligation. As another example, products with digital elements, according to the CRA EU regulation [11], must follow compliance with corresponding security requirements, specified by the CRA.

- *To apply security in the entire Software Development Lifecycle (SDLC).*

Security requirements of a product should be identified from its design phase and continuously monitored until its final completion in all phases within the CI/CD pipeline.

- *To leverage security in view of crises caused by radical environmental and/or geopolitical and/or societal changes.* Such crises can unexpectedly affect the security status of a product. For instance, political realignments have historically impacted the global technology (e.g., restricted access to cloud computing services for some nations due to geopolitical conflicts).

Maintaining robust security in today's digital landscape is crucial. Security requirements are met by implementing effective security specifications, measures, and controls (see Section 4.1). Developing a measurable and actionable set of requirements—aligned with core concepts like the CIA triad—enables organisations to select appropriate security specifications and controls for their products and services, achieving the desired level of protection. Informed decision-making relies on thorough assessment of products and services by identifying, analysing, and estimating threats, vulnerabilities, and risks (see Sections 4.1, 4.3 and 4.4). A cybersecurity risk assessment should be performed whenever changes to the threat landscape or other factors that may affect the security posture (as documented above) are identified.

In addition, compliance with the existing cybersecurity regulatory framework is essential to attest that organisations adopt efficient security management for their products and services, and the security measures they use are valid and consistent in meeting current market security needs. Adhering to existing cybersecurity mandates can enhance security in organisations, reinforce their preparedness against security issues, increase their cyber resilience and promote their competitiveness in the modern digital market.

Current EU regulations, including the Cyber Resilience Act [11], the NIS 2 Directive [12], and the Cybersecurity Act [13], encourage businesses to adopt risk assessment and compliance procedures, helping them establish a robust and systematic security posture.

## **2.2 Security evaluation and compliance**

This Section presents the interrelations between legal instruments of ICT evaluation and introduces an enhanced security model that integrates risk and conformity assessment concepts.

### **2.2.1 Subjects of evaluation and legal instruments interrelations**

Cybersecurity embraces all activities needed to protect network and information systems, their users and all other parties that can be affected by cyber threats [13]. A variety of EU legal



instruments (including<sup>3</sup> but not limited to [11],[12],[13]) have been developed to embrace and support the security of products and services.

The Cyber Resilience Act (CRA) [11] defines a *Product with Digital Elements* (PDE) as a product meant for commercial use. A PDE consists of a software or hardware, supported by remote data processing for performing to perform at least one of its functions. It is available on the market, with the intended purpose of a direct or indirect logical or physical data connection to a device or network. Indicative examples of PDEs are smart wearables, IoT devices, smart thermostats, or connected toys. An *ICT product* is a broader concept of a product<sup>4</sup>, defined by the Cybersecurity Act (CSA) [13] as “*an element or a group of elements of a network or information system*”. Indicative examples of ICT products include a network-attached storage system, a smartphone, a server in an organisation’s local network, an IoT device, or a smart card. An *ICT service*, according to the CSA [13], is a service engaged entirely or partially in the transfer, storage, retrieve or processing of information utilising network and information systems. A telecommunication system, a cloud computing service used to store mobile data, or a Software as a Service (SaaS), such as video conferencing, are representative examples of ICT services. Digital products and services are subjects of evaluation to assess their security and compliance with the current cybersecurity regulations, such as the CRA [11], CSA [13] and NIS 2 Directive [12].

The CRA [11] aims to regulate manufacturers of PDEs to cover the security throughout the product’s lifecycle (DevSecOps [40]–[41]) to safeguard consumers and businesses based on products’ criticality classification [42].

The CSA [13] aims to “*achieve a high level of cybersecurity, cyber resilience and trust*” within the European Union (EU)” ICT ecosystem [43] (cf. Section 3). In this regard, it regulates certification stakeholders (i.e., ENISA, and authorised bodies, such as, attestation bodies and testing labs – cf. Section 4.6). The Commission Implementing Regulation (EU) 2024/482 [14], initiates the first harmonised European Cybersecurity Certification Scheme (EUCC) of ICT products. The EUCC is based on the Common Criteria certification framework, i.e., ISO/IEC 15408 series [44]–[46]. The Cybersecurity Act targeted amendment [47] aims to enable the future adoption of European certification schemes for “*managed security services*”<sup>5</sup> to improve alignment with NIS 2 Directive [12]. In this respect, a candidate EU Cybersecurity certification for Managed Security Services (EUMSS) is under development [48]. Moreover, a proposal for a revised Cybersecurity Act,

---

<sup>3</sup> The references provided here refer only to the EU Regulations that have a direct relation to the current Doctoral Thesis.

<sup>4</sup> It does not necessarily refer to a product promoted for commercial use. It can be, for example, a firmware of an organisation, such as a server that is part of an organisation’s communication network, etc. ICT products may include all technical means used to manage information and support communication by processing, storing, or transmitting data (e.g., a workstation, including hardware and its software). An ICT product or PDE may refer to the same product if it is promoted for commercial use (e.g., an IoT device or a smartphone). In addition, an ICT product may be a component of a PDE (e.g., the operating system of a smartphone).

<sup>5</sup> Covering areas such as incident response, penetration testing, security audits and consultancy.

including an updated cybersecurity package of CSA to strengthen its objectives has been published [49].

The NIS 2 Directive [12], replaced its predecessor the NIS Directive [50] has established a European competence in cybersecurity to protect the digital single market. It highlights the necessity of creating a risk management culture “*for the maintenance of economic and societal activities and Digital Service Providers*”. The NIS Directive urges medium-sized and large entities of critical sectors, to take appropriate cybersecurity risk management measures and promotes incident reporting [51]. A targeted amendment of NIS 2 Directive has been published [52], concerning simplification measures and alignment with the Cybersecurity Act.

Table 1 provides a comparative overview of the cybersecurity regulations mentioned above, considering their main objectives, the actors involved, the size of the targeted companies, the key dates of the regulations, their relation to cybersecurity risk assessment and conformity assessment procedures, and the main topics to which they contribute.

Table 1. Comparative overview of CRA, CSA and NIS 2 Directive.

|                                           | <b>Cyber Resilience Act (CRA) [11]</b><br>(Regulation EU 2024/2847)                                                                                                                                      | <b>Cybersecurity Act (CSA) [13]</b> (Regulation (EU) 2019/881)<br>Targeted Amendment<br>(Regulation (EU) 2025/37 [47])<br><b>EUCC [14]</b><br>(Regulation (EU) 2024/482)         | <b>NIS 2 Directive [12]</b><br>(Regulation (EU) 2022/2555)                                                                                                                                                                               |
|-------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Objective</b>                          | To set mandatory cybersecurity requirements for manufacturers to apply to <b>products with digital elements</b> throughout the SDLC (depending on products default/ important/ critical classification). | To introduce an EU-wide Cybersecurity Certification Framework to raise cybersecurity, resilience and trust to the <b>ICT ecosystem</b> and regulates certification stakeholders. | To achieve a high common level of cybersecurity across the EU by strengthening the cybersecurity capabilities, risk management, incident reporting, and resilience of <b>essential and important entities within the ICT ecosystem</b> . |
| <b>Main actors</b>                        | Manufacturers, customers.                                                                                                                                                                                | ICT stakeholders, cybersecurity certification stakeholders and users of certificates.                                                                                            | Operators of services – industry sectors, ICT supply chain stakeholders, CSIRTs.                                                                                                                                                         |
| <b>Size of companies that applies</b>     | All sizes, including startups, microenterprises, SMEs and large enterprises                                                                                                                              | All sizes, but mostly focused on medium-sized enterprises and large enterprises.                                                                                                 | Medium-sized enterprises, large enterprises (mandatory for 50+ employees or >€10m turnover).                                                                                                                                             |
| <b>Applicability Timeline (key dates)</b> | • <b>10 December 2024:</b><br>Entered into force                                                                                                                                                         | • <b>17 April 2019:</b> CSA<br>Entered into force                                                                                                                                | • <b>16 January 2023:</b><br>Entered into force                                                                                                                                                                                          |

|                                                  |                                                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                  | <ul style="list-style-type: none"> <li>• <b>11 September 2026:</b> Starts reporting obligations</li> <li>• <b>11 December 2027:</b> Main obligations applications starts</li> </ul>                                                                                                                        | <ul style="list-style-type: none"> <li>• <b>27 February 2024:</b> Implementing regulation of EUCC entered into force on <b>27 February 2025:</b> Implementing regulation of EUCC fully applied February 2025.</li> <li>• <b>4 February 2025:</b> Targeted amendment entered into force (improve alignment with NIS 2 Directive)</li> <li>• <b>21 January 2026:</b> Cybersecurity Act 2 ("CSA2") proposal published</li> <li>• <b>2024–2027:</b> Transition from national schemes to EU-level certification</li> </ul> | <ul style="list-style-type: none"> <li>• <b>17 October 2024:</b> Transposition deadline</li> <li>• <b>18 October 2024:</b> Measures enforcement starts with penalties</li> <li>• <b>20 January 2026:</b> Proposal for targeted amendment published (improve alignment with CSA)</li> </ul>                                                                                                              |
| <b>Relation to cybersecurity risk assessment</b> | Directly (throughout the SDLC)                                                                                                                                                                                                                                                                             | Direct                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Direct                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Relation to conformity assessment</b>         | Direct                                                                                                                                                                                                                                                                                                     | Direct                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Indirect                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Targeted topics</b>                           | <ul style="list-style-type: none"> <li>• Extends CE marking<sup>6</sup> to products compliance with cybersecurity requirements</li> <li>• Addresses the existing inadequate level of security on products and the lack of timely security updates.</li> <li>• Facilitates the identification of</li> </ul> | <ul style="list-style-type: none"> <li>• Raises the customers security confidence and comparability of ICT products to address the lack of trust in the ICT ecosystem.</li> <li>• Mutual recognition across Member States to address cybersecurity certification fragmentation</li> <li>• Adoption of EU-wide harmonised certification scheme replacing</li> </ul>                                                                                                                                                    | <ul style="list-style-type: none"> <li>• Stringent incident handling: harmonizes security and incident reporting requirements across all EU countries to reduce cybersecurity fragmentation</li> <li>• Focuses on cybersecurity awareness and cyber hygiene</li> <li>• ICT risk-based cybersecurity framework for common understanding</li> <li>• Focuses on emerging threat landscape (e.g.</li> </ul> |

<sup>6</sup> Guarantees that the product complies with the CRA requirements and national market surveillance authorities will ensure enforcement of the rules. It visibly, legibly and indelibly indicate the product's conformity with this Regulation to move freely within the internal market<sup>315</sup>.

|  |                                    |                                                                                                                                                                   |                                                                                                                                                               |
|--|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | cybersecurity features on products | multiple national schemes <ul style="list-style-type: none"> <li>• Strengthens supply chain visibility</li> <li>• Strengthen cybersecurity sovereignty</li> </ul> | ransomwares) and supply chain attacks) <ul style="list-style-type: none"> <li>• Introduces accountability of the top management for non-compliance</li> </ul> |
|--|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|

Key takeaways of the interactions of these cybersecurity regulations are described below:

- CRA involves risk assessment at the product layer (DevSecOps), while the NIS 2 Directive applies across systems, infrastructures, and organisations' layers of the ICT ecosystem (cf. Section 3.2.3). The CSA aims to ensure security and raise trustworthiness across the ICT ecosystem via certification scheme verification.
- The three regulations indicate cybersecurity risk assessment as a mandatory security process to be adopted from stakeholders of the digital ecosystem.
- Conformity assessment procedures directly apply to CRA and CSA. The application of CRA refers to either self-conformity assessment or third-party conformity assessment procedures (depending on the criticality of products), while EUCC evaluation for cybersecurity certification is mostly recommended for CRA products requiring a stringent evaluation (some categories of important products and the critical products in the CRA product classification [11]). For the application of the EUCC, only third-party conformity assessment procedures are valid.
- CRA aim to provide security-by-design, while CSA measures the trust, and the NIS 2 Directive guides organisations on how to stay resilient.
- Types of products, such as medical devices, aviation products, or automotive systems are excluded from CRA regulation and covered by sector-specific regulations. The NIS 2 Directive applies to operators of the corresponding industry sectors.
- All the above cybersecurity regulations together can establish end-to-end cyber resilience from code to product, system operations and the entire ICT ecosystem.

To this end, the cybersecurity regulations of the CRA, CSA, and NIS 2 Directive are complementary to each other, recommending: i) risk-based assessments to manage the security of products and services and ii) conformity assessment which is a set of procedures to assess the compliance of products and services with the cybersecurity regulations. The risk assessment and conformity assessment concepts, their processes and their interplay are described in the following section (cf. Section 2.2.2).

## 2.2.2 The enhanced security model

Sections 2.1.2 and 2.2.1 presented the need for performing risk assessment on a product or a service to assess and manage risks and evaluate whether these products and services meet compliance requirements with the current regulatory framework.

*Cybersecurity risk assessment* is the process of identifying, analysing, and evaluating cyber risks, threats and vulnerabilities of information systems and products. It aims to develop and implement a risk management plan for treating the identified risks, while considering mitigations provided by security controls [53]. ISO/IEC 27k family of standards [54] is the widely known series of international standards that sets a framework for Information Security Management Systems (ISMS). Specifically, ISO/IEC 27001 [55] sets requirements for implementing ISMS. ISO/IEC 27005 [56] guides on performing a cybersecurity risk assessment considering the requirements of ISO/IEC 27001 [55]. Threat identification, vulnerability assessment, and impact analysis are the three primary factors for identifying and estimating cyber risks on products or services (cf. Section 4.1).

According to the CRA regulation [11], before a product with digital elements enters a market, it shall demonstrate to the provider or consumer that it is secure, performs as promised and satisfies requirements based on several evaluation criteria, such as efficiency, reliability and sustainability. To this aim, risk assessment procedures are needed.

*Conformity assessment* is the process of evaluating and demonstrating whether specified requirements, rules or claims associated with the subject for evaluation (e.g., a product or service) have been fulfilled [13],[57] (usually addressed by a standard applicable to regulation). The conformity assessment integrates a set of activities, including but not limited to testing, inspection, validation, verification, certification, and accreditation. To investigate whether a product with digital elements fulfils specified requirements based on the CRA a conformity assessment is required.

Cybersecurity certification is the *formal attestation* that the under evaluation product or service covers security requirements addressed by a standard or a scheme after conducting a third party conformity-assessment by an authorised accreditation body.

The CSA regulation [13] establishes a common EU framework for cybersecurity certification, while the EUCC implementing regulation [14] sets the rules for an initial generic EU cybersecurity certification scheme, based on the Common Criteria (CC) certification framework (i.e., ISO/IEC 15408 series). A high-level concept of the CC-based certification framework is provided in the following to explain how risk assessment and conformity assessment are integrated in the cybersecurity certification evaluation.

The CC certification framework defines the product or service (or parts of them) that will be the subject of evaluation, as the *Target of Evaluation (ToE)*. *Evaluation* is described by the CC certification framework, Part 1 [58] (i.e., ISO/IEC 15408-1 [44]) as the assessment of a ToE against specified security requirements and assurance criteria. Assurance is considered the grounds of confidence that a ToE meets the specified security requirements [44]. To specify the security requirements of the ToE, risk assessment procedures shall be performed to assess the ToE's security and scrutinise the needs for an efficient control policy that will meet. The security requirements are defined by implementation-independent statements. These statements compose the Protection Profile [44] of the subject for evaluation, including a set of elements that are further analysed in Section 4.6.6. The security requirements can be covered by security specifications and

the implementation of security controls. The security requirements statements, along with the security and assurance claims included in the Protection Profile, are assessed by the evaluator (conformity assessor). The latter determines whether they are covered to reach cybersecurity certification. The conformity assessment process integrates these procedures. ISO/IEC 15408 sets the evaluation criteria and requirements; ISO/IEC 18045 [59] is complementary and provides a generic methodology for the actions to be performed to evaluate their application, according to the CC framework.

Consequently, the CSA and CRA indicate the performance of both risk assessment and conformity assessment procedures by relevant actors. The synergy of both risk assessment and conformity assessment processes is required to provide an end-to-end evaluation for attesting the security, according to the specified criteria, of products or services. Depending on the subject matter of the evaluation, the operators involved and the perimeter and depth of the evaluation, NIS 2 Directive principles should be considered to assess the security of the subject matter (e.g., for supply chain service evaluation).

There is limited research effort analysing the interplay of risk and conformity assessment concepts. The risk and conformity assessments relations were presented at a generic level in [60]–[61]. Moreover, ENISA in [62] presents a conceptual approach of risk, security and assurance concepts and their interrelations.

The current dissertation explored an initial research of a standards-based framework that integrates risk and conformity assessment concepts, which was presented in [63]. A dual-use methodology that combines risk and conformity assessment processes is described in [15].

Figure 2 presents an enhanced security model developed within the current research work. The model builds upon the Extended Information Security Risk Model of [60] and expands it, based on [63], providing additional flows between the risk and conformity assessment concepts to further analyse and visualise how they converge. Moreover, the model presents a flow diagram depicting relationships between information security risk and conformity assessment concepts, as previously discussed. Figure 2, illustrates at the upper side of the diagram the information security, flows related to the risk assessment procedure. For example, some flows indicate that threats exploit vulnerabilities that may lead to a security event, which impacts information assets (ToE). The relevant family of standards is displayed. At the bottom of Figure 2 flows associated with IT evaluation and conformity assessment are displayed. For instance, assurance adheres to objectives, and risk treatment relies on the identified security requirements. Another flow visualises the flow of assurance criteria defining the depth of the risk assessment that will be performed. Furthermore, Figure 2, presents the relationships between the risk assessment and conformity assessment concepts and the CRA, CSA and NIS 2 Directive regulations, and visualises their interplay.

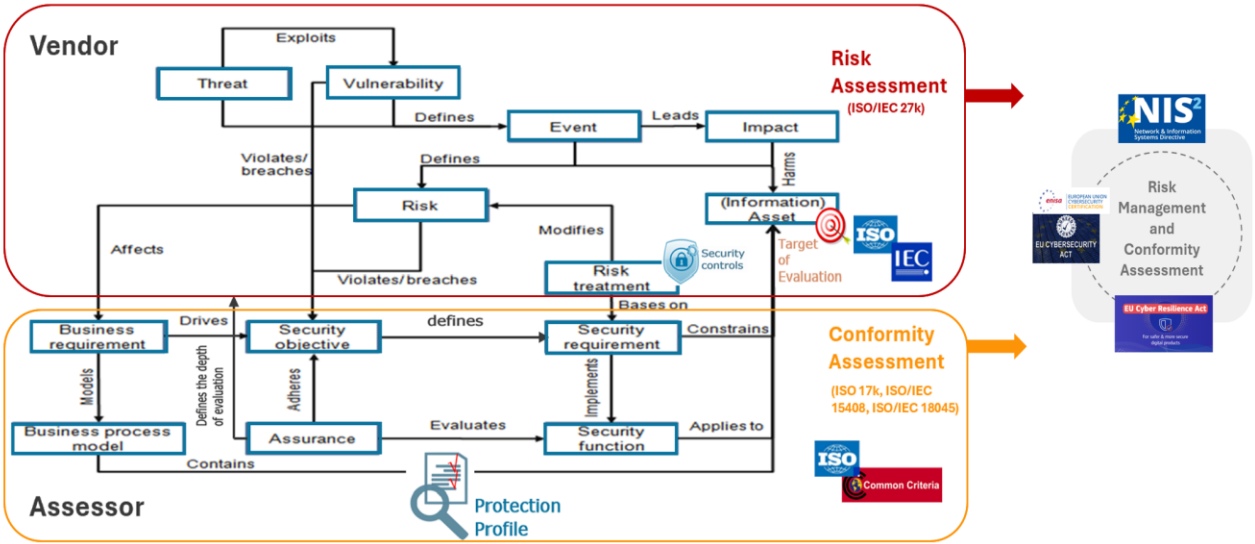


Figure 2. Enhanced security model [60] depicting relations of risk and conformity assessment concepts.

The enhanced security model aims to visualise the relationships and flows between risk and conformity assessment concepts and the relevant regulations.

Based on this model, the current work develops a methodology that integrates both risk assessment and conformity assessment procedures, providing an end-to-end evaluation to facilitate readiness for cybersecurity certification and security compliance procedures.

### 3. The ICT ecosystem

In the previous section, the digitalisation of products and services in modern economies was analysed. The concepts of Products with Digital Elements (PDEs) and products and services, including Information Communication Technologies (ICTs), were presented, according to the definitions provided by existing cybersecurity regulations (i.e., the CRA [11] and CSA [13], respectively). This section aims to present the main elements, actors and their operational environment which interact throughout the entire ICT ecosystem.

#### 3.1 ICT structures and concepts

In the current digital age, networks, IT systems and electronic communications play a pivotal role in global society, becoming the main driving forces of the economy [13]. The growing advancements and increased use of digital technologies, such as Industrial Internet of Things (IIoT), 5G communications, and AI agents, have strengthened the connectivity between products and services. They are almost fully operating within the EU single market [64] through the use of Information and Communications Technologies (ICTs). The latter are considered ubiquitous technologies for gathering, storing, retaining, retrieving, processing, displaying, representing, organising, managing, securing, transmitting, and exchanging data and information [65] (e.g. microelectronics, wearable technologies, software applications, mobile telephony, signal processors, satellite communications, etc). European community's societal and financial activities are underpinned by products, services and processes utilising ICTs [13].

In our digital world, products are complex. They may comprise several heterogeneous primary elements [13], including software, hardware and firmware, which are the building blocks of a product, supporting its functionalities, the technical, business and security requirements for its intended use, considered as “assets”. A widely recognised definition of asset derives from the ISO/IEC 27002:2022 international standard from an information security perspective, as anything (e.g. hardware, software, network, information) that has value (tangible or intangible) to an entity [66]. The proposal for the EU Cybersecurity Act 2 [49] defines “ICT assets” as software or hardware in the network and information systems, utilised by entities. ISO/IEC 15408-1 [44] defines an asset as an entity that the owner of a Target of Evaluation (see Section 2.2.2, and Section 4.6) has presumably placed value on.

In the current dissertation, the definition of the EU Cybersecurity Act 2 proposal is adopted for assets, represented as the fundamental elements in the ICT ecosystem (see Section 3.2.3). In terms of IT evaluation for conformity assessment perspective (see Chapter 7), assets are interpreted as the primary elements of a complex ICT product, considered as a Target of Evaluation, according to the ISO/15408-1 definition [44] (see Section 2.2.2, and Section 4.6). An ICT asset (e.g., a software appliance or an operating system) can be the “ICT product” itself or an element of an ICT product (e.g., an operating system in a mobile device).

“ICT systems” encompass assets operating for their functioning. An organisation system of facilities, equipment and services [67] required for the operation of an entity (e.g. enterprise,



organisation, government) is considered an “ICT infrastructure”. ICT infrastructure may be regarded as the aggregation and interconnection of multiple ICT systems (cyberphysical systems), including hardware, communication networks, software platforms, data-processing resources, and supporting facilities. Furthermore, “ICT services” rely on ICT systems, networks, and infrastructures for their delivery and operation, while, conversely, ICT infrastructures and systems can be managed, monitored, and supported through ICT services.

ISO/IEC 27000:2018 international standard [53] identifies “process” as a group of interconnected or interacting activities capable of turning inputs into outputs. From a business perspective, a process is perceived as a structured set of activities designed for achieving specified business outcomes [68]. The CSA regulation [13] describes an “ICT process” as a set of activities conducted to “*design, develop, deliver or maintain an ICT product or ICT service*”. ***The current work combines the above technical [53], business [68] and ICT aspects of process, considering it as a set of actions taking place within the ICT ecosystem and develops business models to utilise them in the proposed risk management methodology*** (see Chapter 6).

ICT stakeholders are the actors within the ICT ecosystem. Drawing upon the CSA regulation [13] and ISO 28k family of international standards on security and resilience, “ICT stakeholders” are individuals, groups, or organisations that affect (or they are affected by) or have a vested interest in the development, operation, security, governance, or use of ICT systems, ICT services, ICT infrastructures, or ICT processes [6]. ICT stakeholders can be a variety of entities or individuals, such as users, customers, ICT service providers, software vendors, cloud providers, system administrators, regulators, cybersecurity authorities, suppliers, employees, and third-party contractors.

On top of the ICT ecosystem is the supply chain. A “supply chain” is considered a globally distributed, interconnected set of entities (i.e., organisations, companies, individuals), processes and services that relies upon a cyberdependent web of ICT infrastructures and networks to leverage the flows of products, services and information from a source to an end-customer/user [6],[69]. The ISO 28001:2007 international standard on supply chain security [70] specifies the supply chain, as a linked set of resources and processes activated upon placing a purchase order, starting from the sourcing of raw material, continuing with the manufacturing, processing, handling and delivery of goods and related services, ending with the purchaser. The proposal for the EU Cybersecurity Act 2 [49] specifies an “ICT supply chain” as a group of ICT services, ICT products and ICT processes incorporating activities and actors participating at all stages upstream of a product being placed or a service delivered on the market. Thus, the ICT supply chain are considered all stages before a product reaches the market or customer. The ICT product is the outcome of the ICT supply chain.

This work adopts all above concepts to analyse the ICT supply chain (sections 3.2 and 3.3). It analyses its hierarchical, business, technical, horizontal and vertical aspects to develop the ICT supply chain model, (cf. Section 3.2.3) which will be used in the proposed risk management methodology (see Chapter 6).

## 3.2 ICT Supply Chains

This section aims to introduce the ICT supply chain. It describes its driving forces, studies its classification and finally develops the ICT supply chain model, which is used in the CyberICT Risk Management Methodology.

### 3.2.1 Introducing the ICT Supply Chains

Although the underlying principles of supply chain management have concerned commercial and industrial activity for more than a century, the concept was formally introduced in the literature in the early 1980s [71]–[72]. In previous decades, supply chain management aimed to address specific requirements, such as large-scale alterations, re-engineering and downsizing-related activities for cost reduction. The use of digital technology on transportation modes and logistics environments has expanded the borders of the supply chain's performance. ICT supply chains have become the blood veins of global trade and economy, where individual operators and organisations coming from dispersed geographic locations and different critical sectors (e.g. health, finance, energy, power and transportation) collaborate in exploring new labour markets and providing compound services towards building an innovative, vibrant and secure Digital Single Market [6]. Furthermore, enterprises and other entities operating within the supply chains are highly dependent on ICTs, exchanging a vast amount of information [6].

A complex network of various organisations, diffused across multiple tiers and distant locations, is considered a global ICT supply chain [73]. This global dimension of the ICT supply chains strengthens and broadens the relationships among ICT stakeholders, facilitating horizontal integration of enterprises and generating cross-organisational synergies to increase their competitiveness [74]. Considering this far-reaching complexity of ICT supply chains, their management relies on the systemic, strategic coordination of the traditional business functions and the tactics applied within a particular company and the ICT stakeholders across the ICT supply chains, aiming to improve the long-term performance of the individual companies and the supply chain as a whole [6],[69],[75].

The strategic nature of the ICT supply chain management and its successful performance can create a competitive advantage. *Expanding the integration behaviour among operators within the global ICT supply chain* is required for efficient supply chain management [69].

### 3.2.2 ICT Supply Chain Driving Forces

The ICT stakeholders involved in the globally dispersed network of the ICT supply chain may face individual or combined threats or have isolated weaknesses, which can become vulnerable to adversaries' malicious activity (e.g., information tapping, counterfeit, system compromise). In this vein, the interdependent nature of ICT-enabled supply chains can propagate these threats and weaknesses in the entire ICT supply chain, jeopardising its entire operation [6]. For example, the Shadow Hammer operation in 2018 took advantage of an update utility on a global computer manufacturer, which impacted approximately a million users since it was promoted to customers through the manufacturer's official website [76]. Therefore, the protection of ICT interrelated systems and the security of information exchange within the ICT supply chain have positive

relations to its performance. The NIS 2 Directive [12] emphasises that the security of network and information systems is crucial for the seamless operation of the cross-border movement of goods, services, and people throughout the ICT supply chain. Thus, *maintaining the security of ICT systems in the supply chain is a driving force to keep the supply chain's regular performance.*

The ISO/IEC 27000:2018 international standard of information security identifies *integrity* as “a property of accuracy and completeness”[53]. Integrity in the ICT supply chain aims to ensure that operations adhere to established best practices and standards, while also meeting necessary resilience requirements [12],[77]. Most ICT stakeholders, may be aware of the integrity concept, but they have not considered it in association with their normal operations [77]. The literature reviews show that best practices and guidance on ICT supply chain integrity are limited and can hardly be applied [6],[77]. Wherever they are implemented, *they are based on traditional security or procurement frameworks and they lack supply chain self-insight* [6],[77]. Nevertheless, recent efforts, such as NIST 800-161 [78] and the proposal of the EU CSA 2 regulation [49], aim to limit this gap.

Regarding ICT supply chain *sustainability*, there are several open issues:

- The ISO 14k family of international standards provides key elements for building a sustainable supply chain strategy to reduce the environmental impact and promote efficient waste management. In this context, product design, waste and energy use shall increase alignment with environmental goals.
- Advancements in production technologies (e.g., increasing automation using AI-based technologies, robotics, quantum technologies, digital twins for real-time process simulation) are transforming supply chains [79]. Nevertheless, the use of advanced technologies may create a new emerging (unknown) threat landscape which cannot be encountered yet due to the lack of awareness.
- Servitisation of industries [79] promotes one-stop-shop Product-Service Systems (PSS) and Everything-as-a-Service (XaaS), which creates tighter dependencies across the ICT supply chain dispersed nodes, expanding the attack surface.
- Current geopolitical tensions (cf. Section 2.1.1) have led to the decline of distant investment in geopolitically distant countries. This drop in Foreign Direct Investment (FDI) creates gradual disruptions to the ICT supply chains, downsizing digital sovereignty. Furthermore, with the rise of “friendshoring”<sup>7</sup>, a nation’s cyber hygiene and regulatory framework have become key factors in attracting investment from allied countries [79]. In this vein, cyber resilience is regarded as a strategic asset.

Sustainability in the global ICT supply chain seeks to integrate environmental, social, and economic objectives [79], while enhancing brand reputation, reducing environmental impact, and increasing long-term profitability [81]. *A sustainable supply chain is directly linked to*

---

<sup>7</sup> Selecting ICT supply chain partners from countries that are politically aligned.

*maintaining the supply chain security and focuses on developing and utilising technologies that facilitate sector-specific collaboration to improve business, societal impact, and cyber resilience [81].*

The ISO 22301:2019 international standard [82] affirms that Supply Chain Continuity is the intersection of Supply Chain Management and Business Continuity Planning. Supply Chain Continuity research is limited [83]. Ill-handled performance throughout the supply chain can lead to service disruption and discontinuity. The loss of supply chain continuity could have a devastating impact on a national, regional or even global extent. This is because ICT supply chain interactions do not follow single paths directly from a starting point to an endpoint. They may follow intermediate node routings. An indicative example is the automobile Industry, which transfers vehicles to the end customer via a series of forwarders and service providers across the Vehicle Transport Chain. In this vein, the loss of a contained link would impact the other parties interacting. As another example, a stevedore and dockers' labour strike within the Maritime Transport Supply Chain could lead to unexpected delays in delivering a commodity to the consumer.

Structures in the ICT supply chain are visualised as a fishbone diagram [77], and the loss of continuity can threaten the ICT supply chain resilience due to either natural causes (e.g. physical disaster), or human unintended (e.g. accidental fire) or even intended (e.g. cyberattacks) causes.

The Confidentiality, Integrity and Availability (CIA) triad, together with the outlined secondary features, are enablers for sustainable ICT supply chains. The ISO 28001:2007 [70] provides requirements and guidance for organisations to establish and document reasonable levels of security within the global ICT supply chain.

The issues mentioned previously can be addressed by adopting an effective ICT supply chain security policy which focuses on enhancing organisations' corporate strategy and ensuring business continuity [6]. Business continuity is the payoff of comprehensive Business Continuity Planning and Disaster Recovery, ensuring that ICT stakeholders preserve operational functionality in the event of disruptive incidents. *Robust supply chains are built with continuous awareness and vigilance through the implementation of Business Continuity Planning [6].*

### **3.2.3 ICT supply chain classification**

The current section provides the outcomes from continuous research work, based on [6], [15],[63],[84] publications created during this dissertation, to identify literature related to the ICT supply chain classification (Section 3.2.3.1) and develop the ICT supply chain model (Section 3.2.3.2).

#### **3.2.3.1 Related work**

The literature reviews a variety of efforts for identifying and conceptualising supply chains classification under various and different perspectives, such as the works describe in the following, derived from multiple disciplines, including studies of more than 300 research works.

Mentzer [69] and Power [75] review, categorise, and synthesise existing supply chain management concepts and frameworks. Lee in [85] analyses supply chain key capabilities, such as agility, adaptability, and alignment, stressing the complexity of diverse interest between partners involved throughout the ICT supply chain. A high-order topological representation of the ICT supply chain is presented in [86].

Several works present supply chain classifications, considered either from managerial and/or operational perspectives, as mentioned in [87]. The systematic literature review in Pennekamp et al. (2023) [88] analyses supply chain characteristics, structural complexity, information flows and technical perspective. The works of [89] and [90] are flagship outlets in decomposing supply chains into key layers, such as strategies, enablers, processes, data analytics, flows, and features.

Such efforts may provide clear supply chain perspectives from business, managerial, technical and/or operational aspects. Nevertheless, there is limited discussion over sector-specific views. In addition, few works combine the above concepts in supply chain analysis. They do not present holistically different views of technical/ICT and business perspectives in both horizontal (cross-sectoral) and vertical (sector-specific) aspects within an ICT supply chain network.

The current doctoral thesis has developed a holistic supply chain model that conceptualises the ICT supply chain from business, technical, horizontal and vertical aspects, illustrating relations and actors involved, presented in Section 3.2.3.2.

#### 3.2.3.2 The ICT supply chain model

Based on the outcomes of the research work of [84] and additional work, presented in publications [6], [15] and [63], the ICT supply chain model is analysed into the following aspects:

- ***ICT supply chain hierarchies.***

The ICT supply chain model is decomposed into the following top-down hierarchical layers:

- **The ICT Supply Chain Service (SCS) layer.** According to the definitions provided in Section 3.1, a supply chain service is considered a network of entities that operate upon placing a purchase order (supply chain operators) and their supporting units and processes that function for the transaction of resources [91] for the provision of the service and its delivery to the end- customer/user. An indicative example is the Vehicle Transport Service upon an importer's request of purchasing vehicles from a manufacturer. The ICT SCS layer encompasses all the following layers.
- **The ICT infrastructure layer.** ICT SCS are implemented by a group of ICT/OT infrastructures that interoperate for its provision. As described in Section 3.1, the current layer aggregates all components of the ICT system layer, i.e., multiple ICT interconnected systems and their premises, facilities, devices and equipment. The layer includes all infrastructure that operate for all processes that are executed for the provision of the ICT SCS. Such processes include the primary (high-level) processes and the secondary processes that support them. For instance, in the Vehicle Transport Service, port and logistics infrastructures interoperate for delivering the vehicles' order from the manufacturer to the importer. Port and logistics SCADA infrastructures may operate for

all relevant processes that are executed for the provision of the Vehicle Transport Service. Such processes may be primary (high-level) processes, such as vehicles' unloading on a vessel, and secondary processes, such as formalities for the stevedoring.

- **The ICT system layer.** The current layer comprises all assets embedded in an ICT system (cyberphysical system), including devices, equipment, operating systems, applications, and their operational environment. For instance, the ICT system layer in the Vehicle Transport Service example may include a SCADA system to monitor the unloading of the vehicles from the port terminal to the vessel. For example, the Human Machine Interface (HMI) is the environment of the SCADA remote control system that controls it enabling Human-Computer Interaction (HCI). The HMI screen and the software operating system are the assets of the SCADA system.

- **Actors.**

ICT stakeholders are all actors (cf. Section 3.1) participating in the supply chain hierarchical layers of the ICT ecosystem. They are considered the operators of the ICT SCS. They can be either individuals, or groups, or organisations that have a legitimate interest throughout the ICT supply chain performance. ISO 28001:2007 international standard of supply chain security [70] identifies "business partners", as all contractors, suppliers or service providers that support an ICT stakeholder in its functions throughout the ICT SCS. For example, in the Vehicle Transport Service an ICT stakeholder can be a Port and its business partners can be the Customs, a Ship Agent or a Broker.

- **Business aspect.**

The ICT SCS is operated through the completion of a set of processes. ICT processes within the supply chain is a set of activities involved directly or indirectly for the provision of the ICT SCS to the purchaser. An ICT process is executed by ICT stakeholders and/or business partners across the ICT supply chain hierarchical layers or within a layer.

ICT processes of the ICT SCS integrate business logic (e.g., data and information flows) and generate dynamic management flows involving products, information, cash, knowledge, and/or ideas. Moreover, the business logic of an ICT process may contain any legal/regulatory restrictions and supporting documentation. In ICT supply chain environments, the actors have to deal with several business processes in their regular operations. During an ICT process operation, several business partners may be involved (e.g., suppliers, manufacturers, distributors, retailers, logistics providers, service providers, and customers) [15]. An ICT process can be implemented either by ICT stakeholders or by ICT elements of the supply chain (e.g. ICT infrastructure and facilities, systems and assets). ICT assets play a crucial role in ICT processes, as they are the resources necessary to support the execution of those processes and contribute to the provision of the ICT SCS. Furthermore, inside the ICT SCS, assets are interconnected and may support several business processes.

ICT processes may rely on organisational objectives and they can reflect B2B or multiple relationships within the ICT SCS. The ICT supply chain management encompasses all the supply chain processes operating for its performance. The supply chain processes are

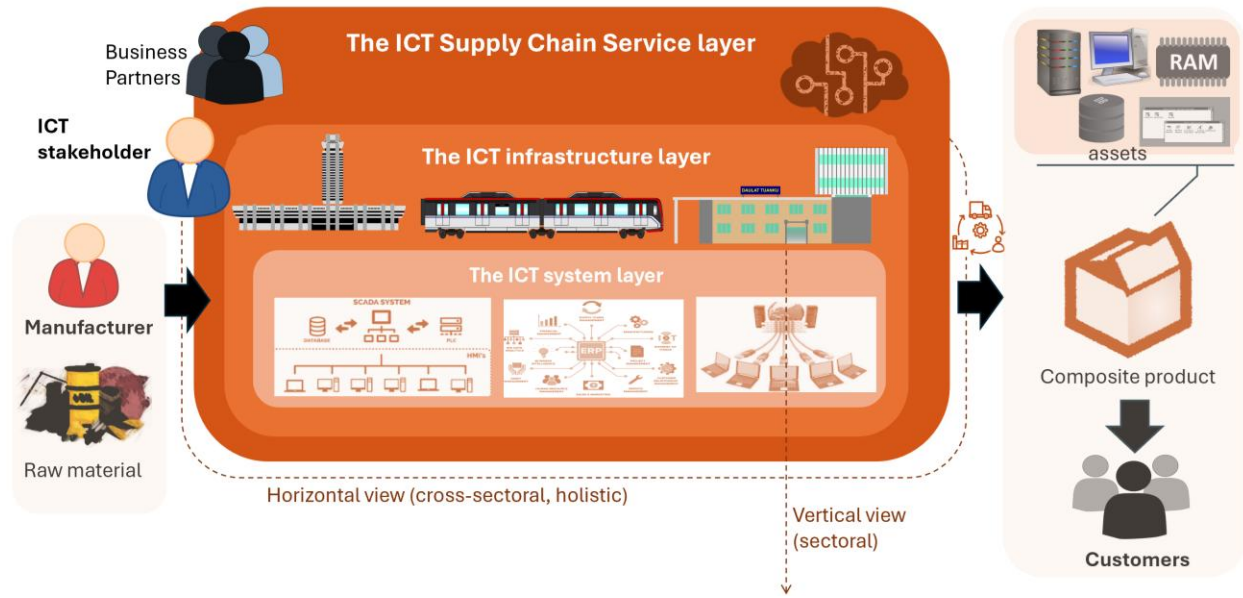
executed either manually by a human being or automatically or semi-automatically through system functions of CII or with the combination of both. Handling them manually is often a difficult, time-consuming and costly, which can easily undermine their execution making and distract business entities from their goals [92]. As mentioned in Section 3.2.1, a successful Supply Chain Management strategy must focus on the identification and support of key supply chain processes which aims to ensure the continuity of the ICT SCS performance continuity. The key-process identification aims to support the impact analysis in a risk assessment process, to estimate the effect of a potential disruption (i.e. a security event) of the ICT SCS (cf. Section 4.5 **Error! Reference source not found.**). In modern multi-scale business environments, the identification and analysis of the critical processes within the ICT SCS, can be accomplished through business cartography and process mapping.

ICT processes can be highly structured, analysed, simulated and evaluated by business analysts to support complex business problems and balance business risks [93]. In this context, business process modelling techniques, knowledge management and ontology-based approaches, can be adopted, as described in Section 3.4. *Modelling ICT processes is a good practice for describing particular aspects of the ICT SCS and defining hierarchies between supply chain management activities.* It exploits software engineering and modelling specifications to visualise and optimise the ICT processes and improve the effectiveness of its performance. In this respect, business analysts and ICT supply chain experts can explore business goals and reconsider the managerial objectives. The ICT supply chain modelling is important for ICT supply chains to enhance integration and increase interoperability [94].

- **ICT supply chain dependencies.**

The hierarchical layers of the ICT supply chain engage multiple ICT interdependencies. These interdependencies can be analysed across different dimensions:

- **Horizontal dependencies.** It includes all cross-cutting dependencies existing between the different hierarchical ICT supply chain layers for the provision of the ICT SCS. An ICT SCS may reflect the interplay of a set of industries. For instance, the Vehicle Transport service engages ICT stakeholders and infrastructures from a variety of industries, including the Automobile, maritime transport, and logistics industries. The inherent dependencies across diverse industries for implementing ICT processes that support the provision of ICT SCS, encompassing the ICT stakeholders involved, the relevant parts of their infrastructures, systems, and assets, are considered in the ICT SCS analysis (holistic-technical aspect).
- **Vertical dependencies.** The vertical dependencies analysis of the ICT SCS relies on a sector-specific view that considers only the inherent interrelations between the ICT processes, infrastructures, systems and assets within a specific industry. This type of ICT SCS analysis is a snapshot of the holistic-technical ICT SCS analysis. It delves into a deeper examination of the interactions occurring between individual ICT stakeholders and relevant business partners for the provision of the ICS SCS (sectoral aspect).



The proposed risk assessment methodology for ICT SCS, presented in Chapter 6 adopts the current ICT SCS model considering different types of risk analysis, i.e., horizontal or vertical, based on the above rationale.

### 3.3 Critical Information Infrastructures and services within the EU

The current section describes the concept of criticality in the EU Information Infrastructures (cf. Section 3.3.1) and presents a use case example of a supply chain (cf. Section 3.3.2).

### 3.3.1 Definition of criticality on infrastructures and services

The NIS 2 Directive [12] categorises entities into essential and important. The entities' criticality depends on their importance at the national or regional level for the sector in which they reside or other interdependent sectors within the EU, the type of service they provide, and their size.

The NIS 2 Directive [12] identifies the criticality of services, considering the impact they can cause on critical societal or economic activities from their operations. Any disruption to those activities —whether intentionally or unintentionally — may affect the performance and resilience of the entire ICT supply chain. For example, a SCADA monitoring service crash in a Port while the vehicles' unloading process is taking place on a vessel can have a devastating impact on the port terminal, such as damaging the infrastructure and the vehicles, or even injuring the personnel. In this regard, the disruption of the SCADA monitoring service may cause serious delays in delivering the vehicles to the purchaser, degrading the performance of the Vehicle Transport Service.

Infrastructures are considered critical depending on i) whether they are owned by operators of essential or important services (as applied to Annex I, II of the NIS 2 Directive [12]), and ii)



whether an incident on those infrastructures could have major disruptive effects (e.g., transboundary cross-sectoral impact), which is due to the inherent interdependencies of the interconnected infrastructures. Moreover, the NIS 2 Directive characterises “Critical Information Infrastructures” (CIIs) as those on which “the smooth functioning of the internal market depends”. Entities falling within the scope of the NIS 2 Directive shall comply with cybersecurity risk management measures and reporting obligations [12].

CII operators and network operators are key players in ICT SCS's performance and maintenance of security and reliability. In this respect, efficient risk management and incident response strategies on CIIs, estimation of the cascading effect throughout the entire ICT supply chain, collaboration of the ICT supply chain key-players and security awareness initiatives are required for establishing a comprehensive and consistent cybersecurity framework within the EU that safeguards the information exchange.

### **3.3.2 The Maritime and Logistics Supply Chain**

This section presents a use of an ICT supply chain, including CIIs and services, according to the NIS 2 Directive [12]. Main infrastructures, systems, technologies and architectures of the Maritime and Logistics Supply Chain (MLoSC) are presented as a result of the works of [84],[95]-[97] publications conducted for the current doctoral research. This supply chain inspired the real-life scenarios created to demonstrate and test the applicability of the proposed supply chain risk management methodology (cf. Section 6.4).

#### **3.3.2.1 Maritime and Logistics ecosystem**

Maritime Transport is a complex activity, including all the structures, modes and equipment required for the carriage of passengers or goods via sea, also known as the (seaborne), namely passengers and cargo shipping, accomplished through vessel transfer operation. Maritime transport is seen as the driving force of international trade and the backbone of globalisation [84]. According to the NIS 2 Directive [12], Water Transport includes all entities related to “inland, sea and coastal passenger and freight water transport”.

Over the past two decades, Maritime Transport has soared. According to the United Nations Conference on Trade and Development (UNCTAD)<sup>8</sup> annual report [21], in 2025, it surpassed the \$35 trillion. According to UNCTAD statistics [98] and the International Maritime Organisation (IMO), approximately 80%-90% of the volume of international trade in goods is carried through Maritime Transport. The percentage becomes higher for most developing countries. The high amount of EU imports and exports by sea in recent years [99] indicates that maritime transport is the main transportation mode of the EU. Maritime Transport dominates international trade, considered a critical industry sector for the EU [99]-[101].

The rapid growth of ICT and its consolidation in the global maritime industry have evolved and restructured the modes of maritime transportation, such as container transport, into collaborating

---

<sup>8</sup> UN General Assembly on Trade and Development.

supply chains [20]. The advent of “containerisation intermodalism” is a consequence of the multimodal and physical integration of heterogeneous transport modes and the emerging demand for value-added logistics services [20]. This has gradually increased the convergence of maritime and logistics, promoting organisational integration as a bearing requirement [20].

In recent years, a growing number of maritime companies have enhanced their business strategies with maritime logistics processes to improve their financial and operational performance. This has generated a primary need for an academic research study. Domain experts focus their research on the coupling of maritime logistics, maritime transportation, and port supply chain management concepts [20],[94]. The literature reviews the maritime transport industry's shift to supply chain and logistics integration. *The Maritime and Logistics Supply Chain (MLoSC) includes multiple and composite interdependencies of different types and nature, such as physical, cyber, informational, among actors and CII that support operations of the combined maritime transport and logistics industry* [84],[95]. An example of this complex combination is displayed in Figure 4 illustrating a bundle of CII interoperating during the MLoSC performance.

ENISA's report related to Port Cyber Risk Management [102] classifies infrastructures and services into three main categories of activities: i) cargo-related, ii) passengers and vehicle transport-related, and iii) fishing-related. Furthermore, it identifies seven critical services for the Maritime Transport and Logistics Industry, as presented in Table 2.

According to the NIS 2 Directive [12], operators of inland, sea and coastal passenger and freight water transport companies are considered essential operators, delivering services of high criticality, including works and equipment contained within ports, embedding operators of Vessel Traffic Services. The cornerstone of the maritime transport and logistics industry is port communities, encompassing a number of stakeholders to carry on land-sea connection. Table 2 provides an overview of the key players and critical elements of the Maritime and Logistics Supply Chain (MLoSC).

EU ports are considered one of the main CII in Europe [12]. Port facilities are a location where the ship/port interface, encompassing areas such as anchorages, awaiting berths and approaches from seaward. MLoSC services are implemented by CII. ENISA in “Port Cybersecurity Risk Management” report [102], identifies a few categories of CII systems, depicted in Table 2.

Industrial Control Systems (ICS) are a representative example of OT systems of the MLoSC, designed to collect and store data to delineate and control industrial processes. ICS systems are mainly distinguished into Distributed Control Systems (DCS) and Supervisory Control and Data Acquisition (SCADA) systems. SCADA systems monitor and control dispersed assets of industrial plants via centralised data acquisition and supervisory control techniques ([84],[95]-[96]). SCADA infrastructures are utilised in several industrial sectors (e.g., oil refineries, Liquefied Natural Gas - LNG-, power plants, manufacturing and transportation), playing a vital role in the

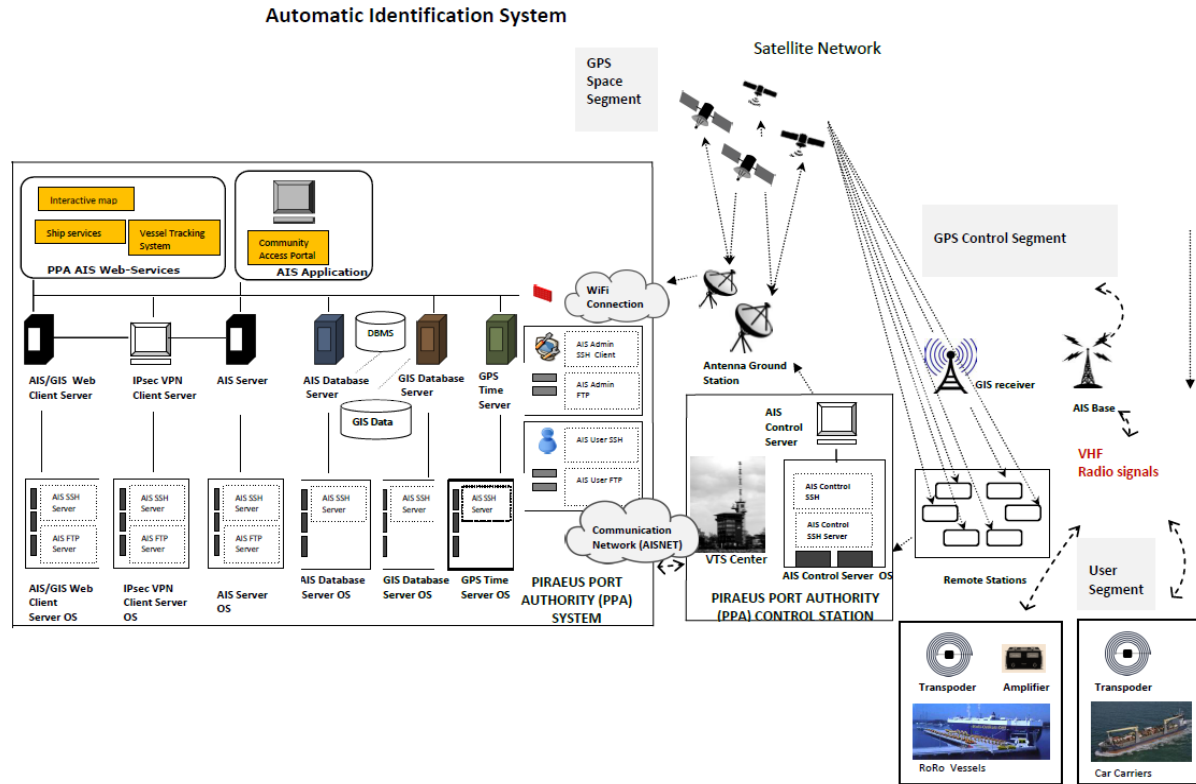


Figure 4. Satellite (SAT) communications and Automatic Identification Systems (AIS) interacting within the Maritime and Logistics Supply Chain for the transport of vehicles.

Maritime and Logistics Supply Chain. Most physical processes within a MLoSC service (e.g. vehicles and cargo loading/unloading, LNG distribution and storage) are executed with autonomous or semi-autonomous mechanical physical systems and machineries (e.g. ships, trucks, cranes, electronic gates/fences) under the control of sophisticated SCADA systems, including Master Terminal Units (MTUs), Human Machine Interfaces (HMIs), historic data storage, etc) [96].

The Port Community System (PCS) is an electronic platform which connects the multiple systems operated by a variety of organisations, involved in the port's supply chain. In addition, the Terminal Operating System (TOS), the Vessel Traffic Management System (VTMS) and the Ship Information System (SIS) are critical ICT systems within the MLoSC. ICT systems within Maritime Logistics and Supply Chains (MLoSCs) facilitate transparent interactions among maritime operators through shared networks enabling stakeholder collaboration across extensively interconnected nodes using IoT solutions and cloud computing services [97].

Network and Communication components include VHF and RFID communications, switches, routers and hubs, and the Electronic Data Interchange (EDI) protocol. Information and data assets are navigation data, such as the Automatic Identification System (AIS) and operational data related to logistics and shipping services. CCTVs, X-rays, face recognition and authentication systems and loudspeakers are indicative examples of Safety and security systems [97]. Those

systems are managed by a group of users, e.g., port personnel, IT specialists, and external users. Table 2 summarises the main actors and elements of the MLoSC.

Table 2. Maritime and Logistics Supply Chain critical actors and elements.

| Maritime and Logistics Supply Chain                                                                                      |                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NIS 2 Directive [12]                                                                                                     |                                                                                                                                                       | ENISA Report [102]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Examples                                                                                                                                                                                                                                                                                                                                      |
| Operators of Essential Services                                                                                          | Critical Information Infrastructures<br>(systems, and environment)                                                                                    | Critical ICT services                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Critical ICT systems                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | ICT Stakeholders<br>(Key players)                                                                                                                                                                                                                                                                                                             |
| <ul style="list-style-type: none"> <li>• Inland, sea and coastal passenger</li> <li>• Freight water transport</li> </ul> | <ul style="list-style-type: none"> <li>• Ports</li> <li>• Operators of Vessel Traffic Service (VTS)</li> </ul> <p>(including works and equipment)</p> | <ul style="list-style-type: none"> <li>• Ship berthing services (e.g., towing, mooring, crew services, berth allocation services)</li> <li>• Vessel loading/unloading services (stevedoring) (e.g., forklifts and gantry crane operations)</li> <li>• Temporary storage and staying services (e.g., baggage handling, food and shopping facilities)</li> <li>• Distribution and transfer services (e.g. luggage control, cargo scanning)</li> <li>• Supporting services (e.g., management of dangerous goods)</li> <li>• Security and safety services (e.g., CCTV surveillance, emergency population warning, port lighting)</li> <li>• Authorities Services (e.g., sea rescue, navigation services, vessel traffic control)</li> </ul> | <ul style="list-style-type: none"> <li>• Management System (VTS system)</li> <li>• Port Community System (PCS)</li> <li>• Port Management Information Systems (PMIS)</li> <li>• Maritime traffic control systems</li> <li>• Security and safety systems</li> <li>• Terminal Operating Systems (TOS)</li> <li>• IT/OT systems (e.g., Industrial Control Systems -ICS &lt; SCADA or Distributed Control Systems -DCS)</li> <li>• Networking systems</li> <li>• Vessel Traffic</li> <li>• Enterprise Resource Planning (ERP)</li> <li>• corporate systems (emails)</li> </ul> | <ul style="list-style-type: none"> <li>• Port Authorities</li> <li>• Port Terminal operators</li> <li>• Service providers</li> <li>• Other involved entities (e.g., local agent, ship owner, ship agent, carrier agent, marine underwriter, ship-broker and other authorised bodies, such as Customs, port police and coast guard)</li> </ul> |

EU regulations and ENISA are the legal instruments of MLoSC regarding cybersecurity topics. In addition, sectoral governmental agencies, shipping LEAs, and prominent standardisation bodies are enlisted in the following [103]:

- International Maritime Organisation (IMO), which sets international obligations within the MLoSC

- European Maritime Safety Agency (EMSA), which aims at eliminating the risk of maritime accidents, ship emissions and the loss of human lives at sea
- Baltic and International Maritime Council (BIMCO), which concerns global membership, affairs, and business practices
- UN Conference on Trade and Development (UNCTAD), which coordinates trade-related, investment and development issues.
- The International Convention for the Safety of Life at Sea (SOLAS) is a global maritime treaty in developing safety standards for the construction, equipment and operation of merchant ships.

Port infrastructures have expanded their communication channels throughout the years [98]. They aim to improve their efficiency and reduce their costs. The value of maritime logistics systems is directly related to the customers' satisfaction and influences the performance of the logistics supply chain [84]. According to this purpose, *the desired goal is to explore ways to develop cost-efficient, agile transport networks, to improve sea and inland communication nodes, to facilitate maritime stakeholder flows and to upgrade the quality of Port supply chain services by managing risks* [20].

#### 3.3.2.2 Supply chain phases and ICT processes of Maritime and Logistics

The Maritime and Logistics Supply Chain (MLoSC) involves complex interactions among numerous stakeholders with diverse objectives and requirements. It encompasses both physical operations, such as docking, loading, unloading, storage, transportation, and inspection, and cyber operations, including customs clearance, pre-arrival notifications, and ISPS documentation management. MLoSC processes rely on interconnected physical and cyber assets, integrating domestic and international transportation, warehouse management, inventory control, and information technologies.

Due to the heterogeneity and interdependence of maritime and logistics networks, identifying key business processes within the MLoSC is challenging and varies depending on the operational perspective. Previous studies [20],[104]-[105] established the collaborative supply chain management framework for port logistics chains through various concepts, such as demand, vehicle, order management integration, port terminal operations, shipping management, Dry bulk and tanker logistics, quality assurance and environmental performance. Later studies [106]-[108] evolved maritime logistics supply chain concepts toward resilient, AI-enabled, and optimisation-based approaches.

Considering the main actors, critical services, infrastructures and the systems identified for the MLoSC in Section 3.3.2.1, the MLoSC service can be divided into four main phases [84],[95]:

- i) Purchase Phase. It involves procurement and contractual processes between the importer and the manufacturer, such as Order Dispatch, and Contract Agreement for the purchase
- ii) Shipment Phase. It encompasses processes for maritime transportation and shipping arrangements, such as Shipment Contract Preparation & Negotiation, Manifest/Bill of

Landing Issuance/Registration, Ship Formalities Arrangements, Loading processes, and Shipping Arrangements

- iii) Pre-Arrival Phase. It aggregates all processes for port preparation and customs interactions. The Local Agent assigned for the Importer manages various activities for the vessel docking, ranging from vessel unloading and Port terminal arrangements to Customs formalities. Indicative processes include Port's Services Requested, Insurance Contract Preparation and Negotiation Process, Claims Handling Port Services and Delivery Phase. This phase relies on processes for docking, unloading, and final transportation activities. As the vessel approaches the port destination, it deals with all services and formalities requested by the Local Agent, encompassing processes such as Vessel Unloading and Final Transportation Procedures.
- iv) Port Services and Delivery Phase. This phase relies on processes for docking, unloading, and final transportation activities. As the vessel approaches to the port destination, it deals with all services and formalities requested by the Local Agent, encompassing processes, such as Vessel Unloading and Final Transportation Procedures.

Since critical services encompass multiple interrelated processes, effective analysis requires identifying the most prominent processes affecting service continuity and supply chain integrity [102]. The focus shall be on the critical ICT services processes, conducting targeted business impact analyses, following specific maritime logistics objectives [103]. In this respect, process modelling techniques and semantics can facilitate the identification of the supply chain key elements, as presented in Section 3.4.

### **3.4 Knowledge management, semantics and ontologies in the ICT ecosystem**

The current section includes content from publications [92]-[93],[109]-[110] developed for this doctoral research. It presents the concepts of business process management, business process modelling, knowledge management, semantics, ontologies, challenges and their use (see sections 3.4.1-3.4.2). The content of this section facilitated the dissertation research to identify the knowledge management frameworks utilised in the CyberICT Risk Management Methodology (see Section 3.4.2.1).

#### **3.4.1 Business process management**

In this section topics of business process management and business processes modelling are discussed. Business process models are used in this dissertation as an auxiliary structuring tool to represent and visualise complex ICT processes of ICT supply chain services.

##### **3.4.1.1 The importance of business process modelling in the ICT ecosystem**

Business Process Management (BPM) is the set of activities dealing with organising, automating, monitoring and controlling business processes in organisations [93]. The primary goals of modelling business processes are distinguished into five main categories:

- sense-making
- computer-assisted analysis
- quality management
- model integration in an information system
- apply the model as a framework for a system development project.

Process mapping is assumed the identification, description and illustration of all the flows of a work via flowcharts, process models and business diagrams. The process mapping is implemented through business process modelling techniques.

Business process models are formal representations of business processes [93]. Moreover, they can be stored and accessed, enabling sharing of enterprise know-how, providing the reuse of the modelled business processes.

A good practice to model processes of the ICT supply chain is to follow the business process management lifecycle:

- i) Design the strategy of the supply chain against its performance.
- ii) Analyse and model supply chain processes using Key Performance Indicators (KPIs). Key supply chain processes are identified and associated with KPIs to provide a structured and balanced representation of supply chain information, including services, costs, collaborating entities, resources, and assets.
- iii) Make the supply chain processes executable by developing them in a BPM software application.
- iv) Further analyse and monitor the processes using querying modelling and information retrieval techniques.
- v) Evaluate and optimise the supply chain processes using simulation methods to simulate real-life use cases. This “process view” of the supply chain services can leverage the performance of the supply chain.

MacCarthy and Ivanof in [111] analyses how digitalisation affects every stage (plan, source, make, deliver) and how businesses gain an edge through visibility and resilience. Grefen and Vanderfeesten in [112] provide a multidisciplinary comprehensive overview of modern BPM research which demonstrates that process-oriented approaches can improve organisational efficiency, adaptability, and digital innovation.

The alignment of supply chain processes and technologies with organisational structures, sector-specific dependencies, and performance metrics enhances supply chain transparency. The adoption of theories such as the Unified Service Theory (UST) enables the measurement and modelling of supply chain process capabilities [113].

#### 3.4.1.2 Business process modelling

Business process modelling is hitherto directly expressed with process modelling languages [93], such as UML Activity Diagrams, Business Process Modelling Notation (BPMN) [114], Event-

driven Process Chains (EPCs), RosettaNet, Activity Decision Flow Diagram (ADF), the family modelling language of Integration Definition (IDEF), the Electronic Business using the Extensible Markup Language Business Process Specification Schema (ebXML BPSS). Business process modelling notations intend to increase the abstraction level in software deployment and enhance the processes with semantic information [93].

Nonetheless, business process modelling faces challenges related to information complexity, inconsistent semantics, and heterogeneous terminology, which can hinder information exchange and limit machine interpretability. As information on business process models is getting deeper and more complex, business process management toolkits are required to support efficient information retrieval [92]-[93].

The dynamic and complex nature of digital information necessitates accurate and holistic information retrieval. A key challenge in business process management is translating high-level business requirements into machine-interpretable representations for analysis and execution. The complexity of business process information poses challenges to existing languages *fostering a growing gap between the business world (administrative view) and that of information management and retrieval (IT's view)* [93].

Another challenge in business process information management is the “*change of medium*” [115]: When a radical change to the structure of a business process is performed or its primary information is enriched or updated, applications hinder to correspond and restructure the model due to the insufficient level of automation in the process execution. Moreover, another crucial point is that developing graphical models under formal specifications lacks simplicity. Therefore, it can mostly be done by business analysts as expert knowledge is required and training business users would take a considerable time, generating a much more noticeable cost to an enterprise. Business analysts primarily focus on the application-domain when depicting business processes rather than concerning the business-domain. The fact that they cannot be aware of all the particular aspects of a business process causes a deficiency in business process representation. What is more, the complexity of different terminologies adopted by business entities in process modelling leads to semantically inconsistent interpretations lacking of interoperability in the information exchange between organisations [93].

Semantic technologies could be capable of bridging this gap. Defining the appropriate semantics in business process models will make them a machine-processible computational model that could facilitate supply chain operators to better comprehend their supply chain processes.

Nonetheless, BPMN models in this dissertation are employed as a process-oriented modeling mechanism to represent and visualise the ICT processes in the ICT supply chain, the interdependencies of actors, and operational workflows, enabling structured cybersecurity and risk analysis across digital supply chain environments.



### 3.4.2 Knowledge management and semantics

This section analyses Knowledge Management frameworks and tools, presents concepts of Semantic Business Process Management and explores Knowledge Management aspects in ICT supply chains.

#### 3.4.2.1 Knowledge Management concepts, related standards and tools

Knowledge representation and semantics are directly connected with conceptualisation and ontologies [116]. In terms of Philosophy and Artificial Intelligence theories, ontology is a systematic account of existence where everything that exists can be represented [104]. In computer science, conceptual models aim to explicitly describe the concepts and relational schemas of a domain during the development and implementation phase of an engineering process [92]-[93].

The Nonaka SECI Model [117], a foundational Knowledge Management framework, underlines the importance of knowledge creation, which is achieved via four modes of knowledge conversion:

- *Socialisation (tacit-to-tacit conversion)* is the process of tacit knowledge transfer among individuals exchanging experiences, ideas through meetings, observe others, sharing mental models.
- *Externalisation (tacit-to-explicit conversion)* is the procedure of articulating and organising tacit knowledge.
- *Combination (explicit-to-explicit conversion)* occurs when combining codified information to create new knowledge.
- *Internalisation (explicit-to-tacit conversion)* is the procedure of internalising explicit information in order to analyse and better understand it. Conversion modes are assumed proxy measures for “a spiral” knowledge generation.

The ISO 30401:2018 on Knowledge Management Systems — Requirements [118] is the definitive global standard for modern Knowledge Management. It shifted the field away from treating Knowledge Management as a simple IT database, framing it instead as a core corporate governance requirement focusing on culture, continuous learning, and knowledge flows. The APQC's industry-based standard Knowledge Management Strategic Framework, outlines the stages of Knowledge Management strategy to measure how effectively an enterprise captures, maps, and retains institutional knowledge [119]. In contemporary, Knowledge Management literature frameworks focus heavily on how unstructured data transforms into automated insights. The technical models include [120]-[121]:

- Enterprise Knowledge Graphs (EKG). The foundational data architecture model for modern Knowledge Management. Instead of traditional document folders, EKGs model organisational knowledge as a network of interconnected entities, semantic meanings, and logic-based relationships.
- Cognitive/ AI-Powered KM Architecture (RAG Model): The current reference architecture in literature uses a Retrieval-Augmented Generation (RAG) framework. This model maps

how an organisation utilises large language models to securely query private enterprise databases, bridging the gap between raw data storage and instant, natural-language expert insight.

- Agentic Knowledge Management Frameworks focus on transitioning from passive document searches to active, autonomous AI agents. These models map workflows where agents dynamically read company resources, identify process bottlenecks, and execute corporate tasks independently.

N. Fteimi and K. Hopf (2021) [122] propose an integrative framework for knowledge management in the era of artificial intelligence, focusing on how AI can enhance and support knowledge management processes within organisations.

The article in [123] highlights how AI enhances knowledge management by improving knowledge capture, retrieval, synthesis, and personalization, while emphasizing that effective governance and high-quality knowledge are essential for trustworthy AI-enabled knowledge management.

The paper in [124] proposes a Cyber Spiral Model that integrates knowledge management concepts with the NIST Cybersecurity Framework to enhance cybersecurity knowledge creation and sharing, and discusses the potential role of AI and machine learning.

Standardised risk assessment models (e.g., NIST SP 800-30 [125] or ISO 27005 [56]) mostly focus on explicit knowledge assets. Nevertheless, there are cases where most critical security knowledge exists implicitly in security practitioners without being communicated. For instance, APTs often exploit vulnerabilities that are not yet documented in CVE databases or formal repositories. Security teams in organisations frequently maintain internal records, insights, or heuristics regarding these high-risk vulnerabilities based on prior incidents, penetration testing, or threat intelligence. In such cases, tacit knowledge is difficult to transfer, externalise, explore and conceptualise and identify interrelations. Cybersecurity risk assessment is fundamentally bottlenecked by human intuition, 'gut feelings,' and unwritten expert experiences (tacit knowledge). Existing technical risk models assume data is already perfectly codified (explicit).

While contemporary state-of-the-art literature focuses on highly digitised frameworks like the WISED model (2024) [126] or cognitive-automation extensions [120]-[121]), this research intentionally selects the Nonaka-Takeuchi SECI model for its localised conceptual phase. As supported by modern bibliometric trends [126], the SECI framework is experiencing a significant academic resurgence due to its unique capability to model knowledge conversion axes. Furthermore, because recent studies validate SECI's effectiveness in structured, highly secure, and complex organizational settings [122] and as an enabler for systematic data absorption [127] it serves as the most rigorous epistemological foundation to model the transition of abstract human risk intuition into explicit, machine-readable configurations.

Thus, SECI model [117] was selected strictly as a conceptual lens to methodically extract the unwritten security intuition and translate it into reproducible, structured risk metrics (externalisation) in the CyberICT Risk Management Methodology. It is used as a theoretical basis

for the development of the knowledge representations in the CyberICT Risk Ontology (see Section 6.2.3), which retrieves, analyses and communicates the security-related knowledge.

Conceptual modelling is characterised by three main principles; Modelling language constructs, Application domain gathering and Engineering [128]. The conceptual model of the subject domain can be exploited along with ontology (ontological model) and analysed in detail, enhancing the semantic representation of the subject domain [116]. The difference between ontology and conceptual models is that conceptual models give a more generic, abstract representation while ontology models use specific languages and vocabularies [116]. A considerable advantage of an ontology development in software engineering is its high-level structure, including all possible variations of a concept able to mediate and balance variables between different systems and embrace interoperability [110]. High level data models are also known as semantic models.

In Knowledge Management systems, ontologies are often used to structure a domain of knowledge via formal statements which are interpreted by machines and stored in a knowledge base [110]. As a result, data can be retrieved and extracted from the knowledge base by using automated inference mechanisms and reasoning tools. Semantic technologies utilise knowledge-based approaches and reasoning techniques to represent ontologies and translate it into a machine-processible computational model [110]. The Semantic Web was invented by the innovator of the World Wide Web T.B. Lee and supported by the World Wide Web Consortium (W3C) initiative. According to T.B. Lee, “Semantic Web is not a separate Web but an extension of the current one, in which information is given well-defined meaning, better enabling computers and people to work in cooperation” [110]. The word semantics comes from the ancient Greek word *sēmainō* and its literary *sēmantikós* which means study the meaning, importance, used to define the concept of logical expressions. The Semantic Web is directly linked with the Artificial Intelligence research area, based on knowledge representation rules and assertions. Semantic information that is published on the Web is described by the term of Linked Open Data. Linked Open Data are published data on the Web connecting to each other through concrete statements recommending a Web of Data [110]. These statements follow the Resource Description Framework standard (RDF) [129], which is a W3C specification.

The RDF Semantic Web standard [129], defines classes, subclasses and their properties (slots) aims at knowledge representation following the logical structure of the RDF language, which is based on the idea of making assertions in the form of the subject-predicate-object expression known as ‘triples’. The RDF model consists of resources, properties and statements. Resources are all the things being described by RDF expressions while properties indicate the resources relations. A triple subject-predicate-object expression recommends an RDF statement. A subject is always a resource, predicates are always properties and objects are property values which can either be resources or literals.

The Web Ontology Language (OWL 2) [130] is a semantic standard of W3C of Web ontology language which formally defined semantics. It enables the representation of knowledge through classes, properties, individuals, and data values, and is typically expressed and exchanged as RDF-based documents that can be used alongside other RDF data.

SPARQL Semantic Web standard of W3C [131] is the predominant SPARQL Protocol and RDF Query Language (SPARQL) which derives information from the triple statement pattern of RDF. SPARQL defines the remote protocol for issuing SPARQL queries and receiving the results.

Tools have been developed to address Knowledge Management principles, such as the Protégé [132], knowledge-based Management tool of Stanford University. Protégé is based on a common vocabulary that supports knowledge representation by developing and managing ontologies. Protégé can provide an information retrieval process through simple and complex semantic querying methods using SPARQL [131]. It represents SPARQL query results in XML format documentation. Moreover, Protégé can verify the correctness of structured semantic relationships through the implementation of reasoning mechanisms and inference rules (i.e., using reasoners).

Hermit [133] was the first publishly available OWL ontology Description Logic (DL) reasoner. It performs ontology consistency checking, class classification, and inference of implicit relationships. Based on the hypertableau calculus, it provides efficient reasoning capabilities, enabling rapid classification and analysis of complex ontologies.

FaCT++ [134] is a C++-based tableaux OWL DL reasoner supporting OWL and OWL 2 ontologies. It can operate as a standalone DIG (DL) reasoner or as a back-end for OWL API applications and is one of the default reasoners used in Protégé [132] Semantic Web platform.

Pellet [135] is an open-source Java-based OWL 2 reasoner that supports OWL 2 profiles (including Existential Language) and can be used with the Jena or OWL API libraries. It provides optimisations for nominals, conjunctive query answering, and incremental reasoning, and can be integrated into custom applications. The reasoner Pellet supports OWL 2 DL reasoning along with rule-based inference, explanation services, and incremental reasoning, enabling transparent and interpretable risk analysis.

Unlike HermiT, Pellet facilitates semantic querying and explanation of inferred relationships. Unlike FaCT++, Pellet integrates smoothly with Java-based tools, such as OWL API and Jena. These features make it well-suited for extracting actionable cybersecurity intelligence from complex ontologies (see Section 5.3.4 and 6.2.3).

The research work in Kalogeraki et al (2016) [109] presents an example of the application of the above Semantic Web technologies to employ learning object metadata. Expressing semantics in Learning material can heal interoperability issues and improve information retrieval by providing knowledge representation inherent in xml syntax and applying inference rules. Detecting semantic relations on educational material aims to assess in an abstract level its tutoring content to improve the learning procedure.

#### 3.4.2.2 Semantic Business Process Management

The rapid evolution of technology in Management Information Systems has enabled easy access to a huge amount of complex and specialized business information. The vast amount of business information has created the need for investigating ways to improve the efficiency and effectiveness on business environments and information retrieval techniques. Knowledge Management and Business Process Management can create synergies. Many researchers consider

the combination of semantic technologies with Management Information Systems as a promising approach to confront the aforementioned problems. The combination of Semantic Web technologies with Management Information Systems is a new and growing research area that studies the so-called Semantic Business Process Management (SBPM). The potential of a worldwide standardisation unifying these topics is no longer an unreachable expectation.

The main difference between database models and ontologies relies on the different perception an agent is considered to approach information. Ontologies are built under the Open World Assumption in which an agent or an observer is thought to have incomplete knowledge [110]. In Open World Assumption what has not been stated is assumed to be unknown whether is true or false. Database models follow the principles of the Close World Assumption where an agent is thought to have complete knowledge; therefore what has not been stated is set as false. For example, supposing adding a statement in each different system such as “citizen A is an owner of a sport car and can afford only one car”. If we then add the state “citizen A is an owner of a red car” the Close World Assumption system will set the second statement as a false statement because the red car is considered as an additional car for citizen A which is not allowed in this case. This is because database applications follow the Unique Name Assumption, where every single name is presented by a different entity. Unlikely, the Open World Assumption system would consider the statement of citizen A having a red car as true, making the logical inference that the sport car of citizen A is also red. Hence, Open World Assumption systems are able to infer information that is not explicitly stated in graphical representation using reasoning mechanisms. The OWL Semantic Web language [130] is a typical example of applying the principles of the Open World Assumption. Defining the appropriate semantics in business process models make them fully machine-readable [110].

Semantic Business Process Management is able to create an integrated solution between business’ and IT’s world and to augment the automation level in the Business Process Management lifecycle [110]. In this respect, it can be a solution to bridge the gap between Administrative view and IT’s view, mentioned in the previous section.

In general, the fusion of semantic web technologies and Management Information Systems can leverage the business environments for the following reasons [110]:

- Semantic representation uses structured conceptualisation to build ontologies from natural language. These formal models capture both explicit and implicit domain knowledge and support machine-readable implementations through inference and reasoning.
- Semantic web programming languages and specifications, such as OWL programming language, RDF standard and SPARQL language are open source fast and flexible software. OWL Language and RDF standard can be expressed in other formats, such as OWL/XML as well as RDF/XML which are both human and machine readable. Converting semantic models into XML formats enables extra-organisational data sharing and use. Hence, it simplifies the information exchange and increasing interoperability between organisations.



- Ontology models, instead of traditional business process models, have a semantic dynamic content, supporting run-time knowledge exploitation.
- Ontologies have a formal-structure character, missing from the conventional modelling representation.
- Semantic models are able to share and retrieve information on the Web.
- Adopting semantic techniques in business process models enables business entities to have an explicit presentation of the involving participants' relationships in a process and helps them improve their business performance.
- Semantic annotation enhances business models by enabling automated reasoning that improves query relevance and information retrieval, while also reducing the cost of adapting externally provided reference models.

The research works in [92]-[93] of the current dissertation aimed to combined business process modelling techniques with Semantic Web techniques by representing BPMN 2.0.2, the ISO 19510 [114] Business Process Modelling Notation into an ontology (see Figure 5 and Figure 6). The BPMN ontology was validated using the HermiT, FaCT++ and Pellet reasoners (see Section 8.1)

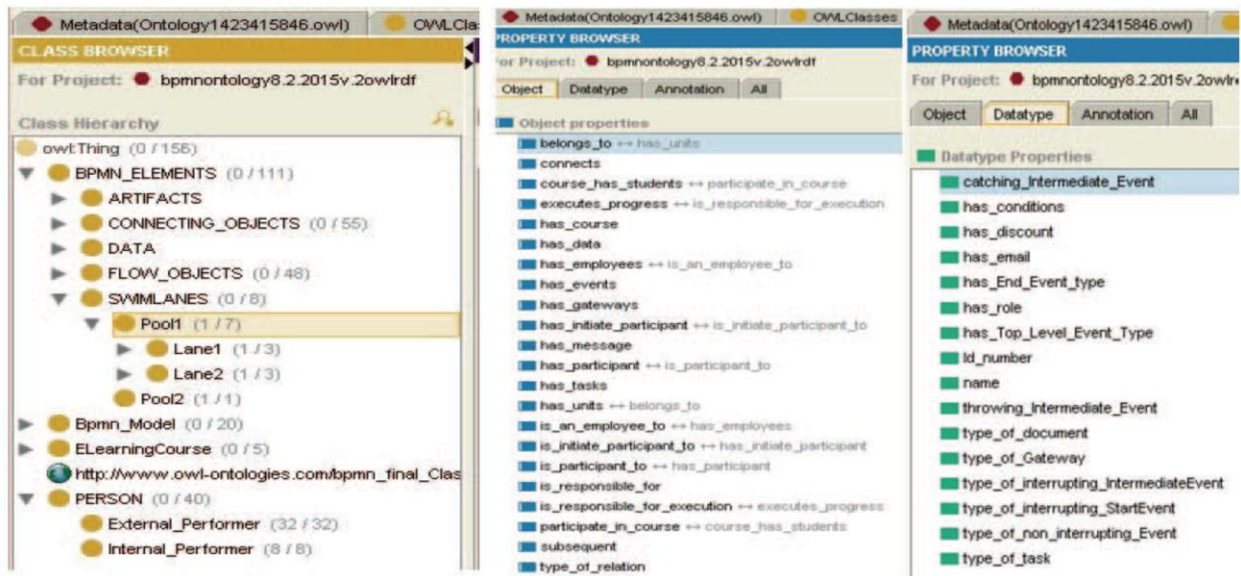


Figure 5. Class hierarchy and object and data properties of the BPMN semantic model [92].

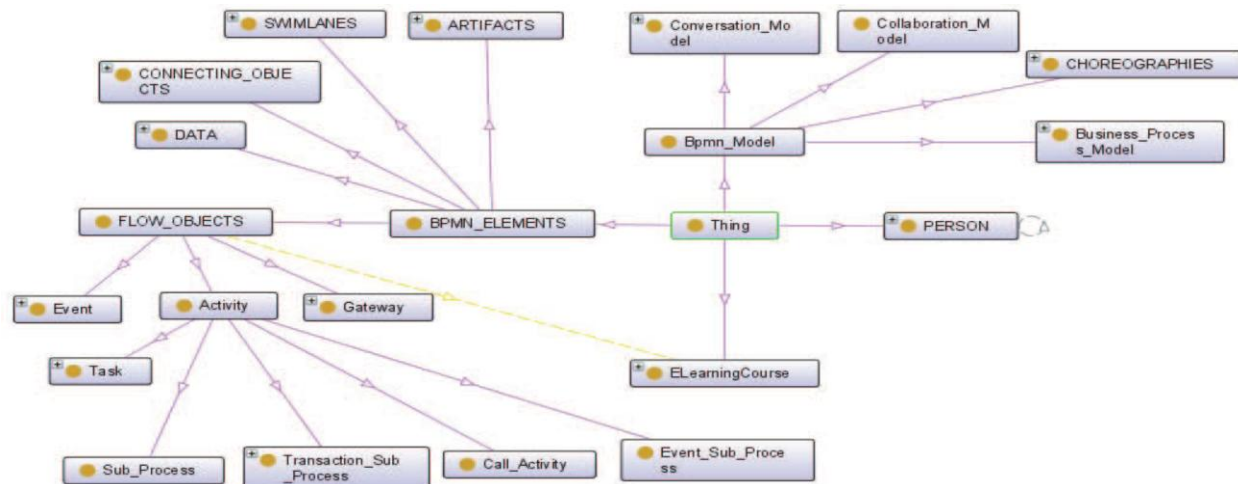


Figure 6. The BPMN semantic model.

### 3.4.2.3 Knowledge Management aspects in ICT supply chains

The ISO 30401:2018 [118] as “management that concerns knowledge utilising a systemic and holistic approach to advance results and learning.

Supply chains are a key application area for Knowledge Management due to their complexity and multi-actor coordination needs. Effective knowledge sharing among partners enhances agility, adaptability, and operational performance, while supporting knowledge creation and improved supply chain strategies. Knowledge Management in supply chains spans knowledge exploitation (sharing) and exploration (creation and learning), with existing research focusing on improving knowledge transfer and organisational learning through various frameworks, including the SECI model [117]. The literature reviews that several research work is concentrated on facilitating knowledge transfer and enhance the business knowledge of enterprises within the supply chain [110].

Knowledge Management can improve supply chain performance in areas such as decision support, risk management, and outsourcing [84],[136]. However, existing studies are largely empirical and rely on traditional data collection methods, lacking integrated approaches. Overall, the literature highlights *key deficiencies in supply chain management that reinforce the need for Knowledge Management-driven integration* [84]:

- the lack of flexibility of information adaptation across multinational synergies due to cross-cultural differences (e.g. different cultural variables and multiple terminologies gathered)
- the use of ICT systems and the supply chain performance have a positive relation
- sustaining issues, such as the problem of knowledge obsolescence due to supply chain complexity and heterogeneity
- the inherent gap between ICT investments and firms sustainable development

- independent Knowledge Management approaches are much more like domain-specific enterprise solutions, which lack of establishing a generic, integrated business strategy among supply chain operators
- there is limited empirical evidence on analysing Knowledge Management processes (adoption, storage, development) and their impact on supply chain performance. Most studies lack integrated methodological approaches and robust quantitative or simulation-based evaluation techniques.
- Consolidating technology and management practices is essential, with IT-based solutions supporting Knowledge Management through improved classification and calibration. Effective frameworks can enhance knowledge transfer, foster inter-organisational collaboration, and enable mutual learning among business partners.

### **3.5 Challenges and remarks for the ICT ecosystem**

Considering the overall analysis of Section 3 for the ICT ecosystem, the following challenges and remarks are concluded.

The ICT ecosystem incorporates a set of multifactors embedding heterogeneous supply chain networks with a set of elements (see the ICT supply chain model in Section 3.2.3.2) which deliver composite products that can be analysed into a set of primary elements, i.e., assets/building blocks (c.f. Section 3.2).

The literature reviews that existing approaches and practices for ICT supply chains are based on traditional security or procurement frameworks and they lack supply chain self-insight. In this respect, to keep the ICT supply chain integrity, methods that consider existing regulations for the ICT ecosystem, such as the NIS 2 Directive [12] and CSA [13] are required to limit this gap and analyse in depth the interdependencies and concepts across ICT complex networks, such as the ICT supply chain networks (c.f. Section 3.2.2 on ICT supply chain integrity).

Critical ICT supply chain services, specifically those that reside in ICT supply chains of combined ICT industries, such as the Maritime and Logistics Supply Chain (MLoSC), include multiple and multi-factor interdependencies of different types and nature, require business, horizontal and vertical analysis, depending of the objective of the evaluation (cf. Sections 3.2.3.2 and 3.3.2).

A sustainable supply chain is directly linked to maintaining the supply chain security and focuses on developing and utilising technologies that facilitate sector-specific collaboration to improve business, societal impact, and cyber resilience (c.f. Section 3.2.2 on ICT supply chain sustainability).

Supply chain service can be interrupted and degrade its performance continuity. An effective ICT supply chain security policy which focuses on enhancing organisations' corporate strategy and ensuring business continuity. Robust supply chains are built with continuous awareness and vigilance through the implementation of Business Continuity Planning (c.f. Section 3.2.2 on ICT supply chain continuity).



Critical Information Infrastructures (CIIs) are considered depending on their potential impact that can be caused to critical societal or economic activities from the intentional or unintentional disruption of their operations. To ensure the efficient performance and resilience of the global ICT supply chain, identifying criticalities on ICT products and ICT supply chain elements is required. In this respect, process modelling and semantic web techniques can facilitate the ICT analysis and identification of the criticality of the elements in the ICT ecosystem (cf. Section 3.3).

The fusion of Semantic Web technologies and Management Information Systems can leverage the complex ICT environments, facilitate the ICT analysis and limit the growing gap between the business world and the IT world. Most existing Knowledge Management approaches for ICT analysis are empirical in nature, using evidence-based techniques and traditional methods for collecting data, which lack of adopting a holistic view. The literature reviews popular deficiencies of supply chain management, which dictate the importance of applying Knowledge Management techniques to achieve supply chain integration (cf. Section 3.4).

A comprehensive and consistent European cybersecurity framework that enables and safeguards the information exchange is driven by efficient risk management, thorough estimation of the cascading effects throughout the entire ICT ecosystem, collaboration of the ICT supply chain key-players and security awareness initiatives (cf. Section 3.3). Considering the above, the following challenges are identified:

- There are limited approaches that analyse the technical complexity of ICT products and the high interdependencies between the ICT supply chain services to assess their security.
- To assess the security of ICT products and their ICT supply chain services, the ICT ecosystem needs to be analysed from diverse perspectives: business – oriented analysis, holistic technical (horizontal) analysis and sector-specific (vertical) analysis. This diverse, multi-factor security analysis can contribute to the maintenance of integrity, sustainability, and continuity of the global ICT supply chain.
- The use of process modelling and semantic web techniques can facilitate the security analysis of complex ICT environments. The application of Knowledge Management practices in complex ICT networks of supply chains, can leverage the security knowledge and information exchange.

## 4. Security concepts and approaches

This chapter analyses concepts of security from multiple perspectives. Section 4.1 provides major definitions of cybersecurity risk management. Section 4.2 presents the existing legal framework and best practices in cybersecurity. Section 4.3 provides state-of-the-art risk assessment approaches, whereas Section 4.4 defines risk metrics, prediction measurements and discusses existing approaches. Section 4.5 scrutinises domain specific topics on ICT supply chain security. Section 4.6 analyses topics on cybersecurity certification and conformity assessment. Eventually, Section 4.7 summarises the outcomes of this chapter and identifies challenges.

### 4.1 Security concepts definition, dimensions and interrelations

“Security” in an abstract definition (including physical and cybersecurity dimensions) is the protection of objectives against deliberate (intentional) negative effects. “Information security” or “cybersecurity” is defined by the widely recognised family of international standards on information security ISO/IEC 27k [54] as the preservation of Confidentiality, Integrity, and Availability (CIA triad) of information, and other properties, such as authenticity, accountability, non-repudiation, and reliability [53]. The aim of cybersecurity is to safeguard network and information systems, as well as the users of such systems, other individuals, society, organisations, and nations, from cyber threats and risks [13],[137].

When considering the entire ICT ecosystem, i.e., everyone, everything, and every process involved in building, handling, supporting, or delivering an ICT product or service before it is placed on the market, cybersecurity broadens its perimeter. It can be defined, according to ISO:28001: 2007 [70], as the *“resistance to intentional acts designed to cause harm or damage to or by the supply chain”*.

“Security management” encompasses all policies, processes, and measures necessary for an entity or a group of entities (e.g., a supply chain) to develop and implement to manage specified security objectives against potential risks, threats and their impact. [53],[138]. Moreover, security management handles possible intentional negative effects. The ISO/IEC 27001:2022 international standard [55] identifies an “Information Security Management System” (ISMS) as the systematic approach of interrelated or interacting elements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving the information security of organisations to achieve business objectives.

“Risk” is formally defined as *“the effect of uncertainty”* (i.e. deviation of the expected) *“on objectives”* of an entity, including the consequences of unwanted security events and changes in circumstances [53],[138]. A barrier to maintaining the security of assets belongs to an entity or a group of entities (e.g. organisations participating in a supply chain) is the likelihood of occurrence of cybersecurity (or cyber) risks. In addition, the Cyber Resilience Act (CRA) [11] and NIS 2 Directive [12] European regulations characterise the cybersecurity risk as *“the potential for loss or disruption caused by an incident”*. To estimate cyber risks, ICT stakeholders undertake cybersecurity risk assessments on their infrastructures. Risk assessment is a comprehensive

process of risk identification, risk analysis, and risk evaluation. Cybersecurity risk assessment aims to provide estimates of risks and their related concepts, namely, security vulnerabilities, cyber threats and impact. Interconnections between ICT products and services can increase the risk and potential to cause disruption of ICT systems or ICT infrastructure operations due to their great heterogeneity and complexity, making them more vulnerable [4].

“Security vulnerability” is defined as a weakness, susceptibility or flaw of an ICT product, ICT service or ICT asset exploited by one or more threats [11]–[12],[53]. Furthermore, it can be considered as a “*functional behaviour*” that “*violates an implicit or explicit security policy*”.

Vulnerabilities can be distinguished into confirmed (known) and potential (unknown). “Confirmed” (known) vulnerabilities [139] are those that have been officially reported as present, or for which functional reproduction (source code available) is possible. For instance, CVE-2021-40353 [140] is a publicly disclosed vulnerability by MITRE of SQL injection.

Unknown vulnerabilities [44],[139] are reports of impacts that indicate a vulnerability is present, but the cause of the vulnerability is not yet known. For instance, a bug has existed in a router's firmware for 3 years, but nobody has discovered it yet. Furthermore, a “zero-day vulnerability” is a vulnerability that could have been publicly disclosed, but there is no available fix/patch yet. For instance, in 2023, a critical zero-day SQL injection vulnerability in the MOVEit Secure Managed File Transfer software was exploited by the Cl0p ransomware threat actor [141]. The attackers exploited a previously unknown flaw to steal data from many organisations worldwide before patches were fully deployed.

“Impact” is the result of an unwanted incident which can cause harm to an asset or an organisation, or any other entity or a group of entities (e.g. a supply chain) .

The EU regulations CSA [13], CRA [11], and NIS 2 Directive [12] define a “cyber threat” as any potential situation involving an event or action that could cause damage, disruption, or undermine the operations of network and information systems, their users and other persons.

A threat can be anything that can exploit a vulnerability to breach security and negatively affect the organisation's critical data or systems. A threat can be either intentional (e.g., an individual hacker or a criminal organization) or accidental (e.g., the possibility of a workstation malfunctioning). The Cybersecurity Risk Assessment methodology of the current dissertation focuses on the intentional nature of cyber threats.

A cyber threat can be implemented by a cyberattack, which is an attempt to damage, modify, disable or gain unauthorised access to an ICT asset, including any effort to expose, steal, or misuse it [53]. The actor who launches a cyberattack is considered an “attacker” or “adversary”. The ISO/IEC 27032:2023 international standard on cybersecurity [137] and NIST SP 800-30 “Guide for Conducting Risk Assessments” [125] define such actors as individuals or groups intent on implementing detrimental activities through deliberate exploits to steal or disrupt availability to ICT elements. The attack vector encompasses the path or means utilised by an attacker or adversary to launch a cyberattack [137]. “Threat Assessment” is an intermediate step of a risk assessment process aiming to estimating the credibility and impact of a potential threat implementation and the probability of the threat implementation.

Over the past decade, malicious activities have evolved significantly, becoming widespread across the ICT ecosystem, increasing their volume or prevalence and their potential impact. Adversaries have become highly sophisticated (e.g. Lazarus, Fancy Bear-APT28 threat groups) and able to utilise significant resources for advanced malware development [5] from multiple attack vectors found freely available (e.g., via the Deep and the Dark Web). They may use advanced techniques to infiltrate an organisation and remain hidden for a long-term period to achieve their malicious goals. Such techniques may include social engineering (e.g., spear phishing and zero-day exploits), custom and stealthy malware (e.g., polymorphic malware), persistence and latest movement (e.g., credentials harvesting) and Command and Control (e.g., DNS tunnelling) [5],[142] to achieve objectives, such as stealing information and disrupting operations. These sophisticated, sustained cyberattacks, where an adversary goes undetected in a network, are considered Advanced Persistent Threats (APTs). APTs are, by nature, persistent, adaptive, and determined, continuously adjusting their tactics to evade defences and achieve long-term objectives [143].

ENISA, in its annual report for threat landscape [3], identifies ransomware, Malware-as-a-Service (MaaS), social engineering, threats against data, threats against availability (Distributed Denial of Service – DDoS) and information manipulation as the most critical threats. In addition, it foresees the following type of attacks as future trends up to 2030 in the cyber threat landscape, i.e., DDoS attacks, ransomware attacks, Living Off Trusted Sites (LOTS) attacks<sup>9</sup>, whereas geopolitics can drive malevolent operations as well. Moreover, ENISA in the “Cybersecurity Threat Landscape Methodology” [144], collects and analyses cybersecurity threat information from public, private, governmental, and intelligence-related sources. It produces annual, sectorial, and thematic threat landscape reports to support situational awareness, risk management, and decision-making for governments, CERTs/CSIRTs, and critical infrastructure. In addition, it identifies threat actors, attack vectors, Tactics, Techniques, and Procedures (TTPs), and vulnerabilities, and provides actionable recommendations using standardised frameworks, such as MITRE ATT&CK [142] and the Cyber Kill Chain [145].

Considering relations between risks, vulnerabilities and threats, cyber risk refers to the potential that cyber threats will exploit security vulnerabilities found on an ICT asset (or a group of ICT assets) and therefore can harm an organisation or other entities [56]. To estimate risks, a common generic formula is the following [125]:

$$\text{Risk} = (\text{Threat} \times \text{Vulnerability}) \times \text{Impact}$$

$$\text{or } R = (T \times V) \times I$$

Where “Threat x Vulnerability” or “(T x V)” value represents the probability of the undesirable event occurring. “Impact” or “I” represents the consequence of the asset loss to the asset owner.

---

<sup>9</sup> LOTS attacks are techniques of conducting malicious activities in the victim's system by utilising its legitimate software and functions available.

Nevertheless, modern cybersecurity risk frameworks have evolved. Frameworks enhance the risk multiplication, including likelihood/probability modes in calculation using scoring systems and ICT frameworks [146]–[147]. Risk modelling has become more granular, context-aware and adaptive (e.g., [125],[148]–[152], incorporating probabilistic reasoning, threat intelligence, attack dependencies and Bayesian inference, adaptive security techniques, such as real-time behavioural analysis and AI/ML prediction models to increase their efficiency and accuracy (see Section 4.4). Furthermore, risk models may incorporate threat actor capability, attack vectors, interrelate CTI frameworks, and control effectiveness to qualitatively assess risk and attack likelihood.

Decision makers review the risk assessment results to select appropriate security controls and end up with a proper risk mitigation strategy by conducting a cost-benefit analysis. In this context, risk management is dealing with specified objectives, possible effects that can affect those objectives and their related uncertainties. The ISO:27000:2018 [53] defines “Risk management” as bunch of collaborative processes to direct and control an entity concerning cyber risks. These processes perform identification, quantification and management techniques to estimate ICT stakeholders’ risks and balance the use of opportunities for gains with minimising vulnerabilities and losses. Cybersecurity risk management incorporates the risk assessment process starting from setting the boundaries of the assessment to identify risks, ending up with risk calculation and risk treatment [55].

The ETSI Technical Specification (TS) 102 165-1 [152] identifies “mitigation” *“as the limitation of the negative consequences of a particular event”*. Risk mitigation strategy includes concepts of diminishing uncertainties, protecting assets from risk exposure, identifying potential sources of risks. “Risk treatment” is a set of processes to modify risks to reach specified levels [53]. It is the final action of risk management. “Countermeasures” are protective actions or controls implemented to prevent security threats from succeeding or to minimise their potential impact and consequences [138]. “Security controls” may include, but are not limited to, processes, policies, devices, practices or other conditions and/or actions which maintain and/or modify risk. Controls may not always exert the intended or assumed modifying effect [53]. A successful risk management includes decision making in formulating effective security policies and control strategy, according to the entity’s security requirements and the design of business continuity and disaster planning. It relies on risk assessment and the entity’s risk appetite to effectively treat and manage risks and threats upon specified thresholds.

A security threat was previously characterised as an unwanted event. A security “incident” can be an individual or a series of either unwanted or unexpected information security events that occur to compromise ICT networks, systems, services or assets or compromise and its operations indicating a possible breach of a policy or controls’ failure [53],[153]. The NIS 2 Directive [12] defines incident as the loss of availability, authenticity, integrity or confidentiality of stored, transmitted or processed data throughout the ICT network and its systems and services.

Risk management techniques can be either proactive or reactive or both:

- Proactive risk management techniques focus on preventing risks before they occur. These techniques involve identifying potential threats, assessing vulnerabilities, implementing security controls, continuous monitoring, employee training, and predictive analysis to minimise the probability and impact of future incidents.
- Reactive risk management techniques address risks after an incident or failure has occurred. They emphasize incident response, damage containment, recovery procedures, forensic analysis, and corrective actions to reduce operational disruption and prevent recurrence.
- Combined (hybrid) risk management techniques integrate proactive prevention with reactive response mechanisms. They continuously monitor and predict risks while also adapting strategies based on detected incidents and real-time feedback, enabling more resilient and adaptive security management.

As previously described, adversaries can use a variety of advanced techniques and tools to initiate advanced targeted intrusions. In many cases, adversaries take the advantage of the multiscale and interconnected nature of ICT infrastructures to attack third parties [4]. In this line, appropriate security solutions required to support and facilitate the detection and analysis of cyberattacks and threats on ICT infrastructures, and raise the awareness on cyber risks [4]. The NIS 2 Directive [12] *urges ICT stakeholders to manage cybersecurity risks systematically, implement minimum security measures, such as incident handling, business continuity, access control, and report significant incidents to secure ICT supply chains and improve the operational resilience of Critical Information Infrastructures that are essential or important to the EU economy.*

## **4.2 Legal Framework, standards, guidelines and best practices in cybersecurity**

Cybersecurity standards on a global scale are exhaustive, appealing to several types, such as glossaries, guidelines, methods, and objectives (e.g. IT evaluation, requirements identification, risk management and technical specifications). This chaotic range of standards towards the rapid pace of technological and threat evolution hinders stakeholders (e.g., security architects/developers, policymakers, testers, auditors) from discovering which standards best meet their security needs. The current section presents the existing cybersecurity regulatory background related to the current doctoral thesis and analyses the challenges towards the harmonization of standards by identifying relationships between the EU regulation and prominent cybersecurity standards. The current section presents content of the research work conducted in [18].

### **4.2.1 Cybersecurity regulation**

The European Union enforces a strict, comprehensive regulatory framework for cybersecurity, targeting critical ICT infrastructures, ICT supply chains, ICT products and services, data privacy and data protection. In Section 2.2.1, the Cyber Resilience Act (CRA) [11], the Cybersecurity Act (CSA) [13] and the NIS 2 Directive [12] roles in the ICT ecosystem and its interrelations were

analysed. Apart from those, there are several other EU regulations supporting the security of the EU digital market. This section provides a summary of key EU regulations related to the ICT ecosystem. The key regulations are grouped into specific categories that are most relevant:

- Critical Infrastructure Protection
- Product security and certification
- Data privacy and data protection
- Emerging technologies
- Cyberdefence

Nevertheless, the EU regulations, presented in the following, may have a direct or indirect relation with other regulation categories. The identified regulations are all connected directly or indirectly to safeguard the ICT ecosystem.

#### 4.2.1.1 The EU Cybersecurity strategy

The EU Cybersecurity strategy [10] for the digital decade, published on December, 2020, aims to secure digital services and infrastructure through 2030 and establish a Joint Cyber Unit. It highlights on securing the EU digital single market under the following three main pillars:

- **Resilience, technological sovereignty and leadership.** It drives security to resilience, technological sovereignty and leadership through the following main topics:
  - Critical Infrastructure and critical services protection. It aims to ensure the security and resilience of the digital ecosystem promoting relevant regulations, such as the NIS 2 Directive.
  - Building a European cyber shield by promoting security-related information exchange across multiple stakeholders. It encourages the collaboration and support of Computer Security Incident Response Teams (CSIRTs) and Security Operations Centres, or SOCs.
  - Building an ultra-secure communication infrastructure by encouraging space-based communication capabilities to ensure the security and safety of EU and its Member States critical missions and operations. It promotes the support of the European Union Governmental Satellite Communications initiation, national security actors and EU institutions bodies and agencies. Moreover, it aims to secure Quantum Communication Infrastructure (QCI) and deploy new and more secure forms of encryption.
  - Securing the next generation of broadband mobile networks supporting 5G and future generation technologies.
  - Envisaging an Internet of Secure Things promoting ICT products and services security. It illustrates the Cybersecurity Act importance on raising the resilience and trustworthiness. In addition, the Cyber Resilience Act is directly connected, as it provides fundamental requirements for securing products with digital elements.

- Targeting at greater global Internet security. This goal aims to be addressed by investing in DNS root system security.
- Reinforcing presence on the technology supply chain.
- Promoting Cyber-skilled EU workforce. It invests in research, innovation and development initiatives related to the protection of the EU cyberspace against threats and encourages awareness activities(e.g., SMEs support under Digital Innovation Hubs).
- **Building operational capacity to prevent, deter and respond.** This pillars relies on the following aspects.
  - Creating a joint cyber unit collaboration with security communities towards developing a comprehensive crisis management framework
  - Tackling cyber crime
  - Reinforcing the cyber diplomacy to prevent, discourage, deter and respond to malicious cyber activities
  - Boosting cyber fence capabilities
- **Advancing a global and open cyberspace**
  - Promoting EU leadership on standards, norms and frameworks in cyberspace. It recognises the importance of cybersecurity standards and its fragmentation (see Section 4.2.2) and reinforces standardisation harmonisation activities.
  - Cooperation with partners and the multi-stakeholder community. It aims to open cyber dialogues with third parties and establish regular and structured exchanges with regional stakeholders to promote a multi-stakeholder model for Internet governance.
  - Strengthening global capacities to increase global resilience by promoting the creation of an EU Cyber Capacity Building Board.

#### 4.2.1.2 Critical Infrastructure Protection

The main EU regulations directly related to the protection of critical infrastructures is presented in the following.

##### **The CER Directive**

The first regulation to report on the Identification and Designation of European Critical Infrastructures and highlight the need to improve their protection was the EU Council Directive 2008/114/EC (2008) [154]. Currently, it has been replaced with the Critical Entities Resilience Directive (CER) Directive (Regulation (EU) 2022/2557) [155]. The CER Directive significantly expands the scope of regulated sectors of the EU Council Directive 2008/114/EC. It is designed to strengthen the resilience of organisations that provide essential services across the European Union. Moreover, it aims to protect the critical infrastructures and essential services against cyberattacks, natural disasters, terrorism, hybrid threats and public health emergencies, insider threats and operational disruptions. It elaborates on topics of physical, operational, and organisational resilience.



## **The NIS 2 Directive**

As presented in Section 2.2.1, it is the most critical regulation on network and information systems security. The NIS 2 Directive (Regulation (EU) 2022/2555) [12],[52] is the descendant of the NIS Directive (Regulation (EU) 2016/1148) [50], which was initiated in 2016 in response to the need for reinforcing the Critical Infrastructure Protection at national and union level for robust internet security [156]. The initial NIS Directive was issued as a part of the EU Cybersecurity strategy aiming to raise the cybersecurity awareness across the EU. The focus was on three parts: i) national capabilities, ii) cross-border collaboration and iii) National supervision of critical sectors. The NIS Directive engaged public administration and key-players in the private sector to apply network and information security risk management on their Critical Information Infrastructures (CIIs). In 2023, it was replaced by the NIS 2 Directive.

The NIS 2 Directive aims to improve the resilience and incident response capacities of CIIs, focusing on measures to improve their security. The mitigation strategy relies on: i) leveraging the EU preparedness by setting relevant requirements, ii) encouraging information exchange and collaboration among all EU Member States, and iii) creating a cross-sectoral security ICT culture. Compared to the original NIS Directive [50], the NIS 2 Directive (EU 2022/2555) [12] strengthens cybersecurity obligations by expanding the scope of covered sectors. It introduces stricter enforcement and penalties, enhances risk management and incident reporting requirements, improves vulnerability disclosure processes, and establishes stronger supervisory measures across EU Member States.

The Implementing Regulation (EU) 2024/2690 [157] aims to provide details on the technical and methodological requirements for NIS 2 implementation. Furthermore, it clarifies when an incident is “significant”, specifies risk-management obligations for DNS cloud, data centre, content delivery network, managed service, and social networking providers, and ensures uniform application of the NIS 2 framework across sectors.

As described in Section 2.2.1, a proposal [52] for targeted amendment of NIS 2 Directive has been released in January 2026, to enhance alignment with the Cybersecurity Act [13].

## **The DORA regulation**

DORA (Digital Operational Resilience Act), Regulation (EU) 2022/2554 [158], is a binding regulation for the financial sector (e.g., banks, insurance, and investment firms) and their critical third-party ICT providers. It enforces strict rules on ICT risk management for mandatory digital resilience testing (including threat-led penetration testing), and systematic incident reporting.

### **4.2.1.3 Product security and certification**

The most representative regulations for product security and cybersecurity certification are described below.

## **The Cyber Resilience Act**

The Cyber Resilience Act (CRA), Regulation (EU) 2024/2847 [11], is a critical regulation for securing Products with Digital Elements (PDEs). It sets mandatory cybersecurity requirements

for PDEs place on the EU market. As described in Section 2.2.1, it focus on security across the Software Development Lifecycle (SDLC). Therefore, manufacturers must ensure security-by-design on their products, deliver mandatory security updates throughout their CI/CD pipeline and report on exploited vulnerabilities. The CRA entered into force in December 2024, with phased applicability; vulnerability reporting starts in 2026 whereas full compliance applies from December 2027, as presented in Section 2.2.1.

Several amendments have been published in order to further analyse its topics, including but not limited to: secure-by-design obligations, lifecycle security support, mandatory vulnerability reporting,, CE marking for cybersecurity compliance, stricter rules for critical products (indicating stringent conformity assessment for important” and “critical” digital products), Software Bill of Materials (SBOM) indications to manufacturers to maintain transparency of products’ software components and dependencies, and expanding the certification framework for managed security services.

### **The Radio Equipment Directive**

The Radio Equipment Directive (RED), Directive 2014/53/EU [159], is an EU regulation that establishes requirements for safeguarding products related to radio equipment placed on the European market. It aims to ensure that wireless and connected devices remain safe, interoperable, and secure. RED may rely on the provision of requirements related to safety, efficient radio spectrum use, cybersecurity, and market and compliance. It applies to wireless and radio-enabled products. RED aims to strengthen the security and reliability across the EU digital market.

### **The Cybersecurity Act**

In June, 2019 the Cybersecurity Act (CSA), Regulation (EU) 2019/881 [13], was published, as the first regulation to cybersecurity certification. Precisely, it aims it realised an EU-wide cybersecurity certification framework for ICT product, ICT services and ICT processes. The regulation consists of two main parts: i) highlights the role and mandate of ENISA, and ii) sets the cybersecurity certification framework for the ICT ecosystem. As mentioned in Section 2.2.1, a targeted amendment [47] for adopting in the future a certification scheme for “managed security services” was published in 2025, and During January 2026, a proposal [49] for CSA 2 was also published.

### **The EUCC Implementing regulation**

The Commission Implementing Regulation (EU) 2024/482 [14], complements the CSA by introducing the Common Criteria-based cybersecurity certification scheme for ICT products. Moreover, it identifies a set of security and assurance requirements for stringent conformity assessment of ICT products.

### **The regulation on accreditation**

The regulation (EC) No 765/2008 [160] sets out a framework for accreditation of conformity assessment bodies and market surveillance relating to products placed on the EU market.

#### 4.2.1.4 Data privacy

This category encompasses the most critical regulations regarding data security and privacy.

##### **The General Data Protection Regulation**

The Regulation (EU) 2016/679 on General Data Protection Regulation (GDPR) [161] is the EU's main law for protecting personal data and privacy of individuals. It applies to any organisation that collects or processes personal data of EU residents, regardless of where the organisation is based. GDPR sets rules in lawful processing of personal data, minimisation of data and purpose limitation, individuals' rights (access, deletion, portability), breach notification obligations, and accountability of organisations processing data. It strongly depends on cybersecurity measures, as it requires from organisations to implement "appropriate technical and organisational measures" to ensure data security.

##### **The eIDAS 2**

The European Digital Identity (eIDAS) 2, Regulation (EU) 2024/1183 [162], updates the eIDAS, regulation (EU) No 910/2014 [163]. is a regulation on electronic identification and trust services, harmonised with the NIS 2 Directive. Compared to the eIDAS, it enhances concepts, such as the Digital Identity Wallet (EUDI Wallet), security and interoperability requirements, and provides stronger rules for trust services and improvements for EU cross-border authentication.

##### **The ePrivacy Directive**

The ePrivacy Directive (2002/58/EC) [164] relies on topics of confidentiality on electronic communications. It also governs the use of cookies and similar technologies, requiring user consent for storing or accessing information on devices.

##### **The Data Governance Act**

The Data Governance Act [165] establishes a framework for secure and trustworthy data sharing within the European Union. It promotes the reuse of public sector data, regulates data sharing intermediaries, and supports voluntary data sharing for the public good (data altruism). It aims to increase data availability while ensuring compliance with privacy, security, and transparency requirements.

#### 4.2.1.5 Emerging technologies

The most critical regulations on emerging technologies related to cybersecurity are presented in the following.

##### **The Chips Act**

The Chips Act, Regulation (EU) 2023/1781 [166] aims to strengthen the EU semiconductor ecosystem by raising the chip production capacity, eliminating external supplier dependency, and improving supply chain resilience. It aims to promote relevant research and innovation activities and enhance technological sovereignty and strategic autonomy.

## **The Artificial Intelligence Act**

The Artificial Intelligence Act (AI Act) [167], Regulation (EU) is the first comprehensive EU regulation for securing AI systems used, developed or placed on the EU market. It identifies risk tiers on AI systems. High-risk AI systems must explicitly prove robust cyber resilience against manipulation, data poisoning, and adversarial attacks before entering the EU market. The AI Act aims to ensure that AI systems are safe, trustworthy, and respects fundamental rights while promoting innovation across the EU.

## **The EU Blockchain legal and regulatory framework**

While there is no yet a proposal for regulation, the European Union has implemented a comprehensive legal and regulatory framework for blockchain [168] related to Distributed Ledger Technologies (DLT), i.e., pilot regime regulatory sandbox, and crypto-assets, primarily through the Markets in Crypto-Assets (MiCA) [168]. The framework aims to secure blockchain technologies and ensure legal certainty for blockchain use in finance, supply chains, and public services.

## **The Quantum Act (proposal)**

The European Commission has adopted a Quantum Strategy [169] in July 2025 envisaging to position Europe as a global leader in quantum by 2030. Moreover, a Quantum Act proposal [170] is under development by Commission work programme 2026 legislative initiative, which is planned to be released during the second quarter of 2026. The Quantum Act proposal aims to focus in three complementary dimensions: i) coordinate relevant research and innovation investments across the EU, ii) leverage the EU industrial capacity in quantum technologies design and production, and iii) ensure the security and resilience of quantum supply chains.

### **4.2.1.6 Cyberdefence**

In this category, the primary regulatory framework on cyberdefence is described.

## **The EU Cyber Solidarity Act**

The EU Cyber Solidarity Act, Regulation (EU) 2025/38 [171], which amended the Digital Europe Programme (Regulation (EU) 2021/694) [172], establishes measures to strengthen solidarity within the EU and raise its preparedness towards enhancing the incidence handling and incident response capacity. The EU Cyber Solidarity Act complements the NIS 2 Directive, Cyber Resilience Act and CER Directive. It resides in the EU's cyber defence and resilience strategy.

## **The Cybersecurity Crisis Management Blueprint**

In June 2025, EU adopted the Cybersecurity Crisis Management Blueprint [173], which aims to coordinate activities in view of a large-scale cyberattack realisation across the EU Member States. The Cybersecurity Crisis Management Blueprint focuses on managing European cyber crises and incidents to reinforce the cyber resilience across the EU digital single market.

#### 4.2.2 Challenges in cybersecurity standards

Over recent decades, the increasing reliance of business processes and services on digitally connected ICT systems has significantly expanded the attack surface, exposing organisations to a growing range of security vulnerabilities and weaknesses. As adversaries gain more advanced capabilities and broader access to sophisticated offensive tools (including those available via Deep and Dark Web ecosystems), security requirements have become increasingly stringent to counter evolving threats, such as botnet-driven DDoS attacks [174], ransomware variants (including locker and crypto-ransomware [175]), and advanced malware employing evasion techniques like memory obfuscation and code injection.

Empirical evidence highlights the scale and impact of these threats. For instance, coordinated campaigns such as RapperBot (2022) [174] demonstrated large-scale brute-force exploitation of IoT devices across thousands of IP addresses globally, underscoring systemic weaknesses in connected infrastructures. Sector-specific incidents further illustrate the consequences of cyberattacks, including COVID-19-related intrusions [176] targeting healthcare systems that resulted in significant data breaches and exposure of sensitive patient information. Similarly, the compromise of Uganda's mobile money infrastructure in 2020 [176] led to prolonged disruptions in financial transactions, illustrating the potential for cyber incidents to destabilise critical national services.

In response to this evolving threat landscape, continuous development of security standards, best practices, and governance frameworks is essential. Standardisation efforts aim to address heterogeneous organisational requirements across sectors and supply chains, while enhancing the resilience, preparedness, and defensive capacity of cyber-physical and digitally dependent infrastructures. The landscape of cybersecurity standards seems chaotic due to its complexity and the rapid pace of technological and threat evolution. This perceived chaos stems from several factors:

*Plethora of Standardisation bodies:* There are numerous cybersecurity standards, frameworks, and guidelines, each developed by different organisations, governments, and industry groups. These include ISO/IEC, NIST, ETSI, CEN/CENELEC, and sector-specific bodies, such as HIPAA from healthcare, FISMA from finance, and IMO, BIMCO from the maritime sector. The variety can be overwhelming, especially for organisations operating internationally or across multiple sectors.

*Rapid Technological Change:* The Rapid technological advances — including cloud computing, the Internet of Things (IoT), Artificial Intelligence (AI), and quantum computing — are increasingly challenging the adequacy and relevance of existing cybersecurity standards. New technologies often outpace the development and implementation of appropriate security measures.

*Evolving Threat Landscape:* Cybersecurity threats are constantly changing, with cybercriminals developing new tactics, techniques, and procedures. Standards must continuously evolve to address emerging threats, necessitating frequent updates and revisions that can contribute to a perception of fragmentation and instability.

*Compliance Complexity:* Organisations often find themselves needing to comply with multiple standards simultaneously, which can be costly and resource-intensive. The effort to accommodate

diverse requirements can create ambiguity and a perception of disorder, particularly when standards overlap or contradict.

*Industry-Specific Needs:* Different industries face unique cybersecurity challenges, leading to the development of industry-specific standards. While necessary, this specialisation further fragments the cybersecurity standards landscape.

Cybersecurity management standards, for instance, are developed by all the abovementioned standardisation bodies adopting different views; the list of these standards is globally exhaustive, appealing to several types (e.g. glossaries, recommendations, guidelines, methodologies, metrics) and various topics (e.g. IT evaluation, security requirements identification, sectorial needs, risk management, and technical specifications). This fragmented landscape of standards can impede stakeholders—including policymakers, developers, security architects, system integrators, auditors, testers, and risk assessors across various sectors—from determining which standards best align with and adequately address their specific requirements.

The implementation of various EU policies and directives (e.g., the Cybersecurity Act [13] enforces Europe to accelerate its efforts in developing and adopting European standards [177]. Nonetheless, harmonised security standards can provide a technical basis to assess the security of ICT processes/products/services and benefit the EU Digital Single Market (DSM) and international digital markets. To this aim, the EU asked the European standardisation organisations (e.g. ETSI, CEN/CENELEC) to assess the existing standards and conduct a gap analysis to implement its decision for harmonising standards [178]. In this context, there is a compelling need to organise cybersecurity standards into coherent thematic groups to enhance understanding of their scope and intent, thereby supporting stakeholders in selecting the most appropriate standards to meet their specific security requirements.

Research efforts addressing these challenges are attracting significant interest from both European and global industries. Recently, ENISA published an analysis of standardisation requirements supporting cybersecurity policy [179], which primarily functions as a risk management catalogue rather than a comprehensive taxonomy of cybersecurity risk management standards. The report further outlines methodologies and tools used to support the implementation and conformance of these standards. Moreover, ENISA has published a framework on distinct cybersecurity skills [180]. The Joint Research Center (JRC) of the European Commission has issued a sectoral categorisation covering multiple domains [181]. This work was considered as input in the current doctoral thesis which has developed an ontology for cybersecurity standards based on industry interests [18]. The ontology is presented in Section 5.3.

#### **4.2.3 Cybersecurity as standardisation priority in policymaking**

This section presents the importance of cybersecurity standardisation in policymaking.

Regulation (EU) No 1025/2012 [182] on European standardisation defines standard as a model specification issued by a recognised standardisation body for repeated and continuous use, although compliance with it is not mandatory. Model specification is documentation on technical

requirements addressing a product, process, service or system. Standards can be issued either by an international, European or national standardisation body.

A Technical Specification (TS) is a normative document, approaches an international standard in detail and completeness. Nevertheless, it has not yet passed through all approval stages (considering either premature or not reached consensus). A Technical Report (TR) is informative and non-normative, analysing specific topics with complementary information (e.g., testing approaches, measurements, methodologies, and test cases). A Publicly Available Specification (PAS) aims to boost standardisation activity towards rapidly evolving technologies and respond to an urgent market need.

ISO/IEC 17000:2020 [57] describes cybersecurity standard as a technical document used as a rule, guideline, or definition. Standards are developed from a group of interested parties (i.e. manufacturers, consumers, regulators of particular material/products/processes/services) and provide a consensus-built, repeatable dimension [183]. *European Standards (EN)* are implemented by ETSI [184] the national CEN and CENELEC [185]. Harmonised standard is a European standard created by a recognised European standardisation body (i.e., CEN, CENELEC, or ETSI) upon relevant request from the European Commission for the application of the EU harmonisation legislation [182].

Following the discussion in the previous section, cybersecurity is considered a high standardisation priority since cyber threats impact multiple sectors. In this vein, cybersecurity standards are not just technical documentations. They are enablers for enhancing the security of ICT stakeholders and raising their awareness, as they codify security best practices and state-of-the-art techniques. They aim to bring innovation, reinforce the security preparedness and increase interoperability across diverse industries.

As cybersecurity and data protection rapidly grow, technical and application domains are changing. The application of emerging technologies, such as augmented reality, global AI, Adversarial Learning, etc., in our daily businesses and the use of digital identity [31] by citizens requires specific practices and guidance on how to manage and monitor and concurrently maintain the security within organisations. The work in [186] stresses the need to boost standardisation initiatives and policymaking associated with AI security. More standards for securing AI, 5G and IoT are gradually developing by prominent standardisation bodies, addressing various aspects at different levels, with overlaps and diverging approaches [187].

The following section presents critical EU cybersecurity regulations and describes standards as building blocks of the EU security policies. It identifies the interplay of EU legislation with European and international standards aiming to create corresponding relationships (where possible) to raise clarity, cohesiveness and reduce the fragmentation.

#### **4.2.4 Critical cybersecurity standards, guidelines and best practices**

In the modern digital era, the cyberdependent ICT products, services, systems and supply chains have raised the need for guidance, technical specifications and best practices documentation to facilitate horizontally and vertically the ICT ecosystem at different regions, nations and

populations. This growing need has employed the fragmentation of cybersecurity standards. There is a chaotic list of standards related to various cybersecurity aspects. The current section presents the most critical standards for cybersecurity risk management, conformity assessment and cyber resilience for the ICT ecosystem.

#### 4.2.4.1 Standards related to risk management.

The ISO 31000:2018 [188] standard provides guidelines for risk management by introducing a systematic process that addresses general perspectives applicable both to physical and information security systems. The IEC 31010:2019 [189] aims to consult organisations on the selection and application of risk assessment techniques among a variety of situations. The techniques are willing to provide help in decision making wherever there is uncertainty, to introduce specific risk information as part of the risk management process. The risk analysis relies on the planning, implementing, verifying and validating the use of the techniques.

The NIST SP 800-30 [125] assists ICT stakeholders to manage and mitigate their cybersecurity risks. The Risk Management Framework (RMF) of NIST for information systems and organisations “NIST SP 800-37 Rev. 2” [190] provides a System Life Cycle approach to manage security and privacy risks. The RMF model proposes real-time risk management to deliver cost-effective and efficient decision-making. The NIST Cybersecurity Framework (CSF) 2.0 [191] provides flexible guidance for managing cybersecurity risk across all types of organisations, regardless of size, sector, or maturity level. It defines a common set of high-level cybersecurity outcomes that help organisations understand, assess, prioritize, and communicate their cybersecurity activities effectively.

The ISO/IEC 27k family of international standards on information security provides a variety of standards associated with ISMS (ISO/IEC 27001 [55]) and cybersecurity risk assessment (ISO/IEC 27005 [56][55]) that establish a holistic approach to information security applicable to all organisations, regardless of type, size, or sector. The ISO/IEC 27000:2018 standard [53]) provides a comprehensive glossary for information security management systems (ISMS). The ISO/IEC 27002 [66] is an international standard providing guidance for organisations looking to establish, implement, and improve an ISMS. It offers best practices and control objectives related to key cybersecurity aspects including access control, cryptography, human resource security, and incident response. ISO/IEC 27006:2015 [192] standard identifies the requirements for bodies providing audit and certification of the ISMSs.

#### 4.2.4.2 Sectorial cybersecurity standards

A variety of standards are provided for evaluation criteria on IT and information technology. To address the risks posed by cyberattacks and help ensure high levels of protection CEN and CENELEC’s JTC 13 ‘Cybersecurity and Data Protection’ have released a series of European Standards (ENs), such as the EN ISO/IEC 19790:2020 [193] on topics of Information technology, security techniques and security requirements for cryptographic modules and iv) the EN ISO 29134:2023 [194] that concerns information technology and Security techniques and gives guidelines for privacy impact assessment. The ETSI TR 187 011 [i.2] [195] method provides



guidelines concerning how to apply ISO/IEC 15408-2 [i.28] [45] requirements to ETSI standards and gives guidelines for security objectives. In this line, ETSI TR 187 002 [i.3] [152] presents examples on security functional requirements and on security objectives.

Technical standards for ISMS and IT security are identified. IT-Grundschutz catalogues [196] is a German BSI technical standard for management system for information security (ISMS) and IT security, engaging technical, organisational, IT-view and personnel aspects. IT-Grundschutz delivers a systematic approach to information security, which is applicable to ISO/IEC 27001. The Federal Information Security Management Act (FISMA) is a part of the US E-Government Act of 2002 for improving the management of electronic government services and processes. It guides federal agencies to develop, document, and implement an information security and protection program. The OWASP Application Security Verification Standard (ASVS) [197] sets a basis for testing web application technical security controls and proposes a list of requirements for secure development. The Cloud Security Alliance Cloud Controls Matrix (CCM) [198] provides fundamental security principles to guide cloud vendors and assist prospective cloud customers in assessing the overall security risk of a cloud provider. The CSA CCM presents a controls framework of security concepts and principles that are aligned to the Cloud Security Alliance guidance in 13 domains.

Most of these standards specify framework conditions for the risk management process, but they don't delve into predefined methods for the risk analysis or risk assessment. This is a reason why in many cases there are differences in the adopted risk assessment process within the specific areas of application, making a direct comparison of the results difficult.

#### 4.2.4.3 Standards related to security evaluation and conformity assessment

Prominent standards and frameworks on information security and cybersecurity certification, linked with cybersecurity risk assessment and IT evaluation are provided in the following.

ISO/IEC 15408 series reflect the Common Criteria Framework which establishes the concepts, principles, techniques and criteria for IT security evaluation and its complementary ISO/IEC 15408-2:2022 [45] defining the security assurance elements and ETSI-TVRA methodology [152], acknowledging inherent factors on which the attack potential is dependent, as mentioned in Section 2.2.2. The ISO/IEC TR 15446 [199] is a technical report that provides guidance on the application of Common Criteria, particularly focusing on how to construct and structure Protection Profiles and Security Targets for IT security evaluation.

ISO/IEC 17000-series (17000:2020 [57], 17020:2026 [200], 17021:2015 [201], 17024:2026 [202], 17025:2026 [203] and 17065:2012 [204]) is an international set of standards that mainly provides from the general concepts and principles for conformity assessment to guidelines and good practice recommendations. It also defines the requirements of bodies to be competent in performing reviews and inspection activities, as well as the ones they need to follow in order to approve a certification. Specifically, the ISO/IEC 17025 [203] aims to prescribe the operations of the testing and calibration laboratories and identify a set of requirements which demonstrate that laboratories produce valid evaluation results. The ISO/IEC 17065 [204] defines the requirements

for bodies certifying products, processes, and services. It ensures that certification bodies operate impartially, consistently, and competently when conducting conformity assessments.

#### 4.2.4.1 Standards related to ICT supply chain security

NIST in its latest version “Framework for Improving Critical Infrastructure Cybersecurity” [205] promotes a set of industry standards, guidelines, and best practices for managing cyber supply chain risks and provides a common language that gives insights at all levels within an organisation and in all aspects of the supply chain, allowing stakeholders to better comprehend their relationships and interactions across the ICT supply chain. In NIST.IR.8276 [76], Cyber Supply Chain Risk Management (C-SCRM) is identified as the multidisciplinary approach to manage supply chain risks and key practices are set for supply chain organisations of different size, scope and complexity in order to robust the C-SCRM function and thus ensure the business resilience. NIST SP 800-161 [78] incorporates practices of the SCRM for Federal Information Systems and Organizations providing guidance to federal agencies on identifying, assessing, and mitigating ICT supply chain risks at all levels of their organisations.

ISO 28000:2007 [138] is a management system standard designed to improve supply chain security, particularly for logistics and transport organisations. It defines requirements for establishing, implementing, and maintaining a security management system, with a focus on ensuring supply chain security assurance. The standard is applicable to organisations of all sizes involved in supply chain operations.

The ISO 28001:2007 [70] provides specific guidance for implementation of a security management system for the supply chain. It is intended to assist organizations in establishing reasonable levels of security and improve risk-based decisions for the supply chains’ protection.

The ISO 28004:2014 [206] reports on the security management supply chain systems and gives guidance for the implementation of the ISO 28000:2007 [138]. Nevertheless, several standards from the previous sections can be used for ICT supply chain security.

Figure 7 provides an initial classification of this dissertation of standards related to Supply Chain Security Management. An ontology of cybersecurity standards has been developed and described in Section 5.3.

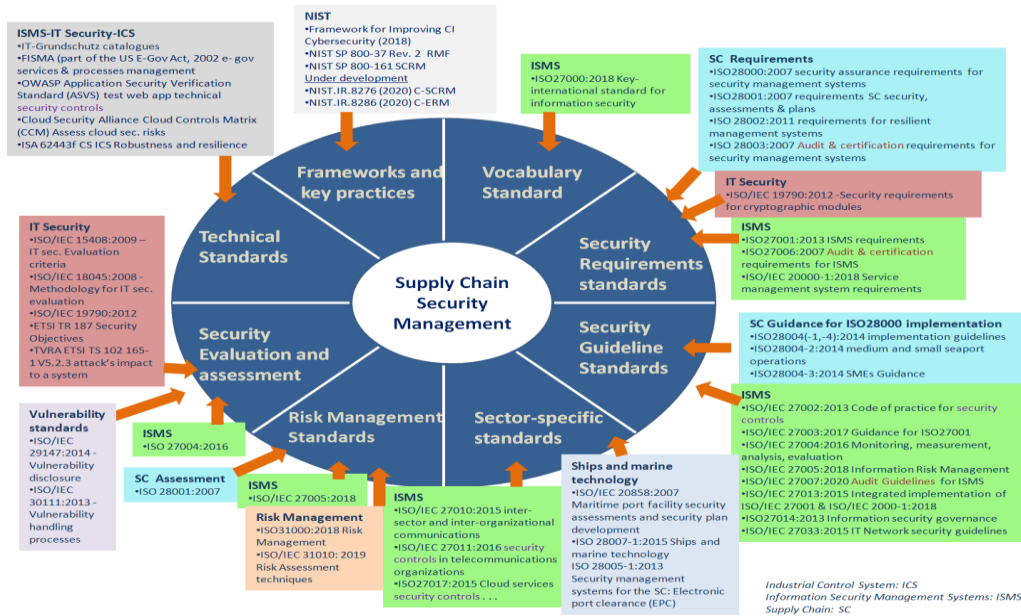


Figure 7: Major Standards and frameworks of Security Management.

#### 4.2.5 Relations of EU legislation with international standardisation

Security policies in Europe drive us to use and develop standards. For instance, the NIS 2 Directive on Security of Network and Information Systems [12], the most important EU legislation instrument, requires assessing and managing cyber risks among interconnected Critical Information Infrastructures (CIIs). The Radio Equipment Directive (RED) 2014/53/EU [159] Critical Entities Resilience Directive (CER) Directive [155], and the Cybersecurity Resilience Act (CRA) [11] stress the need for Critical Infrastructure Protection and introduce common cybersecurity requirements to apply throughout the expected lifecycle of devices, respectively. ETSI TR 103 866 V1.1.1 [207] and indicative families of standards, i.e., ISO2700x and ISO2800x series, can guide stakeholders to raise compliance with such directives. CEN and CENELEC have introduced numerous sector-specific cybersecurity standards to stress the CIIs security requirements of critical EU industries [208]. Consequently, security standardization brings trustworthiness to ICT products, spreads knowledge among multiple stakeholders, increases CII protection, and secures digital services.

Cybersecurity certification efforts are accelerating in Europe [63],[152] due to the Cybersecurity Act (CSA) [13], the EU legislation which promotes the certification of EU ICT products, services and processes, addressed by the European Cybersecurity Certification Scheme (EUCC) of the Implementing Regulation (EU) 2024/482 [14], and two additional ENISA cybersecurity certification schemes, i.e., the recently published proposal of the Cloud and AI Development Act (CADA) [209] indicating a cybersecurity certification scheme that covers both cloud and AI services, and the EU5G scheme draft, including the Embedded Universal Integrated Circuit Card (eUICC) specifications [210]. The CSA [13], as described in Section 2.2.1, relies on international standards for ICT evaluation and conformity assessment [44]–[46],[59],[204]. Furthermore, cybersecurity certification addresses market fragmentation, increases security, and strengthens

stakeholders' confidence to establish a competitive and resilient EU DSM. ISO and IEC are working on creating a universal cybersecurity labelling framework (ISO/IEC 27404 [211]), aiming to guide the development and implementation of IoT certification. This involvement is crucial for aligning this new standard with already established IoT security standards, such as ETSI EN 303 645 [212] and NISTIR 8425 [213] guidance, the primary works for most IoT device specifications worldwide.

Nonetheless, security policies are highly interrelated within the EU. For instance, the CSA sets the need for privacy and data protection regulation [161] and for electronic transactions protection in the internal market (eIDAS regulation) [162]. Privacy and data protection promoted by GDPR [161] and ePrivacy Directive [164]. In this context, privacy-by-design specifications, privacy assessment and management standards are required, such as EN 17529:2022 [214], ISO 3300x series on process assessment [215], ISO/IEC 2700x family of standards [54], and CEN ISO/IEC/TS 27006-2:2022 [192], ISO/IEC 27701:2025 [216] on privacy information management. The European Data Act [217], which complements the Data Governance Act [165] (i.e., a key-pillar of the EU strategy of data), developed to define measures, rules and mechanisms related to industrial data and their accessibility, starts getting into force.

The CSA emphasises the requirement of securing the growing EU markets of the chip industry (i.e., automated cars, cloud and IoT connectivity, space, defense and supercomputers). Chips assumed strategic assets playing a critical role in ICT supply chains. To leverage technological leadership, the EU has published the European Chips Act [166]. In this vein, CEN CENELEC promoted an initiative to strengthen the microchip standardisation effort in the EU, which was assigned to the German commission DKE that led to the establishment of a completed Standardisation Roadmap for Trusted Chips [218].

Eventually, the CSA highlights the importance of analyzing emerging technologies. To this aim, the European Artificial Intelligence Act [167] regulation proposal is prepared to secure AI-based systems within the EU borders. CEN CENELEC, upon the European Commission's request, has established the Joint Technical Committee 21 to produce standardisation deliverables on AI [219].

To improve the preparedness, detection, and response to large-scale cybersecurity incidents across the EU, the European Commission proposed the EU Cyber Solidarity Act [171], applied using international standards on incident management, such as ISO/IEC 27035 [153] and NIST recommendations for incident handling [220].

All these EU regulations correspond to the EU Cybersecurity Strategy [10] aiming to “build resilience to cyber threats and ensure citizens and businesses benefit from trustworthy digital technologies” (see Section 4.2.1.1). Table 3 presents direct or indirect relations between indicative EU legislative instruments and corresponding international or European standards classified into the diverse cybersecurity dimensions illustrated in Section 4.2.1.

Table 3. Security Standards relations with EU regulation.

| Cybersecurity Dimensions / EU Regulation                                                                                                                 | Standard/Framework/ Best Practices                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Critical Infrastructure Protection and Cyberdefence/</b><br><br>NIS 2 Directive, CER Directive, DORA, Solidarity Act                                  | <p><u>CIs and Risk Assessment:</u> ISO2700x, ISO/IEC 27033, ISO2800x, ETSI TR 103 866 V1.1., ISO/IEC 15408, ISO/IEC 18045, EN 17640, ISO 31000, IACS Recommendation on Cyber Resilience (2020), ANSI/ISA-62443-3-2-2020, ISA-TR99.00.01-2007, Supply chain cybersecurity: new guidance from the NCSC, ISO 13053, ETSI TS 102 165-1:2017, NIST SP-800-53 Cybersecurity Framework, NIST SP-800-37 Risk Management Framework , NIST SP-800-161, ETSI TS 102 165-1, BSI-Standards 100-2/100-3, OWASP Risk, NISTIR 8276 Key-Practices in Cyber Supply Chain Risk Management, CVRF, ISA/IEC 62443-3-2, IWA 31:2020, ISO 22301, ISO/IEC 27035</p> <p><u>Threat taxonomies:</u> OWASP, CAPEC MITRE, FISMA, STRIDE, ATT&amp;CK MITRE</p> <p><u>Vulnerabilities disclosure:</u> ISO/IEC 29147:2018, EN-ISO/IEC 29147:2020, ISO/IEC 30111:2019, EN-ISO/IEC 30111:2020, TR103838, CVE MITRE, CVSS 3.1 FIRST, OSV</p> <p><u>Incident Management:</u> ISO/IEC 27035, NIST Incident Response Framework, NIST SP-800-61</p> <p><u>Emergency Management:</u> ISO 22322, ISO 22327, ISO 22326- Security and resilience</p> |
| <b>Product Security and/or Certification/</b><br><br>CRA, RED regulation, CSA, EU 765/2008, EUCC Implementing Regulation, AI Act, Chips Act              | <p><u>Certification schemes:</u> EUCC (initiated by ENISA), EUCS</p> <p><u>IT Evaluation:</u> ISO/IEC 15408, ISO/IEC 18045</p> <p><u>Conformity Assessment/Audit:</u> ISO/IEC 27006, ISO/IEC 27007, ISO/IEC 17000, ISO/IEC 17007, ISO/IEC 17021series, ISO/IEC 17019, ISO/IEC 17020, ISO/IEC 17024, ISO/IEC 17025, ISO/IEC 17065, ISO/IEC 17067, ISO 19011</p> <p><u>EU 5G scheme and eUICC specification:</u> 3GPP TR 33.894 V0.5.0 (2023-02), ISO/IEC 27404, ETSI EN 303 645, NISTIR 8425</p> <p>GSMA Network Equipment scheme (Security Assurance-by-design)</p> <p>CHIPS R&amp;D Metrology Program (NIST), EN 17640, ISO/IEC 15408, CENELEC JTC 13 WG3-DKE standards.</p>                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Data Privacy/</b><br><br>GDPR, ePrivacy Directive, Data Act, Data Governance Act, eIDAS 2 (including sector-specific EU Health Data Space regulation) | <p><u>Privacy Assessment/Information Management:</u> EN17529:2022, ISO 3300x series on process assessment, ISO/IEC 2700x information security series, CEN ISO/IEC/TS, 27006-2:2022, ISO/IEC 27701, ISO/IEC TR 27550:2019, BS10012, CEN CWA 16113</p> <p><u>Identity Management:</u> ISO/IEC 23220, ISO/IEC 27460, ISO/IEC 29100, ISO/IEC 29101, ISO/IEC 27701, ISO/IEC 27018</p> <p><u>Encryption:</u> ISO/IEC 18033, ISO/IEC 11770-3, ISO 13491, ISO/IEC 19772:2020, ISO/IEC 18033-6, ISO 13492</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Emerging Technologies/</b><br>AI Act, CADA proposal, Markets in Crypto Assets (MiCA), EECC, Blockchain – DLT                                          | <p>ISO/IEC TR 5469, IEC TS 62998-3, Stocktaking National and Regional Cybersecurity Policy (2021), NIST AI 100-2e2023ipd–Adversarial Machine Learning, ISO/IEC 27005, ISO/IEC 27563, ISO/IEC 23894, ISO/IEC 24028, ISO/IEC 5338</p> <p>3GPP TR 33.894 V0.5.0 (2023-02), ETSI EN 303 645 Cybersecurity for Consumer IoT, ISO /IEC 20000, ISO/IEC 27033, IPv6, MANRS, IoT–RFC-9200, RFC-8613, ACE-OAuth framework, EDHOC, ECHC, GSMA/3GPP, GSMA SAS-UP/SAS-SM, EU 5G scheme, EU Toolbox for 5G Security (ENISA)</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

#### **4.2.6 The need for cybersecurity standardisation classification**

The literature reviews [221]–[222] the challenge of updating and combining existing security standards is highly raised. Over the past three decades, ICT standards have risen exponentially by a non-stop standards-making ecosystem. ETSI's effort to enumerate standards venues associated with CRA identified more than 750 of them, originating from different ICT communities of various types of institutional arrangements, technologies, services and working groups [223].

The JRC Technical Report [181] describes cybersecurity as an interdisciplinary domain engaging a wide use of its application to all industry sectors, embracing different sizes and types of enterprises (e.g., SMEs/MEs, large enterprises), various dimensions (e.g. cyber/physical) utilising multiple sources addressing some of the most widely-accepted standards, international working groups and classification systems.

This standardisation priority of cybersecurity drove the development of several Standard Development Organisations (SDOs), often overlapping in terms of interests and goals and may even, occasionally, act as competitors, which may lead to inconsistencies and redundant requirements that may be confusing to businesses and hurdle their effective use [224].

The list of security standards is wide-ranging and exhaustive, hindering stakeholders from determining which standards can cover their organisational needs. The great variety of standards, recommendations and best practices hinders identifying their interrelations, which would facilitate their understanding.

Considering all these drawbacks of the chaotic list of similar, different, or overlapping security standards, there is a compelling need for their classification into conceptual groups which could better communicate their existence and use to stakeholders.

ETSI standardisation body has identified basic principles and practices for ICT standardization and provided a classification of the different types of standardization documents in terms of their scope and addressed stakeholders, examining whether they provide requirements or recommendations (normative documents) or communicate relevant information, followed by all SDOs [224]. Moreover, the International Classification for Standards [225] classifies international, regional, and national technical standards and other normative documents designed to map standards in general with every economic sector and virtual activity of humankind used. Notwithstanding, the classification does not address specific aspects of security.

Few attempts to further conceptualise standards have been published already. ENISA has provided a risk management standards framework which analyses standardisation requirements in support of cybersecurity policy and outlines gaps in the domain [179]. The risk management library can guide stakeholders to apply them in their organisations without providing a taxonomy. JRC Technical Report on European Cybersecurity Centers of Expertise Map [181] provides a high-level classification and set of definitions of widely-known standards, international working group classification systems, regulations, best practices, and recommendations in the cybersecurity domain. Nevertheless, the work does not address relations with stakeholders' cybersecurity skills. The European Cybersecurity Skills Framework (ECSF) of

ENISA [180] aims to profile twelve typical cybersecurity professional roles along with their identified titles, missions, tasks, skills, knowledge and competencies and facilitate individuals, employers, and providers of learning programs within the EU to bridge the gap between the cybersecurity professional workplace and learning environments. The work does not include relations to cybersecurity standards.

The literature reviews limited research work on security standardisation classification. The work in [226] provides a narrative review of the most frequently used cybersecurity standards and frameworks based on existing research work and their application to assist organisations in selecting the cybersecurity standard that best fits their cybersecurity requirements. The work mainly differentiates cybersecurity standards from frameworks and does not further categorise them into cybersecurity conceptual groups. They group international cybersecurity standards into general, local regulation, and industry-specific standards and map the relationship between the literature review and future research. The proposed classification does not consider stakeholders' aspects. It could be enriched with current trends (e.g., IoT security, blockchain-based cybersecurity, etc.). Tsohou et al. [227] review, analyse and classify information security standards in the clauses of the ISO/IEC 27001:2005 [55] to facilitate security practitioners in understanding the plethora of security standards. The current work is limited to specific ISO/IEC standards and does not address other standardization activities of information security.

The necessity for organisations to adhere to multiple standards at once can be both expensive and labor-intensive. Striving to fulfil diverse requirements often results in confusion and a perceived disorder, particularly when conflicting or overlapping standards.

The current dissertation proposes a cybersecurity standards ontology (see Section 5.3) aiming at helping organisations understand which, how, and when to use cybersecurity standards depending on the use.

### **4.3 Risk assessment approaches and tools**

Risk assessment is a core cybersecurity activity aimed at protecting assets and minimising failure-related costs. It identifies and evaluates risks based on organisational objectives and infrastructure, typically producing a list of threats with associated probabilities in line with established standards. Foundational principles stem from the National Academy of Sciences (Red Book)<sup>10</sup> and are further reflected in modern guidance, such as NIST SP 800-82 [228].

Risk is defined through three core elements: event, likelihood, and severity. Events represent potential losses arising from uncertain or certain adverse conditions, while likelihood refers to their probability or frequency of occurrence. Various mathematical frameworks, including

---

<sup>10</sup> The National Academy of Sciences (NAS) "Red Book" typically refers to the foundational 1983 National Research Council report: "Risk Assessment in the Federal Government: Managing the Process", Committee on the Institutional Means for Assessment of Risks to Public Health, National Research Council; The National Academies Press: Washington, DC, USA, 1983.

probability theory, expected utility theory, Dempster-Shafer theory [229], and fuzzy set theory [230], are used to model uncertainty under different conditions. Uncertainty is commonly classified as aleatory, epistemic, or arising from imprecision, with the latter two being particularly relevant in software and complex systems, where incomplete knowledge and vagueness contribute to risk.

During the last decades, a number of risk concepts, risk assessment algorithms and tools have evolved from research, designed to maintain the security on ICT infrastructures and associated systems. Several methods implement quantitative risk assessment calculations, such as the work of Son, Song, and Lee (2023) [231]. There is a variety of past, well-known, outstanding risk management methods and risk assessment tools, which can be found in ENISA's inventory of risk management and risk assessment methods [232], such as the ISO/IEC 27005 [56] approach, the EBIOS method used by ANSSI (National Cybersecurity Agency of France), the OCTAVE methods [233] (OCTAVE-S, OCTAVE Allegro, OCTAVE FORTE) based on the OCTAVE threat model, which relies on a-priori distribution of subjectively estimated probabilities utilising the Bayesian approach using UML modelling language. Specifically, the latest version OCTAVE FORTE [234][231] is a structured risk management approach, but it is resource-intensive, highly qualitative, and relies on expert judgement, which can introduce subjectivity. It is also complex and difficult to scale in large organisations, focuses mainly on organisational rather than evolving technical risks, and has limited integration with modern automated and real-time security tools. The CRAMM method is used to identify, analyse, and manage information security risks in IT systems [235]. OCTAVE and CRAMM are risk assessment frameworks that prioritise assets and vulnerabilities. They both function well in legacy systems; nevertheless, they lack scalability and are not well suited for modern distributed systems [235].

Existing risk assessment approaches both qualitative (i.e., NIST 800-30 [125] OCTAVE [231]-[234]) and quantitative or combined (ISO 27005 [56]) either disregard or use limited computational techniques that lack exploring and comparing risk assessment results. In addition, they fail to consider the rapidly evolving cyber threat landscape. Security assurance techniques for large-sized enterprises applied both to composite and basic systems (i.e., NIST 800-30 [125], IT-Grundschutz) face limitations in analysing management and operational issues and give low collaborative capabilities.

The AURUM research work in [236] proposes an automated approach for supporting risk analysis and utility-based decision-making in cybersecurity management. Wang, Neil and Fenton (2020) [237] proposed the Extended FAIR-BN approach to cybersecurity risk assessment by implementing and extending the FAIR model to improve probabilistic risk estimation. Bayesian risk assessment methodologies (e.g., [236],[231],[237]) have as a main disadvantage that they refer to their partial subjectivity, the need for a potentially vast amount of training data and the difficulty of being applicable to new situations (subjective choice and Bayesian updates of the a-priori models).

Traditional risk assessment methods, such as the Spanish public sector "Magerit" open methodology and the French-developed "Mehari" risk management method of Clusif, provide a harmonised and structured risk analysis, asset-based and scenario-based, respectively [238]. Most



of these methods and tools apply the commonly known rule of thumb "risk = probability x potential damage" [239].

BowTie is a risk analysis method with a wide use, such as the research works in [240]-[243]. The traditional BowTie method is globally used in risk analysis, but it inherits limitations from fault tree analysis (FTA) and event tree analysis (ETA) [240]. It struggles to represent the complexity of modern systems, especially under uncertainty and when technical, human, and organisational factors are not fully integrated into barrier and human error assessments [240]. The CORAS method allows the incorporation of several different risk assessment processes the recognition of the probability of an attack is done a-priori to any risk assessment and not automatically [244]. Nonetheless, the CORAS method does not provide for the frequency of reassessment and continuous risk management [244]. Another credible approach based on the collaboration among organisations is the Cyber/Physical Security Management system (CYSM) approach [245] The MEDUSA's research method [246] sets a number of concepts, algorithms, and tools evolved from research, specially designed to protect the IT infrastructure and associated systems. According to MEDUSA, choosing the right method and the right tool for risk analysis and risk evaluation proves to be complicated.

Thamarai Selvan and Ambikapathy (2025) [247] review cybersecurity risk management literature and identify key research gaps and limitations in existing approaches:

- Lack of standardised and unified risk assessment frameworks across domains.
- Limited quantitative and data-driven approaches, with heavy reliance on qualitative expert judgement.
- Insufficient handling of dynamic and evolving cyber threats in real time.
- Weak integration between risk management and emerging technologies (e.g., AI, automation, cloud/IoT environments).
- Poor support for supply chain and interconnected system risks.
- Limited scalability to complex, large-scale ICT environments.
- Inadequate integration of risk management with organisational decision-making and governance.

## **4.4 Risk Metrics and Prediction Measurements**

The current section aims to present the major variances of risk management metrics to calculate cyber risks on ICT-related assets. In addition, it reports on measurements to estimate the cascading effects, risk propagation and risk prediction for assessing the impact of an attack realisation to interconnected ICT infrastructures.

### **4.4.1 The risk metric variance**

The risk calculation as stands in many risk assessment methodologies, is the outcome of the probability of a threat to materialise and the impact on the organization or infrastructure.

“Measurement” is the process to determine a value whilst “measurement method” is assumed a logical sequence of operations, described in generic, that aims to quantify an attribute with concerns a specified scale [53]. The goal of a risk metric variance is to develop a benchmark that is capable of measuring the security risks in terms of improving their capacity of transparency and thus increasing the ICT infrastructures resilience. A measurement system may target at estimating the performance of ICT infrastructures and providing suggestions for improvement. Effective and valuable metrics should count on quantitative models, be objective, reachable, iterative, report concerning time relying on a formal model of a standardised approach.

As presented in Section 4.1, cyber risks can be characterised in terms of likelihood or in terms of consequence or a combination of these two variables to measure security risks. Cyber risks can impact ICT infrastructures on firm performance and they are highly dependent to the implemented mitigation strategies [248]. Complex ICT infrastructures participating in supply chain networks may adopt various and different types of measurements to calculate risks, i.e. assessment measurements (e.g. threat taxonomies and vulnerabilities labeling), mitigation strategies, risk classification enablers and consequences due to multiple, heterogeneous features the ICT interconnected infrastructures engage as they operate for different industries [248]. To manage cyber risks, there are two main types of strategies; resilient, which are reactive-based, such as contingency planning and continuity of operations (COOP) [249] that focus on recovering after a disruption and robust which aim to keep the ICT infrastructures performance during the disruption [250].

Cyber resiliency concerns a system’s ability to withstand and recover from cyberattacks. Behzadi, O’Sullivan, and Olsen (2020) [250] highlight that it can be assessed using metrics covering system performance, capabilities, adversary activity, and risk factors. Resilience scoring relies on threat modelling and can use data from real environments, simulations, or expert judgement to evaluate outcomes such as vulnerabilities, impacts, and overall risk levels.

Cyber metrics are divided into static measures, based on established cybersecurity best practices, and dynamic measures, which reflect real-time system response and cyber resilience. They are often analysed using a Red-Blue adversarial model, where attackers (Red) and defenders (Blue) interact to evaluate mission effectiveness and system resilience [251].

In respect to dynamically risk level measurements, there are metrics for calculating the level of risk in global and complex environments delivering dynamic streams of information using inference rules and reasoning techniques to produce new knowledge outputs and thus increase the situational awareness and expand the limits of information reliability and trust [252]. Such semantic-based techniques generate knowledge representation through ontology development (risk ontologies). A dynamic risk management solution can help cybersecurity experts to better supervise ICT infrastructures concerning both real-time events and new threat knowledge [252].

Dynamic risk analysis is considered an iterative process of identifying, analysing and assessing information sources and risks in a system or organization dynamically and in a (near) real-time manner [253]. It is performed for information only available at runtime to accurately identifying and estimating risks towards rapidly changing circumstances and not throughout the entire

lifecycle of ICT systems as traditional static methods do. Cheimonidis and Rantos (2023) [253] review dynamic cybersecurity risk assessment approaches and show that Artificial Intelligence/Machine Learning (AI/ML) techniques and Bayesian networks are widely used, particularly in intrusion detection systems. They also find that these models commonly rely on vulnerability data inputs and are typically validated through case studies or simulations.

Risk assessment methods are generally classified as qualitative, quantitative, or hybrid. Qualitative methods, such as the research work in [242], use descriptive scales (e.g., low/medium/high) to assess likelihood and impact but lack precise measurement and often ignore interdependencies. Quantitative methods, such as the research work in [241], rely on numerical data and mathematical models to estimate risk more precisely. Monte-Carlo simulation approaches, such as the work in [254], are capable of performing a deep analysis on the uncertainty subjects. A main issue of quantitative risk assessment is that in most cases, data taken for the analysis can be insufficient data or there is a great majority of variables that impede the analysis process. There are remarkable examples of recent semi-quantitative risk assessment approaches, such as the work of Amro, Gkioulos, and Katsikas (2023) [255]. Nguyen et al. (2025) [256] present a semi-quantitative risk assessment approach that combines qualitative judgment with quantitative estimation to evaluate risk levels, demonstrating its application from environmental hazards (rainfall-induced landslides) to assessing risk to people in buildings.

The dynamic probabilistic risk assessment method Diao et al. (2024) [257] conducts risk analysis for electric grid systems under cyberattacks. It proposes an approach to model and simulate the behaviors of critical entities engaged in ICT operations. The work of Wang, Neil and Fenton (2020) [237], mentioned in Section 4.3, is considered a hybrid approach, as it overcomes traditional FAIR limitations by combining quantitative data and qualitative-expert knowledge. It incorporates objective, historical, and numerical metrics into a probabilistic model while using subjective probabilistic, causal relationships, and organisational factors to bridge empirical data gaps. The research works in [240],[243] (mentioned in Section 4.3) are other indicative examples of hybrid risk assessment approaches.

The current thesis presents a hybrid risk assessment approach for estimating cyber risks in complex and heterogeneous ICT supply chain environments. It assesses the cyber risk at the asset individual level and the cumulated risk and evaluates the cumulated impact on ICT infrastructures that operate in an ICT supply chain service in case of a cyberattack, considering their interdependencies. Moreover, qualitative values are mapped onto probabilities using a semi-quantitative scale in light of estimating the probability that a vulnerability is exploited by an attacker with specified skills.

#### **4.4.2 Threat Taxonomies, threat measurements and vulnerability labelling**

In this section, threat taxonomies, threat measurements and vulnerability labelling practices are presented.

Threat taxonomies provide a common language for classifying cyber threats and supporting the identification of attacks and security incidents in ICT infrastructures. Widely used taxonomies are typically developed by CERTs or internationally recognised organisations.

The NIST SP 800-30 threat taxonomy [125] classifies threat sources and events to support risk assessment, distinguishing between adversarial, accidental, structural, and environmental threats. ENISA in [258] has provided through a comprehensive analysis and assessment a foresight of emerging cybersecurity threats. OWASP threat taxonomy [259], which is a threat modelling application for analysing the security of an application. STRIDE [260] is a threat categorisation, founded by Microsoft and utilised by WASP, for the identification of threats by classifying adversary's goals.

Concerning Cyber Threat Intelligence (CTI) representations, the OASIS STIX [261] standard represents and shares cyber threat intelligence in a structured, machine-readable format. It enables consistent description of threats and observations, supporting faster and more effective detection, anticipation, and response to cyber attacks, often used together with TAXII for automated information exchange. STIX 2.1 integrates frameworks, such as MITRE ATT&CK [142], a widely used knowledge base of adversary tactics and techniques based on real-world observations, supporting the development of threat models and cybersecurity methodologies.

The Cyber Kill Chain [145], developed by Lockheed Martin, is a framework for identifying and preventing cyber intrusions. It defines seven stages of an attack, helping analysts understand adversaries' tactics, techniques, and procedures and improving attack visibility.

The European Union Vulnerability Database (EUVD) [262], launched in 2025, provides a centralized repository for tracking cybersecurity vulnerabilities across the EU. It supports NIS 2 compliance by cataloguing vulnerabilities with severity ratings, sector impacts, mitigation references, and links to related MITRE CVEs, facilitating coordinated cross-border vulnerability management.

The WASC Threat classification [263] categorises web application threats into a set of common attack classes, providing a standardized framework for understanding and addressing web security vulnerabilities.

A major advancement in risk assessment is the incorporation of threat intelligence and machine learning technologies. These capabilities enable organisations to proactively identify emerging threats and vulnerabilities in near real time. Threat intelligence provides timely information on evolving attack trends, while machine learning techniques analyse large volumes of data to detect anomalous patterns and support the early identification of potential risks before they escalate.

OpenCTI [264] is a cyber threat intelligence platform that enables structured storage, management, and correlation of threat data to improve analysis and decision-making. MISP [265] is a collaborative threat intelligence platform designed for sharing, storing, and correlating indicators of compromise and cybersecurity information among trusted communities.

Security vulnerabilities are scored (enumerated and characterised) by their security attributes as well. The Common Weakness Enumeration (CWE) of MITRE [266] is a list of common language for software weaknesses and vulnerabilities. Its Common Weakness Scoring System (CWSS) delivers prioritisation of software weaknesses in a concrete, flexible, open manner [266]. The Common Weakness Risk Analysis Framework (CWRAF) is a collaborative, community-based framework for scoring software weaknesses hosting content of various business domains [267].

CPE (Common Platform Enumeration) [268] is a standardised naming scheme by MITRE used to uniquely identify hardware, software, and operating system platforms in a consistent format for vulnerability management. It is maintained by the MITRE Corporation and widely used in security tools (e.g., CVE, NVD) to link vulnerabilities to affected products. In this regard, MITRE provided the Common Vulnerabilities and Exposures (CVE) [140] providing an identification number to publicly known security vulnerabilities, which is supported now by the National Vulnerability Database (NVD) of NIST [269], a US Government repository of standards-based vulnerability information. The Common Vulnerability Scoring System (CVSS) [139] is an open industry standard for estimating the severity of computer system security vulnerabilities.

The OSV (Open Source Vulnerabilities) [270] is a database and service that provides structured, machine-readable information about vulnerabilities in open-source software to support automated vulnerability tracking and dependency security management. GitHub Advisory Database is a curated collection of security vulnerabilities in open-source dependencies, used to provide alerts and automated dependency security updates within GitHub projects [271].

MITRE CAPEC [272] is a Common Attack Pattern Enumeration that aims to enhance the security knowledge with known attack patterns carried out by cyber criminals to exploit known weaknesses on cyber assets. The Process for Attack Simulation and Threat Analysis (PASTA) is a risk-centric methodology that models cyber attacks from the attacker's perspective to identify threats, simulate attack scenarios, and evaluate business impact for informed risk-based decision-making.

VERIS (Vocabulary for Event Recording and Incident Sharing) [273] is a structured framework for classifying and describing cybersecurity incidents using a standardised set of attributes, enabling consistent incident reporting, analysis, and threat intelligence sharing. The CSIRT incident classification sets guidelines required for Computer Security Incident Response Team (CSIRT) Incident Managers (IM) to clarify the case category, the level of criticality and sensitivity for each specific CSIRT case.

#### **4.4.3 Attack modelling and attack prediction**

Threat assessment is considered the process of formally evaluating the level of threat to an information system or enterprise and clarify the nature of the threat. As mentioned in Section 4.4.2, threat modelling contributes to the evaluation of risk metrics, during the risk management procedures. Threat Modelling can utilise Attack Trees or Attack Graphs, which are well-established approaches to employ threat scenarios during the risk assessment process [249]. A vulnerability assessment is an overall estimation of assets security weaknesses through which the existing and potential threat landscape within an ICT network can be valued. The development of threat scenarios is able to delineate the underlined threat landscape and thus facilitate the threat knowledge and improve the visualisation [249].

Attack modelling is considered a useful tool in risk assessment of supply chain complex cyberphysical systems (e.g., SCADA systems) [222]. On such systems, attack vectors are strongly dependent on considerations regarding the technical and operational environment where an attack takes place. On this account, attack graphs are data structures that are able to model all

possible avenues of a network attack. Attacks on ICT systems may cause disruption or decelerate the performance of an ICT supply chain service. Attacker's profile is a parameter of in-depth security risk analysis to identify security risks in large-scale networks, such as in ICT supply chains. The attacker's profile [152],[165] in compound networks of ICT supply chain services appears to have one or a combination of the following characteristics. Attackers increasingly target ICT stakeholders and third-party vendors with weak or outdated security controls to gain initial access [1]. Once compromised, these entry points are used to move laterally into the wider ICT network of the supply chain [1],[9],[274]. Breaches may involve malware insertion into software updates or stolen credentials that enable unauthorised remote access, ultimately allowing attackers to infiltrate connected organisations [274]-[275].

To evaluate the vulnerability of ICT networks the effects of interconnected relations must be considered. A typical process of vulnerability analysis can be conducted via scanning tools identifying individual vulnerabilities. Attack graph paths represent sequences of atomic exploits that an attacker uses to progress toward a malicious goal, such as gaining administrative access to a critical system. They are widely used for security analysis, including detection, defense planning, and forensic investigation. Attack modeling began in the late 1980s as a manual process for estimating cyberattacks, which was time-consuming and error-prone [276]. In the late 1990s, automated attack graph generation emerged using mathematical models, and modern approaches use attack graphs to identify possible attacker paths and support cyber defence and prevention [277].

Attack graph metrics are grouped into structural, probabilistic, time-based, and stochastic measures to evaluate network security and attacker progression. Attack graphs model systems as directed graphs where nodes represent states and edges represent exploits leading to more compromised states. They are used to analyse attack paths, showing systems dependability, and complex multi-step attack sequences [278] through probabilistic and quantitative methods [279], especially for large-scale networks. They can become highly complex even for small networks [279].

Dependability includes attributes such as availability, reliability, safety, confidentiality, integrity, and maintainability [280]. Ahmad et al. (2023) [280] explore the concept of dependability in 6G networks by reviewing its key attributes, including reliability, availability, safety, security, and resilience. They discuss the impact of emerging technologies, such as AI, edge computing, and network slicing on network dependability and identify future research challenges for building secure and resilient 6G communication systems [280]. Zhang et al. (2024) [281] present a stochastic, data-driven attack model targeting critical data of cyberphysical systems and propose defense strategies that enhance system resilience by prioritising the protection of important information.

Attack graphs model multi-step, vulnerability-based attacks. Traditional reliability methods include block diagrams and fault trees, while more advanced approaches use Markov models and Bayesian attack graphs for dynamic risk analysis and defence optimisation. Block Diagrams and fault trees aim to ensure that a service is operating correctly, covering the "absolutely necessary" [282]. For instance, the research work in [283] introduces a tri-level optimisation model

to evaluate the performance of power systems for their optimal defending resource allocation to enhance cyberphysical security.

Sophisticated approaches rely on Markov models, such as the research work in [279] and the augmented Markov Game framework, which models coordinated multi-agent attacks under progressive detection [284], and fuzzing-driven attack graph generation frameworks [277]. The Hidden Markov Model (HMM), Variable Length Markov Model (VLMM), and Variable Order Markov Model (VOMM) are diverse variants that are utilised for attack prediction [285]. Moudoud et al. (2022) [286] propose a novel AI-based detection and prediction HMM-based module that observes the behaviour of IoT devices and predicts their future actions. The module aims to improve detection accuracy and reduce detection latency compared to existing false data injection attack detection methods. An approach of a Markov model-based cybersecurity framework for exploitability analysis using the Common Vulnerability Scoring System (CVSS) data provides vulnerability estimations and predicts cyberattacks [287]. Amin et al. (2021) [288] present a cyber deception approach for predicting the most likely sequence of attack paths and deploying decoy nodes along the predicted paths. The approach employs transition probabilities in HMM to predict the attack path. It combines reactive (graph analysis) and proactive (cyber deception technology) defence, aiming to encounter the attacker's lateral movement. To this end, HMM-based models have been extensively employed to estimate Multi-Stage network Attacks (MSAs); nevertheless, determining the optimal training parameters remains a significant challenge [289].

Bayesian attack graph generation for dynamic security risk management is presented in [290] and [291]. Specifically, the research work in [290] introduces the RTECA (Real-Time Episode Correlation Algorithm) method, aiming to detect MSAs by correlating security events in real-time. The framework was tested on a DARPA dataset and observed a high accuracy of results. The research work in [291] proposes a Bayesian Network-based framework for predicting cyberattacks by combining conventional cybersecurity indicators with unconventional external signals. The approach does not solely rely on intrusion detection systems or system logs. The authors explore whether publicly available information can enhance the attack prediction estimation.

The fault/event trees, the Markov model-based and Bayesian network approaches are different methods to predict cyberattacks on the basis of low levels of alerts. A limitation of these methods is that they either require to capture expert knowledge to generate the attack plan or indicate the use of ML algorithms to train such models frequently for each incoming alert [285].

Topological Analysis of Network Attack Vulnerability (TVA) builds a so-called exploit dependency graph that contains information about conditions of an exploit and then searches this graph to combine various vulnerabilities [292].

Multihost, multistage, Vulnerability analysis (MulVAL) is an open-source automated network security analysis framework driven by logic programming. It relies on modelling, simulation, and generation of logical attack graphs across enterprise networks. It is a network security analyser based on Datalog which encodes all vulnerability and configuration related information as

Datalog facts [292]. A reasoning engine captures components' interactions across the network [292]. Several attack graph approaches adopt MulVAL [293]. Li and Li (2021) [294] provide an optimisation algorithm using the MulVal attack graph considering atomic attack weight and attack distance for acyclic attack graphs and the cost versus benefit of security reinforcement. Stan et al. (2022) [295] present a MulVAL-based approach that models attacks in the design stage of network protocols, and specific industrial networking architectures.

The Network Security Planning Architecture (NetSPA), originally developed by researchers at MIT Lincoln Laboratory in 1979, is a highly scalable, automated system designed to efficiently generate worst-case attack graphs [296]. NetSPA models how an attacker can navigate through an enterprise network by chaining together software vulnerabilities, trust relationships, and firewall configurations [292],[297]. The exploration of attacks based on threat intelligence data is collected using cloud-based web service in [298]. The attack surface classification methodology of mobile malware with known threat actors through automated tactics, techniques and procedures (TTP) and IoC analysis is described in [274],[299].

Simulation techniques can facilitate the assessment environment and deepen the analysis of attacks. A simulation-driven approach is a composite process aiming to discover and execute possible attack paths, based on a suitable formalism. Attack graphs model the attack steps, executed by a set of threat agents to produce risk-related results and allow the subsequent simulation. Several studies use testbeds or simulations when applying attack graphs to assess the vulnerabilities across assets within the ICT networks [293]. To this end, a thorough analysis of attack graphs is required in the vulnerability assessment on communication networks, such as IoT networks [293]. Dynamic simulation models, can provide more accurate predictions relying on as many involved simulation models as possible.

Autonomous AI agents can adapt attack strategies dynamically in real-time based on network defense reactions. Reinforcement Learning (RL) has gained increasing attention in cybersecurity due to its ability to autonomously learn effective strategies for detecting and mitigating previously unseen cyberattacks [300]-[301]. Unlike Supervised Learning, RL learns through interactions with the environment and trial-and-error, making it well suited to dynamic cybersecurity scenarios where labeled data are scarce and threats continually evolve [301]. Li, Fayad, and Taylor (2021) [302] introduce the Cyber Gym for Intelligent Learning framework, specifically designed to train and evaluate autonomous Deep Reinforcement Learning (DRL) agents to enhance adversarial attack simulation for cybersecurity with real-life scenarios from MITRE ATT&CK [142]. Oh, Kim and Park (2024) [301] propose a modified DRL framework to enable realistic, unpredictable attack simulations mapped directly to real-world tactics.

Dynamic graph and architecture modelling approaches can explore how a cyberattack dynamically alters the topology or conditions of a target network. Wang, Xiong, and Wang (2024) [303] use Bayesian attack graphs combined with digital twins to dynamically predict and visualise evolving attack paths in industrial environments. Iturbe et al. (2024) [304] introduce a simulation-driven framework that utilises graph-based threat modeling to evaluate and execute attack paths.



Multi-agent and risk decision simulations significantly advance attack modeling by shifting the focus from static, predictable vulnerability checklists to dynamic, strategic, and human-like confrontations. Armenia et al. (2021) [305] present a dynamic simulation-based framework to assist SMEs in evaluating cyber risk exposure and assess the cost-effectiveness of different cybersecurity investments. Piplai et al. (2022) [306] propose a knowledge-guided two-player reinforcement learning framework that models cyberattack–defense interactions as a competitive simulation game, enabling agents to learn adaptive attack and defense strategies. The approach integrates domain knowledge to improve learning efficiency and realism in simulated cybersecurity scenarios.

Traditional data mining methods such as ML, deep learning, and statistical approaches are often insufficient for coping with rapidly evolving cyber threats [301]. This motivates a shift toward scenario-based, expert-driven decision-making and highlights the need for continuous cybersecurity research and innovation to address increasingly dynamic attacks [301].

#### **4.4.4 Cascading effects and limitations**

There are multiple causes of cascading failures. In some domains, the cascading behaviour can be identified to model cascading failure adequately. General observations of cascading failures underline the distinction of two phases: the slow cascading phase, in which the system seems to carry out a proper operation, and the fast cascading phase where the system is out of control.

A variety of the existing studies are focused on the modelling of interdependent networks and theoretical analysis of the cascading effects. The theory of random graphs analyses behaviours in real-world networks [307]. It has been typically used to investigate single networks. Nevertheless, a framework which identifies important topological properties of large-scale networks which vary under different scenarios is described in [307].

Another generic characteristic is the difficulty of measuring the impact of cascading failures because of the high complexity and many indirect costs. The literature reviews limited data available on incidents that caused cascading effects. Whenever possible, historical data is used in combination with expert knowledge to keep the number of assumptions limited. Concerning cascading failures in ICT complex networks, most current studies involve only single network models because it is difficult to represent real-world network systems of supply chains, which engage multiple attributes and functions and interdependent network models [308]. Panda and Bower (2020) [309] investigate and analyse correlations between traditional risks of critical infrastructures (according to the Sendai framework) and cybersecurity risks with corresponding cascading effects to identify characteristics of complex and interrelated shocks and stresses.

Following the analysis of Section 4.4.3, cascading effects models are broadly classified into topological, stochastic, dynamic simulation, and agent-based approaches for analysing risk propagation in ICT infrastructures. Topological models focus on network structure, stochastic models simulate probabilistic failures, dynamic models provide detailed system-level simulations, and agent-based models capture interactions between entities. Each approach has strengths and limitations in accuracy, complexity, and applicability for real-time risk prediction.

From the literature review [282],[285],[292],[299],[310] the key strengths and limitations of each cascading failure modelling approach are presented in the following:

### **Topological models**

- Strengths: Simple, general, scalable, and applicable across different types of networks.
- Limitations: Even using Graph Neural Networks (GNNs), which learn the complex structural patterns of millions of nodes without manual feature engineering and predict the impact of a structural node failure with much higher precision, topological models are oversimplified; often ignore system dynamics and may give inaccurate or ambiguous results for specific domains.

### **Stochastic models**

- Strengths: Capture uncertainty and probabilistic behaviour; useful for simulation and prediction of failure propagation. AI models can dynamically adjust failure probabilities over time based on real-time telemetry streams, accurately capturing time-dependent, non-linear uncertainties.
- Limitations: AI is entirely dependent on data quality. Thus, trained on poor historical failure data can make incorrect assumptions about network behavior and its probabilistic predictions can be incorrect. Training deep probabilistic models requires massive computational power.

### **Dynamic simulation models**

- Strengths: High accuracy; capture system behaviour, interactions, and mitigation actions in detail. AI-based approaches act as a "surrogate model," drastically cutting down the computational expense. This allows highly detailed system-level simulations to run fast enough for real-time risk prediction, solving complex, computationally expensive, and often unsuitable for real-time analysis.

Limitations: While AI can help speed up specific calculations, high-fidelity dynamic simulations (e.g., Hardware-in-the-Loop) still require enormous processing power. Running a full-scale, accurate simulation of a major cyberphysical infrastructure attack in real-time remains a massive engineering hurdle [311].

### **Agent-based models**

- Strengths: Highly detailed; model interactions between individual entities and support rich "what-if" analysis. AI allows the agents to learn from their environment, adapt their behavior dynamically, and discover unexpected cascading paths that human programmers would never think to hardcode.
- Limitations: DRL and Multi-Agent RL algorithms require significant modelling effort and data; can become complex and hard to validate or generalise. Even when DRL model is used for agents [302],[306], the model can become a "black box." It is incredibly difficult to mathematically prove or validate why an AI agent made a specific choice. Training these agents requires millions of simulation steps (high data/effort), and an agent trained on

one specific network layout usually fails to generalise when moved to a different network architecture.

There is a research gap in cybersecurity guidelines and evidence-based methods for accurately predicting attack impacts. Predictive analytics addresses this by using ML and anomaly detection to identify threats in real-time without known signatures, improving early warning capabilities. Nonetheless, effective predictive risk metrics for dynamic and evolving vulnerabilities remain limited, and the application of advanced analytics is still in early development stages. Despite the multiple existing works on such topics, *there is still ground for research to investigate methods that focus on extending the risk impact analysis in complex ICT networks.*

The proposed cybersecurity risk management methodology, estimates the vulnerability exploitability across networks of ICT supply chain services considering intrinsic vulnerability characteristics and attacker's specific attributes and estimates the impact, including ICT experts knowledge. It follows an evidence-based approach to estimate credible vulnerability chains based on a confirmed security event.

#### **4.4.5 Knowledge Risk Management and ontology models**

Ontology-based solutions support dynamic security assessment by modelling and analysing cyber threats to improve risk understanding and situational awareness.

Sánchez-Zas et al. (2023) [312] propose an OWL ontology-based framework for real-time risk management and cyber situational awareness, enabling structured representation of security knowledge to support timely threat assessment and decision-making in dynamic environments. They use SPARQL rules to infer knowledge and estimate dynamically the risk level. Preuveneers and Joosen (2024) [313] propose an ontology-based cybersecurity framework designed to support AI-enabled systems by structuring security knowledge for improved reasoning, threat detection, and decision-making. The framework relies on OWL representation of the STIX 2.1 standard [261] of OASIS. It aims to enhance cybersecurity across AI-driven applications by enabling more consistent and automated risk assessment. Martins et al. (2022) [314] propose a framework for the conceptual characterisation of ontologies, aimed at systematically describing and comparing ontology features and structures. The framework is applied to the cybersecurity domain to support clearer ontology design, evaluation, and reuse in security-related applications. Oliveira et al. (2022) [315] propose an ontology-based model of security focused on risk treatment, providing a structured conceptualisation of security controls and mitigation strategies. The proposed Reference Ontology for Security Engineering (ROSE) aims to improve the clarity and consistency of representing security risk treatment decisions within conceptual modeling frameworks.

Knowledge Risk Management can have a significant value on ICT supply chain organisations performance expanding the borders of the enterprise's innovativeness, responsiveness, sustainability, and agility [316]. Adopting knowledge management techniques in risk management can facilitate academic researchers and practitioners to better comprehend the risk management processes [316] against the evolving threat landscape in the ICT ecosystem.

Kovačević and Radenković (2020) [317] present the SAWIT approach aiming to improve the cybersecurity knowledge of employees by using collaborative learning and assessment within the specified knowledge transformation model. The approach utilises the Nonaka and Takeuchi's knowledge conversion SECI model [117]. Neto et al. [318] present a systematic literature review of knowledge-based risk management approaches, exploring how knowledge representation and management techniques support risk identification, assessment, and decision-making. The review highlights existing methods and identifies research gaps, such as:

- Limited comprehensive frameworks that effectively combine the above risk management areas.
- The lack of a widely-adopted model or ontology for capturing, sharing, and reusing risk knowledge across projects and organisations.
- Existing methods often rely heavily on expert judgment, with limited use of intelligent reasoning or automated knowledge inference.
- Many proposed approaches have been evaluated only through case studies or conceptual examples, with little evidence from large-scale industrial deployments.
- Most solutions are designed for static risk assessment and do not adequately capture evolving risks or facilitate continuous knowledge updates.

*In complex ICT networks, knowledge risk management can enhance decision-making and strengthen organisational performance, agility, and resilience, while integrating knowledge management techniques helps better address evolving ICT risks.*

The current dissertation employs ontology-based models to excavate meaningful risk knowledge (both implicit and explicit) of the ICT ecosystem and their interdependent ICT infrastructures. The models articulate and externalise cybersecurity information using knowledge structures, semantic relations, reasoning capabilities and modelling visualisation techniques aiming to increase the organisational learning of ICT stakeholders and enhance their understanding of ICT infrastructures' interdependencies and their security specificities across the networks of ICT supply chain services.

## **4.5 Disruptions and security challenges in ICT supply chains**

The section identifies critical topics that can lead to a supply chain disruption. Disruptions are analysed in the context of the supply chain performance. Challenges and requirements related to supply chain security and risk management are discussed, including the specific case study of Maritime and Logistics Supply Chain (MLoSC) security.

### **4.5.1 Causes leveraging ICT supply chain discontinuity**

Globalisation and digital transformation have expanded and interconnected supply chains, improving efficiency, visibility, and collaboration while increasing system complexity and uncertainty [6]. However, strong ICT interdependencies also amplify the impact and propagation

of disruptions across ICT supply chain networks. These disruptions range from routine operational issues to rare but high-impact “black swan” events, which can cause severe and unpredictable long-term consequences [72]. Black swan events can be triggered on different accounts, such as warfare and terrorism (e.g. 9/11 terrorist attack), natural disasters (e.g. the 2019–20 Australian bushfire season colloquially known as “Black Summer”), etc [72].

A recent example of a black swan event is the COVID-19 pandemic, which severely disrupted global supply chains, caused major economic losses, and led to widespread fatalities. Its full impact on supply chain performance remains uncertain, but it triggered significant disruptions such as plant closures, supply shortages, and cascading effects across interconnected networks. The pandemic also created extreme demand uncertainty, illustrated by events like the negative oil prices in 2020 due to reduced consumption during lockdowns [72]. Overall, COVID-19 demonstrated how black swan events can propagate across global supply chains, producing long-lasting, multi-level disruptions and domino effects.

Supply chain operations can be disrupted partially or entirely by various factors, including organisational changes, financial and economic instability, and demand uncertainty such as the bullwhip effect [319]. Additional risks arise from social unrest, regulatory issues, and geopolitical tensions, all of which can significantly impact supply chain performance, continuity and reliability of critical services, affecting economic and societal functions. They can result from physical attacks, cyber intrusions, or combined cyberphysical threats, sometimes leading to severe consequences such as system compromise or loss of life [95].

The NIS 2 Directive [12] assesses incident impact based on users affected, duration, and geographical scope, while increasing reliance on interconnected digital assets has made supply chains more vulnerable to emerging cyber risks. Thus, the management of modern ICT supply chains should rely on effective, efficient and up-to-date security policies that analyse how to improve the Critical Information Infrastructure (CII) protection and raise their preparedness. On this account, the emerging security issues on network and information systems create a compelling need for closer and tighter international relations and collaborations that are envisaged to improve the current security standards, facilitate the information exchange (NIS 2 Directive), create competence networks, synergies of trust and build a global roadmap that will reflect the various multiple aspects of security.

#### 4.5.1.1 Barriers in the supply chain service performance

Globalisation has expanded the geographical scope of supply chains, creating diverse communication channels across long distances. This expansion creates a variety of reasons to trigger a supply chain disruption (i.e., ubiquitous business changes, financial/micro-/macroeconomic factors, implementation of legal/regulatory or geopolitical or social risks, etc.) [6]. Consequently, ICT supply chains are confronted with the following challenges [2],[6],[84]:

- Interconnected ICT supply chain networks raise the complexity and uncertainty of the supply chain systems. CII interdependencies among complex ICT networks leverage the potential impact and its propagation in case of a supply chain disruption.

- Supply chain interruptions can be divided into operational (i.e., lead-time and demand upsets) and disruptions caused not so frequently but can have long-term impact on the supply chain performance when they occur with long-lasting propagation (i.e., a black swan event, such as the COVID-19 outbreak).
- Implementation of security risks: the exploitation of physical, cyber or combined threats from adversaries impinges on the supply chain's regular performance, which can in some occasions lead to tremendous results (i.e., physical or environmental disaster, human injuries).
- Implications of security disruptions are categorised into the following parameters: (i) the number of users affected by the disruption, (ii) the incident lifespan and (iii) the geographical spread concerning the area affected by the incident.
- The multiple asset interdependencies over interconnected supply chain systems increase the security threats and their propagation, requiring a rigorous protection of their security.

Supply chain disruption can be eliminated or encountered:

- By modern ICT supply chain environments that rely on effective, efficient and up-to-date security policies focusing on the CII's protection and on improving their preparedness.
- By structuring strong long-term relationships among supply chain operators.
- Stronger collaborations of composite expertise and mutual brainstorming can leverage the quality of the current security standards, facilitate the information exchange, and analyse deeper all aspects of security.

#### 4.5.1.2 Attacks in modern ICT supply chains

Over the last decades, the management of security in supply chains has turned out to be a complex process because of the increasing involvement of digital resources (e.g., information systems, IoTs, cloud computing, etc.) and the rising number of multiple entities collaborating through their heterogeneous systems for the operations of a supply chain, that can be even from different Industry sectors (such as energy, transportation, IT, government, maritime industry, etc.) [6]. The multimodal technology, interactive software capacity and sound exposition to information overload challenges the threat landscape, turning it into a new reality. ICT supply chains are becoming attractive targets of skilled adversaries who are proficient at committing sophisticated attacks of tremendous and long-term consequences, both physical and cyber [2],[4],[275],[320].

The 9/11 terrorist attack is a serious physical attack example that provoked a few thousand fatalities and injuries, which additionally cost nearly 10000 cancer diseases within the last seventeen years to first responders and other people who were in the World Trade Center area by that moment and impacted economically the global supply chain [275]. Somali piracy, a socio-political, environmental and commercial threat, hit the busiest shipping lines of the maritime supply chain. Sophisticated cyberattacks are gradually evolving and intensifying [4], [275]. For

example, the ransomware WannaCry NHS attack in the spring of 2017 cancelled more than 19,000 healthcare appointments in the UK and cost the NHS £92m and shut down around 200,000 computers in over 150 countries, demanding ransomware payments to recover [275]. EasyJet's nine million customers' email accounts' compromise in May 2020 by hackers enabled them to obtain access to personal travel information, including over 2,208 customers' credit card details [321].

Geopolitical changes and ongoing military and political conflicts, such as the Russia-Ukraine war, the Israel-Palestine conflicts, increased cyberattacks, whereas the potential of personal data leaks threatens the global digital economy.

Considering the increasing digitalisation of ICT supply chain operations and the highly interconnected nature of modern supply chains (see Section 2.1), the impact of cybersecurity incidents has become more significant than ever. Such incidents can lead to data breaches with severe socio-economic consequences, compromise the security and resilience of ICT supply chains, disrupt critical political and economic activities, cause environmental damage, and, in extreme cases, threaten human life [6],[275]. In this sense, new potential entry points for cybersecurity risks (e.g., obsolete security infrastructure or outdated hardware/software, infected devices on a corporate network, and lack of appropriate security protocols across partners) can be exploited by actors (e.g., cybercriminals, Anonymous, LulzSec hackers, cyber espionage role-players, and extortionists) by any means, such as by realising APT attacks to reach sensitive data using sophisticated tools which hurdle the possibility of these cyber aggressors being identified [4],[6].

Multiple attack vectors pertain to a supply chain attack performance involving the application layer, social engineering, unauthorised access, malicious code, and reconnaissance and networking-based service attacks that take advantage of applications, host and client operating systems, and even networking equipment [4]. In this context, adversaries use such techniques to catch valuable data assets (i.e., financial transaction information, user credentials, insider information, etc.) either within the cyber-mature ICT organisations or using them as a stepping stone to bypass the organisation's boundaries and intrude on other entities by exploiting vulnerabilities of the interdependent ICT infrastructures across the supply chain [4].

#### 4.5.1.3 Open security issues in ICT supply chains

Current section aims to address open issues related to security in modern ICT supply chain environments.

As described in the previous sections, nowadays, adversaries may be able to commit sophisticated attacks in large-scale networks of ICT supply chain services. For example, attackers may disrupt smart grid operations by gaining unauthorised access to remote power control systems and exploiting vulnerabilities in interconnected ICT assets to obtain elevated privileges. Other supply chain attacks may also result in data breaches and the theft of sensitive information.

In the new digital era, the protection of the interconnected ICT infrastructures is mandatory to prevent or mitigate the ICT supply chain's pressing security challenges [4]. In this vein, ICT

supply chain operators must deeply comprehend the nature of these challenges. Collaboration among ICT supply chain entrepreneurs to share and analyse information regarding past supply chain attacks [4] and their inherent risks could help them acquire such knowledge. Moreover, enterprise investment in cybersecurity remains relatively low, highlighting the need for a more comprehensive and proactive investment strategy (see Section 1.1).

Another important issue to ensure the ICT supply chain resilience is *to estimate the ICT supply chain risks concerning different aspects* (business, holistic-technical, and sectoral; see Section 3.5).

An ICT Supply Chain Service (SCS) may embrace multiple industry sectors (e.g., the Vehicle Transport Service, which encompasses Maritime Transport, Automotive, logistics industries, etc.). In this line, actors and components of *multi-sector ICT supply chains require thorough analysis considering their interdependencies*. Furthermore, the business entities involved and their business goals, the ICT processes, and the technical particularities and security specificities of the CIIs need to be explored from both interorganisational and cross-sectoral views within the ICT supply chain [15],[63],[322].

A risk assessment process incorporates subsequent steps of intermediate assessments regarding the estimation of the vulnerability level, threat level, risk level and impact level. Threats can be analysed in a twofold dimension: at process (business) level and at asset (operational) level. *The complexity of cyber assets of CIIs and their heterogeneity require both proactive and reactive practices along with evidence-based techniques and prediction analytics* to respond to frequent dynamic changes.

#### 4.5.2 ICT Supply Chain Risk Management

The literature reviews several challenges affecting the supply chain risk management of ICT/cyberphysical systems.

The work in [323] analyses how human task modelling techniques support the identification of cyber threats on supply chain operators' tasks. AlHarmali et al. (2024) [324] highlights key limitations in existing cyber risk assessment approaches. Many methods rely on oversimplified or non-comprehensive metrics for estimating impact and likelihood, which can lead to inaccurate risk evaluations. Some approaches consider only either the cyber or physical layer of a system when assessing impact, rather than both, resulting in incomplete analysis. Others equate likelihood with successful vulnerability exploitation, even though exploitation does not necessarily lead to actual system damage or a successful attack. Additionally, several methods determine overall risk based on a single factor, which can underestimate real cyber threats. Conversely, some approaches may overestimate risk because they fail to account for defensive measures that reduce system exposure. Overall, these gaps show that current methods often lack balanced, multi-factor, and defence-aware risk modelling [6], [324]. In addition, as discussed in previous sections, public threat intelligence can be outdated and may not reflect an organisation's specific context. Scenario-based methods often oversimplify complex cyberphysical environments and fail to accurately model real threat events. Thus, relying on past attack data is also limited, as it may not capture evolving threats or enable real-time learning (see Section 4.4.4). Additionally, expert judgements can introduce bias and heuristic errors, reducing the reliability



of risk assessments [323]. As a result, AlHarmali et al. (2024) [324] identify the following factors for effective risk assessment in cyberphysical systems based on the limitation derived from the systematic literature review:

- Well-defined risk model
- Trustworthiness of Cyber Threat Intelligence
- Consistency of Cyber Threat Intelligence Interpretations
- Automation support.

They emphasise in their work the need for a cyber risk assessment approach of more than a collaborative approach to leverage the risk assessment's effectiveness. In this vein, real-time learning from cybersecurity incidents can improve risk assessment by incorporating up-to-date, organisation-specific threat information [324]. Automation - especially through ML tools- enables continuous learning from incidents and threat intelligence, updating risk assessments as events occur (see Section 4.4.3). This reduces manual effort, minimises human error and inconsistency, and improves the collection, sharing, and use of cybersecurity knowledge.

Apart from network science, there are other approaches and methodologies that can be used to assess asset criticality within supply chain management [15]. Kim et al. (2025) [325] proposed a STRIDE-based threat modelling framework for distributed control systems (DCSs) in oil refinery environments. The identified threats were validated against realistic threat scenarios of DCSs, including Stuxnet, BlackEnergy 3, and Triton and corresponding mitigation strategies were presented. To combat the cyber threat evolving landscape targeting complex ICT networks, such as DCSs, approaches that minimise manual steps and subjective internal discussions by pivoting toward highly automated workflows are required. Dayarathne et al. (2025) [326] propose a hybrid deep learning-based cybersecurity framework that enhances the detection and mitigation of cyberattacks in smart cyberphysical power systems, thereby improving grid resilience and operational reliability. Zhou et al. (2022) [327] demonstrate a real-time hardware-in-the-loop simulation platform allowing users to dynamically configure DoS and data tampering attacks on power networks. Cherdantseva et al. (2016) [222] stress the need for more effective cyber-risk assessment approaches capable of capturing the complexity of cyberphysical systems. For example, AlHarmali et al. (2024) [324] found that existing risk-assessment methodologies for cyberphysical systems continue to exhibit limited effectiveness, insufficient validation, and shortcomings in risk quantification and operational applicability.

According to the aforementioned literature, most current risk management methods lack concentrating on a mounted technical perspective that takes into account the specificities of the ICT infrastructures. Within this framework, the existing approaches don't deepen the analysis in assessing the risks of the ICT supply chain elements. This is the main challenge that this doctoral thesis aims to contribute upon ICT supply chain risk management methodologies.

### 4.5.3 Security in the Maritime and Logistics Supply Chain

This section delves into sectorial security observations of critical industry sectors of the Maritime and Logistics Supply Chain (MLoSC).

#### 4.5.3.1 Disturbance in Maritime and Logistics Supply Chains

The Maritime and logistics sectors have been characterised as critical sectors of the EU economy [19]. The Maritimer Logistics Supply Chain (MLoSC) is considered the backbone of international trade and a key engine to drive globalisation [21].

The fusion of Maritime and Logistics Industries involves multiple players from both domains containing an exhaustive list of heterogeneous infrastructures. Disruptions in the MLoSC could have a serious impact in the Maritime and logistics industry sectors [1],[6],[84],[275],[320]: i) significant loss of cargo, ii) decrease productivity, iii) threaten the resilience of critical assets, iv) increase supply chain's costs, v) cause financial disasters, vi) harm the environment, vii) threaten the healthcare, and viii) jeopardise the maintenance of safety and security of citizens or governments. For example, a disruption in the oil tankering supply chain in 2010, due to an accidental oil spill realised by a seafloor oil gusher leading to the explosion of the BP's oil rig caused serious environmental harm killing 11 workers [328].

In the modern era of highly interdependent Maritime Logistics environments, a limited capacity of a process can affect the whole chain of processes causing a bottleneck upstream [72]. In addition, the lack of high-quality infrastructure or low-performing MLoSC services can generate extra costs for supply chain stakeholders [19]. In this regard, CIIs of the inland waterway network, required to be upgraded and enhanced with innovative technological models of intelligent multimodal transport systems [20]. Such investments could overcome these bottlenecks. Additionally, they could lead to the reduction of human errors and the provision of efficient and sustainable communication networks and drive the creation of new job opportunities. Thus, MLoSC stakeholders must reconsider their current structure and provide fundamental changes including the adoption of modern digitalised infrastructure skills [19]- [20]. A contribution to this effort could be the definition of common standards at EU level and the development of new cross-border relationships between EU countries [6], [18],[181].

The global digitalisation trend and the current regulation framework and policies ports are facing new challenges associated with ICTs [19]. As Ports tend to rely more on such technologies, new challenges appear in the area of Information Technologies and Operation Technologies [19]. Threats to CIIs, stem from different sources, including national actors criminal hackers, and cyberterrorists. During the last decade, maritime infrastructures have increasingly attracted the attention of adversaries [19],[103]. The increasing digitalisation and interconnectedness of maritime operations, including shared networks, IoT, and cloud services, have expanded attack surfaces and heightened the risk of cyberattacks on maritime cyber assets.

For example, a serious MLoSC disruption that concerns cyberattacks is the 2017 ransomware cyberattacks Petya, (or NotPetya) resulted in shutting down terminal activities in some commercial ports causing economic loss in leading shipping and oil companies worldwide, such

as AP Moller-Maersk [275]. To encounter these security threats, supply chain performance assessment is a key element. Summarising, the deficiencies of CIIs that can cause such disruptions in the MLoSC are:

- A limited capacity of a process can affect the whole chain of processes causing a bottleneck upstream. The application of intelligent multimodal transport systems could overcome these bottlenecks.
- The lack of high-quality infrastructure or low-performing MLoSC services can lead to additional costs.
- To face the previous issue, technologies of CIIs should be advanced with innovative technological models, which could cause the reduction of human errors, the provision of efficient and sustainable communication networks, create new job opportunities.
- Inland water transport has begun to lose its comparative advantage, which can be overcome with the adoption of modern digitalised infrastructure skills (i.e., definition of common standards at EU level etc)
- Port threats on CIIs, stem from different sources attracting more adversaries (i.e. national actors, criminal hackers, and cyberterrorists) as a result of the digital revolution (rapid technology evolution in the maritime industry evolves, transparent interactions among maritime operators are stored on shared network, etc).

#### 4.5.3.2 Maritime threats and coordinated attacks

In the recent years of digital evolution, cybercrime is highly increasing all over the world, deploying new methods, using advanced technologies and sophisticated weapons [4].

MLoSCs are complex cyberphysical systems, owned by different national and foreign infrastructures, ensuring seamless and swift product/data exchange from the producer down to the end consumer [1]. As described in Section 3.3.2, cargo ships are connected to ports and other MLoSCs operators through a plethora of communication and data links, such as satellite networks, conventional radio channels and GIS networks. Their navigation is widely reliant on electronic solutions, such as GPS satellite navigation; Galileo, the EU's independent global navigation satellite system (GNSS); Radar ARPA-Radio Direction and Ranging, and telemetry. SCADA systems, just-in-time systems, Automatic Identification Systems (AIS), the Electronic Chart Display and Information System (ECDIS), intermodal maritime-based logistics, transnational integrated information platforms and remote control mechanisms are maritime CIIs imposing a high security risk due to their data-interchange nature [19]. Such installations play a vital role in the maritime industry, as they analyse and display information related to maritime and logistics operations. SCADA systems have significantly improved logistics, maritime transport, and control operations by leveraging advanced automation and data analysis capabilities to reduce operational delays and achieve considerable cost savings [1].

The critical role of these systems in the operation of port critical infrastructures, coupled with the severe consequences of their compromise (e.g., through a SCADA security breach), makes cyber-

dependent maritime critical information infrastructures (CIIs) attractive targets for adversaries. Such attacks may facilitate a wide range of malicious activities, including sabotage, data corruption, piracy, terrorism, theft, and cyberphysical attacks, potentially leading to supply chain disruptions, human casualties, economic losses, political instability, and environmental damage [1]. For example, attacks on maritime SCADA systems may disrupt critical infrastructure, causing significant operational, economic, and human consequences (see attack scenario in Section 6.4.1). Cyberattacks targeting Port Community Systems (PCS) (e.g., by inserting a malware) may compromise LNG tanker operations, turning LNG tankers into floating bombs and creating detrimental consequences (see attack scenario in Section 6.4.2). Physical attacks (e.g., bombing) in a dry bulk storage area of coal products may create and carry dust by wind to tourist terminals or nearby residences. The potential of a coordinated physical or cyber and/or combined attack in a large port could have a dramatic impact on maritime transport, affecting the economy and social well-being on a global scale [1], [275].

To compromise cyberdependent maritime CIIs, adversaries employ sophisticated, multi-vector attacks that exploit vulnerabilities across both the cyber and physical domains [2]. A typical example of these types of attacks is the cyberattack in the port of Antwerp between 2011 and 2013 which aimed to hijack, divert, steal cargo [103]. Another example is the underwater drone attack in May 2019, where 4 motor tankers were attacked at Fujairah anchorage United Arab Emirates by drones with high grade explosives, what could be characterised as a hybrid maritime threat [329]. A series of maritime ransomware cyberattacks have been identified during the last decade [330], such as the significant data breach of the Svitzer shipping company (a tug operator subsidiary of A.P. Moller-Maersk) in March 2018, where sensitive individual information of nearly 500 Australian employees was exposed as a result of an 11-month active cyberattack [331]. On the 24th July 2018, American shoreside operations of Cosco Chinese shipping giant were hit by a ransomware cyber-attack, affecting telecommunication with vessels, customers and port terminals, including the Pier J terminal at the Port of Long Beach [330]. In June 2020, the Norwegian shipbuilder Vard was hit by a ransomware encryption cyberattack, causing a data breach to the Vard's Langsten shipyard [332]. A high-profile \$10 million ransomware attack targeting a major Adriatic maritime operator, which led to the massive exfiltration of sensitive safety plans, employee records, and operational networks occurred during December 2025-January 2026 [330]. The incident was executed by the Anubis cyber gang, who exploited known but unpatched vulnerabilities in web interface [330].

Cyber threats to maritime CIIs have evolved through time from financially motivated attacks to sophisticated campaigns conducted by hacktivists, APTs, and state-sponsored actors, such as Stuxnet, Flame, Conficker, DuQu, and APT1 [103]. In addition, Somali pirates have expanded their traditional methods of intrusion by employing hackers to gain access to shipping companies' databases and vessel tracking systems to identify vessels with valuable cargoes (thus, many ships that transit the Gulf region turn their AIS off to avoid tracking them). In this regard, to monitor a vessel's course, engineering experiments have demonstrated that low-cost GPS jammers can be used to change a vessel's course by interfering with its navigation systems (GPS, ECDIS, AIS) causing a trackline-following autopilot to inaccurately interpret the ship's position and alter its destination [103]. Moreover, a cyber intrusion can occur in the name of terrorism,

e.g., Russian Business Network [103]. Combating terrorism has been a top priority for the European countries and their ports within the past (e.g., November's 2015 coordinated Paris attacks, the 2016 Berlin Christmas market attack, the June 2017 London Bridge attack, the August 2017 Barcelona attacks etc.) [275]. Maritime cyberterrorism is not a fiction anymore, being a research area of limited academic research [103],[275]. Ports are considered soft targets due to inadequate security measures and limited adoption of advanced authentication and encryption mechanisms [330].

Within this context, the MLoSCs have garnered front-page attention. ENISA addresses the following threats as the most critical for the sector: eavesdropping, interception hijacking, outage, nefarious activity and abuse, physical attacks, failures and malefactions [102]. The EU has strengthened maritime critical infrastructure protection by implementing coordinated action plans (e.g., initiatives with NATO and UN, the CER Directive [155]) supporting cybersecurity research, and establishing policies to tackle illegal shipping and fraudulent operations in Ports and encounter physical, cyber, and hybrid threats.

The increasing sophistication of maritime cyber threats urges security officers and domain stakeholders to protect the MLoSC interconnected CIIs [12], which require adequate risk management techniques to ensure their integrity and safety [1]. Nonetheless, the maritime cybersecurity domain has yet limited research effort. Existing risk management policies in EU Ports are using their own disparate methodologies which hinders the comparison of risk assessment results among the Member States and greatens the appearance of cross-border multi-risks across the MLoSC [221]. The fragmented risk management practices and inability of existing approaches to comprehensively address the security requirements of maritime ICT infrastructures, stress the need for advanced, unified risk assessment and protection mechanisms for maritime CIIs [2],[6]. Effective maritime cybersecurity requires holistic risk management capable of assessing threat propagation, identifying vulnerabilities across interconnected CIIs, and enhancing security awareness through knowledge-driven approaches [84].

This dissertation proposes a cybersecurity risk management methodology that delves into the ICT infrastructure's technical specificities and security particularities, considering their interdependencies and extracting tacit security knowledge using knowledge management techniques. Maritime CIIs are use cases in the dissertation (see Section 6.4) to demonstrate and validate the methodology's applicability.

#### 4.5.3.3 Existing legislation in the maritime sector

This section reviews the principal legal framework governing the maritime sector across both the physical and cyber domains.

A key mandatory framework for physical security in the maritime domain is the International Ship and Port Facility Security (ISPS) Code, established by the IMO and implemented within the European Union through Regulation (EC) No. 725/2004 [333]. The ISPS code is an amendment to the Safety of Life at Sea (SOLAS) Convention (1974/1988) on minimum security arrangements for ships, ports and government agencies that came into force in 2004. It establishes measures to enhance the security of port facilities and ships by defining security requirements, assessment

methodologies, threat detection procedures, implementation guidelines, and the roles and responsibilities of relevant stakeholders.

The IMO's "International Convention for the Prevention of Pollution from Ships", the "MARPOL 73/78" Convention [334], is the primary international framework for preventing marine pollution from ships, addressing both operational and accidental sources of pollution through continuously updated environmental protection measures. The EU Directive 2002/84/EC [335] amends the Directives on maritime safety and the prevention of pollution from ships and on shipboard living and working conditions. In 2026, updates of the "MARPOL 73/78" framework were provided, including Mandatory Container Loss Reporting, New Arctic and Norwegian Sea Emission Control Areas, Stricter Fuel and Carbon Reporting, and Zero-Tolerance for Plastics [334], to improve shipping safety, reduce air pollution, and eliminate marine litter. Moreover, the International Convention for the Safety of Life at Sea (SOLAS), developed and maintained by IMO, establishes international standards for the safety, construction, equipment, and operation of ships, requiring flag states to ensure compliance with maritime safety requirements [336]. The IMO addresses maritime cybersecurity through the Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3/Rev.3) and Resolution MSC.428(98), which requires cyber risks to be incorporated into Safety Management Systems under the International Safety Management (ISM) Code [337]. These measures establish a risk-based approach for identifying, assessing, and mitigating cyber threats to ensure safe, secure, and resilient maritime operations [337].

Regulation (EU) 2025/2434 [338] strengthens the role of the European Maritime Safety Agency (EMSA) in supporting maritime safety, security, environmental protection, and digitalisation across the EU. It expands EMSA's responsibilities to address emerging challenges, including cybersecurity, resilience of maritime infrastructure, pollution response, and the implementation of EU maritime legislation. The Vessel Monitoring Directive, Regulation (EU) 2025/811 [339], mandates the electronic submission of insurance certificates for ships carrying dangerous or polluting cargo in EU waters. This directive enhances maritime safety and environmental protection by integrating these reports into the SafeSeaNet system. The EU Maritime Security Strategy, initiated in 2014 and updated in 2023 [340], strengthens the protection of the maritime domain by promoting cybersecurity, resilience of critical maritime infrastructure, situational awareness, and coordinated responses to evolving cyber, hybrid, and physical threats.

Sector-specific series of the ISO international standard that address maritime security topics. The ISO 28005 Part 1-3 [341] on Ships and marine technology standardises electronic port clearance by defining harmonised message structures, data exchange mechanisms, and interoperability requirements to facilitate secure and efficient information exchange among ships, ports, and maritime authorities. The ISO 20858:2007 [342] specifies guidelines for port facility security risk assessment and developing security plans to enhance compliance with the ISPS Code and improve maritime security. The ISO 28007-1 [343] specifies requirements and best practices for private maritime security companies providing armed security personnel on board ships, promoting consistent, safe, and accountable maritime security operations.

The "Guidelines on Cyber Security on Board Ships", version 4 (2020) [337], was issued by ICS, IUMI, BIMCO, OCIMF, INTERTANKO, INTERCARGO, InterManager, WSC and SYBAss. The

International Association of Classification Societies (IACS) “Recommendation on Cyber Resilience (Rec. 166)” [337] consolidates safety standards for shipboard computer-based systems. In 2021 and 2022, the International Association of Ports and Harbors (IAPH) published official cybersecurity and resilience frameworks for Ports and Port facilities and emerging technologies for the Maritime Supply Chain, respectively [337]. In addition, the Det Norske Veritas (DNV) provides the “Cyber Secure” class notation framework for assessing and certifying the cyber resilience of a vessel’s digital systems [337]. ENISA has published the guidelines of “Cyber Risk Management for Ports” [102] and good practices for “Port Cybersecurity” [344] for safeguarding interconnected ICT and OT systems.

#### 4.5.3.4 Knowledge Management effort in the Maritime and Logistics Supply Chain security

Knowledge management has received increasing attention from maritime logistics specialists to support organisational learning, identify and adopt best practices in supply chain operations, and enhance overall operational expertise and business performance [20]. Although knowledge management is viewed as a strategic asset that can enhance the Maritime and Logistics Supply Chain (MLoSC) performance, its role in intermodal MLoSC services remains insufficiently understood despite increasing adoption in the sector [345]. Despite ICT systems enable sharing of explicit information, tacit knowledge is harder to transfer, creating a need for better knowledge management methods to externalise it and improve security awareness in the MLoSC [346]. Furthermore, according to [346], existing research on sustainability and knowledge management in the maritime logistics industry primarily focuses on internal operations of SMEs, limiting its broader applicability.

Ontology-based models have been proposed within the last decade to structure and formally represent cybersecurity maritime concepts, analysed in [84],[95],[97]. In addition, Bondareva et al. (2026) [347] present an ontological model for cargo port risk management that enhances knowledge representation, risk analysis, and decision support for maritime security and resilience. Sumić et al. (2024) [348] discuss the need for a robust and interoperable information infrastructure to support autonomous ships, which rely on AI and intelligent agents for navigation and operation. They propose the use of ontologies to enable semantic interoperability between ship systems and demonstrates their application through an example ontology for autonomous vessel firefighting systems. Hutschenreuter et al. (2021) [349] present an ontology-based framework for cybersecurity and resilience that enables structured knowledge representation, supports threat and risk analysis, and improves decision-making for protecting complex cyberphysical systems. Arrigan, Emmitt, and Singer (2022) [350] investigate the use of ontologies in the marine domain to improve semantic interoperability, knowledge sharing, and data integration, highlighting their application in supporting the design and operation of autonomous vessels and other advanced maritime systems. They stress that a bridge between implicit and tacit knowledge is needed to explore the multidimensional relationships of the MLoSC. Knowledge management in maritime logistics is still assumed a new research area and its development is at an initial stage [20], [84], [105], [350]. The application of Knowledge Management in existing risk assessment methods appears to be limited. Several works fail to

provide proof of the positive impact of IT solutions on firm performance and do not adequately address challenges such as knowledge obsolescence in supply chain management [84]. The benefits that can be obtained from applying knowledge management techniques on the MLoSC security are summarised as follows:

- The application of knowledge management methods expands MLoSC operators' organisational knowledge, which can help them to improve their decision making.
- There is a cross-organisational need for mutual learning, where an effective conceptual framework can facilitate knowledge transfer among MLoSC operators.
- Knowledge management techniques can externalise tacit knowledge, facilitate information sharing which allows MLoSC operators to build stronger relationships, reinforce their transparency and create new synergies.
- Existing knowledge management solutions do not adequately represent maritime logistics assets and their interdependencies. Knowledge management techniques can help model these relationships and improve the domain understanding.

The current dissertation initiates a knowledge-based methodology, which engages the conceptualisation of MLoSC variables and identifies knowledge management flows between stakeholders' interactions and maritime/logistics asset interdependencies.

#### 4.5.3.5 An outlook of domain-specific security challenges

Martinez et al. (2024) [351] provide a comprehensive review of cybersecurity in the maritime domain, analysing existing standards, frameworks, and research contributions to identify key vulnerabilities and gaps in current approaches. Based on this analysis, it proposes the POSEIDON framework, a holistic cybersecurity management model designed to improve risk management, resilience, and protection of maritime systems by integrating existing standards with new mechanisms tailored to the specific needs of the maritime environment. Larsen and Lund (2021) [352] highlight a lack of human-centred research in maritime cybersecurity. They emphasise the need to improve the understanding of maritime cyber risk perception, enhance personnel training, strengthen organisational cybersecurity policies, and increase the resilience of maritime ICT infrastructures.

As discussed in the previous sections, intermodal systems with a high-level automation mechanisms and data interpretation capabilities, such as the SCADA systems (e.g., telemetry systems, pipelines monitoring systems, data collectors, lift stations and gantry crane crowbars), trigger adversaries to cyberattack. Sophisticated attacks by skilled hackers on maritime ICT infrastructures of the MLoSC can cause not only disruption of its services, but also tremendous damage to the maritime operations even to economies, societies, and environment (see Section 4.5.3.2).

The attacker's profile in SCADA networks appears to have one or a combination of the following characteristics: terrorist, disgruntled employee and insider; state or non-state hacker; malware for Confidentiality, Integrity and Availability (CIA) purposes; hobbyist and script kiddie chasing a



challenge; and hacktivist intruding for political reasons. The research work in [1] created in the context of the current dissertation, scrutinised the causes of vulnerabilities in current SCADA system architecture. Moreover, Ali (2024) [353] reviews cybersecurity threats targeting SCADA systems and examines existing risk assessment methodologies, highlighting common attack vectors, system vulnerabilities, and the importance of adopting comprehensive risk management strategies to improve the security and resilience of critical industrial infrastructures. The underlying causes of vulnerabilities in modern SCADA system architecture are summarised in the following [1], [353]:

- the misconfiguration of the wireless devices
- the high level of interdependency among transportation infrastructure systems
- deficiencies in security controls as lack of cryptography policies used in SCADA networks
- unskilled, naive employees revealing passwords to colleagues ignoring the potential risk
- the accessibility of the ports' transportation systems via networks, devices and software components either directly (wired) or remotely (wireless) for scheduled or corrective maintenance purposes.

Remarkable cyberattack vectors against SCADA systems are:

- database attacks; backdoors and holes in the network perimeter
- cinderella attack on time provision and synchronisation
- communications hijacking and man-in the middle attacks.

These attacks can be classified into five categories of SCADA architecture: (i) on the communication stack, (ii) on the UDP port (attacks appear on the transport layer), (iii) at the application layer (lack of security control for many of the SCADA protocols), (iv) on the hardware, and (v) on the software. SCADA systems are directly linked, and they are cyberdependent. The primary security challenges of the MLoSC targeting domain infrastructures, such as the SCADA infrastructures, considering the existing state-of-the-art on domain risk management are listed below [1]:

- Risk management policies must look through a thorough analysis to identify weaknesses of the underlined CII components operating during the MLoSC performance in a holistic manner.
- There is a compelling need for security methods that enhance domain knowledge and cybersecurity awareness while supporting automated risk management and decision-making to detect, prevent, and mitigate disruptions across the MLoSC.
- There is limited legal effort concerning the maritime cybersecurity addressing issues coming from cyber space. Thus, the legal background need to be enhanced with more cybersecurity sector-specific guidelines and practices.

- Existing approaches inadequately address the complexity of security threats across multimodal maritime logistics environments, highlighting the need for holistic and up-to-date risk assessment methods that analyse threat propagation and supply chain impacts.

Consequently, an effective risk assessment approach for SCADA infrastructures may include the following characteristics [1]:

- A structured body of cybersecurity knowledge using knowledge management practices to organise security knowledge. (Domain-specific recommendation #1)
- Modelling and simulation techniques will allow carrying out different real-life cyberattack scenarios and experimenting with the results. (Domain-specific recommendation #2)
- Risk assessment methods should provide rational decisions and probabilistic-based techniques to scrutinise complex cyberattack scenarios. (Domain-specific recommendation #3)
- Identify common or cross-border scenarios throughout national and regional limits. Engage all relevant public and private CII operators to achieve a comprehensive asset-level understanding of SCADA cyber risks, identify cyberdependencies, and assess their system-wide impacts. (Domain-specific recommendation #4)
- Be compliant with regulations and directives or international standards applying to the domain (e.g., IMO practices and ISO-related standards). (Domain-specific recommendation #5)
- Introduce collaborative practices to facilitate the sharing and transfer of risk-related information across supply chain operators. (Domain-specific recommendation #6)

#### **4.5.4 ICT Supply Chain Requirements**

Considering the challenges identified in the previous sections for ICT supply chains, a set of requirements has been extracted and organised into two main groups.

The first group of requirements refers to the need of evaluating ICT Supply Chain Services (SCS) from diverse evaluation aspects [15],[63]:

- Overall business. Overall business. It identifies and analyses all business-driven elements supporting the service, including processes; partners (suppliers, stakeholders, vendors, and authorities), third parties; data and information flows; decision-making logic; and legal or regulatory constraints.
- Holistic-technical. It is an asset-based, interdependent perspective that extends the business view by including all cyber and physical assets across partners, as well as their interdependencies supporting ICT processes.
- Sector-specific. It provides a focused snapshot of the ICT SCS from a single business partner's perspective, covering only sectoral processes and assets.

The ICT SCS must be fully defined by identifying the ICT stakeholder, the business partners, processes, and interconnected ICT assets, typically supported by modelling tools. Moreover, the ICT SCS criticality shall be assessed [15]. Chapter 6 presents an ICT SCS criticality assessment approach based on the NIS 2 Directive aspects.

The second group of requirements focuses on agreeing on security objectives, thresholds, and risk appetites between providers and partners through a Mutual Recognition Agreement (MRA). Key ICT SCS security requirements may include the following [63]:

- Security-by-design. SCS processes and assets shall be designed using established security practices.
- Least privilege. Access rights should be restricted to the minimum required to perform authorised tasks, supported by strict access controls and the separation of administrative privileges.
- Strong authentication. Robust authentication mechanisms must be enforced; failure may block or terminate access
- Asset protection. Confidentiality, integrity, availability, and authenticity of all SCS assets must be ensured.
- Supply chain integrity. The SCS must remain trustworthy and untampered throughout its lifecycle.
- Documentation transparency. Full documentation of architecture, processes, controls, partners, and policies must be maintained and updated.
- Quality management. Evidence of secure development, quality assurance, and ISMS practices must be provided.
- ICT SCS business continuity. Services must continue operating even after attacks or failures.
- Conformance with law. All partners must comply with relevant regulations and standards (e.g., the NIS 2 Directive, GDPR, and the Cybersecurity Act).
- Information sharing. Incidents and breaches must be reported and shared among partners.
- Data usage restriction. Data collection and processing must be clearly defined and legally justified.
- ISMS-SCS. Security management systems should be extended to cover ICT SCS-specific risk and resilience management.

## **4.6 Cybersecurity certification and conformity assessment concepts**

A thorough analysis of the interactive regulations and the corresponding standards that support cybersecurity certification and compliance evaluation mechanisms was carried out in the previous sections. This section aims to present the main concepts of cybersecurity certification and conformity assessment procedures.

### **4.6.1 Cybersecurity Certification**

Cybersecurity certification is the process of attesting that ICT products and services of an entity apply to all security requirements specified by a cybersecurity standard. In addition, NIST [34] defines cybersecurity certification as a comprehensive assessment of the management, operational, and technical security controls in an information system, in support of security accreditation, to determine whether the controls are implemented correctly, operating as intended, and producing the expected outcome to meet the security requirements for the system. It aims to enhance security, strengthen trust, foster a competitive and resilient market, and reduce market fragmentation.

### **4.6.2 The conformity assessment process**

An introduction to the concept of conformity assessment is provided in Chapter 2. A conformity assessment refers to activities that determine whether a product, system, service, or even person meets specified requirements defined in standards or specifications. These requirements may cover aspects such as performance, safety, efficiency, reliability, durability, and environmental impact (e.g., noise or pollution). Before entering the market, products typically must demonstrate to regulators and buyers that they are safe and perform as expected in terms of energy efficiency, reliability, sustainability, and other criteria [11],[13]. Conformity assessment provides this evidence based on established standards. Its key benefits include [160]:

- Governments can better assess infrastructure resilience and reduce public risk exposure.
- Insurers gain assurance that risks and safety requirements are properly managed.
- Buyers obtain evidence of product safety, performance, and reliability. Investors can trust that best practices are applied, reducing investment risk. Users and consumers are assured that products are safe and meet expected performance levels.

According to ISO 17020:2026 [200], conformity assessment incorporates a set of activities, such as audit, validation, verification certification, attestation, scope of attestation, accreditation, object of conformity assessment, and a set of entities, such as Conformity Assessment Body, Accreditation Body, and the Conformity Assessment System.

Regulation (EU) 765/2008 [160] defines “accreditation” as the attestation by a National Accreditation Body that a Conformity Assessment Body meets the requirements set by harmonised standards and, where applicable, any additional requirements, including those set out in relevant sectoral schemes, to carry out a specific conformity assessment activity.

#### **4.6.3 The European Cybersecurity Certification scheme (EUCC)**

The Common Criteria Recognition Agreement (CCRA) [354] and the Senior Officials Group - Information Systems Security (SOG-IS) [355] (the European recognition of Common Criteria certificates) historically provided Mutual Recognition Agreements [356]. Since February 27, 2026, SOG-IS has stopped issuing new certificates in favour of the EUCC certification framework, established under the EU Cybersecurity Act (CSA) [13]. The CSA gradually replaced national and regional certification schemes, such as the SOG-IS.

The European Common Criteria-based Cybersecurity Certification scheme (EUCC) is currently the only EU-adopted cybersecurity certification scheme. Developed by ENISA and adopted under the Implementing Regulation EU 2024/482 [14]. It focuses on certifying ICT products, services, and processes based on the Common Criteria framework, aligned with ISO/IEC 15408 [44] and ISO/IEC 18045 [59] standards. Additional EU schemes are under development, i.e., the certification scheme for cloud and AI services (CADA proposal [209]) and EU5G scheme [210], mentioned in Section 4.2.5. The main elements of the EUCC (European Common Criteria-based Cybersecurity Certification scheme) include:

- Certification scope – ICT products, ICT services, and ICT processes.
- Common Criteria framework – based on ISO/IEC 15408 (security evaluation criteria).
- Evaluation methodology – ISO/IEC 18045 (standardised security assessment process).
- Assurance levels – defines the degree of confidence in security (e.g., basic, substantial, high depending on evaluation depth).
- Security requirements – functional and assurance requirements derived from protection profiles.
- Evaluation process – structured assessment of product security features and vulnerabilities.
- Conformity assessment bodies – accredited organizations that perform evaluations.
- Certification issuance – formal recognition that a product/system meets EUCC requirements.
- Lifecycle monitoring – ensures continued compliance and vulnerability handling after certification.

#### **4.6.4 Cybersecurity Certification flows**

According to Article 54(e) of the CSA [13], a European cybersecurity certification scheme must indicate whether self-assessment of conformity is allowed. Nevertheless, the EUCC scheme [14], does not accept self-assessment. The EUCC recognises two Assurance Levels, i.e., Substantial and High.

The scheme introduces several new elements, including security objectives and requirements, while allowing vendors a degree of interpretation in implementing security controls. It evaluates whether the Target of Evaluation (ToE) meets predefined security objectives and control

measures when applied according to agreed security guidelines. The framework enables vendors to use certified ICT products, services, and processes to support compliance activities and also allows them to perform self-assessments of the ToE. Alternatively, assessments may be conducted by an approved third-party evaluator designated by the ToE owner.

Accredited Conformity Assessment Bodies (CABs) are eligible to apply the proposed scheme. Article 54(f) of the CSA [13] defines additional requirements ensuring that CABs have the necessary technical competence to assess cybersecurity criteria. CABs are accredited by a National Accreditation Body (NAB) and supervised by a National Cybersecurity Certification Authority (NCSA). The EUCC enables regulatory authorities to reference it within international, European, and national regulations, using criteria defined by the scheme.

At the “Substantial” assurance level, CABs must additionally verify that security requirements are correctly implemented and operating effectively, based on objective evidence and testing of both valid and invalid cases. At the “High” assurance level, they must further confirm that security requirements are fully functional and effective. ENISA reviews the certification outcomes, after which the certificate is formally recognised by the European Commission.

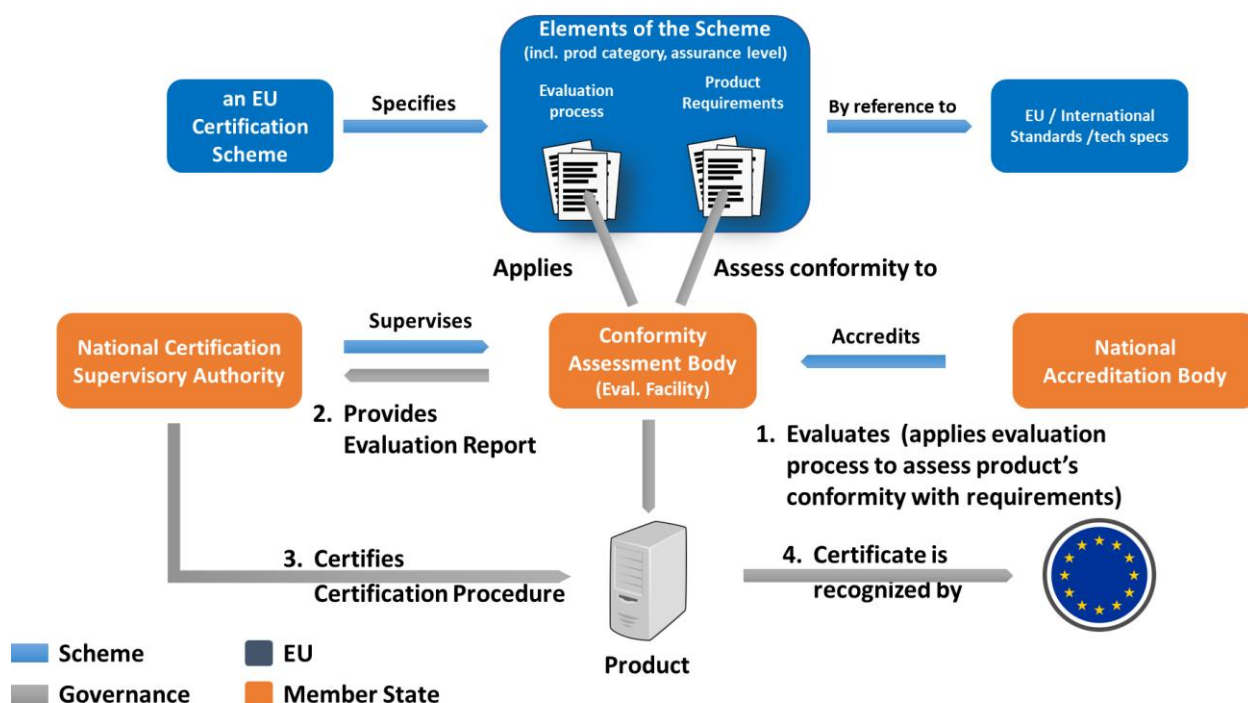


Figure 8. Assessment flows of the EUCC.

#### 4.6.5 Cybersecurity certification process

The certification process follows these main steps:

- Define the scope: Clearly identify the Target of Evaluation (ToE), including system boundaries, components, and functionalities to be assessed.
- Requirements analysis: Define security objectives and requirements, divided into:

- Security Functional Requirements (SFRs): Standardised requirements derived from security objectives, addressing threats, such as tampering or counterfeit components.
- Security Assurance Requirements (SARs): Define how assurance is achieved that SFRs are met. Evaluation Assurance Levels (EALs) indicate the depth of assurance, from EAL1 (basic) to EAL7 (highest). Vulnerability analysis (e.g., AVA\_VAN) is used to assess exploitable weaknesses.
- Stakeholder input: Collect and consolidate requirements from key stakeholders, including expert groups, industry actors, and EU Member States.
- Select EAL: Choose the appropriate Evaluation Assurance Level based on required evaluation depth.
- Select or propose a certification scheme: Use an existing scheme where applicable or develop a new one aligned with Common Criteria and ENISA approval if none exists.

If a new certification scheme is required:

- Define objectives and scope: Specify certification goals and the ToE coverage.
- Identify stakeholders: Engage regulators, industry experts, certification bodies, and Member States.
- Threat and risk analysis: Perform structured risk assessment.
- Select standards/frameworks: Adopt recognised cybersecurity standards.
- Define certification criteria: Specify required controls, functions, and security features.
- Establish EALs: Define assurance levels where applicable.
- Develop procedures: Set evaluation, documentation, and responsibility processes.
- Set up accreditation: Define accreditation for certification bodies.
- Consultation and review: Gather stakeholder feedback and refine the scheme.
- Finalisation: Submit to ENISA for review, pilot, and potential adoption.
- Prepare Security Target: Document security requirements and objectives of the ToE.
- Continuous threat monitoring: Use sources, such as NVD, ENISA, and OWASP.
- Risk management and testing: Apply risk-based evaluation, including functional and penetration testing.
- Documentation: Record all methods, results, and mitigation actions for transparency.
- Submission: Produce and submit the final certification (evaluation) report.

#### 4.6.6 Protection Profile elements

According to the Common Criteria (CC) [44]-[46], a Protection Profile (PP) defines a generic type of Target of Evaluation (ToE). It can serve as a template for Security Targets, a basis for refining other PPs, or as a base for PP modules.

A PP typically includes the following:

- Introduction: reference information and a description of the ToE type. Conformance claims: applicable CC version, conformance to Parts 2 and 3, and alignment with other PPs or packages.
- Conformance statement: evaluation methods used, compatibility rules, and required conformance type.
- Security problem definition: identifies threats, assumptions, and organisational security policies.
- Security objectives: maps solutions to the ToE and its operational environment.
- Extended components: defines additional functional or assurance components not covered by standard CC parts.
- Security requirements: translates objectives into Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) in a standardised form.

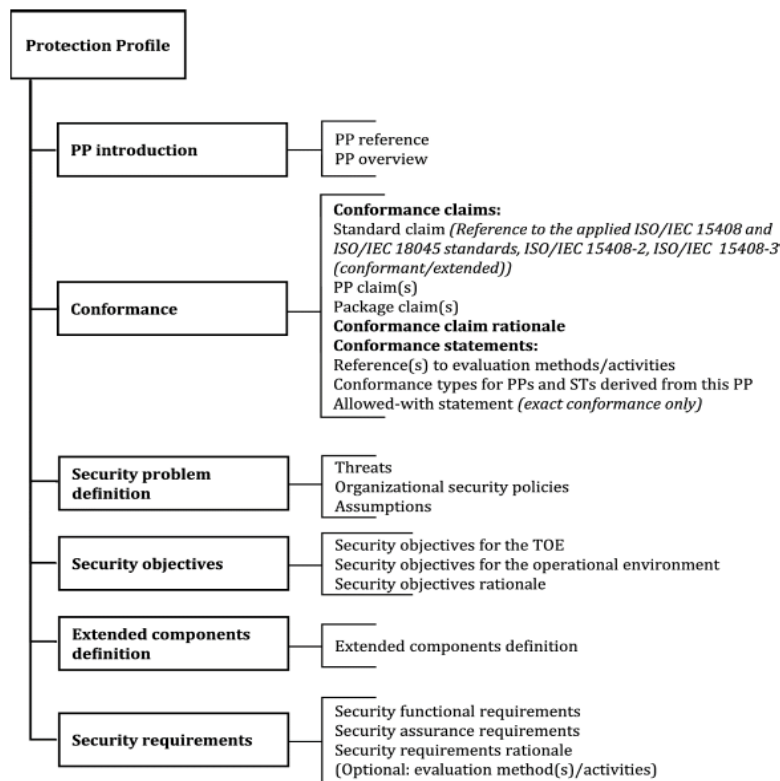


Figure 9. The Common Criteria Protection Profile and its elements.



The ISO/IEC 15408:2026 [44] specifies a Protection Profile as an “implementation-independent statement of security requirements for a Target of Evaluation (ToE) type”. According to ISO/IEC 15408:2026, “Security Problem Definition” is the statement that defines the nature and scope of the security that the Target of Evaluation (ToE) is intended to address. Moreover, “security objective” is considered a statement of an intent to either counter identified threats or satisfy identified organisation security policies or assumptions, or both.

As mentioned in Chapter 2, a “Security Functional Requirement” is a security requirement, which contributes to fulfilling the ToE’s Security Problem Definition (SPD), as defined in a specific Security Target (ST), Protection Profile (PP), PP-Module or functional package. Eventually, the “overall verdict” is considered a statement issued by an evaluator with respect to the result of an evaluation.

#### **4.6.7 Challenges and issues in cybersecurity certification**

Risk management is essential for the development of the Protection Profile (PP). Nonetheless, currently there are limited approaches that integrate risk management and conformity assessment in an one-stop-shop solution [15],[322],[357]-[358]. In this vein, the evolving software and hardware blocks require continuous compliance monitoring.

Another challenge is the fragmented certification market due to lack of unified European schemes [18]. Moreover, certification procedures are usually complex and time-intensive. The several types of PPs existing in the market [359], confuse ICT stakeholders, and it is not clear which is the most appropriate to use to meet their needs. In this respect, the accurate definition, evaluation and classification of composite ToEs and PPs are required. Moreover, there is limited market-wide information sharing, which impedes the composite certification.

Explainable AI (XAI) can act as an effective support mechanism for conformity assessment processes, especially when audit evidence has been gathered and auditors must justify whether the evidence is sufficient to demonstrate compliance with specific security requirements [360]-[364]. The integration of XAI can enhance cybersecurity certification processes by supporting the need for transparency, accountability, and trustworthiness required by frameworks, such as the EU AI Act [187], ISO/IEC 42001 [365], and NIST AI Risk Management Framework [366]. It contributes to conformity assessment by addressing certification challenges through explainable decision-making, enabling verification of AI reasoning. It also improves evidence generation by documenting security decisions and their influencing factors in a traceable, audit-ready form [357]-[358]. Additionally, XAI supports compliance validation by demonstrating how AI-driven recommendations align with regulatory requirements and organisational security policies [357].

### **4.7 Challenges and remarks for securing the ICT ecosystem**

This section summarises the challenges, limitations and recommendations identified in the previous sections of Chapter 4. In this chapter, the following main topics were analysed related to ICT security:

- The legal background of ICT security related standards and best practices.
- State-of-the-art on cybersecurity risk management, including attack modelling techniques, cascading effects and risk propagation.
- ICT supply chain security and risk management topics, including domain-specific analysis of the Maritime and Logistics Supply Chain (MLoSC).
- Cybersecurity certification and risk and conformity assessment integration.

Regarding the regulatory landscape, a key challenge is the fragmentation of cybersecurity standards, as evidenced by the following:

- The plethora of standardisation bodies with overlapping, sometimes contradictory frameworks.
- The rapid technological change (e.g., cloud computing, IoT, quantum computing, and AI types, such as ML and RL) outpaces existing standards.
- Industry-specific needs further fragment the landscape, hindering cross-sector interoperability.

This challenge generates the need for harmonised approaches that guide stakeholders in standards selection, according to their needs, and promote a holistic assurance framework to ensure ICT products' security. In addition, accelerating the development of sector-specific harmonised standards, especially for maritime, IoT, AI, and quantum domains, is recommended. Moreover, the maritime legal framework can be strengthened with dedicated cybersecurity guidelines aligned with the NIS 2 Directive [12], CRA [13], CER Directive [155], EU Maritime Security Strategy [340], and IMO Resolution [337] for maritime cybersecurity.

Existing risk management efforts and attack modelling techniques present the following limitations:

- Traditional risk assessment methods (e.g., CRAMM, BowTie, and Magerit) lack scalability and real-time adaptability for modern distributed systems.
- Quantitative risk assessment methods often suffer from insufficient or biased input data; Monte-Carlo approaches struggle with the volume of variables.
- Several efforts are implemented via web bases that lack concentrating on a mounted technical perspective, considering the technical specificities and security particularities of ICT products and their ICT SCS. In this regard, limited efforts provide a thorough risk analysis of ICTs.
- They lack empirical evidence to predict the impact of an attack.
- Despite the multiple existing attack graph methods that facilitate the realisation of impact assessment, they conduct the assessment in a broader manner that fails to extract security knowledge.

- Bayesian/HMM attack-prediction models require expert knowledge or frequent ML retraining; difficult to generalise across network architectures.
- Predictive risk metrics for dynamic vulnerabilities remain limited; advanced analytics are still in early stages.
- Cascading-failure models, i.e., topological, stochastic, dynamic and agent-based, each face trade-offs accordingly: oversimplification, ignoring system dynamics and data-quality dependency can lead to erroneous assumptions and incorrect probabilistic predictions; heavy computation and insufficient modelling effort of AI-based multi-agent algorithms can lead to black-box opacity.
- Attack graphs become prohibitively complex even for small networks.
- There is still ground for research to enhance attack modelling techniques and the estimation of the impact from a series of potential cyberattacks.

Based on the above, the literature indicates that effective risk management approaches should:

- Adopt hybrid (qualitative and quantitative) risk assessment frameworks capable of modelling multi-sector interdependencies of large-scale networks.
- Include attacker profile, attack-vector modelling, and control-effectiveness measures in risk calculations, avoiding under- or over-estimation.
- Integrate AI/ML and real-time threat intelligence for dynamic, evidence-based risk evaluation; do not only rely on expert judgement.

With respect to ICT supply chain security:

- The attack surface is growing due to digital interdependencies and heterogeneous multi-sector actors.
- Black swan events may not occur frequently, but when they appear they have long-lasting impact in the ICT SCS performance.
- Most solutions rely on static risk assessment and do not capture evolving risks or support continuous knowledge updates.
- Cascading failures are difficult to measure; limited real-world incident data is available.
- Limitation in large-scale industrial validation.
- Sophisticated APTs exploit supply chain entry points (e.g., through unpatched systems, stolen credentials, and malware in updates).
- Existing approaches don't deepen the analysis considering the technical complexity of large-scale networks, such as the ICT SCS networks, to estimate the cyber risks and their cascading effects.

- Maritime/Logistics supply chains face sector-specific risks of intermodal environments, such as SCADA, AIS, ECDIS, and port systems, with fragmented national risk methodologies.
- Maritime knowledge management is nascent; tacit knowledge transfer and cross-organisational learning remain inadequate.

In this vein, establishing collaborative information-sharing mechanisms across ICT supply chain operators will leverage the collection of threat-related information and spread the security knowledge. **Applying knowledge management techniques to supply chain risk assessment procedures can externalise tacit security knowledge and improve cross-organisational learning. Knowledge-based frameworks can improve risk assessment and decision-making, particularly in complex and rapidly changing domains**, such as in the ICT supply chains (e.g., MLoSC). Furthermore, semantic structures, inference rules and reasoning techniques can facilitate the supervision of real-time events and new threat knowledge. A simulation-based approach can contribute to the estimation of risk propagation whereas it produces multiple attack path results that enhance the attack analysis. Unified risk assessment methods for maritime cyberphysical systems, ensuring holistic threat-propagation analysis, are recommended.

Concerning cybersecurity certification and risk and conformity assessment integration:

- There are limited approaches that integrate risk management and conformity assessment in a single solution.
- Existing certification and compliance procedures are complex and time-intensive and must meet multiple simultaneous requirements at high cost.
- Lack of harmonised approaches and guidance on how to create the Protection Profile based on ICT stakeholders' needs.
- Fragmented EU certification market; insufficient market-wide information sharing.

To address the above challenges, one-stop-shop solutions that combine risk management and conformity assessment procedures can leverage the assurance framework of ICT products. Enhancing the security-related information can strengthen the composite certification and reduce fragmentation across EU Member States. Eventually, the application of Explainable AI (XAI) techniques in cybersecurity certification procedures can enhance audit transparency, evidence traceability, and compliance validation.

# PART III:

## RESEARCH UNDERPINNINGS

---

## 5. Research Problem, Requirements, and Conceptual Foundation

This section analyses the research problem of the current dissertation that aims to address, the identified requirements and the specified dissertation objectives (Section 5.1). It provides an overview of all created artefacts of the CyberICT hybrid evaluation framework (Section 5.2) and presents the CyberICT standards ontology (Section 5.3).

### 5.1 Research problem and dissertation objectives

Starting from identifying three main pillars (technological, regulatory and business – see Section 1.1), the preceding sections provided a comprehensive analysis of the ICT ecosystem, examining the prevailing regulatory and standardisation background together with the state-of-the-art in security and risk management, cybersecurity certification and conformity assessment for ICT products and ICT supply chain services (Chapters 2 – 4). The findings of this analysis revealed challenges, research gaps and elicited requirements that further motivated the present dissertation. A short description of the research problem of the current dissertation is the integration of risk and conformity assessment to assess the security of ICT composite products and their corresponding ICT supply chain services, as mentioned in Section 1.3, along with high-level dissertation objectives. This section presents challenges and requirements identified in the previous sections, which served as the basis for defining the dissertation objectives. The mapping of these challenges (Ch #z), requirements (Req #x) and dissertation objectives (DO #y) is presented in Table 4 and analysed in the next sections.

Table 4. Mapping of Challenges with Requirements and Dissertation Objectives.

|                                                                                              | <b>Challenge #1</b><br>(Ch #1)                                       | <b>Challenge #2</b><br>(Ch #2)           | <b>Challenge #3</b><br>(Ch #3)                         | <b>Challenge #4</b><br>(Ch #4)    | <b>Challenge # 5</b><br>(Ch #5)                |
|----------------------------------------------------------------------------------------------|----------------------------------------------------------------------|------------------------------------------|--------------------------------------------------------|-----------------------------------|------------------------------------------------|
|                                                                                              | An integrated framework of Risk Management and Conformity Assessment | Harmonisation of cybersecurity standards | Address the complex nature of large-scale environments | Lack of security typology         | Siloed risk measurements lacking holistic view |
| <b>Requirement (Req) and corresponding Dissertation Objective (DO) mapped with Challenge</b> | Req#1.1,<br>DO#1.1.                                                  | Req#2.1,<br>DO#2.1.                      | Req#3.1,<br>DO#3.1.                                    | Req#4.1,<br>DO#4.1.               | Req#5.1,<br>DO#5.1.                            |
|                                                                                              |                                                                      |                                          | Req#3.2,<br>DO#3.2.                                    | Req#4.2,<br>DO#4.2.               | Req#5.2,<br>DO#5.2.                            |
|                                                                                              | Req#1.2,<br>DO#1.2                                                   | Req#2.2,<br>DO#2.2                       | Req#3.3,<br>DO#3.3.                                    | Req#4.3,<br>DO#4.3.1,<br>DO#4.3.2 | Req#5.3,<br>DO#5.3.                            |
|                                                                                              |                                                                      |                                          | Req#3.4,<br>DO#3.4.                                    |                                   |                                                |

### **5.1.1 Challenge #1: An integrated framework of Risk Management and Conformity Assessment**

Dependencies of digitalisation lurk the evolution of cyber threat surface which rise the demand for advanced security and its continuous monitoring. This leads to the need of measurable and actionable security requirements to facilitate organisations to select appropriate security specifications and controls for their ICT products and services (cf. Section 2.1).

Enhancing information security practices of large enterprises, SMEs and MEs has become a compelling need, especially these days that Europe needs to strengthen its economy and urges ICT stakeholders to be compliant with existing mandates of regulations, such as CRA's [11], and NIS 2 Directive's [13] (cf. Section 2.2.1). Nevertheless, risk and conformity assessments are extremely complicated, and time-intensive processes. In addition, evolving hardware/software building blocks of composite ICT products requires continuous compliance. Another important issue observed is the lack of harmonised standardisation in cybersecurity certification formats and requirements (cf. Section 4.7). ICT supply chain disruptions may propagate across interconnected systems, highlighting the importance of effective security policies and cybersecurity certification in improving resilience and trust.

The complementary cybersecurity regulations of CRA [11], NIS 2 Directive [13][12] and CSA [13] recommend to ICT stakeholders the combination of risk and conformity assessment procedures to manage the security of products, services and their supply chains and assess their compliance at specified levels to be conformant with the existing cybersecurity regulations. The enhanced security model in Section 2.2.2 (Figure 2) reflects the synergy of risk assessment and conformity assessment procedures along with the European CRA, CSA, and NIS 2 Directive regulations interplay. Currently, the state-of-the-art illustrate limited effort in combining risk and conformity assessment concepts (cf. sections 2.2.2, and 4.6). Moreover, the literature reviews lack of approaches that provide structured processes for preparing ICT stakeholders to create the protection profile of composite ICT products. The current challenge elicits the following requirements and relevant corresponding dissertation objectives.

**Requirement #1.1:** Need for measurable and actionable security requirements linked with appropriate security controls.

**Dissertation Objective #1.1:** Develop an approach that creates a measurable and actionable set of security requirements and corresponding security controls that are capable of meeting EU digital market's needs.

**Requirement #1.2:** The synergy of risk assessment and conformity assessment procedures is required to provide an end-to-end evaluation for attesting the security, according to specified criteria and guide ICT stakeholders how to create the Protection Profile of composite ICT products.

**Dissertation Objective #1.2:** Develop an approach that integrates both risk management and conformity assessment procedures guiding ICT stakeholders how to conduct an end-to-end evaluation to facilitate readiness for cybersecurity certification and security compliance procedures and create the Protection Profile of composite ICT products.

### **5.1.2 Challenge #2: Harmonisation of cybersecurity standards**

Cybersecurity regulations can be implemented through the use of relevant cybersecurity standards. Nevertheless, Section 4.2.2 presented that the extensive number of existing cybersecurity standards causes an overwhelming perception of disorder that confuses the ICT stakeholders and security practitioners which are relevant to adopt to meet their security needs. This challenge elicits the following requirements and corresponding dissertation objectives (cf. Section 4.7):

**Requirement #2.1:** Reduce fragmentation of cybersecurity standards

**Dissertation Objective #2.1:** Develop an ontology that classifies cybersecurity standards and enhances their comprehension.

**Requirement #2.2:** Need for harmonised standards-based approaches for assessing ICT products security.

**Dissertation Objective #2.2:** Develop a standards-based approach that combines and harmonises risk management and conformity assessment concepts.

### **5.1.3 Challenge #3: Address the complex nature of large-scale environments**

Chapters 3 and 4 support both from business and security perspectives that there are limited approaches which analyse the technical complexity of ICT products and the high interdependencies between the ICT supply chain services. To this aim, mutual collaboration across the ICT stakeholders is needed to conduct holistic evaluation. The literature reviews limited approaches that deepen the risk analysis of the ICT elements. Most of the existing risk management methods rely on web bases and they lack concentrating on a mounted technical perspective that considers the technical specificities and security particularities of the ICT ecosystem (cf. Section 4.7). A both vertical and horizontal analysis of complex and large-scale environments, such as ICT supply chains, can preserve their integrity, sustainability, continuity and resilience (Sections 3.5 and 4.5). The challenge elicits the following requirements and corresponding dissertation objectives:

**Requirement 3.1:** Need for identifying asset interdependencies

**Dissertation Objective #3.1:** Develop a cybersecurity risk management methodology for ICT products and ICT supply chain services which identifies interdependencies between interconnected ICT assets.

**Requirement 3.2:** Need for identifying criticality on ICT products

**Dissertation Objective #3.2:** Develop a cybersecurity risk management methodology which analyses ICT products and identifies their criticality.

**Requirement 3.3:** Need for identifying criticality on ICT supply chain services, ICT processes and ICT assets

**Dissertation Objective #3.3:** Develop a cybersecurity risk management methodology which estimates criticality on ICT supply chain services, ICT processes and ICT assets.



**Requirement 3.4:** Need for analysing ICT supply chain services from business-oriented, horizontal and vertical evaluation aspects.

**Dissertation Objective #3.4:** Develop a cybersecurity risk management methodology which provides diverse evaluation aspects on ICT supply chain services, i.e., business, holistic-technical, and sector-specific.

#### **5.1.4 Challenge #4: Lack of security typology**

Chapters 3 and 4 discuss that deep comprehension and analysis of the complex ICT ecosystem is required and there are currently poor efforts supporting this. It has been observed throughout the ICT stakeholders (e.g., Supply chain operator of the MLoSC), that there is lack and ignorance of the security culture and compliance to the existing cybersecurity regulatory background is still at an early stage with limited cybersecurity investment in enterprises, especially in SMEs (Chapter 1).

In this vein, cost-effective approaches that enhance the organisational learning of ICT stakeholders are required. The state-of-the-art in Chapters 3 and 4 underscores that the use of process modelling and semantic web techniques can facilitate the security analysis of complex ICT environments (cf. Section 3.4). The application of knowledge management practices in risk management processes can raise the risk awareness and organisational knowledge and ease the information retrieval (cf. Section 4.4.3). Apply process modelling, semantic web technologies, and knowledge management practices can enhance security analysis and information sharing across complex ICT and supply chain networks with a unified security typology.

**Requirement 4.1:** Need for improving comprehension of ICT processes and their embedded actors and elements.

**Dissertation Objective #4.1:** Develop a cybersecurity risk management methodology which uses business process models to visualise business partners participating and assets operating in an ICT process.

**Requirement 4.2:** Need for enhancing organisational learning and security knowledge flows within the ICT supply chain environment.

**Dissertation Objective #4.2:** Develop a cybersecurity risk management methodology that adopts Knowledge Management practices to recognise knowledge management flows and externalise tacit security knowledge within the ICT ecosystem.

**Requirement 4.3:** Create a structured body of cybersecurity knowledge in machine-readable format.

**Dissertation Objective #4.3.1:** Develop a risk ontology to semantically represent ICT supply chain service elements and relevant security concepts.

**Dissertation Objective #4.3.2:** Develop an ontology that classifies cybersecurity standards from diverse perspectives. This challenge is also mapped with the Dissertation Objective #2.1.

### 5.1.5 Challenge #5: Siloed risk measurements lacking holistic view

The previous sections stressed that digital dependencies over ICT interconnected systems or infrastructures increase the security threats and their propagation requiring a rigorous protection of their security. As mentioned in Section 4.7, several existing risk management approaches lack providing in-depth assessment of threats, vulnerabilities and risks and adequately addressing the technical specificities of complex ICT supply chain environments. Moreover, the state-of-the-art demonstrates the lack of balanced, multi-factor risk measurement in risk management approaches and highlights the need for adequate definition of risk and its dependent factors. In this vein, as previously described, a structured body of cybersecurity knowledge using Knowledge Management practices and leveraged by mutual collaboration among ICT stakeholders can enhance the security knowledge. Considering these, complex ICT environments of ICT Supply Chain Services (SCS) require holistic estimation of the cyber risk considering critical interconnections among infrastructure nodes throughout the entire ICT network.

Another research gap existing in several risk management approaches is that they lack empirical evidence to predict the impact of an attack (see Section 4.7). Many attack graph methods may provide broad impact assessments but fail to extract fine-grained security knowledge. Despite the socio-economic importance of tools and techniques for handling security threats there is still no easy, structured, standardised and trusted way for cascading effects and propagation estimations in complex and heterogeneous ICT environments, such as in ICT SCS. Furthermore, attack modelling techniques required to be enhanced on such perspectives. For instance, there is limited effort in investigating how a cyber attacker has moved inside an ICT network to implement a cyberattack that has been realised.

Disruptions of the ICT SCS performance can have low impact occurrence, such as lead-times and demand upsets of business due to operational issues, or a high impact occurrence on the ICT SCS performance with long-lasting propagation. An example for the latter case is a black swan event that manifests from a massive cyberattack on CIIs (e.g., the NotPetya or SolarWinds historical cyber disruptions) or a global crisis (e.g., COVID-19 pandemic outbreak) which can cause a domino effect of tremendous global disruptions. Effective and up-to-date risk management processes can mitigate the ICT supply chain disruptions and enhancing critical information infrastructure preparedness.

**Requirement 5.1:** Need for estimating the impact of potential cyberattacks in ICT supply chain networks

**Dissertation Objective #5.1:** Develop a cybersecurity risk management methodology that uses calculation models to estimate threats, vulnerabilities, risks and their cascading effects.

**Requirement 5.2:** Need for estimating risk propagation in ICT supply chain networks

**Dissertation Objective #5.2:** Develop a cybersecurity risk management methodology that uses calculation models for propagated assessment of vulnerabilities, impact and risks.

**Requirement 5.3:** Need for enhancing attack modelling techniques.

**Dissertation Objective #5.3:** Develop an attack simulation and evidence-based generation model for estimating attack paths in complex ICT networks associated with a confirmed security event.

## 5.2 CyberICT hybrid evaluation framework overview

As presented in Section 1.3, the current dissertation research aims to produce a set of interconnected, rigorously designed artefacts that constitute the CyberICT hybrid evaluation framework of risk management and conformity assessment integration. The primary artefacts of the CyberICT hybrid evaluation framework are the Risk Management Methodology and the Protection Profile preparatory framework.

The CyberICT Risk Management Methodology aims to assess vulnerabilities, threats and risks of composite ICT products and ICT supply chain services. The CyberICT Risk Ontology is a secondary artefact related to the CyberICT Risk Management Methodology. It aims to semantically represent security concepts in the ICT ecosystem. The CyberICT Risk Ontology relies on concepts of a past work occurred within the current dissertation research which proposed an ontology [92]–[93] of the Business Process Management Notation (BPMN) v2.0.2 (ISO/IEC 19510:2013) [114] structure (see Section 3.4.2.2).

The CyberICT Protection Profile preparatory framework aims to provide a stepwise process that guides the ICT stakeholders on how to create the Protection Profile of their ICT product. In addition, this process conducts an end-to-end cybersecurity certification evaluation that allows the ICT stakeholders to get prepared before initiating a conformity assessment with an authorised body. The CyberICT Protection Profile preparatory framework incorporates the CyberICT Risk Management Methodology throughout this end-to-end evaluation. The structured taxonomy of the Protection Profile is a secondary element of the CyberICT Protection Profile, which provides the Common Criteria-based structure of the Protection Profile for an ICT product together with a security classification that interrelates threat categories with security objectives, Security Functional Requirements (SFRs) and security controls.

The Cybersecurity Standards Ontology aims to classify cybersecurity standards and guide ICT stakeholders which to adopt, according to their needs. This artefact can be used either in combination with The CyberICT Risk Management Methodology or with the CyberICT Protection Profile preparatory framework. Figure 10 presents the CyberICT hybrid evaluation framework embedding all the proposed artefacts and their interrelations.

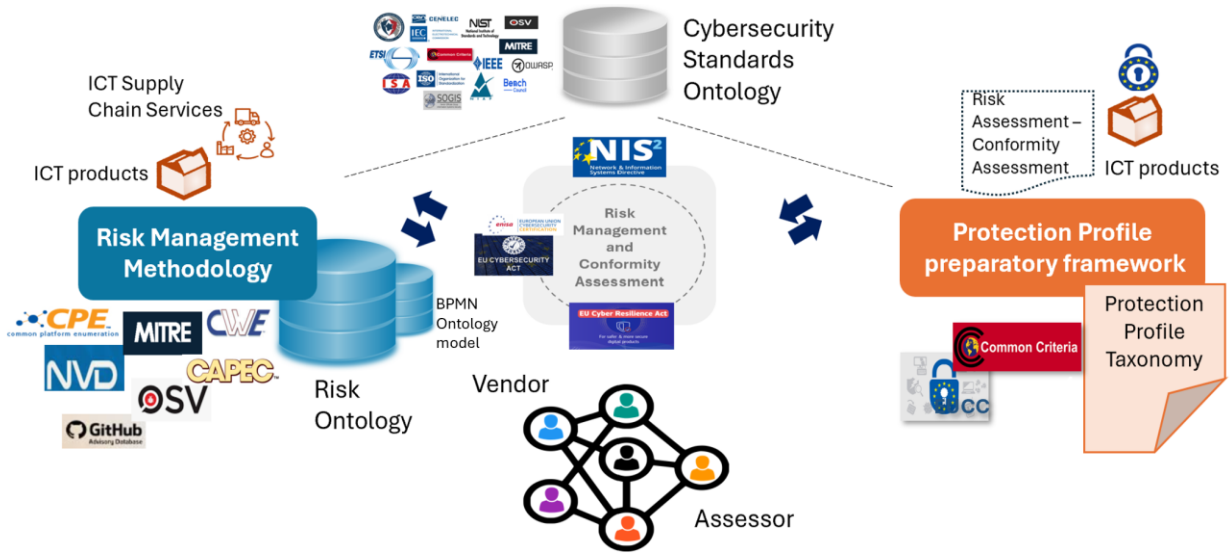


Figure 10. The CyberICT hybrid evaluation framework.

Table 5 presents a mapping between the Requirements (Reqs#) identified in Section 5.1, the Dissertation Objectives (DO#) and the associated artefacts. In addition, for further analysis of the conceptual system design, the identified requirements have been classified into Functional Requirements (FRs) and Non-Functional Requirements (NFRs).

Table 5. Mapping of Requirements, Objectives and Artefacts of the CyberICT hybrid evaluation framework.

| Requirement                                                                                                       | Functional Requirement (FR)/<br>Non-functional Requirement (NFR)                       | Dissertation Objective                                                                                    | Dissertation Artefact                                              |
|-------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------|
| Req#2.1,<br>Req#4.3                                                                                               | NFR#1,<br>FR#8                                                                         | DO#2.1,<br>DO#4.3.2                                                                                       | CyberICT standards ontology                                        |
| Req#1.2<br>Req#2.2<br>Req#3.1,<br>Req#3.2,<br>Req#3.3,<br>Req#3.4,<br>Req#4.1,<br>Req#5.1,<br>Req#5.2,<br>Req#5.3 | FR#2<br>FR#3,<br>FR#4,<br>FR#5,<br>FR#6,<br>FR#7<br>NFR#2,<br>FR#9,<br>FR#10,<br>FR#11 | DO#1.2,<br>DO#2.2,<br>DO#3.1,<br>DO#3.2,<br>DO#3.3,<br>DO#3.4,<br>DO#4.1,<br>DO#5.1,<br>DO#5.2,<br>DO#5.3 | CyberICT Risk Management Methodology                               |
| Req#4.2<br>Req#4.3                                                                                                | NFR#3<br>FR#8                                                                          | DO#4.2,<br>DO#4.3.1                                                                                       | CyberICT Risk Ontology                                             |
| Req#1.2,<br>Req#2.2                                                                                               | FR#2,<br>FR#3                                                                          | DO#1.2,<br>DO#2.2.                                                                                        | CyberICT Protection Profile preparation for Composite ICT products |
| Req#1.1,<br>Req#1.2                                                                                               | FR#1,<br>FR#2                                                                          | DO#1.1,<br>DO#1.2                                                                                         | CyberICT Protection Profile for composite ICT products taxonomy    |

### 5.3 CyberICT standards ontology

The current section presents the research work described in [18], which was conducted in the context of the current doctoral research. During this dissertation, an ontology has been developed to classify cybersecurity standards according to their objective, usage, and sector, aiming to help stakeholders understand their purpose and decide which they should adopt to cover their organisational needs. The taxonomy is represented in a semantic ontology, following the OWL 2 knowledge engineering approach.

The OWL2 ontology-based model was utilised as a supporting mechanism to conceptualise in formal representation diverse cybersecurity standards and harmonise related concepts to identify and extract semantic interrelationships. As mentioned in Section 4.2.6, the developed ontology aims to enhance the research works presented in [179]–[181] by articulating prominent cybersecurity management international standards, best practices, and guidelines into coherent conceptual groups covering distinct security domains and their purpose of use in a machine-interpretable manner. A realistic scenario is described to illustrate the applicability of the ontology.

#### 5.3.1 Ontology building blocks

Taxonomy is a scheme of classification [367] that partitions a body of knowledge and identifies relationships among the pieces [53] of things, concepts, and principles that underlie such classification [181].

The proposed standards-based taxonomy is structured in a step-wised approach based on the NIS 2 Directive [12], JRC Cybersecurity Taxonomy [181] and European Cybersecurity Skills Framework [180]:

- cybersecurity standards are distinguished into four conceptual pillars of different stakeholder’s preferences and their purpose of use
- different standards attributes identified (e.g. year, publication, etc.)
- semantic rules, hierarchies (classes) and relations (properties) specified among the above taxonomy elements to develop an ontology formal knowledge representation.

#### 5.3.2 Structure and Main Pillars

The proposed ontology aims to guide stakeholders (e.g. organisations, practitioners, individuals) on which standard(s) are relevant for them. Relevance is determined by a conceptual four-pillar classification, as presented in Table 6:

Table 6. Conceptual questions and pillars to identify relevant standards.

| Question                  | Conceptual pillar                 | Conceptual Pillar Description                                                             |
|---------------------------|-----------------------------------|-------------------------------------------------------------------------------------------|
| Q1: Where are you?        | I. Industrial sector              | Sector-specific (e.g., transport, finance, healthcare).                                   |
| Q2: Who are you?          | II. Stakeholder Profile           | Security-related professional roles, skills and competencies (e.g. CISO, Auditor)         |
| Q3: What's your interest? | III. Security domain              | Cybersecurity discipline (e.g. Anomaly Detection, Certification)                          |
| Q4: What's used?          | IV. Applications and Technologies | It refers to the applications and technologies utilized by the stakeholder (e.g. IoT, AI) |

The pillars' categories are described below (shown in Figure 11):

- Pillar-I. Industrial Sectors: Fifteen (15) Industrial sectors (categories) are defined, according to their value and impact on the EU economy in case of their services disruption. The categorisation relies on the EU NIS 2 Directive [12] operators of essential/important services distinction and JRC sectorial classification[8].
- Pillar-II. Stakeholder Profile: It provides fourteen (14) different categories of expertise and/or professions related to cyber/physical security based on the ENISA ECSF report [180].
- Pillar-III. Security Domain: It refers to thirteen (13) security fields of knowledge (categories) from both cyber and physical aspects addressing existing security challenges of the EU economy [181].
- Pillar-IV. Applications and Technologies: It corresponds to seventeen (17) types of devices/data/techniques/technologies (categories) utilized by the stakeholder [181].

Since the stakeholder needs are identified in a quad selection set (options from the four pillars), the latter shall specify "why" the entity needs security standardisation. Standard(s)/framework(s)/best practice(s) are distinguished into generic conceptual groups based on their content and purpose of use, as displayed in Table 7 and indicative examples presented in the following:

- ISO/IEC 27000 standard provides a basic vocabulary (Awareness) for information security management (Pillar-III), applied to ICT systems (Pillar-IV) by a CISO (Pillar-II) in the Energy sector (Pillar I).
- ISO/IEC 15408 [44] standard provides the criteria (Requirements Identification) to evaluate security properties (Pillar-III) of IoTs (Pillar-IV), assessed by a cybersecurity auditor (Pillar-II) in Healthcare (Pillar-I).

- The ETSI-TVRA [152] technical specification or ISO/IEC 18045 [59] standard defines (Methodologies) the minimum actions performed by a cybersecurity auditor (Pillar-II) to conduct a cybersecurity risk assessment (Pillar-III) on AI-based systems (Pillar-IV) supporting Maritime Transport (Pillar-I) operations concerning the evaluation criteria (Pillar-III) prescribed in ISO/IEC 15408 [44]-[46] standard.
- ISO 28004 [206] standard provides guidelines (Implementation) to an ICS/SCADA Cybersecurity Analyst (Pillar-II) in the Manufacturing sector (Pillar-I) for the security management (Pillar-IV) of supply chain systems (Pillar-IV), analyzing typical inputs/outputs of supply chain security requirements addressed in ISO 28000:2022 [138] standard.

Table 7. Security management standards classification towards their purpose of use.

| Question                             | Purpose of Use              | Content                                                                                           |
|--------------------------------------|-----------------------------|---------------------------------------------------------------------------------------------------|
| Q5: Why do you need standardization? | Awareness                   | Cybersecurity terms, acronyms, and definitions supporting stakeholders' selections set.           |
|                                      | Requirements identification | Elicit security requirements on a specific topic of interest.                                     |
|                                      | Methodology                 | Select a suitable methodology on topics of security management.                                   |
|                                      | Implementation              | Specify and implement methodology/address requirements: guidance, directions, and best practices. |

Considering the building blocks mentioned above, Figure 11 depicts the structure of the proposed ontology.

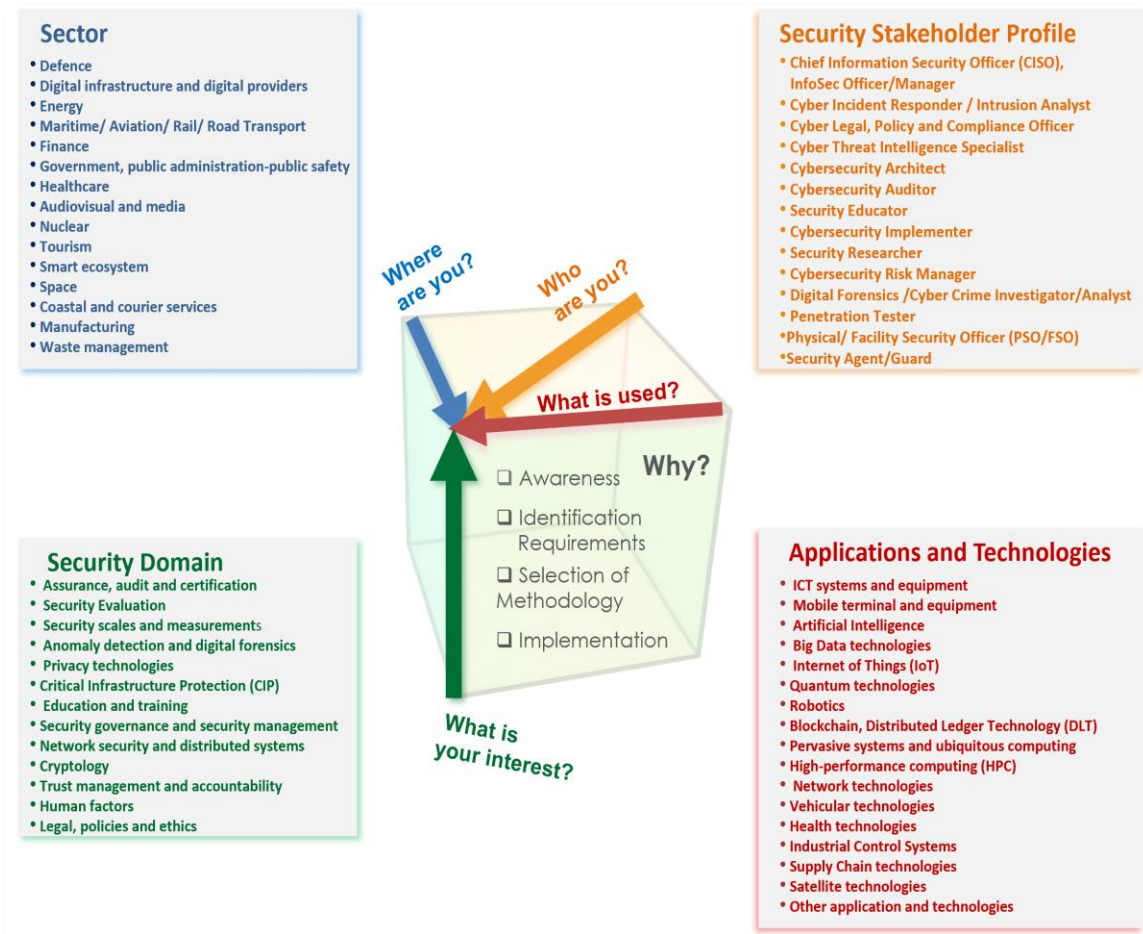


Figure 11. Overall view of the proposed standards-based taxonomy of security management.

### 5.3.3 Semantic Relations

The cybersecurity standards engage a set of attributes:

- **Range:** Indicates their applicability at the International, Regional (e.g. European) or National level.
- **ID/Version/Title/Year:** The standard/framework/best practice publication characteristics, i.e., its ID, version, title, and the year published.
- **Publisher/Technical Committee:** The Standardization Body, Policymaker or other relevant party who developed/published the standard/frameworks/best practice (it can be an association of entities).
- **Purpose of Use (Why?).** Regarding the content, usage is specified following the classification described in Section . Standard/frameworks/best practices can be mapped with one (1) or more purposes of use.
- **Type.** Concerning ISO and IEC technical processes on standards lifecycle and their level of completeness, standards documents can be characterised by the following main types: a



published standard, Technical Report (TR)<sup>11</sup>, Technical Specification (TS)<sup>12</sup>, Approved Work Item (AWI), Publicly Available Specification (PAS)<sup>13</sup>, treaty, best practice or other type of guidance assigned by a relevant entity.

Upon stakeholder pre-defined selections in the ontology, a list of associated standards and their attributes are reported in a tabular structure, as depicted in Table 8.

Table 8. Template of standard attributes.

| Range                             | Type                                                      | Characteristics          | Publisher/Technical Committee              | Purpose of Use                                                        |
|-----------------------------------|-----------------------------------------------------------|--------------------------|--------------------------------------------|-----------------------------------------------------------------------|
| (International/European/National) | (Standard/TR/TS/PAS/AWI/ framework/ best practice/ other) | (ID/Version/ Title/Year) | (Standardisation body/ Policymaker, Other) | (Awareness/ Requirements identification/ Methodology/ Implementation) |

All ontology elements, i.e., standards attributes, pillars, and purpose of use are connected via semantic properties depicted in Table 9. Properties creating reciprocal relationships between two elements generate inverse relations (of inverse properties), e.g., “Operates” and “isOperatedBy”, whereas some properties have a specific type of value, e.g., “Integer”.

Table 9. Ontology’s semantic relations.

| Semantic Property | Semantic further characteristics (where applicable) | Property | Examples of Semantic relations                                                                                                                                                                                               |
|-------------------|-----------------------------------------------------|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Defines           | -                                                   | -        | <ul style="list-style-type: none"> <li>a standard <i>Defines</i> another standard or best practices.</li> <li>Awareness report <i>Defines</i> all other reports (i.e., Requirements, Methodology, Implementation)</li> </ul> |
| Implements        | -                                                   | -        | <ul style="list-style-type: none"> <li>Applications and Technologies <i>Implement</i> Security Domain</li> <li>Best practices/guidelines <i>Implement</i> Requirements</li> </ul>                                            |
| Operates          | Inverse (isOperatedBy)                              | -        | <ul style="list-style-type: none"> <li>Sector <i>Operates</i> Applications and Technologies</li> <li>Applications and Technologies are <i>OperatedBy</i> Security Stakeholder (inverse example)</li> </ul>                   |

<sup>11</sup> TR is informative and non-normative, analyzing specific topics with complementary information (e.g., testing approaches, measurements, methodologies, and test cases).

<sup>12</sup> TS approaches an international standard in detail and completeness. Nevertheless, it has not yet passed through all approval stages (considering either premature or not reached consensus).

<sup>13</sup> PAS aims to boost standardization activity towards rapidly evolving technologies and respond to an urgent market need.

|            |                              |                                                                                                                                                                              |
|------------|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Recommends | Inverse<br>(isRecommendedBy) | <ul style="list-style-type: none"> <li>Best practices <i>Recommend</i> methodologies and frameworks</li> </ul>                                                               |
| ResidesIn  | -                            | Security Stakeholder <i>ResidesIn</i> Sector                                                                                                                                 |
| Evaluates  | Inverse<br>(isEvaluatedBy)   | <ul style="list-style-type: none"> <li>A Methodology <i>Evaluates</i> Requirements</li> <li>Security Domain <i>Evaluates</i> Applications and Technologies</li> </ul>        |
| Title      | -                            | <ul style="list-style-type: none"> <li>Cybersecurity Standards (e.g. ISO/IEC 15408) have <i>Title</i> Information, security, cybersecurity and privacy protection</li> </ul> |
| Publisher  | -                            | <ul style="list-style-type: none"> <li>Cybersecurity Standards (e.g. 2700x related) have <i>Publisher</i> ISO and IEC</li> </ul>                                             |
| IdVersion  | -                            | <ul style="list-style-type: none"> <li>Information Security standard requirements has <i>IdVersion</i> ISO/IEC 27001</li> </ul>                                              |
| Year       | Integer value                | <ul style="list-style-type: none"> <li>ISO/IEC 27001 Standard lastly published in <i>Year</i> 2022</li> </ul>                                                                |
| Range      | -                            | <ul style="list-style-type: none"> <li>ISO 28001 <i>Range</i> is International</li> </ul>                                                                                    |

Concerning taxonomy hierarchies, the following semantic rules are identified:

- A Pillar (e.g. “Pillar-III: Security Domain”) is a classOf category (e.g. “Cryptology”), whereas a category is subclassOf Pillar
- All classes/subclasses can have a set of values/instances (e.g. “Cybersecurity\_Standards” class has “ISOIEC15408” instance)
- All classes, subclasses and instances can be subjects and objects, associated with semantic properties
- Semantic properties (e.g. “Defines”, “Supports”, etc.) are relationships between a subject (e.g. “Cybersecurity\_Standard”) and an object, (e.g., “Purpose\_Of\_Use”)
- Special characteristics of semantic relations between classes and/or instances (e.g. Inverse relations, Integer values) are expressed via semantic properties.

The proposed taxonomy is represented in semantic ontology structure using OWL 2 language of description logic and RDF framework in Protégé Open-source Ontology Editor [132]. It is built on the main taxonomy elements, described previously:

- the four-conceptual pillars represent four superclasses embedding subclasses to address the corresponding categories.
- attributes/types of standards and related reports are represented by five superclasses, i.e. range, type, (publication) characteristics, publisher/technical committee and purpose of use, containing subclasses to express the corresponding options, analysed in Table 8.

- all classes may embed several individuals (instances of ontology's classes), e.g. "Methodology" class of "Purpose of Use" superclass contains the "ISOIEC18045" individual.
- all instances are connected via object properties with other instances or via data properties specific values (e.g. integer, Boolean, etc.) to declare their semantic relations Table 9.
- all semantic rules previously described are followed in the current ontology

Figure 12 illustrates the high-level structure of the OWL2 ontology, Figure 13 depicts indicative ontology's individuals and semantic relations (properties) of Table 9 expressed in RDF framework. In Figure 13, the different colors in the arrows between individuals represent their connections with different properties, e.g. dark orange for property Range, yellow for property Evaluates. The pink arrows represent the relations between classes and individuals, e.g. class "International" hasIndividual "ISOIEC15408". The ontology was validated using the Reasoner Pellet (see Section 8.1).

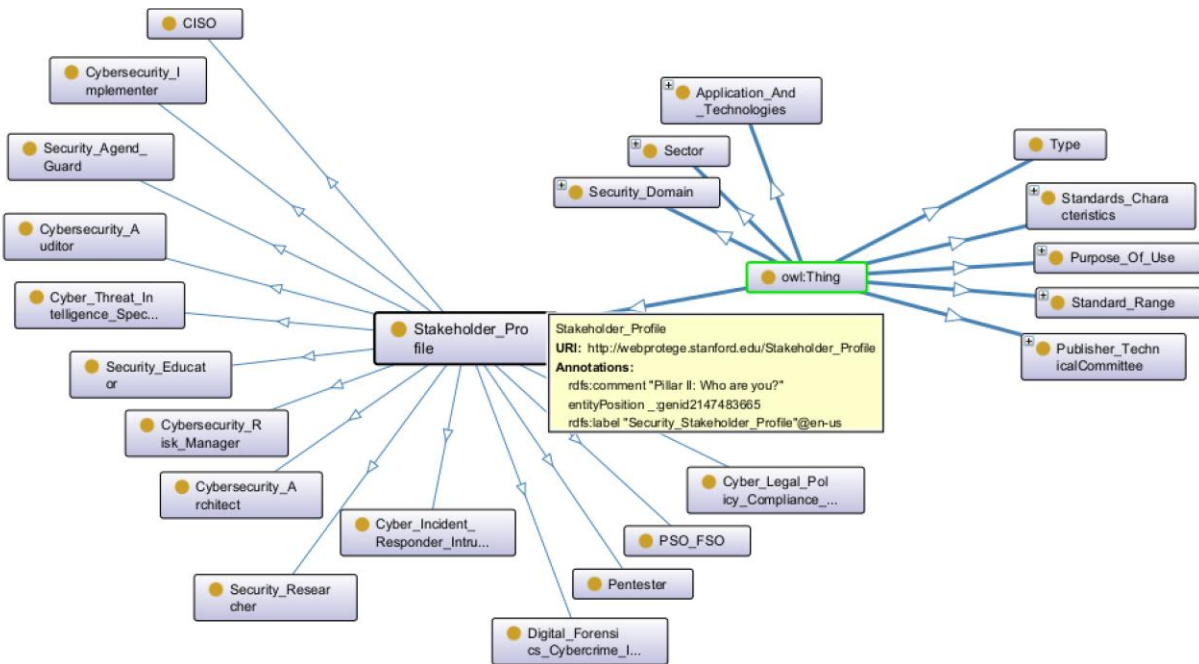


Figure 12. A snapshot of the Cybersecurity Standards ontology structure illustrating the Stakeholder's profile and relations between classes.

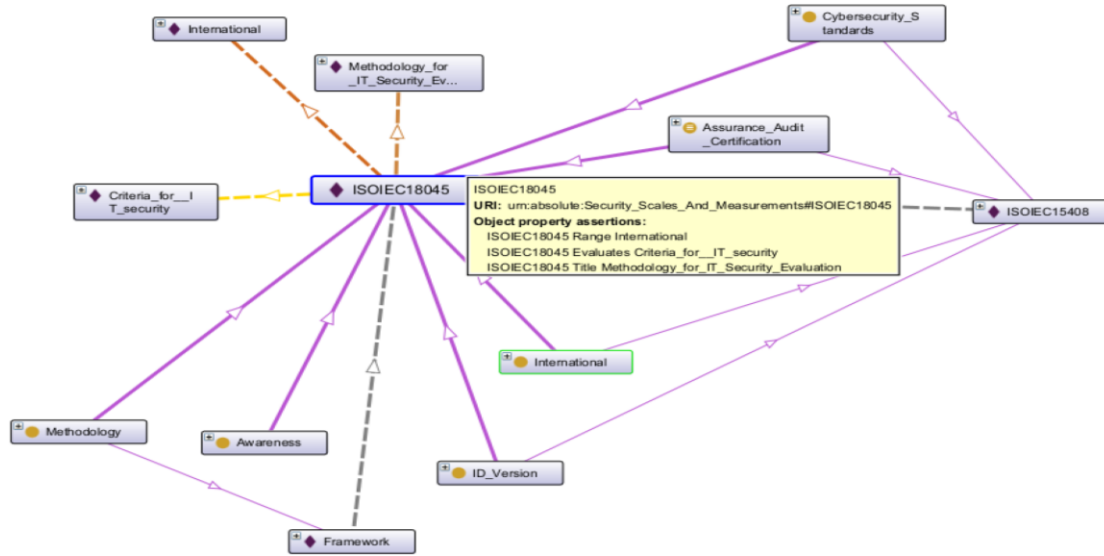


Figure 13. Cybersecurity Standards indicative instances depicting their semantic relations expressed via RDF semantic object and data properties in Protégé.

### 5.3.4 Ontology application

This section presents a real-life scenario related to an ICT stakeholder's specific criteria to illustrate the application of the proposed taxonomy. Section 5.3.4.1 describes the use-case scenario and Section 5.3.4.2 provides the generated results.

#### 5.3.4.1 Scenario description

The interested party has answered the relevant conceptual questions Q1-Q4 of the ontology as presented in the following, showing in italics the subsequent selections on the ontology, according to the scenario:

- Q1: He works in the Maritime Transport (Pillar-I: Sector)
- Q2: He is a/an CISO/InfoSec Manager (Pillar-II: Security Stakeholder Profile)
- Q3: Aiming to assess the organization's infrastructure for cyber risks and investigate whether the Target of Evaluation (TOE) meets cybersecurity requirements upon specified risk appetite and assurance level (Pillar-III: Security Domain; the current scenario resides in the "Evaluation, Assurance, audit and certification" category)
- Q4: The TOE is the vessel management system which utilizes AI Technologies and Machine Learning algorithms (Pillar-IV: Applications and Technologies)

Following the proposed ontology, the preferences on the conceptual pillars are depicted.

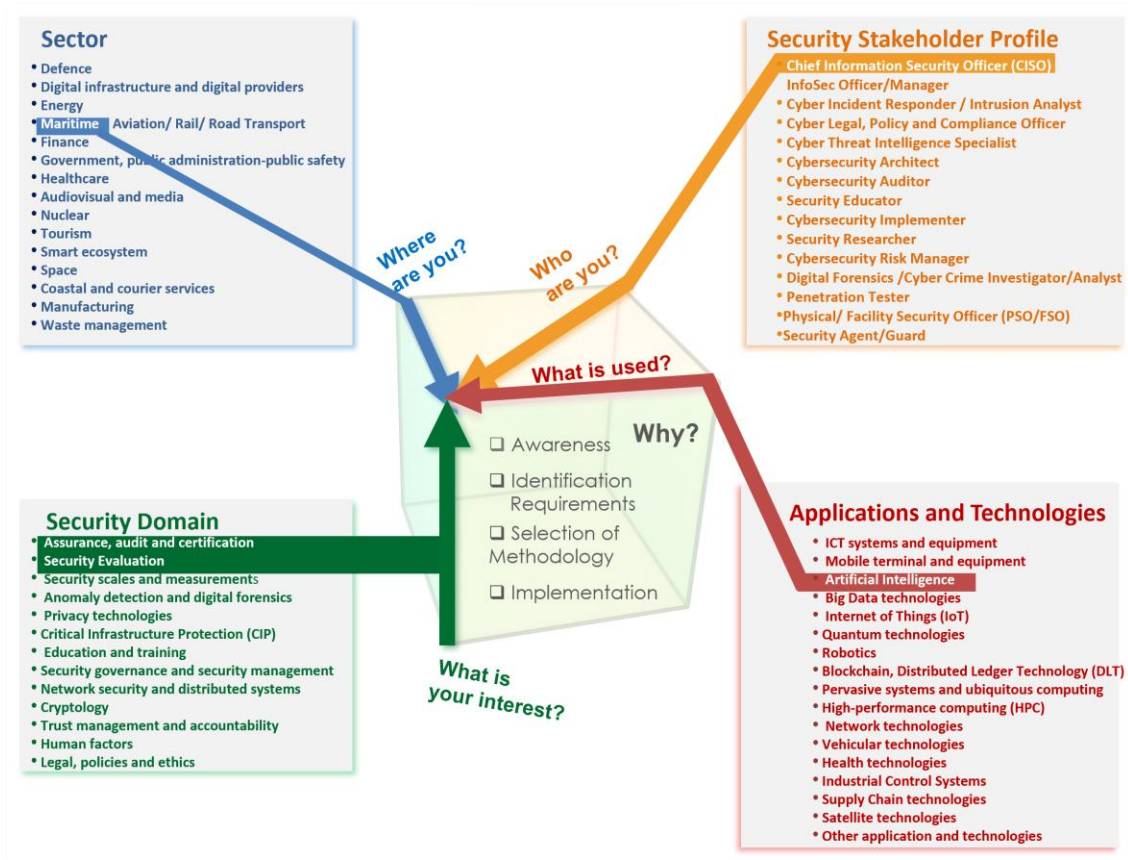


Figure 14. Quad selection of stakeholders on the conceptual pillars of the taxonomy to identify relevant Standards/Frameworks/Best practices for the ToE security management.

Concerning standards purpose of use, all categories are relevant (e.g. requirements/methodology/implementation standards help assessing risks, awareness standards in understanding the threat landscape).

#### 5.3.4.2 Results

Novel AI-based technologies produce a wave of new diffused threats which cannot be holistically identified, prevented, and controlled as these technologies are still a new area of investigation. Future research could explore potential weaknesses and means to improve their security. Considering that emerging technologies can be partially protected, the AI technologies category (Pillar-IV) of the proposed taxonomy aims to gather information on prominent existing standards developed to address threats and vulnerabilities of AI systems and eliminate these security gaps. Standards/Frameworks/Best practices for AI-based systems are presented under two perspectives:

- standards and practices for utilizing AI technologies to secure interconnected systems (AI security)
- standards for securing AI-based systems (Secure AI).

The ETSI Industry Specification Group on Securing Artificial Intelligence (ISG SAI) has developed standards to preserve and improve the security of AI-based systems focusing on three topics:

- using AI to enhance security
- encounter attacks that leverage AI
- securing AI-based systems from attacks

AI-based Standards/Frameworks/Best Practices of the current results, are generated considering the scenario pre-defined criteria. The overall ontology's results are depicted in a tabular structure, reflecting Standards/Frameworks/Best Practices and their attributes (cf. Table 9), according to stakeholder's preferences (four pillars) and standards' purpose of use. Some of them were found in more than one pillars categories. The results, presented in Table 10, were prioritised following stakeholders' preferences (four pillars). Standards related to IT Evaluation and conformity assessment for Maritime Transport infrastructures, specifically for AI-based systems, are prioritised along with some indicative methodologies and frameworks proposed for adoption.

Table 10. Standards/Frameworks/Best practices delivered results towards stakeholder's pre-defined criteria.

| <b>Range</b><br>(International<br>/Regional/Eur<br>opean level) | <b>Type</b><br>(Standard/<br>TR/TS/PA<br>S/ AWI/<br>framework<br>k/ best<br>practice/<br>other) | <b>ID/Version/Title/<br/>Year</b>                                                                                                                      | <b>Publisher/<br/>Technical<br/>Committee</b><br>(Standardiz<br>ation Body/<br>Policy<br>maker,<br>Other) | <b>Purpose of Use</b>                           | <b>Pillar/Category</b>                    |
|-----------------------------------------------------------------|-------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|-------------------------------------------------|-------------------------------------------|
| International                                                   | Standard                                                                                        | ISO/IEC 18045:2022<br>Methodology for IT Security<br>Evaluation                                                                                        | ISO/IEC                                                                                                   | Awareness/<br>Methodology                       | Maritime Transport<br>Security Evaluation |
| International                                                   | Standard                                                                                        | ISO/IEC 27001:2022<br>Information security,<br>cybersecurity, and privacy<br>protection — Information<br>security management<br>systems — Requirements | ISO/IEC                                                                                                   | Requirements<br>Identification /<br>Methodology | InfoSec Manager                           |
| International                                                   | TS                                                                                              | ISO/IEC TS 27008:2019<br>Information technology —<br>Security techniques —<br>Guidelines for the assessment<br>of information security<br>controls     | ISO/IEC                                                                                                   | Methodology                                     | InfoSec Manager                           |

|               |          |                                                                                                                                                                          |         |                                                         |                                |
|---------------|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|---------------------------------------------------------|--------------------------------|
| European      | TS       | ETSI TS 102 165-1 ETSI-TVRA (Threat Vulnerability Risk Analysis)                                                                                                         | ETSI    | Awareness/ Methodology                                  | Security Evaluation            |
| International | Standard | ISO/IEC 23894:2023 Information Technology- Artificial Intelligence- Guidance on risk management                                                                          | ISO/IEC | Awareness/ Methodology                                  | Secure AI                      |
| International | AWI      | ISO/IEC AWI TS 5471: Artificial intelligence — Quality evaluation guidelines for AI systems                                                                              | ISO/IEC | Implementation                                          | Secure AI                      |
| International | AWI      | ISO/IEC AWI TS 6254: Information technology — Artificial intelligence — Objectives and approaches for explainability of ML models and AI systems                         | ISO/IEC | Awareness/ Methodology                                  | AI Security                    |
| International | Standard | IEEE P2807.1 - Standard for Technical Requirements and Evaluation of Knowledge                                                                                           | IEEE    | Awareness/ Requirements Identification/ Methodology     | AI Security                    |
| International | Guidance | AI RM Framework (2 <sup>nd</sup> Draft September 2022)                                                                                                                   | NIST    | Methodology                                             | Secure AI, Security Evaluation |
| European      | Standard | ETSI GR SAI 001 v1.1.1 (2022-01)                                                                                                                                         | ETSI    | Awareness/ Methodology                                  | Secure AI                      |
| European      | Standard | ETSI GR SAI 002 v1.1.1 (2021-08)                                                                                                                                         | ETSI    | Requirements Identification                             | Secure AI                      |
| European      | Standard | ETSI GR SAI 005 v1.1.1 (2021-03)                                                                                                                                         | ETSI    | Methodology/ Implementation                             | Secure AI                      |
| International | Guidance | AI Policy Contributions (2022)                                                                                                                                           | NIST    | Implementation                                          | Secure AI                      |
| International | Standard | ISO 28001/28002:2007 Security management systems for the supply chain — Best practices for implementing supply chain security, assessments, and plans — Requirements and | ISO     | Awareness/ Requirements Identification / Implementation | InfoSec Manager                |

|                                                          |                |                                                                                                                                                                         |         |                                           |                                                       |
|----------------------------------------------------------|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|-------------------------------------------|-------------------------------------------------------|
| guidance / Development of resilience in the supply chain |                |                                                                                                                                                                         |         |                                           |                                                       |
| International                                            | Standard       | ISO 28003:2007 Security management systems for the supply chain – Requirements for bodies providing audit and certification of supply chain security management systems | ISO     | Awareness/ Requirements Identification    | Assurance/Audit/ Certification                        |
| International                                            | Standard       | ISO 20858:2007 Port facility security assessments and security plan development                                                                                         | ISO     | Awareness/ Methodology                    | Maritime Transport                                    |
| International                                            | Certification  | Onboard ship certification                                                                                                                                              | DNV     | Requirements Identification               | Maritime Transport                                    |
| International                                            | Standard       | ISO/IEC 17067:2013 – Conformity Assessment – Fundamentals of product certification and guidelines for product certification schemes                                     | ISO/IEC | Awareness/ Methodology                    | Security Evaluation<br>Assurance/Audit/ Certification |
| International                                            | Standard       | ISO/IEC 17021-1:2015 Conformity assessment – Requirements for bodies providing audit and certification of management systems                                            | ISO/IEC | Awareness/ Identification of Requirements | Assurance/Audit/ Certification                        |
| International                                            | Standard       | ISO/IEC 17020:2012 Conformity assessment – Requirements for the operation of various types of bodies performing inspection                                              | ISO/IEC | Awareness/ Identification of Requirements | Assurance/Audit/ Certification                        |
| European                                                 | Best Practices | Cyber Risk Management for Ports (2020)                                                                                                                                  | ENISA   | Methodology/ Implementation               | Maritime Transport                                    |
| European                                                 | Best Practices | Port Cybersecurity - Good practices for cybersecurity in the maritime sector (2019)                                                                                     | ENISA   | Awareness/ Methodology/ Implementation    | Maritime Transport                                    |
| International                                            | TR             | ISO/IEC TR 15443: 2012 Security Assurance Framework                                                                                                                     | ISO/IEC | Awareness/ Methodology                    | Assurance/Audit/ Certification                        |



|               |          |                                                                                                                                                                       |         |                                |                                   |
|---------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|--------------------------------|-----------------------------------|
| International | TR       | ISO/IEC TR 15446:20-<br>Information Technology-<br>Security techniques                                                                                                | ISO/IEC | Implementation                 | Assurance/Audit/<br>Certification |
| International | Standard | ISO/IEC DIS 27006-1<br>Requirements for bodies<br>providing audit and<br>certification of information<br>security management<br>systems                               | ISO/IEC | Requirements<br>Identification | InfoSec Manager                   |
| International | Standard | ISO/IEC 27014:2020<br>Information security,<br>cybersecurity, and privacy<br>protection — Governance of<br>information security                                       | ISO/IEC | Methodology                    | InfoSec Manager                   |
| International | Standard | ISO/IEC 27021:2017<br>Information technology —<br>Security techniques —<br>Competence requirements for<br>information security<br>management systems<br>professionals | ISO/IEC | Requirements<br>Identification | InfoSec Manager                   |

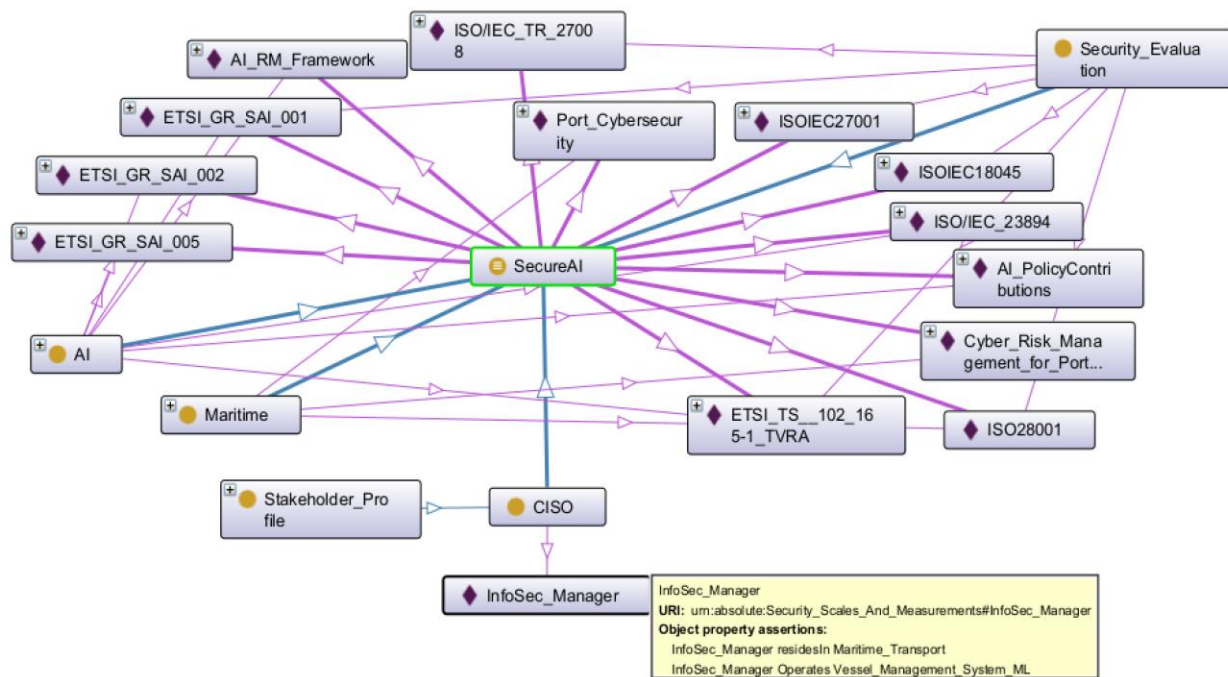


Figure 15. A combination of cybersecurity standards, frameworks and best practices related to security evaluation of AI/ML-based infrastructures together with sectoral cybersecurity guidelines for maritime transport.

# PART IV:

## Cybersecurity risk management methodology for ICT products and supply chain services

---

## 6. CyberICT Risk Management Methodology

This Section presents the CyberICT Risk Management Methodology and the corresponding risk ontology. It presents their demonstration, practical adoption and the evaluation approach.

### 6.1 Building Blocks

This section highlights the scope and objectives of the CyberICT Risk Management methodology, indicates the models, practices and aspects of standards the current risk assessment adopts.

#### 6.1.1 Scope and Objectives

The primary objective of the CyberICT Risk Management methodology is to provide a holistic view of the ICT attack surface by exploring ICT products with technical complexity and/or heterogeneous dependent ICT infrastructures across large-scale interconnected supply chain networks. The proposed methodology enables ICT operators to represent their infrastructures through business models and analyse in-depth the inherent cyberdependencies within an entity and across various interconnected networks to understand the technical specificities and security particularities.

CyberICT provides a Cybersecurity Risk Management methodology allowing ICT operators to identify, analyse and estimate threats, vulnerabilities, risks and their cascading effects on composite ICT environments, such as composite products and their ICT supply chain services (Section 3.2). The CyberICT hybrid evaluation framework relies on a foundational knowledge management framework, which helps extract both explicit and implicit security knowledge during risk analysis, improving the understanding of the ICT product's security posture. Cybersecurity risk assessment and risk management concepts are semantically represented (see Section 6.2.3) to promote cybersecurity awareness and guide ICT stakeholders on how to thwart or mitigate threats and risks in complex ICT infrastructures. The CyberICT Risk Management methodology contributes to challenges #3-#5, provided in Section 5.1, and follows the corresponding Dissertation Objectives (DOs), which are further analysed below for ICT products and ICT SCS:

- Analyse and decompose ICT products into their primary elements (i.e, ICT assets) to understand their security posture.
- Assess the security of an ICT product which can help ICT Manufacturers and Product Owners to get prepared for EU conformity assessment procedures related to CRA [11] or CSA [13]
- Calculate individual risks in ICT assets and estimate their propagated and cumulative values, in case a stringent security evaluation is required/adopted.
- Identify and measure all relevant cyber threats and risks of an ICT product and its ICT supply chain elements (in case it's on the risk assessor's objective to go through a further security analysis).

As previously presented, CyberICT also guides interested parties in conducting risk assessments on the product's supply chain networks. In terms of ICT supply chain risk assessment, CyberICT Risk Management methodology aims to:

- Analyse the ICT Supply Chain Service (ICT SCS) network and break it down into its main elements (i.e., ICT services, ICT processes and ICT assets) to assess their security in a holistic-technical approach (end-to-end ICT supply chain service risk assessment)
- Promote different aspects of analysis on complex ICT supply chain networks, i.e., business-agnostic, holistic-technical and sectoral analysis.
- Promote threat intelligence and enhance knowledge about potential attacks, tactics using standards-based threat catalogues (e.g., MITRE ATT&CK [142] and CAPEC [272]) and investigate the adversary's profile and the cyberattack course within a large-scale ICT network by exploring attack graphs.
- Delve into the technical characteristics of a cyberattack and explore all possible attack paths an adversary could follow through the ICT supply chain network in relation to a specific confirmed event.
- Investigate complex threat scenarios utilising business modelling and knowledge management methods.
- Compute the risk propagation on the underlying product, system, or infrastructure, and prioritise risks.
- Identify key processes and assets on ICT SCS, considering their criticality to the provision of the ICT SCS.
- Guide ICT stakeholders to conceive a proper mitigation strategy.
- Delineate how the security controls are mutually agreed and adopted by ICT stakeholders and business partners participating in a supply chain, considering the risk results and the indicated defence strategies.

### **6.1.2 Regulatory background, related security standards and best practices**

CyberICT Risk Management methodology relies on the ICT product, ICT service, ICT process and ICT supply chain definitions of the CSA regulation [13] and its recent CSA 2 proposal [49]. It adopts the concepts of information security assets and Information Security Management System (ISMS) of ISO/IEC 27001:2022 [55] international standard to create the ICT inventory the under evaluation ICT elements. It is based on the ISO/IEC 27005:2022 [56] stepwise risk assessment procedure for the identification of threats and vulnerabilities which enable the estimation of risks and their corresponding risk levels. It relies on security and resilience concepts of supply chain management systems, identified in ISO 28000:2022 [138], ISO 28001:2007 [70], and ISO 28004-1:2007 [206] international standards to identify the risk assessment process to assess the security of ICT supply chains.

Regarding the technical analysis of ICT assets, it utilises the Common Platform Enumeration (CPE) of MITRE [268]. For the threat analysis, it utilises threat-related catalogues and attack tactics of MITRE (i.e., CAPEC [272] and, ATT&CK [142]). To identify vulnerabilities on ICT assets, it utilises widely recognised open repositories i.e., CVE MITRE [140] – NIST National Vulnerability Database (NVD) [269], Open Software Vulnerability (OSV) database [270] and Github Advisory [271]. In addition, it adopts the Common Weakness Enumeration (CWE) of MITRE [266]. For guiding on mitigation measures it utilises the NIST Special Publication (SP) 800-53 [368].

To analyse the identification and evaluation of cybersecurity incidents, addressed by the NIS 2 Directive [12], CyberICT estimates how an attacker has moved inside an entity to perform an intrusion and analyse incident-related information in the potential of a confirmed security event. This is generally based on concepts of NIST Incident Response Lifecycle [369] and ISO/IEC 27035 [153].

The CVSS 3.1 [139] of FIRST contributes to calculate the vulnerability exploitability level using the MESS exploitability subscore formula. In addition, the MISS modified impact subscore formula in relation to the scope metric contribute to calculate the impact level. The environmental group metrics of CVSS 3.1 are additionally mapped with the asset criticality scale.

The Attacker's Profile is created by adopting the attacker's capacity and attacker's location, specified in NIST SP 800-30 [125], which is the gold standard framework for conducting risk assessments within organisations. Moreover, it contributes to calculate the vulnerability exploitability level.

### **6.1.3 Business Process Models**

As described in Section 3.4.1, the business process modelling language BPMN 2.0, which reflects the ISO/IEC 19510 [114] is used to create business models when analysing complex ICT networks, such as in ICT Supply Chain Services (ICT SCS), to decompose the service into its primary elements by identifying a set of key ICT processes (see Step 1 of the methodology). Furthermore, the business process models delineate the part of the ICT infrastructure(s) used, and the corresponding systems and their assets operating for each ICT SCS process identified. Business process models may also be used for visualising an attack scenario on an ICT infrastructure (see Section 6.4.1). Business process models are mostly used to improve the understanding of the ICT SCS elements and their security issues. They are utilised as an auxiliary tool to support the business analysis of the ICT supply chain model.

### **6.1.4 Ontology-based Models**

A cybersecurity risk ontology has been created to illustrate the security concepts of ICT products and supply chain services, and their interrelations (e.g., between weaknesses, vulnerabilities and threats). To this aim, the widely recognised knowledge management Nonaka SECI model is used to explore knowledge management flows in the ICT ecosystem. Moreover, the foundational knowledge management framework of SECI model [132] is utilised as a conceptual framework to drive the transformation of abstract cybersecurity knowledge into a machine-readable format (see Section 6.2.3).

To develop the CyberICT Risk Ontology, a list of semantic web W3C standards are utilised: OWL 2 [130] semantic language and RDF [129] framework are utilised for this purpose to externalise implicit knowledge and support the thorough comprehension of the explicit knowledge by defining semantic relations between the security concepts of products and their supply chains. Moreover, the SPARQL semantic query language [131] is utilised to structure queries within the risk ontology and elicit security information.

### 6.1.5 Attack Simulation, cumulative and propagation assessments

The CyberICT Risk Management Methodology uses the Vulnerability Chains Discovery method, described in [276],[370], to generate vulnerability chains and deliver all possible attack paths and patterns. The methodology investigates via simulated scenarios the exploitation of vulnerability chains through inferred attack paths to conduct vulnerability assessment and estimate the cascading effects of risk implementation and risk propagation. As long as the vulnerability chains are generated, an attack prediction recommending system approach is provided [276] following an attack classification process that prioritises the attacks by utilising a k-nearest neighbour-based algorithm and a multi-level collaborative filtering method [379]. The attack graph generation algorithm of the Vulnerability Chains Discovery method defines a set of propagation and attack path construction rules to estimate the risk propagation [276],[370].

The CyberICT Risk Management Methodology relies on the Vulnerability Chains Discovery method [276],[370] and the definitions and calculation models of the MSCRA approach [371] – [372] regarding the Entry Chain, Cumulative Chain, the individual propagated and propagated assessments to calculate the corresponding vulnerability, impact and risk levels (see sections 6.2.2.4 and 6.2.2.6. Specifically, the CyberICT Risk Management Methodology enhances these computation models by adjusting in these calculations the individual vulnerability exploitability and the exploitation level chain models developed during the current dissertation research. Specifically, the latter models enhance the MSCRA approach and the Vulnerability Chains Discovery method by adopting a weighted scoring model that considers intrinsic vulnerability technical characteristics and attacker-specific characteristics based on the CVSS 3.1 [139] specification metrics and NIST attacker's capability, intention and location [125].

The Attack Simulation and Evidence Chain Generation (ASECG) model (see Section **Error! Reference source not found.**) uses the Vulnerability Discovery method to estimate all alternative chains of sequential vulnerabilities on the ICT assets. To achieve this, the Vulnerability Chains Discovery method [276],[370] executes logic rule-based reasoning mechanisms to build the attack graph and generate the attack paths. The Attack Simulation and Evidence Chain Generation (ASECG), created in the context of the current dissertation research, enhances the Vulnerability Discovery method by developing an algorithm that estimates and prioritises the attack paths associated with a specific confirmed security event delivering credible vulnerability chains.

### **6.1.6 Additional related work**

Additional research works were considered for specific aspects of the current CyberICT Risk Management Methodology. Specifically, the proposed methodology relies on the research works in [245]-[246], [371] and enhances supply chain and security concepts.

The asset criticality rule regarding the use of the betweenness centrality algorithm was based on the work presented in [15]. Asset interdependencies were based on generic aspects, presented in [373].

The game-theoretic algorithm implementations in [372]-[373] present optimal ways of selecting attacker and defender actions for considering the identification of mitigation strategies. These algorithms are not used in the calculations of the proposed CyberICT Risk Management Methodology. They are only mentioned in step 6 as recommended techniques to be considered by the ICT stakeholders and business partners when exploring potential mitigation strategies.

### **6.1.7 Users of CyberICT Risk Management methodology**

The CyberICT Risk Management Methodology is used by actors of the ICT ecosystem. Since it refers to both ICT products and ICT SCS, target groups are considered the ICT manufacturers, ICT product vendors, ICT service providers, entrepreneurs importers, and ICT supply chain operators. In the CyberICT Risk Management Methodology the party that initiates the risk assessment process, and it is the main actor of the assessment is considered the primary “ICT stakeholder”, whereas other entities and experts involved are considered “Business Partners”. Moreover, sectorial professions, such as SCADA/EMS operators, industry experts, such as Ship Agents, Carrier Agents, Local Agents, Terminal Operators, forwarders, Marine Underwriters and other experts can be considered as secondary users. Nonetheless, the CyberICT Risk Management Methodology engages multiple actors of the ICT ecosystem.

In terms of ICT security, it directly involves, Risk Assessors, Risk Managers, IT security experts, Cybersecurity professionals and DevSecOps Engineers. CISO, SOC and other relevant security professionals, from the categories of the CyberICT Standards Ontology, shown in Section 5.3. Concerning the use of the Attack path Simulation and Evidence Chain Generation (ASECG) model, the primary users could be Intrusion Analysts, Log Analysts, and Incident Managers. At a greater extent, Laboratory testers, Policy makers, CERTs, CSIRTs, and standardisation bodies could be also involved.

The proposed CyberICT Risk Management Methodology is designed to apply to all types and sizes of entities, i.e., SMEs, MEs, Large Enterprises, non-profit organisations, Military-Defence and governmental agencies and academics and research organisations. At a greater extent, users of certificates, IT auditors, Accredited test labs, Policymakers, CERTs, CSIRTs, and standardisation bodies.

It shall be noted that a cybersecurity risk assessment process is a complex and time-consuming process (especially for the ICT SCS evaluation of large-scale networks), where multiple departments are involved to capture the information required (e.g., operational department to

identify the infrastructure operations, security department or external vendors for conducting the threat, vulnerability and risk analysis, etc.

## **6.2 Design and development of the CyberICT Risk Management methodology**

This section presents the Cybersecurity Risk Management methodology for ICT products and their ICT supply chain services. Section 6.2.1 provides an overview of CyberICT methodology, while Section 6.2.2 analyses it step by step. Section 6.2.3 describes the risk ontology developed.

### **6.2.1 Methodology Overview**

This section provides an overview of the CyberICT Risk Management methodology, including key characteristics and the overall structure.

#### **6.2.1.1 Key characteristics at a glance**

CyberICT Risk Management methodology is a knowledge-based, evidence-driven and collaborative methodology for managing cyber risk of ICT products and their ICT Supply Chain Services (SCS). It is knowledge-based as it produces an ontology model aiming to represent cybersecurity risk assessment knowledge in a formalised and structured manner (See Section 6.2.3).

This approach deals with ICT products and ICT infrastructures and can be respectively applied to complex ICS systems, such as SCADA systems to assess their cyber-risks. Its dynamic and collaborative notion derives from an evidence-driven Supply Chain Risk Assessment holistic approach, which is implemented towards a step-by-step procedure. It reflects diverse evaluation aspects of the ICT SCS and their ICT elements, enabling cooperation and risk-handling transparency among the ICT stakeholders and generating unique evidence about risk assessment and mitigation.

#### **6.2.1.2 Overall structure**

The CyberICT Risk Management methodology is distinguished into two phases:

- **Phase I – Cybersecurity Risk Assessment**  
The Cybersecurity Risk Assessment phase includes all successive steps required to conduct the Risk Assessment (RA) process for the ICT product and/or ICT SCS, which are under evaluation. The Risk Assessment phase begins with defining the scope and boundaries of the assessment and concludes with establishing a framework for estimating cyber risks associated with ICT assets. In addition, it aims to generate evidence-based insights from alternative scenarios, considering potential adversaries' courses of action.
- **Phase II – Cybersecurity Risk Management**



The Risk Management phase encompasses all the subsequent steps required to identify the optimal defence to treat the estimated risks and specify the appropriate risk monitoring that prevents or mitigates the risk propagation to the product or ICT SCS.

Each of the phases enfold a set of subsequent steps and substeps, as shown in Figure 16. Each high-level step and its corresponding substeps are formalised in a three-level tabular approach, i.e., “Input”, “Activity”, “Output”, which utilises the following template:

Table 11. Methodology structural template.

| Step X. 1 <sup>st</sup> level step<br>Step X.n. 2 <sup>nd</sup> level step<br>Step X.n.z 3 <sup>rd</sup> level step |                                                                                                                          |
|---------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <b>Input</b>                                                                                                        | <i>It describes the prerequisite of the particular step.</i>                                                             |
| <b>Activity</b>                                                                                                     | <i>It presents the content of the particular step.</i>                                                                   |
| <b>Output</b>                                                                                                       | <i>It illustrates the result of the particular step, including resources, documentation and other existing material.</i> |
| <b>Example</b>                                                                                                      | <i>It provides a short example of the step to enhance comprehension.</i>                                                 |

As indicated in Table 11, the examples provided in the template are intentionally concise in order to facilitate the reader’s understanding of the methodology steps. The applicability of the proposed methodology to detailed use cases is presented in Section 6.4.

Figure 16 presents the overall structure of the CyberICT Risk Management Methodology.

| Risk Assessment Phase                                             |                                                                                                                             |                                          |                                                          |                                                                                                                                                                                                                                                                                                                     |                                      | Risk Management Phase                                                                    |
|-------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------|----------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|------------------------------------------------------------------------------------------|
| Step 0<br>Set the boundaries of the Cybersecurity Risk Assessment | Step 1<br>Modelling-based cartography                                                                                       | Step 2<br>Cyber Threat Intelligence      | Step 3<br>Vulnerability and Impact analysis              | Step 4<br>Attack Simulation and Evidence Chains Generation                                                                                                                                                                                                                                                          | Step 5<br>Risk estimation            | Step 6<br>Risk treatment                                                                 |
| Step 0.1<br>Define the Subject to be Evaluated                    | Step 1.1<br>Define Criticality on ICT Products and ICT Supply Chain Services                                                | Step 2.1<br>Cyber Threat Identification  | Step 3.1<br>Individual Vulnerability Assessment          | Step 4.1<br>Generation of Vulnerability Chains<br>Step 4.1.1 Identify Asset Dependency Graphs<br>Step 4.1.2 Define Entry Points<br>Step 4.1.3 Define Target Points<br>Step 4.1.4 Perform Individual Vulnerability Assessment<br>Step 4.1.5. Produce Vulnerability Chain                                             | Step 5.1<br>Individual Risk Analysis | Step 6.1<br>Mitigation Strategies Identification – Risk Compliance to Security Assurance |
| Step 0.2<br>Mutual Agreement of the Perimeter of the Assessment   | Step 1.2<br>ICT Stakeholder and Business Partners Identification                                                            | Step 2.2<br>Vulnerability Identification | Step 3.2<br>Vulnerability Exploitation                   | Step 4.2<br>Recurring process Activation<br>Step 4.2.1: Points of Compromise – Indicators of Compromise<br>Step 4.2.2: Reconstruction of Potential Attack Paths<br>Step 4.1.3: Attacker's Profile Identification<br>Step 4.1.4: Prioritisation of Potential Attack Paths<br>Step 4.1.5.: Pruning Process Activation | Step 5.2<br>Cumulative Risk Analysis | Step 6.2<br>Optimal Mitigation Strategy Selection and Implementation                     |
| Step 0.3<br>Define the Scope of the Assessment                    | Step 1.3<br>ICT Analysis and Modelling<br>Step 1.3.1: ICT Product Analysis<br>Step 1.3.2: ICT Supply Chain Service Analysis | Step 2.3<br>Cyber Threat Scenarios       | Step 3.3<br>Individual Impact Analysis                   |                                                                                                                                                                                                                                                                                                                     | Step 5.3<br>Propagated Risk Analysis |                                                                                          |
|                                                                   |                                                                                                                             | Step 2.4<br>Cyber Threat Assessment      | Step 3.4<br>Cumulative Vulnerability and Impact Analysis |                                                                                                                                                                                                                                                                                                                     |                                      |                                                                                          |
|                                                                   |                                                                                                                             |                                          | Step 3.5<br>Propagated Vulnerability and Impact Analysis |                                                                                                                                                                                                                                                                                                                     |                                      |                                                                                          |

Figure 16. The CyberICT Risk Management Methodology.

### 6.2.2 Methodology analysis

This section presents analytically the CyberICT Cybersecurity Risk Management methodology in a stepwise approach. Steps 0-5 support the Risk Assessment Phase I, while step 6 applies to the Risk Management Phase II (see Section 6.2.1).

#### 6.2.2.1 Step 0. Set the boundaries of the Cybersecurity Risk Assessment

Before the cybersecurity risk assessment of the ICT product commences, a set of initial steps should be executed to set the boundaries of the assessment:

- Step 0.1. Define the subject to be evaluated
- Step 0.2. Mutual agreement of the perimeter of the assessment
- Step 0.3. Define the scope of the assessment

The following table summarises Step 0.

Table 12. Set the boundaries of the Cybersecurity Risk Assessment.

| Step 0. Set the boundaries of the Cybersecurity Risk Assessment<br>Step 0.1. Define the subject to be evaluated<br>Step 0.2. Mutual agreement of the perimeter of the assessment<br>Step 0.3. Define the scope of the assessment |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Input</b>                                                                                                                                                                                                                     | Standards, security policies, security controls and other baseline information and documentation required before the cybersecurity risk assessment begins.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Activity</b>                                                                                                                                                                                                                  | Definition of the RA boundaries (i.e., assessment's scope, requirements, perimeter, key modules to be evaluated). Agreement through formal documentation on the assessment conditions and subject to be evaluated, consensus on the risk levels to be reached, commitment to undertake appropriate security controls.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Output</b>                                                                                                                                                                                                                    | Boundaries of the cybersecurity risk assessment are set. Agreement as a formal documentation (e.g. SD, SDA, MRA) on the subject, scope, perimeter and conditions of the evaluation.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Example</b>                                                                                                                                                                                                                   | <p><u>Input:</u> The vehicles SCADA-based system is based on ISO/SAE 21434 international standard on Road Vehicles Cybersecurity Engineering [374].</p> <p><u>Activity:</u> The subject to be evaluated is a vehicle, focusing its evaluation perimeter on its SCADA-based ICT components. A deep security evaluation will be conducted to analyse the security of a critical ICT supply chain service related to the vehicle's transport, i.e., the Vehicle Transport Service (VTS). The holistic-technical evaluation aspect will be adopted for the cybersecurity risk assessment analysis.</p> <p><u>Output:</u> A Mutual Recognition Agreement (MRA) was established between the automobile manufacturer and a U.S.-based vehicle IT provider. An accompanying detailed Security Declaration (SD) specified the risk levels to be addressed, the applicable security controls, and the mutual commitments to be implemented following the assessment.</p> |

Step 0 and its embedded steps are further described in the following.

### Step 0.1 Define the subject to be evaluated

As an initial step, the subject to be evaluated must be identified. As described in the previous chapters (i.e., Chapter 3 and Chapter 4), the ICT ecosystem is a complex system comprising various elements. The subject of evaluation can be one of these elements of the ICT ecosystem, or a group of elements (see Section 3.1). Moreover, a subject of evaluation can be an ICT product, a part of an ICT product, or an ICT product and its ICT supply chain services. The selected item or unit that will pass through the cybersecurity risk assessment process is considered the subject of evaluation.

### Step 0.2 Mutual agreement on the perimeter of the assessment

The ISO/IEC 20000-1:2018 international standard on “Service management systems’ requirements” [375] identifies an SLA as a business agreement between business partners that clarifies the content of risk assessment as a service, its subservices, goals and targets. Cybersecurity risk assessment can be executed in various cases and entities, as described in the following.

**i) Cybersecurity risk assessment within an organisation.** To perform a cybersecurity risk assessment in real ICT environments, a Service Level Agreement (SLA) including a security declaration shall be defined and signed between the organisation initiating the assessment and the suppliers participating in the specific cybersecurity risk assessment process.

**ii) Cybersecurity risk assessment of an ICT Supply Chain Service (ICT SCS).** If the evaluation includes an ICT Supply Chain Service (ICT SCS), the ICT stakeholder and the involved business partners shall establish an agreement to define the boundaries, objectives, and content of the underlying ICT SCS. The international standard ISO 28001:2007 on supply chain security [70] further requires a security declaration, which is a formal statement through which business partners commit to specifying the security measures (i.e., security controls applied to SCS assets) implemented within the ICT SCS.

Moreover, in the event of a collaborative cybersecurity risk assessment, as in the ICT SCS case, ICT stakeholders are engaged to describe, at a minimum, how goods and cyberphysical instruments operating within the ICT SCS are safeguarded, related information is protected, and these security measures are demonstrated and verified. In this respect, the current methodology sets the prerequisite for all involved business partners to sign an SLA agreement upon the examination of ICT SCS and an embedded Security Declaration (SD) to predefine [246]:

- the ICT assets, operating in the ICT processes of the ICT SCS, that are subject to evaluation;
- the security measures already implemented for the ICT assets of the ICT SCS for the ICT stakeholder and each business partner involved;
- that all participants have reached consensus on the risk level(s) of the ICT SCS that they wish to achieve. The security level has been recorded;
- that all participants declare their commitment to undertake appropriate controls (whether required) to reach the ICT SCS security level (that they have agreed upon).

iii) **Cybersecurity risk assessment enhanced with a conformity assessment perspective.** In case a cybersecurity risk assessment is conducted on an ICT product and/or ICT SCS service with the purpose of contributing to a conformity assessment process<sup>14</sup> (see Section 4.6), the involved partners are required to construct and sign, apart from the Security Declaration (SD), a Mutual Recognition Agreement (MRA) if non-EU members are involved.

An indicative format of a potential Security Declaration and Statement of Application (SDA), enhanced with ISO 15408 [44] and ISO 28000 [70] concepts, is provided in Appendix C.

### Step 0.3 Define the scope of the assessment

The boundaries of the cybersecurity risk assessment are set according to the signed contractual agreement. The scope and objectives of the assessment are defined along with the key components of the subject to be evaluated. In addition, the ICT stakeholders and the involved business partners shall collaborate to determine the scope of the subject of evaluation and the expected outcomes of the cybersecurity risk assessment process, in alignment with their business objectives [84]. The ICT structures and concepts are adopted (cf. Section 3.1), such as the ICT supply chain model (cf. Section 3.2.3.2) and security concepts (e.g., security vulnerability, cyber threat, and attack scenario) of adopted standards (e.g., ISO/IEC 15408, ISO/IEC 27k and ISO 28k series).

If the purpose of the evaluation is enhanced with conformity assessment concepts, the scope is expanded. For example, in addition to producing risk assessment results, the scope may include the creation of a Protection Profile for an ICT product and/or the evaluation of its claims by either a self-assessor or a third-party Conformity Assessment Body (CAB), depending on the adopted assurance level, as described in Section 4.6.

Furthermore, in case an ICT SCS is under evaluation, the current step defines its evaluation aspect considering the three dimensions defined in the ICT supply chain model (Section 3.2.3.2):

- **Business aspect.** It aims to explore the business aspect of the ICT SCS by identifying and assessing key business-related elements that directly support the ICT SCS provision. It considers processes, business partners and third parties, facilities, business logic (e.g., data flows and decision-making), and applicable legal or regulatory constraints. The evaluation scope includes all ICT SCS processes, partners, and data involved in the ICT SCS without including the technical details of ICT assets.
- **Holistic-technical aspect.** It aims to expand the business aspect by incorporating an asset-based, interdependent perspective of all activities involved in delivering the SCS. It includes business processes, business partners, and all cyber and physical assets supporting the ICT SCS, complemented by asset models that illustrate asset

---

<sup>14</sup> For instance, to assess the product's compliance against the Cyber Resilience Act [11] requirements or create a Protection Profile to go through a cybersecurity certification evaluation procedure according to an adopted EU cybersecurity certification scheme [14][13].

interdependencies. Therefore, the evaluation scope includes assessing the security of ICT SCS processes, ICT assets of the involved participants, and related data.

- **Sectoral aspect.** It aims to assess the ICT SCS towards vertical dependency analysis. It is a sector-specific technical aspect of a single business partner participating in the ICT SCS. The evaluation scope includes the ICT sectoral processes and assets hosted and operated by the focused business partner to support the provision of the ICT SCS.

#### 6.2.2.2 Step 1. Modelling-based cartography

The aim of the current step is to analyse and model the ICT product and the ICT SCS. This step is further analysed into lower level steps, as shown below, and explained in the following sections.

- Step 1.1 Define criticality on ICT products and ICT Supply Chain Services
- Step 1.2 ICT stakeholder and business partners identification.
- Step 1.3 ICT analysis and modelling
  - Step 1.3.1 ICT product analysis
  - Step 1.3.2 ICT Supply Chain Service analysis

The following table summarises Step 1.

Table 13. Modelling-based cartography.

| Step 1. Modelling-based cartography<br>Step 1.1. Define criticality on ICT products and ICT Supply Chain Services<br>Step 1.2 ICT stakeholder and business partners identification<br>Step 1.3. ICT analysis and modelling<br>Step 1.3.1 ICT product analysis<br>Step 1.3.2 ICT Supply Chain Service analysis |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Input</b>                                                                                                                                                                                                                                                                                                  | Signed agreements and cybersecurity risk assessment perimeter and conditions to be considered.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Activity</b>                                                                                                                                                                                                                                                                                               | <p>The scope of this step is to set the boundaries of the ICT product and ICT SCS analysis based on their criticality. The current step aims to analyse and model the subject to be evaluated. The under examination ICT product and ICT SCS are decomposed into their main elements:</p> <ul style="list-style-type: none"> <li>• The ICT product is decomposed into its main elements</li> <li>• The ICT SCS is analysed following the ICT supply chain model structure, presented in Section 3.2.3.2.</li> </ul> <p>The analysis depends on the selected evaluation aspect to be followed. Key elements are identified.</p>                    |
| <b>Output</b>                                                                                                                                                                                                                                                                                                 | <ul style="list-style-type: none"> <li>• Definition of the business partners involved and their representatives that will participate in the cybersecurity risk assessment process.</li> <li>• Identify criticality of ICT products, ICT SCS, ICT processes and ICT assets</li> <li>• ICT product analysis and decomposition into its primary elements</li> <li>• Record of key ICT processes, ICT infrastructures and ICT systems</li> <li>• ISMS (asset inventory)</li> </ul> <p>Creation of technical models (e.g., ICT architecture models) and business process models for the above topics, according to the evaluation aspect adopted.</p> |

|                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Example</b> | <p><u>Input:</u> Signed MRA and SDA</p> <p><u>Activity:</u> A short example of an ICT product analysis is mentioned in the corresponding section. Furthermore, indicative examples of the Vehicle Transport Service ICT supply chain service are presented across the sections of step 1 to illustrate the ICT SCS analysis.</p> <p><u>Output:</u> Tablet ICT product analysis, Vehicle Transport Service models and criticality identification, as presented with short examples across the sections of Step 1.</p> |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Step 1 and its corresponding sub-steps are presented in the following.

A seven-layer model-centric approach is developed to analyse the ICT components before identifying security information (e.g., threats and vulnerabilities). The model-centric approach is presented in Figure 17 and described in the following sections.

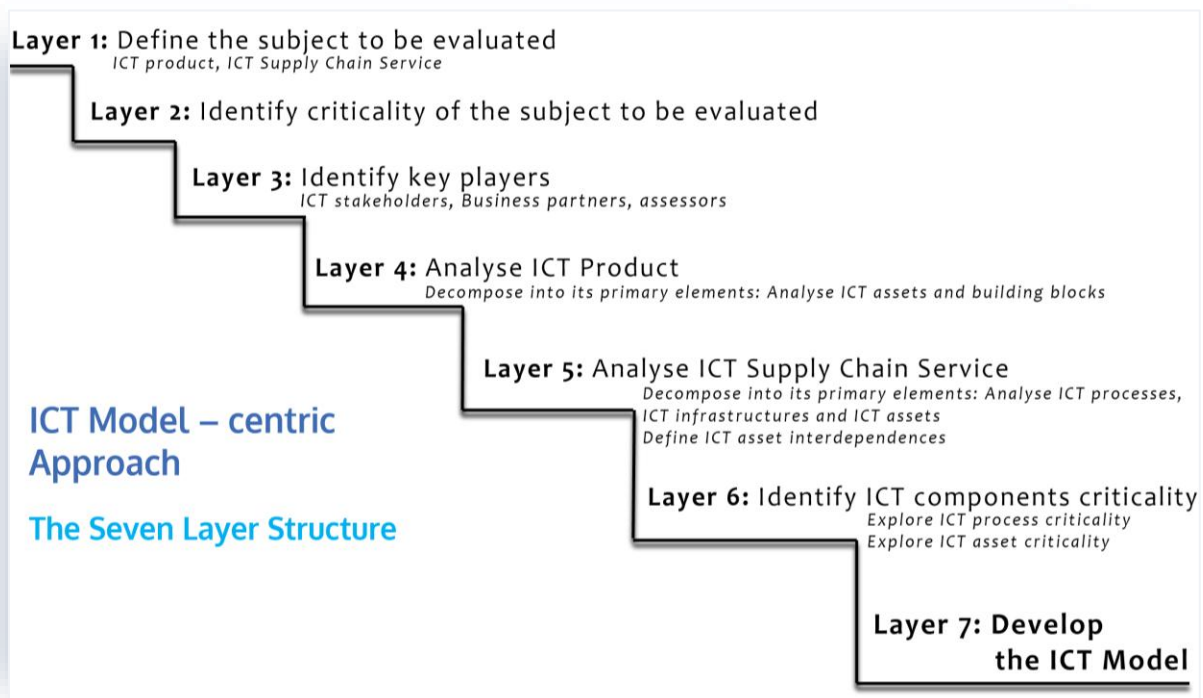


Figure 17. ICT model-centric cartography.

### Step 1.1 Define criticality on ICT products and ICT Supply Chain Services

The ICT product and ICT SCS are decomposed into their main elements to analyse process-centric and asset-centric views depending on the selected evaluation aspect (see Section 3.2.3.2 and Section 6.2.2.1). Key ICT elements are identified.

**Analysis based on the evaluation aspects.** The business evaluation aspect includes the identification of the cybersecurity risk assessment players (i.e., the ICT stakeholder and the business partners participating in the assessment) and the ICT processes of the subject that is evaluated. The holistic-technical evaluation aspect aims to identify ICT asset technical views of the ICT product and ICT SCS and their cross-cutting dependencies from an horizontal

perspective. As mentioned in Section 6.2.2.1, the holistic-technical includes the business evaluation aspect. Nonetheless, the sectoral evaluation aspect provides ICT asset views related to a single business partner that interacts with the ICT stakeholder who initiates the current cybersecurity risk assessment. The sectoral evaluation aspect incorporates the business evaluation aspect, but only from a vertical sector-specific view.

The criticality of the ICT product and the ICT SCS are recognised before the analysis starts. The identified criticality will define the security assurance perimeter in view of a conformity assessment performance or a protection profile creation (see Chapter 7).

- **ICT product criticality.** The Cyber Resilience Act (CRA) [11] defines the criticality of a Product with Digital Elements (PDE) based on its cybersecurity relevance and the potential impact that may result from its compromise. Moreover, the CRA distinguishes products into different categories and classes, based on:
  - the product's core cybersecurity functionality
  - the extent to which a compromise could affect other systems, networks, or users,
  - the scale and severity of potential adverse effects, and
  - the product's role in protecting critical infrastructures or digital ecosystems.

In this line, CRA defines three main categories, summarised below:

- *Default products.* Standard products with digital elements that are not explicitly classified as important or critical.
- *Important Products (Two different classes, according to their criticality)*
  - *Important Products – Class I.* Products with significant cybersecurity functions or products whose compromise could affect many other devices or users (e.g., VPNs, password managers, browsers, routers, SIEM systems, and identity management systems).
  - *Important Products – Class II.* Products are considered more critical due to their higher cybersecurity impact and systemic importance (e.g., hypervisors, industrial firewalls, IDS/IPS systems, and tamper-resistant microcontrollers). These products are subject to stricter conformity assessments.
- *Critical Products.* Products whose failure or compromise could severely disrupt cybersecurity functions or critical infrastructures. Examples include smartcards, secure elements, smart meter gateways, and hardware security modules

The more critical the product is, the more stringent the assessment is performed (see Section 4.6 and Chapter 7.) For instance, an encryption mechanism for the military sector is considered a “critical” product requiring stringent assessment.

- **ICT Supply Chain Service (SCS) criticality.** The criticality at supply chain service level is defined by the NIS 2 Directive [12]. Furthermore, as presented in Section 3.3, criticality on SCS is assessed based on their value and impact on the EU economy in case of their disruption. In this context, the ICT stakeholder who initiates the cybersecurity risk assessment, may consult the following table to determine the ICT SCS criticality, which



relies on the CyberICT probability scale (see Table 87) and NIS 2 Directive rationale of Operators of Important Services (OIS) and Operators of Essential Services (OES) (see Table 88).

Table 14. ICT Supply Chain Service criticality scale based on NIS 2 Directive [12] aspects.

| ICT Supply Chain Service description                                                                                                                                                                                     | Qualitative scale |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|
| ICT SCS is neither an essential nor important service, according to NIS 2 Directive. The ICT stakeholder is not a provider of essential or important supply chain services.                                              | Very Low (VL)     |
| ICT SCS is an important service, according to NIS 2 Directive. The ICT stakeholder is a provider of important supply chain services.                                                                                     | Low (L)           |
| ICT SCS is an essential service, according to NIS 2 Directive. The current service is European (only EU members are involved). The ICT stakeholder is a provider of essential EU supply chain services.                  | Moderate (M)      |
| ICT SCS is an essential service, according to NIS 2 Directive. The current service is international (at least 1 non-EU member is involved). The ICT stakeholder is a provider of essential global supply chain services. | High (H)          |
| ICT SCS is a military/defense service. The ICT stakeholder is a provider of essential service (national security, law enforcement).                                                                                      | Very High (VH)    |

As an example of the above, the Vehicle Transport Service, including business partners from non-EU Member States referring to water transport of vehicles is considered an essential service of high criticality.

### Step 1.2 ICT stakeholder and business partners identification

The ICT stakeholder who initiates the cybersecurity risk assessment identifies the key business partners that interact:

- during the SDLC of the ICT product (e.g., software development vendors, cloud service providers, etc.)
- for the provision of the ICT SCS (e.g., importer, governmental agency, logistics agent)
- for the performance of the current cybersecurity risk assessment (e.g., managed security service provider).

Each business partner defines the participants of their organisation who will be engaged in the cybersecurity risk assessment process. Business partners may originate from different categories, including service providers, commercial partners, governmental entities, and auditing organisations.

### Step 1.3 ICT analysis and modelling

The current step incorporates different sub-steps for the ICT product and ICT SCS further analysis respectively:

#### Step 1.3.1 ICT product analysis

This step refers to ICT product analysis. As presented in Section 3.1, ICT products may be complex, comprising a set of primary elements, *individual building blocks/components, which are considered ICT assets. The current step* employs a hybrid top-down strategy to decompose a composite ICT product into its primary assets. The ICT assets can be identified in a twofold manner:

- According to the MITRE Common Platform Enumeration (CPE) identifier [268], a naming scheme that provides technical details of assets (i.e., asset name/ description/ asset vendor/ asset type and version).
- Following the automated Software Bill Of Material (SBOM) scanning identification (PURL-based) approach. Specifically, ICT assets are described as Package URLs (PURL), i.e., they identify and locate specific software packages in a unified way across programming languages, package managers, packaging conventions, tools, APIs, and databases. SBOMs are considered a structured list of components of a software product, including libraries, dependencies, and modules used in the software, their versions, licences and suppliers or origins. An approach to scan a container and create the SBOM is using open source Command Line Interface (CLI) tools, such as Syft [376] and Trivy [377] container scanners. Such tools scan container images (e.g., Docker image) and extract package metadata (generate SBOM files in CycloneDX or SPDX format) by identifying all included software components via PURLs.

A short example to the ICT product analysis is a tablet that has a database and an operating system. The operating system may have MITRE CPE “cpe:2.3:o:google:android:14.0:\*:\*:\*:\*:\*” (Google Android-based), while a lightweight database may have MITRE CPE “cpe:2.3:a:sqlite:sqlite:3.42.0:\*:\*:\*:\*:\*”.

#### Step 1.3.2 ICT Supply Chain Service analysis

This step refers to the ICT SCS analysis. The current step aims to further analyse the ICT SCS by utilising a modelling approach developed during the current dissertation [84],[378] that implements a combined technique of process-centric and asset-centric views to crystallise the business and technical perspectives of the ICT SCS accordingly. To decompose the ICT SCS into its main elements, the ICT supply chain model, described in Section 3.2.3.2, is adopted. The ICT supply chain model is developed gradually through the implementation of the following consecutive steps. The ICT SCS is further analysed into:

- **key ICT processes** contributing to the provision of the ICT SCS to ensure its continuity. The identification of prominent ICT processes for the ICT SCS provision aims to support the impact analysis in the risk assessment process for estimating the effect of a potential disruption (i.e. a security event) of the ICT SCS.

- **key business partners participating** in the ICT processes (key participants) to identify interactions and information flows within the processes
- **key ICT infrastructures and ICT systems** functioning for the provision of the ICT SCS
- **ICT assets operating** for the underlying ICT infrastructure, along with their technical specifications (using the ICT asset analysis twofold approach indicated in step 1.3.1).

**ICT process and business partners analysis.** As described in Section 3.4, in modern multi-scale business environments, business process modelling visualisations can facilitate the comprehension and analysis of critical ICT processes within the ICT SCS. Thus, ICT processes and business partners participating in the processes are designed and modelled. Primarily, the ICT processes are recorded, using the template below (see Table 15) to describe the ICT processes and the business partners involved in each process.

Table 15. ICT process analysis template.

| ICT Supply Chain Service (ICT SCS) |                         |                                                        |
|------------------------------------|-------------------------|--------------------------------------------------------|
| ICT process                        | ICT process description | Business partners involved in the identified processes |
| $P_b,$<br>(where $b \in N$ )       | .....                   | $bp_i,$<br>(where $i \in N$ )                          |

Then, the ICT processes are analysed and codified into flowchart diagrams (business process diagrams) [96] by utilising business process modelling languages, such as the BPMN 2.0.2, following the relevant ISO/IEC 19510:2013 international standard [114]. The developed BPMN models aim to represent the embedded steps of each ICT process, the partners involved, highlight their roles within the process and the interactions between them. The modelling of the ICT processes provides a process-centric view of the ICT SCS, aiming to assist ICT stakeholders and business partners in enhancing comprehension of the supporting processes [84],[378].

**ICT infrastructure analysis.** The aim is to construct high-level infrastructure representations of critical ICT systems and ICT assets operating within the ICT process, highlighting business partners' communications and transactions.

Table 16. High level ICT infrastructure analysis template.

| ICT Supply Chain Service (ICT SCS)                       |                    |
|----------------------------------------------------------|--------------------|
| ICT Business process                                     |                    |
| Business partners involved in the identified ICT process | ICT infrastructure |
| $bp_i,$<br>(where $i \in N$ )                            | .....              |

**ICT asset analysis.** The ICT assets that constitute the ICT infrastructures are analysed. Within this step, asset technical specifications are denoted either manually or utilising automated tools

(i.e. scanners), as described in Step 1.3.1. Such features are “asset category” (i.e., hardware, software, application, etc.), “product name”, “product version”, and “vendor”. The set  $A_{i,j}$  represents the cyber assets  $j$  of the business partner  $i$  involved in the process  $b$  (see Table 17). These asset characteristics have been represented in an ontology structure, analysed in Section 6.2.3. To this end, an ISMS inventory is produced reflecting all cyber asset characteristics.

Table 17. ICT asset technical specifications template.

| Node ID | Asset Code | Name  | Category                        | Product Name | Version | Vendor |
|---------|------------|-------|---------------------------------|--------------|---------|--------|
| $bp_i$  | $A_{i,j}$  | ..... | Application/<br>Hardware/<br>OS | .....        | .....   | .....  |

**Assets interdependencies.** Interrelations and interconnections between cyber assets are defined. Investigations into how specific cyber assets operate within the ICT SCS are made. A cyberdependency of assets is considered a pair of ICT assets (asset nodes) interrelations and/or interconnections (edge) aiming to fulfil an electronic service/operation across communication networks [84],[378]. Cyberdependencies are identified among assets in pairs (see Section **Error! Reference source not found.**). Asset cyberdependencies rely on a twofold approach [84]:

- the dependency type.* The dependency type identifies how a cyber asset pair is interdependent in a supply chain service. The current methodology adopts the dependency types of [84]: 1. Hosting; 2. Exchange data/information; 3. Storing; 4. Controlling; 5. Processing; 6. Accessing; 7. Installing; 8. Trusted; 9. Connecting. The first asset  $A_{i,j}$  is named the source asset and the second asset is defined as the destination asset  $A_{x,y}$ . The set  $D(A_{i,j}, A_{x,y})_c$  indicates the interdependencies of all cyber asset pairs  $(A_{i,j}, A_{x,y})$  in the ICT SCS, where  $c$  is the type of cyberdependency
- the dependency access vector.* The dependency access vector defines the location of the two cyber assets interacting through a communication network within the ICT SCS. The current methodology utilises the dependency attack vector scheme of CVSS 3.1 [139], i.e., Physical (P), Adjacent Network (A), Local (L), Network (N) [84].

Asset characteristics and cyberdependencies are shown in Table 18. The asset dependency types were identified in [84], which was conducted during the current dissertation based on aspects of the work in [379]. Moreover, they are conceptualised and represented semantically, as described in section 6.2.3.

Table 18. ICT asset matrix.

| Node ID (Xi) | Asset Category                | Asset Source | Asset Destination | Dependency type (c)                                                                                         | Dependency access vector                                        |
|--------------|-------------------------------|--------------|-------------------|-------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|
| $bp_i$       | Application<br>Hardware<br>OS | $A_{i,j}$    | $A_{x,y}$         | 1. Hosting<br>2. exchange data/information<br>3. storing<br>4. controlling<br>5. processing<br>6. accessing | Physical (P)<br>Adjacent Network(A)<br>Local (L)<br>Network (N) |

|  |  |  |  |                                              |  |
|--|--|--|--|----------------------------------------------|--|
|  |  |  |  | 7. installing<br>8. trusted<br>9. connecting |  |
|--|--|--|--|----------------------------------------------|--|

Table 19. Identification of ICT supply chain elements.

| Category of Component            | Defined Component        | Description                                                                                                                                           |
|----------------------------------|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| Business Process                 | $P_b$                    | Business process $b$ in an ICT SCS $n$                                                                                                                |
| Business Partner                 | $bp_n$                   | Business partner $n$ in an ICT SCS $n$                                                                                                                |
|                                  | $bp_i$                   | Business partner $i$ in an ICT process $b$                                                                                                            |
| Asset                            | $A_{i,j} / A_{x,y}$      | Asset $j$ of the business partner $i$ participating in an ICT process $b$ / Asset $y$ of the business partner $x$ participating in an ICT process $b$ |
| Cyberdependency                  | $c$                      | Cyberdependency is a digital interconnection between two assets which relies on the types defined in Table 18                                         |
| Cyberdependency between assets   | $(A_{i,j}, A_{x,y}), c$  | A cyberdependency for a pair of assets<br>( $A_{i,j}$ = resource asset, $A_{x,y}$ = destination asset, $c$ = cyberdependency)                         |
| All SCS assets cyberdependencies | $D(A_{i,j}, A_{x,y}), c$ | All possible pairs of the above sets in the under examination ICT SCS ( $A_{i,j}$ = resource asset $A_{x,y}$ = destination asset)                     |

The ICT SCS model can leverage organisational knowledge. The models produced in the current step analyse deeply the under-evaluation ICT SCS aiming to enhance the business partners' knowledge. **This approach aims to contribute to the challenge**, described in Section 5.1, **on limited supply chain knowledge and the need for enhancing the organisational learning of ICT supply chain operators**. An indicative short example of the application of the above approach is presented in the following.

Table 20. Analysis of "Ship Formalities Arrangement" ICT process.

| Vehicle Transport Service (ICT SCS) |                                                                                                                                                                                                                                                                                |                                                        |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------|
| ICT process                         | ICT process description                                                                                                                                                                                                                                                        | Business partners involved in the identified processes |
| Ship Formalities arrangement        | Customs clearance and docking arrangements are essential maritime transport processes involving coordination between ship agents, customs authorities, port authorities, and AIS-based vessel communication systems to enable authorised vehicle shipment and port operations. | Customs, Port Authority, Ship Agent, Local Agent       |

Table 21. High level ICT infrastructure analysis.

| Vehicle Trasport Service (ICT SCS)            |                                                                                                                                   |
|-----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| Ship Formalities Arrangement                  |                                                                                                                                   |
| Business partners involved in the ICT process | ICT infrastructure                                                                                                                |
| Customs (bp <sub>0</sub> )                    | Customs Integrated Network.                                                                                                       |
| Port Authority (bp <sub>1</sub> )             | Port Community System (PCS), Automatic Identification System (AIS) (interacting with the Ship Information System), SCADA systems. |
| Ship Agent (bp <sub>2</sub> )                 | Electronic devices/communication with other systems via web services.                                                             |
| Local Agent (bp <sub>3</sub> )                | Playing the role of vessel's communication with the Port Authority through the AIS.                                               |

The “Ship Formalities Arrangement” ICT process is represented in the following business process model using the BPMN 2.0.2 busoness process modelling notation.

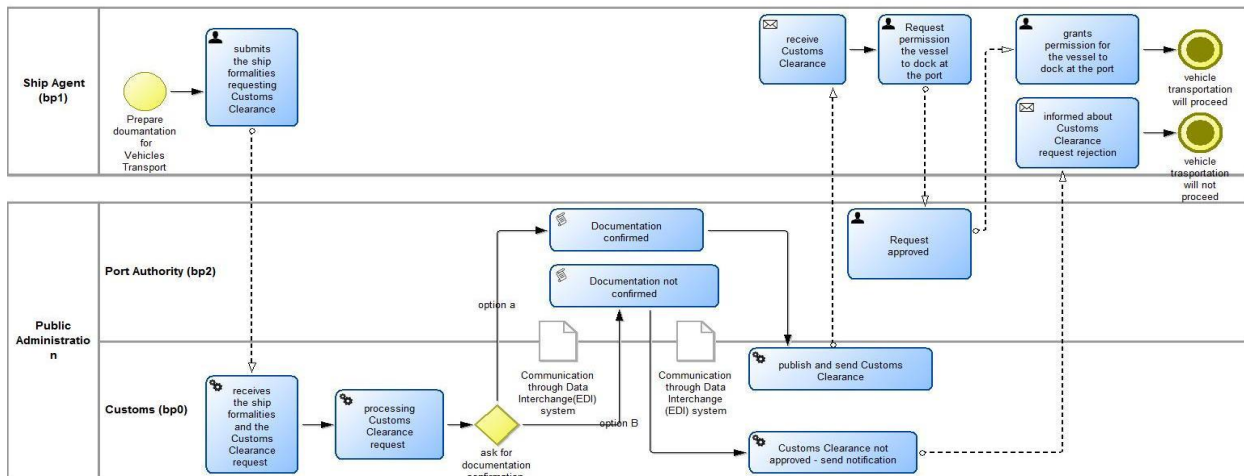


Figure 18. ICT process representation in a business process model.

To enhance the understanding of the ICT infrastructures involved, ICT architectures and additional documentation could be considered (see Section 6.4).

Table 22. ICT asset technical specifications template.

| Node ID        | Asset Code       | Name                   | Category           | Product Name               | Version                                 | Vendor               |
|----------------|------------------|------------------------|--------------------|----------------------------|-----------------------------------------|----------------------|
| Port Authority | A <sub>1,1</sub> | PCS Operating System   | OS                 | Microsoft Windows Server x | Windows Server x (Version y, Release z) | Microsoft            |
| Port Authority | A <sub>1,2</sub> | PCS application Server | Server Application | Apache HTTP Server         | Apache HTTP Server Version e            | Apache               |
| Port Authority | A <sub>1,3</sub> | PCS application Server | Application        | Wordpress                  | Wordpress version r                     | Wordpress foundation |

Table 23. ICT asset matrix.

| Node ID (Xi)   | Asset Source                               | Asset Destination                        | Dependency type (c) | Dependency access vector |
|----------------|--------------------------------------------|------------------------------------------|---------------------|--------------------------|
| Port Authority | PCS application Server (A <sub>1,2</sub> ) | PCS application (A <sub>1,3</sub> )      | 1. Hosting          | Local (L)                |
| Port Authority | PCS application Server (A <sub>1,2</sub> ) | PCS Operating System (A <sub>1,1</sub> ) | 7. Installed On     | Local (L)                |

**Estimate the ICT process and ICT asset criticality.** Large-scale networks, such as supply chain networks, for instance, networks of Vehicle Transport or Aviation Logistics services, are highly interconnected, distributed, and dynamically evolving networks. In such heterogeneous, dispersed networks, asset criticality and process criticality cannot be assessed independently. The technical and business models developed from the ICT SCS analysis presented above show that ICT assets operations and ICT processes execution engage dependency structures. In such chaotic environments, cybersecurity incidents may propagate across organizational and technical boundaries, producing cascading operational effects (see Section 6.2.2.4) that are not observable through isolated asset analysis.

The literature reviews as primary supply chain security dynamic concerns (see Section 4.7) the prioritisation of infrastructures and processes, preservation of cybersecurity enablers, such as the Confidentiality, Integrity, Authentication (CIA triad), promotion of supply chain continuity for maintaining sustainable supply chain environments (discussed in Section 3.2.2) that leverage their security leading to corresponding supply chain security requirements (e.g., supply chain integrity, continuity, and supply chain assets protection), presented in Section 4.5.4. In this line,

for the criticality assessment of ICT processes and ICT assets supply chain elements, the following factors matter:

- the operational importance of supported ICT processes
- the degree of process dependency on the asset
- the existence and sufficiency of resilience mechanisms, such as backup and disaster recovery procedures
- the structural position of the asset within the supply chain dependency graph.

To estimate the criticality of ICT processes and assets within the ICT supply chain network, the model of business processes criticality and asset centrality provided in [15] is adopted. The model is utilised to estimate the criticality of ICT processes and ICT assets within the ICT supply chain network in terms of contextual severity, operational criticality, business-agnostic prioritisation, and environmental contextualisation for identifying vulnerability severity scores based on CVSS 3.1 Environmental group (see Section 6.2.2.4). The adopted model does not aim to directly estimate cyber risks and attack path cascading effects. It is used to capture operational importance, process dependency, resilience characteristics, and structural significance of ICT assets within the ICT supply chain network. The model aims to refine vulnerability severity assessment from an organisation-specific and business-agnostic perspective, supporting the business evaluation aspect of ICT SCS.

The adopted business process and asset criticality model defines a set of sequentially applied rules that support the assessment of ICT process and asset criticality within the ICT supply chain network. The model invites ICT stakeholders and business partners participating in the ICT SCS to apply these rules in sequence to determine the operational and business criticality of processes and assets across the ICT supply chain network.

Considering that asset criticality and ICT process criticality are interdependent concepts, the model in [15], defines a set of rules, which are summarised in the following:

- **ICT process criticality.** The business process importance is explored considering: i) the CIA triad (*ICT Process Rule #1*). Confidentiality ensures that sensitive and valuable information is accessible only to authorised individuals or entities. Integrity involves maintaining the completeness and correctness of data, ensuring that it is not modified or tampered with in an unauthorised or unintended manner. Availability ensures that authorised users have timely and uninterrupted access to the information and resources they require to perform their tasks. ii) the existence of a backup/disaster plan also can affect the importance of the ICT process (*ICT Process Rule #2*). Considering the above, the following rules are defined:
  - **ICT Process Rule #1.**
    - If the loss of the ICT process CIA does not affect the normal provision of the ICT SCS, the process criticality can be assessed with a value either “Very Low” or “Low”.



- If the loss of the business process CIA affects the normal provision of the supply chain service, the process criticality, can be assessed with a value either “Moderate” or “High” or “Very High”
- **ICT Process Rule #2.**
  - If a backup/disaster plan exists, business process criticality level decreases (-1)<sup>15</sup>
  - If a backup/disaster plan does not exist, business process criticality level increases (+1) (if it is “Very High” from the previous rule stays “Very High”). If the backup plan is sufficient, the business process criticality level decreases (-1)<sup>16</sup>.
  - If the backup plan is considered not sufficient enough to entirely replace the ICT process, and additional effort or resources may required to be utilised, the ICT process criticality level increases (+1)<sup>17</sup> (if it is Very High from the previous rule stays Very High).
- **ICT asset criticality.** Calculation of asset criticality over the ICT supply chain network depends on i) the ICT process(es) criticality the asset supports (*ICT Asset Rule #1*), ii) the number of ICT processes (ratio of the number of processes in which the asset participates to the total number of processes) in which the asset is used (*ICT Asset Rule #2*), iii) the existence of a sufficient backup plan (*ICT Asset Rule #3*), and iv) the position of the asset in the asset model (*ICT Asset Rule #4*) based on two perspectives. The first perspective is related to how many entry points the targeted asset can be reached. In this regard, ICT asset criticality is raised if there is a high number of asset entry points that are mission-critical to reaching the targeted ICT asset. The second perspective relies on the length of the path between an asset entry point and the ICT observed asset (target point) across the ICT SCS network. ICT asset criticality is decreased if the length between an asset entry point and the asset target point is long. To estimate the asset complexity from such perspectives, the model uses the betweenness centrality algorithm, described in [15]. Graph-theoretic metrics, such as betweenness centrality, are particularly suitable for modelling systemic importance because they capture the extent to which assets act as intermediary nodes within communication and operational pathways. Assets with high centrality represent potential bottlenecks or single points of failure whose compromise may significantly disrupt supply chain operations. Moreover, the algorithm considers nodes with the highest betweenness centrality crucial to the communication in a graph, as they connect a high number of nodes with each other. Removing these nodes from the

---

<sup>15</sup> If the value is “Very Low” from the previous rule, it stays “Very Low”.

<sup>16</sup> Again, if the value from the implementation of the previous rule is “Very Low”, it remains “Very Low”.

<sup>17</sup> If the ICT process criticality level from the previous rule has value “Very High”, it remains “Very High”.

network would lead to huge disruption in the linkage or communication of the ICT supply chain network. To this end, the following rules are adopted:

- **ICT Asset Rule #1:**
  - The asset should inherit the business process criticality in which the asset operates.
  - In case the ICT asset operates for the execution of more than one SCS process, the ICT asset should inherit the SCS process criticality of the worst-case scenario.
- **ICT Asset Rule #2:**
  - If the observed ICT asset is involved in more than 50% of the total number of processes in the ICT SCS, criticality of the asset will be increased for one level, otherwise it remains as it is.
- **ICT Asset Rule #3:**
  - If there is a sufficient backup plan or an alternative procedure for the use of the asset, then the asset criticality decreases at one level (-1), but it cannot turn to a lower level than the criticality of the process involving that asset.
  - In case a backup plan does not exist, the asset criticality increases at one level (+1).
- **ICT Asset Rule #4:**
  - If the calculated asset betweenness centrality is equal to or above the 60th percentile, asset criticality is increased at one level (+1).
  - If the betweenness centrality of an asset is below the 60th percentile, asset criticality is decreased at one level (-1).

Example:

The Ship Formalities Arrangement process of the Vehicle Transport Service is critical, as its loss of CIA would disrupt vehicle shipments through ports. Thus, initial criticality is “High” (ICT Process Rule #1). Nevertheless, the existence of an efficient semi-automated contingency plan reduces it to “Moderate” (ICT Process Rule #2).

The Port Community System (PCS) Web Application, which supports multiple ICT processes of the Vehicle Transport Service, inherits the highest criticality of these processes, which is “Very High” (ICT Asset Rule #1). Since it participates in fewer than 50% of the supporting ICT processes, its criticality decreases to “High” (ICT Asset Rule #2). An effective backup plan further lowers it to “Moderate” level (ICT Asset Rule #3). Finally, with asset betweenness centrality calculated above the 60<sup>th</sup> percentile, the PCS Web Application’s criticality increases one level to “Very High” (ICT Asset Rule #4).

### 6.2.2.3 Step 2. Cyber Threat Intelligence

This step aims to identify potential cyber threats on ICT assets. For each threat identified, the probability that the threat will be realised is determined. Furthermore, vulnerabilities are identified on ICT assets and threat scenarios are created. Step 2 is divided into the following steps:

- Step 2.1 Cyber threat identification
- Step 2.2 Vulnerability identification
- Step 2.3 Cyber threat scenarios
- Step 2.4 Cyber threat assessment

Table 24 summarises Step 2.

Table 24. Identify and estimate cyber threats.

| Step 2. Cyber threat Intelligence<br>Step 2.1. Cyber threat identification<br>Step 2.2 Vulnerability identification<br>Step 2.3 Cyber threat scenarios<br>Step 2.4 Cyber threat assessment |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Input</b>                                                                                                                                                                               | ICT asset analysis generated from Step 1. For the case of ICT SCS, ICT assets per ICT process are identified.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Activity</b>                                                                                                                                                                            | This step considers the asset models generated in Step 1 and aims to perform a threat analysis to identify, model and assess the cyber threats lurking upon the ICT assets. Furthermore, it aims to identify vulnerabilities on the ICT assets and create threat scenarios, including asset-vulnerability-threat interrelations. Eventually, it estimates the Threat Level for all threats identified on the ICT assets.                                                                                                                                                                                                                                        |
| <b>Output</b>                                                                                                                                                                              | The output of this step is: <ul style="list-style-type: none"> <li>• A list of identified threats on assets and corresponding Threat Levels (TLs)</li> <li>• A list of identified vulnerabilities on assets</li> <li>• Threat scenarios mapping of individual identified cyber threats with ICT assets and vulnerabilities</li> <li>• The information collected from this step provides Cyber Threat Intelligence insights to the ICT stakeholders and business partners.</li> </ul>                                                                                                                                                                            |
| <b>Example</b>                                                                                                                                                                             | <p><u>Input:</u> ICT asset analysis and dependency graphs of the Vehicle Transport Service</p> <p><u>Activity:</u> For a database asset, the MITRE CAPEC-66 SQL Injection threat is identified. In addition, the CVE-2023-46604 Remote Code Execution vulnerability was identified on the database asset. The MITRE CAPEC-66 SQL Injection threat, can be implemented if CVE-2023-46604 Remote Code Execution vulnerability is exploited on the database asset. This creates a threat scenario. The Threat Level (TL) of the current threat is estimated as "Very High".</p> <p><u>Output:</u> Threat and vulnerability records, threat assessment reports.</p> |

#### Step 2.1 Cyber threat identification

The scope of this step is to map individual identified cyber threats with the ICT assets derived from Step 1. Individual cyber threats are the means by which a potential security incident may occur, affecting a specific ICT asset. As mentioned in Section 4.1, the CyberICT risk assessment

methodology is focused on the intentional nature of cyber threats. Cyber threats are identified as a result of several factors:

- from ICT stakeholders and business partners (Based on their reported threats, internal policies and procedures and their expertise. In addition they may define cyber threats categories to address a specific security problem to create a protection profile of an ICT product that will go through a cybersecurity certification evaluation process, see Section 7 expertise )
- from widely-known repositories of cyber threats, such as CAPEC MITRE [272] classification
- from crowdsourcing (a community of online users/security, experts/stakeholders, such as MISP [265], OSINT [380] communities),
- from intrusion incidents and system logs (see Section **Error! Reference source not found.**)
- from reported exploitations
- from firewall logs
- from reverse engineering of malware
- from social media (discussion groups or forums)
- from Deep and Dark Web mining and knowledge inference from social networking services [378]
- from system configuration information.

The CyberICT risk assessment methodology utilises the MITRE CAPEC catalogue of threats and attack patterns [272] to identify threats on ICT assets reside in an ICT product or an ICT SCS. Using MITRE CAPEC threats, threat-related information for ICT assets can be explored, such as threat description, typical severity, information on attack likelihood explaining how attackers may exploit or misuse an application towards various attack techniques.

MITRE CAPEC threats can support application testers in identifying how attackers may exploit or misuse an application, enabling the evaluation of the application's resilience against various attack techniques.

For the case of ICT SCS, after identifying threats on ICT assets using MITRE CAPEC, an ICT stakeholder can identify all cyber threats related to ICT assets that reside in an ICT process that participates for the provision of an ICT SCS and consider the criticality concepts presented in Step 1. Moreover, Section **Error! Reference source not found.** provides a model for estimating and prioritising attack paths based on a confirmed security event [9]. The output of the current step is the set  $T_s, A_{i,j}$ , which is a group of threats  $T_s$  identified for each ICT asset  $A_{i,j}$ .

## Step 2.2 Vulnerability identification

This step aims to identify security vulnerabilities on ICT assets. To support this, the CyberICT risk assessment methodology utilises information from widely-known open repositories, i.e., CVE of MITRE [140] from NIST National Vulnerability Database (NVD) [269], Open Source Vulnerabilities (OSV) database [270] and Github Advisory [271]. These prominent open

repositories provide a set of vulnerability details, such as vulnerability ID, Vector, Published/Modified dates, and vulnerability description.

These open repositories are selected, according to the following rationale. As explained in Step 1, the methodology identifies ICT assets either with the MITRE CPE [268] identifier or following the PURL-based SBOM approach. To identify vulnerabilities on MITRE CPE-based ICT assets, the NIST NVD [269] database is utilised which supports the MITRE CVE [140] vulnerability naming scheme.

Vulnerability identification for the PURL-based SBOM approach can be achieved through parsing procedures that recognise software components and map them to the widely known open repositories mentioned above. To identify vulnerabilities on SBOMs, OSV [270] is utilised, as it is heavily designed to work with Package URLs (PURLs) and deliver open-source vulnerabilities for software packages across multiple ecosystems, e.g., PyPI (Python), npm (JavaScript), Maven (Java), Go, Rust, etc. Since OSV can track vulnerabilities in open-source packages before a CVE is issued, not all OSV entries have a CVE. Conversely, some CVEs may not have an OSV entry if they're outside open-source ecosystems. GitHub vulnerabilities [271] are primarily defined by affected packages, ecosystems, and version ranges, utilising GHSA identifiers, CVE mappings, dependency graph analysis, and SBOM/PURL mappings. In this vein, GitHub Advisory [271] is utilised as a bridge mapping OSV to CVE whenever possible for easier automation and reporting.

By adopting these vulnerability identification techniques, for each vulnerability  $V_v$  identified on an ICT asset  $A_{i,j}$ , the set  $V_v, A_{i,j}$  is produced. The output of the current step is a list of all  $V_v, A_{i,j}$  sets, namely, all confirmed vulnerabilities identified for all underlying ICT assets.

### Step 2.3 Cyber threat scenarios

A cyber threat scenario is a use case in which a threat can compromise an asset by exploiting vulnerabilities and weaknesses, thereby taking advantage of inadequate security controls. After identifying cyber threats and vulnerabilities in the underlying ICT assets, threat scenarios are identified as combinations of threats and vulnerabilities on the ICT assets. To this aim, CAPEC MITRE threat classification [272] synchronises the MITRE attack identifiers (step 2.1) and associates the identified vulnerabilities (step 2.2) with one or more weakness identifiers (Common Weakness Enumerations – CWEs) [266]. This step produces interrelations of ICT assets with corresponding vulnerabilities and threats (triplet structures of asset-vulnerability-threats). The output of the current step is the triplet structure  $A_{i,j}-V_v-T_s$  which is an interrelation of an asset  $A_{i,j}$  with a vulnerability  $V_v$  and a corresponding threat  $T_s$ . Moreover, it is a combination of asset, vulnerability and threat illustrating that an asset  $A_{i,j}$  can be compromised by a threat  $T_s$ , which can be implemented by exploiting a vulnerability  $V_v$ .

### Step 2.4 Cyber threat assessment

Considering the cyber threats  $T_s$  identified per asset  $A_{i,j}$  (output of step 2.1), the current step performs a threat assessment. It aims to estimate the Threat Level  $TL_{s,A_{i,j}}$  of a cyber threat,  $T_s$ , which is the cyber threat's  $T_s$  occurrence to a given ICT asset  $A_{i,j}$ . To estimate the threat level,

several factors are considered, as described in step 2.1, which can be incorporated to the following high level categories:

- Historical data of past incidents, including threat reports from previous security testing or past risk assessment results, firewall logs, system logs, IoCs, and any additional intrusion detection evidence derived from malware reverse engineering processes or threat records);
- Human experience, expertise, and knowledge, including organisational policies and procedures, professional expertise, and other insights derived from expert analysis, logical inference, and understanding attackers’ intent obtained through malware reverse engineering;
- Web sources and open repositories, including classifications from widely known threat repositories such as CAPEC MITRE, MISP community, crowdsourcing, social media and newsfeed.

The Threat Level (TL) of a specific threat to a given ICT asset is estimated considering the above factors by utilising the threat scale, presented in Table 89 of Appendix D3. The TL estimation relies on the expected occurrence of a threat (historical incidents, expert judgment, web sources). It does not incorporate attacker’s capability or technical exploitability of a vulnerability. The outcome of this step is all TLs for all threats identified to a given ICT asset.

6.2.2.4 Step 3. Vulnerability and impact analysis

This step aims to conduct individual, cumulative and propagated analysis of the vulnerabilities identified on ICT assets in Step 2, estimate their impact and explore corresponding cascading effects. Step 3 incorporates the following steps:

- Step 3.1 Individual Vulnerability Assessment
- Step 3.2 Vulnerability Exploitation
- Step 3.3 Individual Impact Analysis
- Step 3.4 Cumulative Vulnerability and Impact Analysis
- Step 3.5 Propagated Vulnerability and Impact Analysis

Table 25 summarises Step 3.

Table 25. Vulnerability and Impact Analysis.

| Step 3. Vulnerability and Impact analysis             |                                                                                                                   |
|-------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| Step 3.1. Individual Vulnerability Assessment         |                                                                                                                   |
| Step 3.2 Vulnerability Exploitation                   |                                                                                                                   |
| Step 3.3 Individual Impact Analysis                   |                                                                                                                   |
| Step 3.4 Cumulative Vulnerability and Impact Analysis |                                                                                                                   |
| Step 3.5 Propagated Vulnerability and Impact Analysis |                                                                                                                   |
| Input                                                 | ICT asset dependency graphs produced in Step 1. Vulnerabilities identification on ICT assets derived from Step 2. |

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Activity</b> | This step aims to assess the individual vulnerability exploitability on ICT assets considering the intrinsic vulnerability technical exploitability and the attacker's exploitability aspects. In addition, it aims to estimate the potential individual impact from the exploitation of each vulnerability identified on ICT assets and also enables the estimation of the impact that could be caused to the ICT supply chain network. Moreover, this step provides cumulative vulnerability and impact analysis and considers subsequent steps for the construction of potential attack paths. It also analyses the vulnerability propagation and the corresponding impact.                        |
| <b>Output</b>   | <p>The output of this step is:</p> <ul style="list-style-type: none"> <li>• A list of Individual Vulnerability Levels for all ICT assets</li> <li>• A list of Vulnerability Exploitation Levels for all ICT assets</li> <li>• A list of Individual Impact Levels estimation for all ICT assets</li> <li>• Individual Vulnerability Chains and Individual Impact Chain estimates</li> <li>• Entry's Vulnerability Chains and Entry's Impact Chain estimates</li> <li>• Cumulative Vulnerability Chains and Cumulative Impact Chain estimates</li> <li>• Propagated Vulnerability and Impact estimates</li> <li>• Use of propagation rules</li> <li>• Vulnerability chains and Attack graphs</li> </ul> |
| <b>Example</b>  | <p><u>Input</u>: ICT asset analysis and asset dependency graphs of the Vehicle Transport Service. A list of vulnerabilities identified on the ICT assets of the Vehicle Transport Service.</p> <p><u>Activity</u>: Short examples of the current steps are presented after each step.</p> <p><u>Output</u>: Vulnerability and Impact Analysis reports of the Vehicle Transport Service. Attack graphs of the under examination scenario.</p>                                                                                                                                                                                                                                                          |

### Step 3.1 Individual Vulnerability Assessment

Considering the vulnerabilities identified for the ICT assets in step 2.2, the current step aims to estimate the Individual Vulnerability Level (IVL) for each identified vulnerability  $V_v$  to an asset  $A_{i,j}$ . The IVL estimates the probability that a vulnerability  $v$  can be exploited in principle on a given asset  $A_{i,j}$ . It aims to estimate the vulnerability intrinsic exploitability to an asset without considering attacker-specific context, such as the adversary's expertise or operational proximity. To calculate the IVL, the CVSS 3.1 score metrics related to technical exploitability are used, namely:

- the "Modified Attack Vector" (MAV) (Network/Adjacent/ Local/Physical)
- the "Modified Attack Complexity" (MAC) (Low/High)
- the "Modified Privileges Required" (MPR) (None/Low/High)
- the "Modified User Interaction" (MUI) (None/Required), the Individual Vulnerability levels of all identified vulnerabilities on the CII assets are estimated.

The Modified Exploitability Sub Score (MESS) formula of CVSS 3.1 specification is utilised to estimate the Individual Vulnerability Level (IVL) of a vulnerability  $v$  to an asset  $A_{i,j}$

$$MESS_v = 8.22 \cdot MAV \cdot MAC \cdot MPR \cdot MUI$$

considering the CVSS 3.1 values of the above metrics, depicted in the tables of Appendix D4.

**Normalisation of CVSS 3.1 MESS.** After calculating the IVLs for all identified vulnerabilities on the ICT assets, a normalisation procedure is applied to ensure compatibility of the 0-10 scoring scale of CVSS 3.1 across vulnerabilities estimations and compatibility with the CyberICT methodology (see Table 87).

The upper values of these metrics correspond to the highest possible exploitability according to CVSS 3.1:

- MAV=Network
- MAC=Low
- MPR=None
- MUI=None

Conversely, the lowest values of these metrics correspond to the lowest possible exploitability according to CVSS 3.1:

- MAV=Physical
- MAC=High
- MPR=High
- MUI=Required

Based on these metric configurations,  $MESS_{Max}$  represents the upper bound of the CVSS 3.1 modified exploitability metrics and  $MESS_{Min}$  represents the lower bound of the CVSS 3.1 modified exploitability metrics:

- $MESS_{Max} = 3.887042775$
- $MESS_{Min} = 0.2242416$

Then, the Individual Vulnerability Level (IVL) is computed using min-max normalisation as follows:

$$IVL_{vnorm} = \frac{MESS_v - MESS_{Min}}{MESS_{Max} - MESS_{Min}}$$

where,

- $IVL_{vnorm}$  : the normalised Individual Vulnerability Level ( $IVL_v$ ), estimated based on the MESS sub-score value of CVSS 3.1 and CyberICT generic assessment values
- $MESS_v$  : the MESS sub-score value of CVSS 3.1 for a vulnerability  $v$
- $MESS_{Min}$  : the lower bound exploitability of the CVSS 3.1 MESS sub-score
- $MESS_{Max}$  : the upper bound exploitability of the CVSS 3.1 MESS sub-score

This transformation maps the MESS values into a continuous interval:

$$IVL_v \in [0,1]$$

where:



- 0 represents the minimum exploitability condition within the defined metric space
- 1 represents the maximum exploitability condition within the defined metric space

To facilitate interpretability within the CyberICT framework, the normalised IVL values are further mapped into qualitative probability classes, according to the CyberICT generic assessment scale (see Appendix D1).

Table 26. Individual Vulnerability Level (IVL) scale.

| IVL<br>Quantitative Value | IVL<br>Qualitative Value |
|---------------------------|--------------------------|
| 0.00 – 0.19 (0%-19%)      | Very Low (VL)            |
| 0.20 – 0.39 (20%-39%)     | Low (L)                  |
| 0.40 – 0.59 (40%-59%)     | Moderate (M)             |
| 0.60 – 0.79 (60%-79%)     | High (H)                 |
| 0.80 – 1.00 (80%-100%)    | Very High (VH)           |

### Step 3.2 Vulnerability Exploitation

As previously mentioned, the MESS sub-score captures the intrinsic technical characteristics of a vulnerability that facilitate exploitation without considering attacker – specific characteristics such as expertise, resources, opportunities, and operational proximity.

This step aims to estimate the Exploitation Level (EL), namely, the likelihood of successful exploitation of a vulnerability  $v$  to an asset  $A_{i,j}$  considering vulnerability's technical exploitability and adversary's characteristics.

The attacker's profile is identified by:

- the attacker's capability (very low/low/moderate/high/very high) due to specific features his/her intention and capacity based on expertise, available resources, and opportunities. The likelihood of an attacker to perform a cyberattack or a sequence of cyberattacks relies on these characteristics, and the attacker's target - it can be either a specific asset or cause general harm (see Appendix D5)
- the attacker's location, namely, where the specific attacker is positioned operationally relative to the target (physical/local/adjacent/network) (see Appendix D5)

Both of the above attacker's factors are considered equally important. Thus, the attacker's profile is calculated, according to the formula below:

$$P_i = f(\text{Capability}_i, \text{Location}_i)$$

$$P_i = 0.5 \text{ Capability}_i + 0.5 \text{ Location}_i$$

where  $P_i$  is the Profile of the attacker  $i$  considering attacker's  $i$  capability and location.

Within this step, the computation of Exploitation Levels and Exploitation Level Chains is provided. The Exploitation Level (EL) of an identified vulnerability on a specific asset is calculated considering the attacker's profile and the Individual Vulnerability Level (IVL) using the following exploitability fusion model:

$$EL_v = w_1 IVL_v + w_2 P_i$$

where

$EL_v$  : the likelihood of successful exploitation of an identified vulnerability  $v$  on an asset  $A_n$ , considering the technical exploitability of the vulnerability ( $IVL_v$ ) and the profile  $P$  of the attacker  $i$ .

$IVL_v$  : the intrinsic vulnerability exploitability based on the MESS CVSS 3.1 sub-score

$P_i$  : the profile  $P$  of the attacker  $i$  based on the attacker's capability and location (operational situation)

$w_1$  and  $w_2$ : weights of the  $IVL_v$  and attacker's Profile  $P_i$  respectively.

### Weights validation.

The weights  $w_1$  and  $w_2$  of  $IVL_v$  and  $P_i$  respectively are estimated according to the use cases presented below. The aim is to perform a sensitivity (what-if) analysis to determine how different values of independent variables affect the  $EL_v$  calculation.

#### Option 1. Equal weights

$$w_1 = 0.5, w_2 = 0.5$$

**EL Rule #1:** In the absence of empirical evidence supporting the predominance of either vulnerability characteristics or attacker characteristics, equal importance is assigned to both factors.

#### Option 2. Attacker-dependent weights

For low-skilled cyber attackers

$$w_1 = 0.7, w_2 = 0.3$$

as exploitability is mainly determined by the vulnerability itself.

For highly-skilled cyber attackers:

$$w_1 = 0.3, w_2 = 0.7$$

as skilled attackers can overcome many technical barriers.

An indicative example is presented below:

Assuming that  $IVL_v = 0.22$  (Low), i) Attacker's capability = 0.5 (Moderate) , ii) Attacker's capability = 0.75 and Attacker's location = 0.7 (Adjacent Network), the Attacker's Profile is

$$P_i = 0.5 \text{ Capability}_i + 0.5 \text{ Location}_i$$

i) Capability (VL) = 0.07      $P_i = 0.5 \times 0.07 + 0.5 \times 0.7 = 0.385$

ii) Capability (L) = 0.25      $P_i = 0.5 \times 0.25 + 0.5 \times 0.7 = 0.475$

iii) Capability (M) = 0.5      $P_i = 0.5 \times 0.5 + 0.5 \times 0.7 = 0.6$

iv) Capability (H) = 0.75      $P_i = 0.5 \times 0.75 + 0.5 \times 0.7 = 0.725$

v) Capability (VH) = 0.93      $P_i = 0.5 \times 0.93 + 0.5 \times 0.7 = 0.815$

$$EL_v = w_1 IVL_v + w_2 P_i$$

Table 27. Exploitability Level - example 1.

| Capability | $w_1$ (IVL) | $w_2$ (Attacker's Profile) | $EL_v = w_1 IVL_v + w_2 P_i$<br>(IVL <sub>v</sub> =0.22)       | $EL_v = w_1 IVL_v + w_2 P_i$<br>(IVL <sub>v</sub> =0.40)       | $L_v = w_1 IVL_v + w_2 P_i$<br>(Capability <sub>M</sub> =0.60) |
|------------|-------------|----------------------------|----------------------------------------------------------------|----------------------------------------------------------------|----------------------------------------------------------------|
| Very Low   | 0.8         | 0.2                        | EL <sub>1</sub> : $0.8 \times 0.22 + 0.2 \times 0.39 = 0.254$  | EL <sub>1</sub> : $0.8 \times 0.40 + 0.2 \times 0.39 = 0.398$  | EL <sub>1</sub> : $0.8 \times 0.22 + 0.2 \times 0.6 = 0.296$   |
| Low        | 0.7         | 0.3                        | EL <sub>2</sub> : $0.7 \times 0.22 + 0.3 \times 0.48 = 0.298$  | EL <sub>2</sub> : $0.7 \times 0.40 + 0.3 \times 0.48 = 0.424$  | EL <sub>2</sub> : $0.7 \times 0.22 + 0.3 \times 0.6 = 0.334$   |
| Moderate   | 0.5         | 0.5                        | EL <sub>3</sub> : $0.5 \times 0.22 + 0.5 \times 0.6 = 0.41$    | EL <sub>3</sub> : $0.5 \times 0.40 + 0.5 \times 0.6 = 0.5$     | EL <sub>3</sub> : $0.5 \times 0.22 + 0.5 \times 0.6 = 0.41$    |
| High       | 0.3         | 0.7                        | EL <sub>4</sub> : $0.3 \times 0.22 + 0.7 \times 0.73 = 0.577$  | EL <sub>4</sub> : $0.3 \times 0.40 + 0.7 \times 0.73 = 0.631$  | EL <sub>4</sub> : $0.3 \times 0.22 + 0.7 \times 0.6 = 0.486$   |
| Very High  | 0.2         | 0.8                        | EL <sub>5</sub> : $0.2 \times 0.22 + 0.8 \times 0.815 = 0.696$ | EL <sub>4</sub> : $0.2 \times 0.40 + 0.8 \times 0.815 = 0.732$ | EL <sub>5</sub> : $0.2 \times 0.22 + 0.8 \times 0.6 = 0.524$   |

Table 28. Exploitability Level - example 2.

| $w_1$ (IVL) | $w_2$ (Attacker's Profile) | $L_v = w_1 IVL_v + w_2 P_i$<br>(Capability <sub>M</sub> =0.60) |
|-------------|----------------------------|----------------------------------------------------------------|
| 0.8         | 0.2                        | EL <sub>1</sub> : $0.8 \times 0.22 + 0.2 \times 0.6 = 0.296$   |
| 0.7         | 0.3                        | EL <sub>2</sub> : $0.7 \times 0.22 + 0.3 \times 0.6 = 0.334$   |
| 0.5         | 0.5                        | EL <sub>3</sub> : $0.5 \times 0.22 + 0.5 \times 0.6 = 0.41$    |
| 0.3         | 0.7                        | EL <sub>4</sub> : $0.3 \times 0.22 + 0.7 \times 0.6 = 0.486$   |

**EL Rule #2:** The stronger the attacker, the more the exploitation likelihood depends on attacker characteristics rather than intrinsic vulnerability properties.

**Option 3: Weights are derived from the Attacker's Capability score**

Attacker's Capability is normalised:

$$Capability_i \in [0,1]$$

Table 29. Exploitability Level - example 3.

| Capability | $w_1$ (IVL) | $w_2$ (Attacker's Profile) | $EL_v = w_1IVL_v + w_2P_i$<br>(IVL <sub>v</sub> =0.22)        |
|------------|-------------|----------------------------|---------------------------------------------------------------|
| 0.2        | 0.8         | 0.2                        | EL <sub>1</sub> : $0.8 \times 0.22 + 0.2 \times 0.6 = 0.296$  |
| 0.4        | 0.6         | 0.4                        | EL <sub>2</sub> : $0.6 \times 0.22 + 0.4 \times 0.7 = 0.412$  |
| 0.6        | 0.4         | 0.6                        | EL <sub>3</sub> : $0.5 \times 0.22 + 0.5 \times 0.6 = 0.41$   |
| 0.8        | 0.2         | 0.8                        | EL <sub>4</sub> : $0.3 \times 0.22 + 0.7 \times 0.73 = 0.577$ |

- i) Capability (VL) = 0.2      $P_i = 0.5 \times 0.2 + 0.5 \times 1 = 0.6$
- ii) Capability (L) = 0.4      $P_i = 0.5 \times 0.4 + 0.5 \times 1 = 0.7$
- iii) Capability (M) = 0.5      $P_i = 0.5 \times 0.5 + 0.5 \times 1 = 0.75$
- iv) Capability (H) = 0.6      $P_i = 0.5 \times 0.6 + 0.5 \times 1 = 0.8$
- v) Capability (VH) = 0.8      $P_i = 0.5 \times 0.8 + 0.5 \times 1 = 0.9$

**EL Rule #3:**

Thereby:

$$w_2 = Capability_i$$

$$w_1 = 1 - Capability_i$$

$$EL_v = (1 - Capability_i)IVL_v + Capability_iP_i$$

Although the CVSS v3.1 Modified Attack Vector (MAV) metric and the attacker location attribute share similar categorical values (i.e., Network, Adjacent, Local, Physical), they represent fundamentally different concepts and therefore do not introduce overlap within the proposed model. As previously mentioned, MAV is an intrinsic property of a vulnerability, describing the technical pathway through which the vulnerability can be exploited, independent of any specific adversary. It characterises the required access conditions inherent to the vulnerable component and remains constant regardless of the attacker.

The attacker's location represents an adversary-specific contextual attribute, describing the operational position of a given attacker relative to the target system at a specific point in time. This factor is dynamic and depends on the attacker's environment, capabilities, and access conditions.

Nevertheless, to prevent mathematical distortion and resolve the metric overlap between CVSS and NIST SP 800-30, the Exploitability Level  $EL_v$  at the **Asset Entry Point** must be governed by a logical boundary rule.

This rule maps the attacker's operational location  $Location_i$  against the vulnerability's required baseline exposure MAV  $V_{MAV}$  using a strict directional hierarchy:

Network > Adjacent > Local > Physical

Thus, the Exploitability Level for the **Asset Entry Point in a vulnerability chain** is defined as a conditional piecewise function:

$$EL_v = w_1 IVL_v + w_2 P_i \quad \text{if } Location_i \geq MAV$$

$$EL_v = 0 \quad \text{if } Location_i < MAV \quad (\text{see Table 98 of Appendix D5})$$

Where:

- $IVL_v$ : The normalised CVSS Exploitability Subscore.
- $P_i$ : the NIST SP 800-30 Attacker's Profile score derived from capability, intention, and location
- $w_1, w_2$ : The assigned structural weights.

For example, for an asset entry point in a potential attack path a vulnerability that can be technically exploited in the location "Local network" is feasible to be exploited and initiate the attack if the attacker's location is operationally either in the "Local network" or "Physical network". If the attacker is either in the "Adjacent Network" or in the "Network", then the specific vulnerability cannot be exploited by the attacker with the specific location characteristic.

To this end, while both attributes may use similar qualitative labels, MAV captures *vulnerability exposure conditions*, whereas attacker location captures *attacker proximity and operational positioning*. Thus, they are considered as complementary aspects utilised for the estimation of the Exploitation Level ensuring that both vulnerability-centric exploitability (MESS) and attacker-centric exploitability (Attacker's Profile) are explicitly represented.

### Step 3.3 Individual Impact Analysis

This step estimates the Impact levels of each vulnerability  $v$  of all denoted ICT assets  $A_{ij}$ . The Impact level measures the expected effect from the successful exploitation of a vulnerability  $v$  identified in an ICT asset. To estimate the Impact Level ( $IL_v$ ) of a specific asset/vulnerability combination  $A_{ij}, V_n$ , the CVSS 3.1 Modified Impact Sub-Score (MISS) is adopted at first:

$$MISS_v = \min(1 - (1 - CR \times C_{mod}) \times (1 - IR \times I_{mod}) \times (1 - AR \times A_{mod}), 0.915)$$

where,

CR: Confidentiality Requirement  
 $C_{mod}$ : Modified Confidentiality (MC)  
 IR: Integrity Requirement  
 $I_{mod}$ : Modified Integrity (MI)  
 AR: Availability Requirement  
 $A_{mod}$ : Modified Availability (MA)

**Normalisation of CVSS 3.1 MISS.** After calculating the  $MISS_v$  for all vulnerabilities identified on the ICT assets, a normalisation procedure is applied to ensure compatibility of the 0-10 scoring scale of CVSS 3.1 across the vulnerabilities estimations and compatibility with the CyberICT methodology (see Table 87).

Similarly, with MESS:

The CVSS 3.1 explicitly caps MISS at 0.915 (upper bound) to avoid overestimating impact:

$$MISS_{max} = 0.915 \quad (\text{never exceeds } 0.915)$$

If a vulnerability has **all modified impacts = 0** ( $C_{mod} = I_{mod} = A_{mod} = 0$ ), then

$$MISS_{min} = 1 - (1 - 0) \times (1 - 0) \times (1 - 0) = 0$$

$$MISS_{min} = 0 \quad (\text{vulnerability has no impact})$$

The normalised  $MISS_v$  is estimated using min-max normalisation as follows:

$$MISS_{v_{norm}} = \frac{MISS_v - MISS_{min}}{MISS_{max} - MISS_{min}}$$

Where,

- $MISS_{v_{norm}}$  : the normalised  $MISS_v$
- $MISS_v$  : the MISS modified impact sub-score of CVSS 3.1 for a vulnerability  $v$
- $MISS_{min}$  : the lower bound of CVSS 3.1 MISS modified impact sub-score
- $MISS_{max}$  : the upper bound of CVSS 3.1 MISS modified impact sub-score

Thereby, the MESS modified impact values are mapped into a continuous interval:

$$IL_v \in [0,1]$$

where:

- 0 represents the minimum impact from a vulnerability  $v$  exploitation to an asset  $A_{ij}$
- 1 represents the maximum impact from a vulnerability  $v$  exploitation to an asset  $A_{ij}$

Eventually,  $MISS_{v_{norm}}$  is mapped into the qualitative probability scale of CyberICT (see Appendix D1).

According to Table 95, the status scope of the Modified Scope (MS) metric of the environmental group affects the  $MISS_v$  calculation. The  $IL_v$  estimates the consequence from a vulnerability exploitation. It does not consider any attacker's attributes. So, if scope is *unchanged*, the following formula is adopted to calculate  $IL_v$ :

$$IL_v = 6.42(MISS_v)$$

if scope is *changed*, the below formula is used to calculate  $IL_v$

$$IL_v = 7.52(MISS_v - 0.029) - 3.25 \times (MISS_v \times 0.9731 - 0.02)^{13}$$

Eventually,  $IL_v$  is normalised using the following formula:

$$IL_{v_{norm}} = \frac{IL_v - IL_{min}}{IL_{max} - IL_{min}}$$

Eventually, the quantitative value is mapped into the qualitative probability scale of CyberICT (see Appendix D1).

Table 30. Individual Impact Level scale.

| Individual Impact Level (IL)<br>Quantitative Value | Individual Impact Level (IL)<br>Qualitative Value |
|----------------------------------------------------|---------------------------------------------------|
| 0.00 – 0.19 (0%-19%)                               | Very Low (VL)                                     |
| 0.20 – 0.39 (20%-39%)                              | Low (L)                                           |
| 0.40 – 0.59 (40%-59%)                              | Moderate (M)                                      |
| 0.60 – 0.79 (60%-79%)                              | High (H)                                          |
| 0.80 – 1.00 (80%-100%)                             | Very High (VH)                                    |

### **Example**

Assuming there is a vulnerability with the following characteristics:

Table 31. Example of Vulnerability metrics of CVSS 3.1 Environmental Group.

| Metric    | Score | Qualitative Value |
|-----------|-------|-------------------|
| $C_{mod}$ | 0.56  | Very High (VH)    |
| $I_{mod}$ | 0.56  | Very High (VH)    |
| $A_{mod}$ | 0.56  | Very High (VH)    |
| CR        | 1.5   | High (H)          |
| IR        | 1     | Medium            |
| AR        | 1.5   | High (H)          |

Supposing that the Modified Scope (MS) is changed, the  $MISS_v$  is calculated as follows:

$$IL_V = 7.52(MISS_v - 0.029) - 3.25 \times (MISS_v \times 0.9731 - 0.02)^{13}$$

At first,  $MISS_v$  is calculated:

$$MISS_V = \min(1 - (1 - CR \times C_{mod}) \times (1 - IR \times I_{mod}) \times (1 - AR \times A_{mod}), 0.915)$$

$$MISS_V = \min(1 - (1 - 0.84) \times (1 - 0.56) \times (1 - 0.84), 0.915)$$

$$MISS_V = \min(1 - (0.16) \times (0.44) \times (0.16), 0.915)$$

$$MISS_V = \min(0.988736, 0.915)$$

$$MISS_V = 0.915$$

Considering that MS is changed:

$$IL_V = 7.52(0.915 - 0.029) - 3.25 \times (0.915 \times 0.9731 - 0.02)^{13}$$

$$IL_V = 6.6627 - 3.25 \times (0.915 \times 0.9731 - 0.02)^{13}$$

$$MISS_V = 6.6627 - 3.25 \times (0.1649)^{13}$$

$$MISS_V = 6.1266$$

The  $IL_V$  value is normalised:

$$IL_{V_{norm}} = \frac{IL_V - IL_{min}}{IL_{max} - IL_{min}}$$

$$IL_{V_{norm}} = 0.613$$

Thus,  $IL_V$  is 61.3% considered “High”, according to the CyberICT assessment scale.

In the case of an ICT product cybersecurity risk assessment, the above calculations of  $IL_v$  are used to estimate the consequences from a vulnerability exploitation.

If an ICT SCS is the subject of cybersecurity risk assessment, the ICT SCS scores, concerning the ICT process and asset criticality, presented in step 1.3, can be considered to estimate the consequences from a vulnerability exploitation within the ICT supply chain network. To achieve this, the following table provides a mapping of the assets’ criticality with the CVSS 3.1 Environmental group metrics:

Table 32. Environmental group metric values mapped to ICT asset criticality.

| Metric Name                                                                              | Qualitative value | Score | Asset criticality value |
|------------------------------------------------------------------------------------------|-------------------|-------|-------------------------|
| Modified Confidentiality (MC)/<br>Modified Integrity (MI) /<br>Modified Availaibity (MA) | None              | 0     | Very Low                |
|                                                                                          | None              | 0     | Low                     |
|                                                                                          | Low               | 0.22  | Moderate                |



|                                                                                              |             |      |           |
|----------------------------------------------------------------------------------------------|-------------|------|-----------|
|                                                                                              | High        | 0.56 | High      |
|                                                                                              | High        | 0.56 | Very High |
| Confidentiality Requirement (CR)/ Integrity Requirement (IR) / Availability Requirement (AR) | Not defined | 1    | -         |
|                                                                                              | Low         | 0.5  | Very Low  |
|                                                                                              | Low         | 0.5  | Low       |
|                                                                                              | Medium      | 1    | Moderate  |
|                                                                                              | High        | 1.5  | High      |
|                                                                                              | High        | 1.5  | Very High |

The scores are calculated using the  $MISS_v$  formula and afterwards they are normalised using the respective normalisation formula, as presented in the previous example.

The outcome of the current step is a list of Impact Levels (ILs) for all vulnerabilities identified on the ICT assets.

### Step 3.4 Cumulative Vulnerability and Impact Analysis

Vulnerability chains, as described in Section 4, are considered the gradual exploitation of a series of vulnerabilities among interconnected assets. Attack paths are the steps that an adversary takes or may take to plan, prepare for, and execute an attack (see the Glossary of Appendix A).

#### Cumulative vulnerability analysis.

The cumulative vulnerability assessment measures the Exploitation Level (EL) of the identified vulnerabilities considering the adversary's individual actions to satisfy the preconditions required for the exploitation. In particular, it measures the conditional probability that an attacker can successfully reach and exploit each of the vulnerabilities, identified in step 2.2, in a given vulnerability chain originated from all asset Entry Points.

To measure this, the calculated IVLs, the assets' cyberdependencies produced in step 1.3, and the Attacker's (adversary) Profile are considered. The Attacker's Profile relies on the attacker's capability (see Table 96) and location (see Table 97). Within this performance, a rule-based propagation and path construction reasoning approach is followed based on the rules provided in [371]-[372], to generate the chain of sequential vulnerabilities on different assets that arise from consecutive multiple attacks starting from all possible asset entry points (Section 6.2.2.5).

Furthermore, the Individual Chain Vulnerability Level (ICVL)  $ICVL_{C_{k,v}, A_{i,j}, v_{z,A_{x,y}}}$  measures the probability that a vulnerability  $z$ , which resides in an Asset Target Point  $A_n$ , can be exploited given the **specific  $k$ th-Vulnerability Chain  $C$  originated from an Asset Target Point  $A_{i,j}$  with vulnerability  $v$ .**

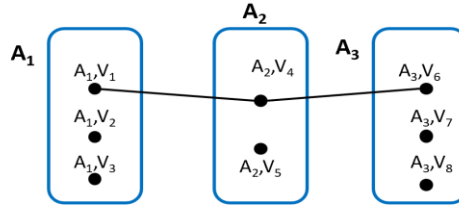


Figure 19. Example of an individual vulnerability chain.

The Entry's vulnerability chains (Entry's Chain Vulnerability Level (ECVL) are **all vulnerability chains originated from a specific Entry Point**  $A_{i,j}$  that can potentially exploit a vulnerability  $z$  which resides in a Target Point  $A_{i,j}$  (considering all its vulnerabilities  $v$ ).

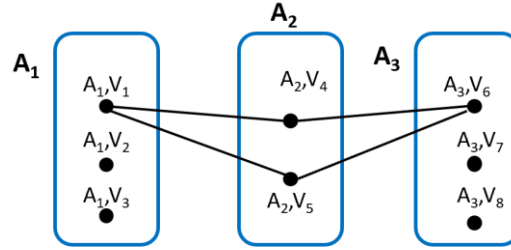


Figure 20. Example of an entry's vulnerability chains.

The Cumulative vulnerability chains includes all Independent Vulnerability Chains  $C_{k,v,A_{i,j},V_{z,A_{x,y}}}$  that can exploit a vulnerability  $z$  which resides in a Target Point  $A_{i,j}$  originated from all Entry Points  $A_{x,y}$ .

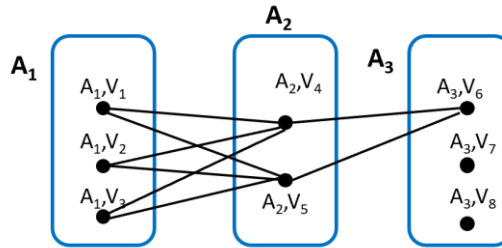


Figure 21. Example of cumulative vulnerability chains.

Regarding the attacker's progfile identification (see Task\_3 of Table 33), the subsequent exploitation of vulnerabilities in the interdependent assets an attacker performs to reach a target point relies on his level of expertise (ICT skilled or pre-mature) and target, namely his capability and his relation with the organisation (whether he is an insider or an outsider), namely his location. To implement the current step the following rules are considered [371]-[372]:

Table 33. Tasks to perform the cumulative vulnerability analysis.

| Task Number | Task Name                                                                    | Task Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------|------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Task_1      | Identify Asset Dependency Graphs                                             | The risk assessor analyses the subject of evaluation (i.e., an ICT product and/or its ICT supply chain network) into its primary elements (ICT assets). Following step 1, the risk assessor identifies asset interdependencies across the underlying network by developing asset dependency graphs.                                                                                                                                                                                                                             |
| Task_2      | Entry Points Identification                                                  | The risk assessor initiates the process defining the Asset Entry Points $A_{x,y}$ from which the attacks will be initiated; these assets are considered as more reachable by an attacker.                                                                                                                                                                                                                                                                                                                                       |
| Task_3      | Target Points Identification                                                 | The risk assessor defines the Asset Target Points $A_{i,j}$ (targeted assets for attacks due to their criticality).                                                                                                                                                                                                                                                                                                                                                                                                             |
| Task_4      | Perform individual Vulnerability Assessment                                  | The risk assessor identifies vulnerabilities on assets and estimates the Individual Vulnerability Level.                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Task_5      | Generate Vulnerability Chains                                                | A rule-based reasoning approach (filters) is provided to generate the chain of sequential vulnerabilities on different assets arising from subsequent multi-steps attacks initiated from the entry points to exploit the vulnerabilities of the target points (see step 3.4). The generated vulnerability chain represents the independent chain that makes accessible the vulnerability $z$ of a specific Asset Target Point $A_{i,j}$ initiated by the exploitation of vulnerabilities $v$ of a given entry point $A_{x,y}$ . |
| Task_6      | Identify Attacker's Profile                                                  | The Attacker's profile is identified concerning attacker's characteristics, such as expertise, knowledge, sources, operational proximity, and the target. The attacker's profile along with intrinsic vulnerability characteristics are considered for the estimation of vulnerability exploitability of a vulnerability $v$ to an ICT asset node.                                                                                                                                                                              |
| Task_7      | Select most accurate Vulnerability Chains – Construct potential attack paths | After calculating vulnerability exploitability metrics, the risk assessor reviews the generated vulnerability chains and selects the most appropriate (ignoring the ones that are not propable/reasonable) chains (see step 3.4 and Section <b>Error! Reference source not found.</b> ).                                                                                                                                                                                                                                        |
| Task_8      | Prioritisation of potential attack paths                                     | The risk assessor measures cumulative metrics and eventually prioritises the potential attack paths according to their criticality considering the given scenario.                                                                                                                                                                                                                                                                                                                                                              |

### Cumulative impact analysis.

The cumulative impact assessment estimates the impact that occurs after a specific asset/vulnerability combination has been exploited by an attacker using any possible (asset) entry point. This is only related to the impact of this specific asset/ vulnerability combination.

Moreover, similarly to the previous vulnerability chains analysis:

- the Individual Chain Impact Level ( $ICIL_k$ ) reflects the effects of the successful exploitation of the vulnerability  $z$  of a Target Point  $A_{i,j}$  originated from a **specific entry point**  $A_{x,y}$  given a **specific**  $k^{th}$ - **Vulnerability Chain**  $C_{k,V_{v,A_{i,j}},V_{z,A_{x,y}}}$  (vulnerability  $v$  is considered to have been exploited).
- The Entry's Chain Impact Level ( $ECIL_k$ ) incorporates the effects of the successful exploitation of the vulnerability  $z$  of the Target Point  $A_{i,j}$  given that **all** independent Entry Chains  $C_{k,V_{v,A_{i,j}},V_{z,A_{x,y}}}$  starting from the vulnerabilities  $v$  of the **specific Entry Point**  $A_{x,y}$  have been exploited.
- The Cumulative Impact Level ( $CIL_k$ ) reflects all the effects of the successful exploitation of a vulnerability  $z$  of a Target Point  $A_{i,j}$  given that **all** independent Entry Chains  $C_{k,V_{v,A_{i,j}},V_{z,A_{x,y}}}$  starting from **all Entry Points**  $A_{x,y}$  have been exploited.

### Step 3.5 Propagated Vulnerability and Impact Analysis

#### Propagated vulnerability assessment.

The propagated vulnerability assessment estimates **how deep into the network an attacker can penetrate** in view of exploiting a series of vulnerabilities. Moreover, it measures the conditional probability that an attacker can successfully reach and exploit vulnerabilities (confirmed and unknown), identified in step 2.2, in a given vulnerability dependency graph. Accordingly, in the propagated vulnerability assessment, a rule-based propagation and path construction reasoning approach is followed [371]-[372], aiming to generate the chain of sequential vulnerabilities on different assets that arise from consecutive multiple attacks starting from a specific asset entry point to exploit a series of vulnerabilities that could reach all possible asset target points.

#### Propagation Rules.

The propagation and path construction rules are based on [276],[370]. They follow a logic-based reasoning approach, which reflects the attacker's profile [125], the attacker's location along with all associated rules that are executed to design the attack graph and construct potential attack paths, as described in [276],[370].

Table 34. Propagation rules ([276],[370]).

| Category of Propagation rule | Propagation rule |
|------------------------------|------------------|
|------------------------------|------------------|

|                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Rules to discover which vulnerabilities, identified on the ICT assets, are accessible by the attacker.                                                   | A vulnerability on an ICT asset is accessible by an attacker if the CVSS Attack Vector (AV) is "Network" (i.e. remotely exploitable) and both the ICT asset and attacker are connected to the same network (e.g. the Internet).                                                                                                                                                             |
|                                                                                                                                                          | A vulnerability on an ICT asset is accessible by an attacker if the CVSS AV is "Adjacent Network" (i.e. exploitable over local network) and both the asset and attacker are connected to the same local network.                                                                                                                                                                            |
|                                                                                                                                                          | A vulnerability on an ICT asset is accessible by an attacker if the CVSS AV has the value "Local" (i.e. requires physical access or local account) and attacker has physical access or a local account.                                                                                                                                                                                     |
|                                                                                                                                                          | A vulnerability on an ICT asset is accessible by an attacker if it can be reached via some other vulnerability of the underlined ICT infrastructure of the ICT product or ICT SCS.                                                                                                                                                                                                          |
| Rule that aims to discover which vulnerabilities, identified on the ICT assets, are exploitable by the attacker.                                         | A vulnerability on an ICT asset is exploitable if it is accessible by the attacker and there exists a viable tool, method or code to exploit it (or if we have no information on the existence of such a tool, method or code) and no suitable security control is in place. Alternatively, an accessible unmitigated vulnerability that only has a theoretical exploit is not exploitable. |
| Rules set to discover which vulnerabilities of the ICT assets can be used as stepping stones (traversed) by the attacker to reach other vulnerabilities. | A connection between two assets is traversable if the starting vulnerability has been successfully attacked and its vulnerability type allows the attacker to use it as a stepping stone to access the Asset Target Point.                                                                                                                                                                  |
|                                                                                                                                                          | A connection between two vulnerabilities affecting assets (or the same asset) is traversable if the starting vulnerability has been successfully attacked and its vulnerability type allows the attacker to use it as a stepping stone to access the final vulnerability of the Asset Target Point.                                                                                         |
| Rules intend to discover the attacker gains after he or she successfully attacks a vulnerability.                                                        | A successfully attacked vulnerability of the gain privilege, execute code or directory traversal type bestows the attacker any access rights available in the asset.                                                                                                                                                                                                                        |
|                                                                                                                                                          | A successfully attacked vulnerability of the execute code type bestows the attacker access to any access rights available in the assets directly connected to the attacked asset.                                                                                                                                                                                                           |
|                                                                                                                                                          | A successfully attacked vulnerability of the execute code, directory traversal, gain information or SQL injection type bestows the attacker access to any data stored by the asset.                                                                                                                                                                                                         |

|  |                                                                                                                                                                      |
|--|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | A successfully attacked vulnerability of the execute code type bestows the attacker access to any data stored by assets directly connected to the compromised asset. |
|  | A successfully attacked vulnerability of the denial of service type makes the asset (and all its vulnerabilities) unavailable.                                       |

### **Propagated impact assessment.**

The propagated impact assessment illustrates the attacker's intention to cause damage on the way at any asset/vulnerability combination. It is defined as the overall impact that takes place when an attacker exploits a specific asset/vulnerability combination and further moves on into the network starting from a specific (asset) entry point.

#### **6.2.2.5 Step 4. Attack Simulation and Evidence Chains Generation**

Step 4 presents the Attack Simulation and Evidence Chain Generation (ASECG) model which aims to deliver credible vulnerability chains in relation to a confirmed security event. The current step encompasses the following steps:

- Step 4.1 Generation of Vulnerability Chains (Step I in Figure 22)
  - Step 4.1.1. Identify Asset Dependency Graphs
  - Step 4.1.2. Define Entry Points
  - Step 4.1.3. Define Target Points
  - Step 4.1.4. Perform Individual Vulnerability Assessment
  - Step 4.1.5. Produce Vulnerability Chain
- Step 4.2 Recurring process activation (Step II in Figure 22)
  - Step 4.2.1. Points of Compromise – Indicators of Compromise
  - Step 4.2.2. Reconstruction of potential attack paths
  - Step 4.2.3. Attacker's Profile identification
  - Step 4.2.4. Prioritisation of Potential Attack Paths
  - Step 4.2.5. Pruning Process Activation.

Table 35 summarises Step 3.

Table 35. Attack Simulation and Evidence Chains Generation.

| <b>Step 4. Attack Simulation and Evidence Chains Generation</b><br><b>Step 4.1 Generation of Vulnerability Chains</b><br>Step 4.1.1. Identify Asset Dependency Graphs<br>Step 4.1.2. Define Entry Points<br>Step 4.1.3. Define Target Points<br>Step 4.1.4 Perform Individual Vulnerability Assessment<br>Step 4.1.5. Produce Vulnerability Chain<br><b>Step 4.2 Recurring process activation</b><br>Step 4.2.1. Points of Compromise – Indicators of Compromise<br>Step 4.2.2. Reconstruction of potential attack paths<br>Step 4.2.3. Attacker’s Profile identification<br>Step 4.2.4. Prioritisation of Potential Attack Paths<br>Step 4.2.5. Pruning Process Activation |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Input</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Attack graphs constructed in Step 3. The list of Individual Vulnerability Levels and Vulnerability Exploitability Levels. IoCs, PoCs derived from logs analysis.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Activity</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | This step aims to deliver the specific attack paths related to a confirmed security event, including the chains of evidence. It estimates the Exploitation Level Chains (ELCs) and the Attack Path Exploitability Level (APEL) after conducting IoC and PoC analysis.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Output</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | It delivers a list of ELCs and APELs. After a pruning process implementation, it provides a list of Credible evidence chains associated with a confirmed security event.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Example</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | <p><u>Input</u>: Log files, intrusion detection evidence, traffic analysis, behavioural analysis derived from external security tools.</p> <p><u>Activity</u>: A database of an Airport’s Flight Information Display (FIDS) system is compromised, according to log analysis. The database exchanges information with several Airport applications and is installed on an operating system. The current step calculates the attack path exploitability of all vulnerability chains of asset graphs that include the FIDS database. Based on the IoC analysis, it explores how the attacker has moved inside the network.</p> <p><u>Output</u>: The outcome is a set of credible evidence chains related to the confirmed security event of the database compromise that provide insight on the attacker’s course within the FIDS Airport’s network.</p> |

Attack graphs describe how an attacker can combine exploitation of multiple vulnerabilities to reach a specific node. The attack path discovery algorithms, described in section 6.2.2.4, compute and deliver all possible attack paths an adversary could follow across all potential asset entry points. Moreover, such algorithms are also able to estimate all the cascading effects and all possible attack paths arising from a specific vulnerability in a given entry point, showing how deeply the adversary is able to penetrate the system. **Nevertheless, they lack the ability to deliver the specific attack paths that concern chains of evidence linking to real security events.**

The incident-related information that resides in diverse heterogeneous ICT systems may include various types of data, i.e., active/unpatched vulnerabilities in the technological infrastructure; misuse detection in the network or in the systems, including both Host-based Intrusion Detection System (HIDS) and Network-based Intrusion Detection System (NIDS) deployment and integration; anomaly detection in the network or in the systems; system availability signals;

network usage and bandwidth monitoring; industry proprietary protocol anomalies; SCADA-related [1]; ICT vulnerabilities; etc. In this vein, the proposed *Attack Simulation and Evidence Chains Generation (ASECG) model aims to enhance the calculation of the utilised attack path discovery algorithm in terms of computing all possible attack paths an adversary could follow in relation to a specific confirmed event that can be identified from various sources* (i.e., log files, network traffic analysis). This raises the need for research into *how to reconstruct attack paths, rebuild their timeline, and prioritise them according to specific confirmed events*.

The proposed ASECG model can represent various cyberattack patterns based on different security incidents within the CIIs, generating multi-order evidence dependencies. Furthermore, it scrutinises the inherent relationships between devices and evidence and represent a timeline of the incident, engaging a map of affected devices and an evidence chain model comprising credible and meaningful chains of evidence. In this manner, the proposed approach can leverage the computation of the cybersecurity risk assessment with such evidence, facilitating rational analysis. Taking into account all the incident-related information received, the ASECG model estimates the cascading effects of various cyberattack patterns and security incidents of the CIIs. It considers based on evidence captured, it explores ongoing attacks and provide contextual attack intelligence, including the attack status and the attacker's location.

Once the cyberattack is identified, a simulation process is performed to reconstruct the attack scenarios and represent the linked evidence. This attack path regeneration enables a deep evaluation of the underlying vulnerabilities, allowing for the detection of where the attack is heading and ultimately identifying the entry and target points of the attack. To address this case, a calculation of all attack paths related to the specific ICT asset(s) is carried out based on evidential data derived from several sources. The attack paths calculation delivers payoffs that match the predefined scenario and produce secure, credible, and valid evidence chains.

The proposed ASECG model is capable of identifying how an attacker has moved inside the infrastructure and further scrutinising their malicious activity. In this context, it can provide valuable insights into a cyberattack's course, and therefore, it could drive the ICT stakeholders and decision-makers to handle the incident effectively and formulate their incident response processes in an efficient manner. An overview of the ASECG model is depicted in Figure 22.



## The Attack Simulation and Evidence Chain Generation (ASECG) Model

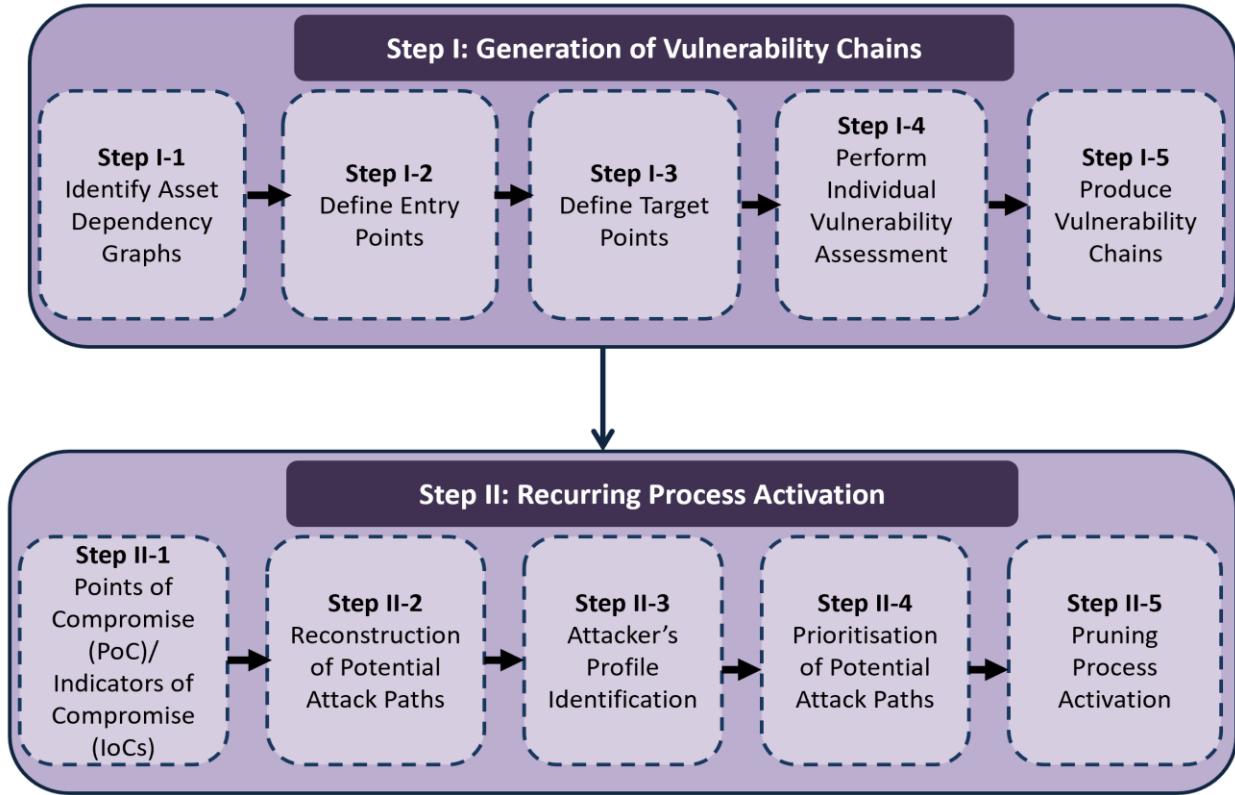


Figure 22. The Attack Simulation and Evidence Chains Generation (ASECG) model.

The ASECG model is based on the approach presented in [9], which was initially developed as part of this dissertation research using FIRST CVSS 2.0 specification metrics and later updated to incorporate FIRST CVSS 3.1 specification metrics. While CVSS 4.0 introduces additional metrics and refinements, this research employs CVSS 3.1 to maintain consistency with the datasets, tools, and validation procedures used throughout the study. Furthermore, CVSS 3.1 remains widely adopted across vulnerability repositories and security assessment platforms. Investigating the adaptation of the ASECG model to CVSS 4.0 constitutes an avenue for future research. Furthermore, the ASECG model enhances the approach in [9] by adjusting the vulnerability exploitability weighted scoring model, described in step 3.2 of 6.2.2.4. The additive formulation was selected because it provides a transparent and interpretable mechanism for integrating technical vulnerability-centric and attacker-specific characteristics into a single exploitability measure.

### Step 4.1. Generation of Vulnerability Chains

The attack path discovery and development algorithm considers as input the outcome of Step 1, “Modelling-based cartography” (see Section 6.2.2.2), Step 3, “Individual Vulnerability Assessment” (see Section 6.2.2.4), and the Vulnerability Chains Discovery method [370], (see Section 6.1.5). It is used to reconstruct attack paths by identifying vulnerability chains whose exploitation could enable potential attack scenarios targeting specific cyberdependent assets. The

attack path discovery relies on unique characteristics, i.e., assets dependency graphs (step 1.3), to calculate all possible non-circular paths attackers could undertake to implement an intrusion. CIIIs of complex ICT networks, such as ICT SCS networks, incorporate a number of dispersed nodes that can be exploited by adversaries to infiltrate a system. The size of attack graphs may vary depending on both the number of vulnerabilities identified within a communication network and the extent to which those vulnerabilities are reachable [276]. Namely, as exploitation capabilities increase, the attack graph expands. The attack graphs are constructed using security information from prominent online repositories, such as the MITRE Common Weakness Enumeration (CWE) [266] and the MITRE Common Vulnerabilities and Exposures (CVE) [140].

The algorithm that discovers and analyses all potential attack paths on CIIIs for complex attack scenarios, given a specific asset cartography adopted by the ASECG model, is presented through subsequent steps, analysed in the Vulnerability Chains Discovery method [370]. Considering that the Vulnerability Chains Discovery method [370] does not calculate all possible attack paths that match a specific confirmed security event, the method is utilised only to generate a list of vulnerability chains (potential attack paths). The subsequent steps to implement the proposed ASECG model are presented in the following. These steps enhance the approach for performing the cumulative vulnerability analysis, described in step 3.3 of Section 6.2.2.4 by developing a model that estimates all credible evidence chains related to a specific confirmed security event. The proposed ASECG model is based on the work published in [9], which was performed in the context of the current dissertation.

#### **Step 4.1.1. Identify Asset Dependency Graphs**

The current step relies on the Asset Cartography and Modeling corresponding step of the risk assessment methodology (illustrated in Chapter 3). In this step, assets are identified, analyzed, and modeled to identify asset characteristics (e.g., asset category, asset vector, version), asset cyber-dependencies, according to specific types of interdependencies (1. hosting; 2. exchange data/information; 3. storing; 4. controlling; 5. processing; 6. accessing; 7. installing; 8. trusted; 9. connecting), and the Access Vector (Physical, Local, Adjacent Network, Network) to develop an asset inventory of an organisation and design asset dependency graphs. Further details and analytical examples of the application of the above assets' characteristics and relations through real-life scenarios are illustrated in the publications [1],[9],[84] which were created during the current dissertation.

#### **Step 4.1.2. Define Entry Points**

Security operators must identify assets that can be highly approachable by adversaries to initiate an attack, considered as entry points.

#### **Step 4.1.3. Define Target Points**

Security operators must identify the most "attractive" assets (critical) for attackers to intrude, considered as target points.

#### **Step 4.1.4. Perform Individual Vulnerability Assessment**

The Individual Vulnerability Level (IVL) estimates the likelihood that an adversary can successfully reach and exploit a specific vulnerability  $v$  on a given asset  $A_n$  (where  $A_n = A_{i,j}$ ). To calculate this, the CVSS 3.1 [139] score metrics related to technical exploitability, i.e., “Modified Attack Vector” (MAV), “Modified Attack Complexity” (MAC), “Modified Privileges Required” (MPR), and “Modified User Interaction” (MUI) are used.

As analysed in Section 6.2.2.4, the IVL is calculated for each identified vulnerability utilising the Modified Exploitability sub-score (MESS) formula of CVSS 3.1 specification [139]:

$$IVL_v = 8.22 \cdot MAV \cdot MAC \cdot MPR \cdot MUI$$

considering the values of the above metrics, depicted in Table 90-

Table 93 of Appendix D4.

After calculating the IVL for all identified vulnerabilities, the normalisation procedure, described in Section 6.2.2.4, is applied to interpret the numeric values from the 0-10 scoring scale of CVSS 3.1 to the quantitative scale 0-1 (or 0-100):

$$IVL_{v_{norm}} = \frac{MESS_v - MESS_{Min}}{MESS_{Max} - MESS_{Min}}$$

Upon normalising the IVL values, the quantitative outcomes are presented in qualitative values following the CyberICT generic assessment scale, presented in Table 87 of Appendix D1.

#### **Step 4.1.5. Produce Vulnerability Chains**

Adoption of a rule-based reasoning approach (filters) presented in [276], which implements the attack path generation algorithm described in [370] to produce the chain of sequential vulnerabilities on different assets that arise from consequential multi-step attacks, initiated from all Entry Points in order to exploit the vulnerabilities of all possible Asset Target Points.

As described in 6.2.2.4, the Individual Chain Vulnerability Level (ICVL) measures the likelihood that a vulnerability  $z$ , identified in an Asset Target Point  $A_n$ , can be exploited via a specific  $k$ th-Vulnerability Chain  $C$  from a specific Asset Target Point  $A_m$ .

The proposed Attack Simulation and Evidence Chains Generation approach aims to identify all possible attack paths that are linked to the specific security event that has been detected. The current step builds all possible vulnerability chains in general, either from a given asset entry point or a given asset target point. Incident-related information is analysed in Step 4.2.1 and considered for the attack path reconstruction to capture only the attack paths related to the specific security event, described in Step 4.2.2.

#### **Step 4.2: Recurring process activation**

To implement the current step, the Attack Simulation and Evidence Chains model follows the developed algorithmic process, presented below.

##### **Step 4.2.1. Points of Compromise – Indicators of Compromise**

Points of Compromise (PoC) refer to the specific entry points  $A_m$ , vulnerable ICT assets, or pathways an attacker uses to infiltrate a network (e.g., a stolen VPN password, a zero-day exploit). Indicators of compromise (IoC) are the digital evidence (artefacts) of cyberattacks on a system or network. They are the footprints left behind from a breach potential (e.g., unusual traffic activity and malware file hashes).

This step analyses such artefacts (IoC) to capture security knowledge regarding the intrusion attempts detected or other malicious traffic or activities. A deep analysis is carried out on these indications provided (i.e., incident alerts that are raised along with the respective notifications, lateral movement, or data exfiltration) to explore which parts of the underlying ICT infrastructure have been compromised, aiming to identify the Points of Compromise (PoC) and elicit information on the particular intrusion technique and malicious behaviour.

#### **Step 4.2.2. Reconstruction of potential attack paths**

Once all the security data has been explored and correlated, the obtained information is used to reconstruct the potential attack paths according to the analysed IoC. Attack paths that do not match the received indications are erased. With respect to the reconstructed attack paths, all vulnerability chains that are linked to the IoC are generated.

#### **Step 4.2.3. Attacker's Profile identification**

The attacker's profile, presented in Section 6.2.2.4, is adopted, which considers the attacker's exploitation aspect, including the attacker's capability (e.g., expertise, available resources, and opportunities), and the attacker's location, namely, the adversary's operational proximity to the underlying ICT network (cf. Table 96 of Appendix D5).

The attacker's factors are considered equally important. The attacker's profile is calculated, according to the formula presented in Section 6.2.2.4:

$$P_i = f(Capability_i, Location_i)$$

$$P_i = 0.5 Capability_i + 0.5 Location_i$$

where  $P_i$  is the Profile of the attacker  $i$  considering attacker's  $i$  capability and location.

Within this step, the computation of Exploitation Levels and Exploitation Level Chains is provided. The Exploitation Level (EL) of an identified vulnerability on an asset considers the attacker's profile and the Individual Vulnerability Level of the potential attack paths remained from the reconstruction process of step 5.2.2. This is achieved using the exploitability fusion model (see Section 6.2.2.4):

$$EL_v = w_1 IVL_v + w_2 P_i$$

where

$EL_v$  is the Exploitation Level of an identified vulnerability  $v$  on an asset  $A_n$ , considering its Individual Vulnerability Level  $IVL$  and the profile  $P$  of the attacker  $i$ .

The  $A_n$  asset node resides in the potential attack paths remained from the reconstruction process of step 5.2.2.

$w_1$  and  $w_2$  are weights of the IVL and attacker's Profile, respectively.

As described in Step 4.1, IoC are artefacts of cyberattack detected within an ICT system or ICT network. The  $EL_v$  values are used to build the Exploitation Level Chains (ELCs). ELCs are considered a sequence of exploitation levels  $EL_v$  of individual vulnerabilities  $v$  on specific asset-vulnerability combinations, related to an IoC. The ELC is used to calculate the exploitability of the vulnerability chain as a propagated analysis. A multiplication operation is performed to illustrate how a set of Exploitation Levels are mapped onto new levels [372].

$$ELC_{v_n} = EL_{v_1} \times EL_{v_2} \times \dots \times EL_{v_n}$$

where:

- $ELC_{v_n}$  is the Exploitation Level Chain that is related to a vulnerability chain that consists of  $n$  number of vulnerabilities
- $EL_{v_j}$  is the Exploitation Level (EL) of vulnerability  $v_j$
- $n \in \mathbb{N}$  is the number of vulnerabilities in the vulnerability chain

Concerning the EL of the compromised node of the asset-vulnerability combination graph:  $EL_{IOC_k} = 1$ , where  $IoC_k$  is a confirmed  $k$ -security event. Furthermore, the Attack Path Exploitability Level (APEL) is computed as a propagation of vulnerability exploitability levels, where observed compromise points  $IoC_k$  are inserted as deterministic states ( $EL=1$ ) representing confirmed traversal of the attack path. Thus, the previous general formula for the ELC becomes as presented below for an ELC related to a confirmed security event:

$$APEL = ELC_k = EL_{v_1} \times EL_{v_2} \times EL_{IOC_k} \times \dots \times EL_{v_n}$$

which can be represented in the following formula

$$APEL = \prod_{i=1}^n EL_{v_i}$$

where:

- $APEL$  is the Attack Path Exploitability, namely the  $ELC_k$ , i.e., the  $k$ -Exploitation Level Chain that is related to a confirmed security event (linked with an IoC)
- $EL_{v_i}$  is the Exploitation Level (EL) of vulnerability  $v_i$
- $i$ = vulnerability index in the attack path and  $n \in \mathbb{N}$  is the total number of vulnerabilities within the vulnerability chain, so  $v_i$  is the starting vulnerability deriving from the asset entry point and  $v_n$  is the final vulnerability that could have been potentially exploited of the asset target point
- $IoC_k \in ELC_k$  is associated with the confirmed  $k$ -security event with an IoC node (PoC)

$$EL_{IOC_k} = 1.$$

The outcome is a quantitative value. Then, the APEL is estimated in a qualitative value considering the CyberICT propability scale (see Appendix D1). The APEL illustrates in a

qualitative value the level of exploitation for a given attack path towards a specific confirmed event associated with a specific IoC. It is noted that in the proposed model, IoCs are treated as attack evidence on observed nodes within a potentially successful vulnerability chain (potential attack paths) and assigned with the exploitation value of 1, allowing them to be seamlessly integrated into the multiplicative propagation framework without altering the underlying chain structure.

#### Step 4.2.4. Prioritisation of Potential Attack Paths

The current step relies on the specific attacker's profile (i.e., capability, location through the network) identified in step 4.2.3. All assets from the graph that the attacker does not have the ability or the access required shall be erased. The attack course is reconstructed, and asset entry and asset target points are identified for each given attack path. In this regard, all possible evidence chains that match the confirmed incident are prioritised according to the worst-case scenario, to the greatest impact (security, financial, environmental) the assets' compromise can cause harm to the interconnected ICT infrastructures and the organisation, which is revealed by categorising the identified attack paths from highest to lowest APEL.

#### Step 4.2.5. Pruning Process Activation

Since the attacker's profile and APEL are identified, these two metrics are mapped to specify the attacker's exploitation capacity towards a given attack path. The attacker's profile is related to a set of characteristics, presented in Table 96 and Table 97 of Appendix D5, i.e., knowledge/expertise, available resources, and opportunities required to exploit a single or a sequence of vulnerabilities. For instance, an attacker with limited knowledge or few available resources and opportunities cannot successfully conduct complex and advanced cyberattacks; he/she can only take advantage of attack paths of high levels of exploitability (APEL). Moreover, as the APEL exploitability decreases, the attacker must possess higher capabilities, resources, knowledge, or privileged conditions to successfully exploit the vulnerability. As a result, the following mapping is developed (Table 36). the attacker must possess extremely high capabilities, resources, knowledge, or privileged conditions to successfully exploit the vulnerability.

Table 36. Mapping of the attacker's capability and the attack path exploitability to identify the attacker's exploitability potential

| Attacker's Exploitation Capacity            |                                                                                                                                                                                   |                                                                                                                                               |
|---------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| Qualitative Values of Attacker's Capability | Description of the Attacker's Capability                                                                                                                                          | Attack Vector towards Exploitability                                                                                                          |
| Very High (VH)                              | The adversary has a very sophisticated level of expertise, is well-resourced, and can generate opportunities to support multiple successful, continuous, and coordinated attacks. | The adversary is capable of implementing an attack path that has VL, L, M, H, or VH level of exploitability in a sequence of vulnerabilities. |
| High (H)                                    | The adversary has a sophisticated level of expertise, with significant resources and opportunities to support multiple successful coordinated attacks.                            | The adversary is capable of implementing an attack path that has L, M, H, or VH level of exploitability in a sequence of vulnerabilities.     |

|               |                                                                                                            |                                                                                                                                        |
|---------------|------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| Moderate (M)  | The adversary has moderate resources, expertise, and opportunities to support multiple successful attacks. | The adversary is capable of implementing an attack path that has M, H, or VH level of exploitability in a sequence of vulnerabilities. |
| Low (L)       | The adversary has limited resources, expertise, and opportunities to support a successful attack.          | The adversary is capable of implementing an attack path that has H or VH level of exploitability in a sequence of vulnerabilities.     |
| Very Low (VL) | The adversary has very limited resources, expertise, and opportunities to support a successful attack.     | The adversary is capable of implementing an attack path only with VH level of exploitability in a sequence of vulnerabilities.         |

Eventually, the prioritised attack paths are reviewed and evaluated against the attacker's exploitation capability, and less important paths are pruned. The remaining attack paths are capable of addressing the given confirmed event, and credible evidence chains are generated. The results can be further explored and guide the ICT stakeholders to set recommendations, to undertake an effective incident response handling policy that could either address or mitigate the effects of the incident. The subsequent steps of the proposed approach are visualised in Table 37, along with the corresponding tasks, construction, and semantic rules applied in the current algorithmic process.

Table 37. Mapping of the attacker's capability and the attack path exploitability to identify the attacker's exploitability potential.

| Step Number     | Step Name                                   | Tasks and Rules                                                                                                                                                                                                   |
|-----------------|---------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step I</b>   | <b>Generation of Vulnerability Chains</b>   | <b>Construct all possible Asset/Vulnerability combinations between an Asset Entry Point and an Asset Target Point</b>                                                                                             |
| <b>Step I-1</b> | Identify Asset Dependency Graphs            | a. Identify assets<br>b. Identify assets characteristics (e.g., type, vendor)<br>c. Identify assets interdependencies<br>c.1 Access Vector<br>c.2 Asset Cyberdependencies<br>d. Construct asset dependency graphs |
| <b>Step I-2</b> | Define Entry Points                         | e. CII operators define assets that are more reachable by the attackers to initiate an attack.<br>f.                                                                                                              |
| <b>Step I-3</b> | Define Target Points                        | g. CII operators define assets of high criticality on their infrastructures that may attract attackers to reach.                                                                                                  |
| <b>Step I-4</b> | Perform Individual Vulnerability Assessment | h. Estimate Individual Vulnerability Level (the exploitability utility of a vulnerability to an asset).                                                                                                           |
| <b>Step I-5</b> | Produce Vulnerability Chains                | i. Generate the chain of sequential vulnerabilities on different assets arising from Entry Points to exploit the vulnerabilities of the Target Points.                                                            |
| <b>Step II</b>  | <b>Recurring Process Activation</b>         | <b>Construct all possible Attack Paths related to a</b>                                                                                                                                                           |

| (step 5.2 of CyberICT risk assessment methodology) |                                          | specific security confirmed event |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------------------------------|------------------------------------------|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step II-1                                          | PoCs/IoC                                 | j.<br>k.                          | Analyse artifacts and incident-related information.<br>Investigate for PoC.                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Step II-2                                          | Reconstruction of Attack Paths           | l.<br>m.                          | Identify all vulnerability chains connected with the IoC.<br>Erase all Attack Paths that are not connected with the IoC.                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Step II-3                                          | Attacker's Profile Identification        | n.<br>o.<br>p.<br>q.<br>r.        | Define Attacker's Profile (Location, Capability).<br>Erase Vulnerability Chains with Asset Entry Points that are not reachable to the attacker.<br>Estimate the Exploitation Levels of vulnerabilities on the developed attack paths (they must all link to the IoC).<br>Estimate the exploitability of all attack paths (APEL) (they must all link to the IoC).<br>The exploitability level of vulnerabilities that reside in the infected asset is 1: exploitability probability $P_{IoC} = 1$ as the asset has already been compromised. |
| Step II-4                                          | Prioritization of Potential Attack Paths | s.<br>t.                          | Prioritise the attack paths to the worst-case scenario (Classify the APEL from "Very High" to "Very Low").<br>Map attacker's capability and APEL to specify the Attacker's Exploitation capacity towards a given attack path.                                                                                                                                                                                                                                                                                                               |
| Step II-5                                          | Pruning Process Activation               | u.<br>v.                          | Pruning Process Activation for all attack paths; the attacker has no exploitability capacity and review remaining attack paths.<br>Evidence Chains generated.                                                                                                                                                                                                                                                                                                                                                                               |

#### 6.2.2.6 Step 5. Risk Estimation

Step 5 aims to estimate the risk considering different aspects: the individual risk, cumulative risk and propagated risk. The cumulative risk and propagated risk are mostly used for large scale, chaotic ICT networks, such as the ICT supply chain service and/or when a rigor and in-depth risk analysis is needed either of an ICT product or ICT network. Step 5 is further analysed into the below steps:

- Step 5.1 Individual Risk analysis
- Step 5.2 Cumulative Risk analysis
- Step 5.3 Propagated Risk analysis

Table 38 summarises Step 3.

Table 38. Risk Estimation.

| Step 5. Risk Estimation           |                                                                                                                                                                       |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 5.1 Individual Risk analysis |                                                                                                                                                                       |
| Step 5.2 Cumulative Risk analysis |                                                                                                                                                                       |
| Step 5.3 Propagated Risk analysis |                                                                                                                                                                       |
| Input                             | The threat levels, individual vulnerability exploitability, cumulative vulnerability and impact analysis, the propagated vulnerability and impact analysis of step 3. |



|                 |                                                                                                                                                                                                                                                                                                                                                  |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Activity</b> | This step aims to calculate the cyber risks of all ICT assets of an ICT product or ICT SCS assets operating for the execution of ICT processes. The individual risk level is estimated. For large-scale networks, such as the ICT supply chain networks and for more rigor and deep analysis, the cumulative and propagate risks are calculated. |
| <b>Output</b>   | Lists of: Individual Risk Levels (RLs), Individual Chain Risk Level (ICRLs), Entry Chain Risk Level (ECRL), Cumulative Risk Level (CRLs), Individual Propagated Risk Levels (IPRLs), Propagated Risk Levels (PRLs).                                                                                                                              |
| <b>Example</b>  | An indicative example is provided within the current section.                                                                                                                                                                                                                                                                                    |

The current step estimates the risk exposure of ICT assets concerning three main types of risks, based on [371]–[372],[379]:

- The individual risk, which represents how dangerous a threat is to a specific ICT asset of an ICT product or an ICT supply chain service.
- The cumulative risk, which estimates the risk exposure of the successful exploitation of multiple vulnerabilities to reach a specific ICT asset embedded in an ICT product or within an ICT network starting from different entry points.
- The propagated risk, which shows how deep into the ICT network an attacker may penetrate in case he/she successfully exploits vulnerabilities found in asset entry points in relation to the corresponding threats.

### Step 5.1 Individual Risk analysis

Risk level estimates *how dangerous threat to a specific SCS asset* within the SCS. The individual risk metric estimates how dangerous are all threats to a specific asset.

Having estimated threat, vulnerability, and impact levels for each identified ICT asset the risk level can be calculated for each particular asset following the well-known multiplication of risk equation presented below:

The individual Risk Level (RL) represents how dangerous all threats  $s$  are to the specific asset  $A_{i,j}$ . After estimating all the Threat Levels  $TL_s$  (step 2), the Vulnerability Exploitation Levels  $EL_v$  (step 3), and Impact Levels  $IL_v$  (step 3), the Risk Level  $RL$  is estimated for each asset  $A_{i,j}$  identified in step 1. To estimate the  $RL$ , the generic risk formula multiplication is utilised:

$$\begin{aligned}
 \text{Risk Level} &= \text{Threat Level} \times \text{Vulnerability Level} \times \text{Impact Level} \\
 \text{Risk Level}_v &= \text{Threat Level}_s \times \text{Exploitation Level}_v \times \text{Impact Level}_v \\
 RL_{s,A_{i,j}} &= TL_s \times EL_v \times IL_v
 \end{aligned}$$

where

$RL_{s,A_{i,j}}$ : The individual Risk Level of a threat  $s$  to a specific asset  $A_{i,j}$  with a vulnerability  $v$  identified on this asset.

$TL_s$ : The estimation of cyber threat  $T_s$  occurrence to a given ICT asset  $A_{i,j}$  based on historical data, human knowledge and expertise, and web sources.

$EL_v$  : The likelihood of successful exploitation of an identified vulnerability  $v$  identified on an asset  $A_{i,j}$  considering intrinsic vulnerability metrics ( $IVL_v$ ) and attacker-specific characteristics (Attacker's Profile  $P_i$ ).

$IL_v$  : The expected effect from the successful exploitation of a vulnerability  $v$  identified in an ICT asset  $MISS_v$

This step produces individual risk analysis, to estimate how dangerous a threat appears on a specific cyber asset.

### Example

Assuming the following values for Threat Level, Exploitation Level and Impact Level:

- $TL_s = 0.7$  -> High (H)
- $EL_v = 0.65$  -> High (H)
- $IL_v = 0.863$  -> Very High (VH)

Using the above risk formula:

$$RL_{s,A_{i,j}} = TL_s \times EL_v \times IL_v$$

$$RL_{s,A_{i,j}} = 0.7 \cdot 0.65 \cdot 0.863 \approx 0.393$$

## Step 5.2 Cumulative Risk analysis

Cumulative risk analysis aims to estimate the risk exposure of the successful exploitation of multiple vulnerabilities, targeting a specific ICT asset starting from various Asset Entry Points.

**The Individual Chain Risk Level ( $ICRL_{s,C_k}$ )** measures the risk for a threat  $s$  exploiting the target vulnerability via a specific vulnerability chain.

$$ICRL_{s,C_k} = TL_s \times ICVL_{C_k} \times ICIL_{C_k}$$

$$ICRL_{s,C_k} = TL_s \times \left( \prod_{i=1}^n EL_{v_i} \right) \times IL_{C_k}$$

where

$ICRL_{s,C_k}$  : the Individual Chain Risk Level of the  $k$ th vulnerability chain

$TL_s$  : the Threat Level of a threat  $s$

$C_k = \{V_1, V_2, \dots, V_n\}$  : is the  $k$ th vulnerability chain of  $n$  vulnerabilities

$EL_{v_i}$  : exploitation likelihood of vulnerability  $V_i$

$n$  : number of vulnerabilities along the chain

$\prod_{i=1}^n EL_{v_i}$  : multiplication of  $EL_{v_i}$  for all  $n$  vulnerabilities to identify the Individual Chain Vulnerability Level (ICVL)

$ICIL_{C_k}$  : the Individual Chain Impact Level of the  $k$ th vulnerability

Each vulnerability chain has an Individual Chain Vulnerability Level:

$$ICVL_{C_1}, ICVL_{C_2}, \dots, ICVL_{C_n}$$

The Entry Chain Vulnerability Level (ECVL), as presented in step 3, is the probability that **at least one** of these chains successfully exploits the target vulnerability.

The **Entry Chain Risk Level** (ECRL) quantifies the risk of a threat  $s$  exploiting a target vulnerability  $z$  through any of the independent vulnerability chains originating from a specific entry point  $A_{i,j}$ . Assuming chain independence, ECR is computed as the complement of the probability that none of the individual chain risks materialise:

$$ECRL_{(s, z, A_{i,j}, A_{x,y})} = 1 - \prod_{k=1}^n (1 - TL_s \times ECVL_{C_k} \times ECIL_{C_k})$$

Assuming chain independence, where

$ECRL_{(s, z, A_{i,j}, A_{x,y})}$ : the Entry Chain Risk Level of a threat  $s$  exploiting a target vulnerability  $z$  on asset  $A_{i,j}$

$TL_s$ : the threat level of a threat  $s$  as stated above

$ECVL_{C_k}$ : Entry Chain Vulnerability Level (ECVL), as presented in step 3, is the probability that **at least one** of these chains successfully exploits the target vulnerability

$ECIL_{C_k}$  The Entry's Chains Impact Level (ECIL) estimates the effect of the successful exploitation of the vulnerability  $z$  of the Asset Target Point  $A_{i,j}$  from a specific Asset Entry Point  $A_{i,j}$

The **Cumulative Risk Level** (CRL) is the risk of a threat  $s$  occurring due to a vulnerability  $z$  that exists in the target point  $A_{i,j}$  considering **all entry points and all vulnerability chains** (CVLs).

Similarily to the above, the risk formula of CRL is:

$$CRL_{s,C_k} = TL_s \times CVL_{C_k} \times CIL_{C_k}$$

where

$CRL_{s,C_k}$ : the risk exposure of a threat from the successful exploitation of **all asset entry points considering all vulnerability chains**

$TL_s$ : The likelihood of the threat  $s$  as defined above

$CVL_{C_k}$ : the likelihood that :vulnerability  $z$  can be exploited considering **all entry points and all vulnerability chains** (CVL).

$CIL_{C_k}$ : the impact resulting from such exploitation considering **all entry points and all chains** (CIL).

## Step 5.2 Propagated Risk analysis

Propagated risk analysis, to calculate how deep into the network an attacker may penetrate in case he/she successfully exploits vulnerabilities identified in (asset) entry points corresponding to threats.

The **Individual Propagated Risk Level** (IPRL) refers to the risk of a threat  $s$  occurring due to a vulnerability  $v$  that exists in an Asset Entry point  $A_{x,y}$  that may cause the exploitation of a specific  $k$ th vulnerability chain.

$$IPRL_{s,C_k} = TL_{(s,A_{i,j})} \times IPVL_{C_k} \times IPIL_{C_k}$$

where

$IPRL_{s,C_k}$  : risk propagation through the specific  $k$ th vulnerability chain

$TL_{(s,A_{i,j})}$  : threat level at entry point  $A_{x,y}$

$IPVL_{(C_k)}$  : probability that vulnerability  $v$  propagates through the specific chain  $C_k$

$IPIL_{(C_k)}$  : propagated impact through the specific  $k$ th vulnerability chain

The **Propagated Risk Level** (PRL) is the risk of a threat  $s$  occurring due to the vulnerability  $v$  existing in an Asset Entry Point  $A_{x,y}$ , considering **all independent propagated chains**:

$$PRL_{s,V_{v,A_{x,y}}} = TL_s \times PVL_{vA_{x,y}} \times PIL_{vA_{x,y}}$$

where

$PRL_{s,V_{v,A_{x,y}}}$  : risk propagation through all independent vulnerability chains

$TL_s$  : threat level  $s$  of an asset  $A_{x,y}$

$PVL_{vA_{x,y}}$  : probability that vulnerability  $v$  propagates through all independent vulnerability chains

$PIL_{vA_{x,y}}$  : the propagated (overall) impact occurring from the exploitation of a specific asset/vulnerability combination through all independent vulnerability chains as the adversary penetrates the ICT network

### Example:

Assuming that vulnerability  $v$ , identified on Asset Entry point  $A_1$ , can propagate through three independent chains where

Entry point  $A_1$ , vulnerability  $v \rightarrow A_1, V_v$

Three independent chains:  $C_1, C_2, C_3$  with the information provided below:

Table 39. Short scenario for estimating the risk propagation.

| Threat Level | Individual Propagated Vulnerability Level (IPVL) | Individual Propagated Impact Level (IPIL) | Vulnerability Chains |
|--------------|--------------------------------------------------|-------------------------------------------|----------------------|
| $TL_s = 0.8$ | $IPVL_1 = 0.5$                                   | $IPIL_1 = 0.6$                            | $C_1, C_2, C_3$      |
|              | $IPVL_2 = 0.4$                                   | $IPIL_2 = 0.5$                            | $C_1, C_2, C_3$      |
|              | $IPVL_3 = 0.3$                                   | $IPIL_3 = 0.4$                            | $C_1, C_2, C_3$      |

To estimate the Individual Propagated Risk Level per chain (IPRL) the IPRL formula is utilised:

$$IPRL_{s,C_k} = TL_s \times IPVL_{C_k} \times IPIL_{C_k}$$

$$IPRL_{s,C_1} = 0.8 \times 0.5 \times 0.6 = 0.24 = \text{Low}$$

$$IPRL_{s,C_2} = 0.8 \times 0.4 \times 0.5 = 0.16 = \text{Very Low}$$

$$IPRL_{s,C_3} = 0.8 \times 0.3 \times 0.4 = 0.096 = \text{Very Low}$$

To estimate the Propagated Risk Level (PRL) it is considered that the propagated risk of the Asset Entry point is the probability that  **$\geq 1$  chain propagates successfully**, multiplied by the **aggregated impact** and threat likelihood:

$$PVL = 1 - \prod_{k=1}^3 (1 - IPV L_k)$$

$$PIL = 1 - \prod_{k=1}^3 (1 - IPC I_k)$$

$$PRL = TL_s \times PVL \times PIL$$

The PVL is calculated:

$$PVL = 1 - (1 - 0.5)(1 - 0.4)(1 - 0.3) = 1 - (0.5 \times 0.6 \times 0.7) = 1 - 0.21 = 0.79$$

Then, the PIL is calculated:

$$IPIL = 1 - (1 - 0.6)(1 - 0.5)(1 - 0.4) = 1 - (0.4 \times 0.5 \times 0.6) = 1 - 0.12 = 0.88$$

Eventually, the Propated Risk Level (PRL) is estimated:

$$PR = 0.8 \times 0.79 \times 0.88 \approx 0.556 = \text{Moderate (M)}.$$

### 6.2.2.7 Step 6. Management and treatment of risks

Step 6 aims to guide the ICT stakeholders and business partners to identify alternative mitigation strategies with respect to risk compliance and security assurance. Moreover, it aims to support the involving parties in selecting and implementing the optimal mitigation strategy. Step 6 is decomposed into the following steps:

- Step 6.1 Mitigation strategies identification – Risk compliance to security assurance
- Step 6.2 Optimal Mitigation strategy selection and implementation

Table 40 summarises step 6.

Table 40. Management and treatment of risks.

| Step 6. Management and treatment of risks<br>Step 6.1 Mitigation strategies identification – Risk compliance to security assurance<br>Step 6.2 Optimal Mitigation strategy selection and implementation |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Input</b>                                                                                                                                                                                            | The specifications and agreement on the conditions of the cybersecurity risk assessment, defined in step 0. The risk assessment results of step 5.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Activity</b>                                                                                                                                                                                         | This step aims to support the identification of mitigation strategies, how to explore, experiment, select and implement the optimal defence to adopt. In addition, it recommends further actions to ensure the validity of the adopted strategies and guarantee the satisfaction of security requirements.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Output</b>                                                                                                                                                                                           | Implementation of security controls, security testing evidence, protection profile (where applicable) and controls documentation, self-assessment or attestation proof to ensure validity                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Example</b>                                                                                                                                                                                          | <p><u>Input:</u> Risk assessment results for a smart vehicle, considered as an ICT product, or the Vehicle Transport supply chain service. Corresponding SLAs and Mutual Agreements.</p> <p><u>Activity:</u> Cost-benefit analysis was conducted and a set of mitigation strategies related to data integrity and repudiation have been explored. The security controls efficiency and effectiveness were evaluated in a recurring process against a set of security requirements, specified while creating the Common Criteria-based Protection Profile. Attack paths alternative scenarios and payoffs were explored in the Vehicle Transport Service case. Secret scanning security testing was conducted to support the controls performance. Eventually, the optimal mitigation strategy is adopted, including cryptographic hashing and Public Key Infrastructure (PKI). The subject of evaluation passed through a third party conformity assessment process by a designated Conformity Assessment Body (CAB).</p> <p><u>Output:</u> list of the implemented security controls, secret scanning testing results, Protection Profile of the smart vehicle ICT product, additional evaluation evidence, Testing Laboratory's evaluation report and attestation of conformity.</p> |

Once the cybersecurity risk assessment process has been accomplished, the final step is to manage the identified cyber risks on the ICT assets to meet the level of security, specified in step 0. As described in Section 4.1, risk treatment is the process of modifying risks considering the security level to be achieved, which has been pre-defined in the commence of the cybersecurity risk assessment process (step 0). Moreover, the ICT stakeholder and business partners involved in the

risk assessment process have mutually agreed to undertake proper security controls according to the risk assessment results.

To achieve this, risk mitigation strategies and actions should be adopted for lessening the negative effects and impacts of threats on ICT assets (see Section 4.1). ISO/IEC 27001 [55] specifies the requirements for establishing, implementing, maintaining and continually improving an ISMS according to the entity's assessment scope. Depending on the risk posture, multiple, diverse risk mitigation strategies can be combined to offer a broader practice of cybersecurity risk management. In general, there are four main types of risk mitigation strategies, introduced by ISO/IEC 27001 [55],[381]:

- **Risk Avoidance strategy:** Eliminating activities or processes that create unacceptable risks. This applies when the consequences are deemed too high to justify/undertake the cost of mitigating potential issues. For instance, banning laptops from leaving company premises approach can be adopted if the risk of unauthorized access is too high.
- **Risk Retention (Acceptance) strategy:** Accepting a risk without taking action is adopted usually when the cost of risk mitigation exceeds the potential impact. This is generally the least preferred option.
- **Risk Sharing (Transfer) strategy:** Transferring part of the risk to a third party, such as through insurance. While this reduces financial exposure, it does not prevent the incident itself.
- **Risk Monitoring strategy:** This is the most common option. It supports continuous monitoring of risks and security controls implementation to prevent their impact from increasing. Examples include safeguards, such as firewalls, multi-factor authentication, and other mitigation measures/actions for privacy and security monitoring.

When an entity decides to adopt a risk monitoring strategy to reduce/eliminate the risk, appropriate security controls must be implemented. Security controls include any process, policy, device, practice, or other actions which modifies the risk. It is possible that controls not always exert the intended or assumed modifying effect. Security controls may generally fall into the following categories:

- **Establishing new rules and procedures:** Creating and documenting policies, plans, procedures, and work instructions to guide secure operations, although simpler processes may not require formal documentation.
- **Implementing technological solutions:** Deploying technologies, such as backup systems, disaster recovery sites, and other security tools to reduce risk.
- **Modifying the organisational structure:** Adjusting roles and responsibilities, including creating new positions or redefining existing job functions, to improve risk management and oversight.

Baselines and security requirements, especially for CIIs and critical ICT products, are defined over time through regulations, standards (e.g., NIS 2 Directive, Cyber Resilience Act,

Cybersecurity Act) and baselines are often available from national Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs).

To improve the selection of effective risk treatment measures and controls, it is important to involve specialists from relevant areas. For example, IT professionals should contribute to technology-related controls, while human resources specialists can support treatments involving training and awareness programs. The final approval of any treatment option should come from the appropriate level of management, such as the CISO, project manager, department head, or senior executive. If responsibilities are unclear, guidance should be sought from a higher management authority [55]. After selecting and planning the treatment measures, the residual risk must be assessed for each previously identified unacceptable risk. Residual risk represents the level of risk that remains after controls have been implemented [55].

#### **Step 6.1. Mitigation strategies identification – Risk compliance to security assurance**

As defined by the ISO/IEC 15408 [44], security assurance is the grounds of confidence that a subject of evaluation meets specified security requirements and pre-defined objectives. The agreement that has been signed (e.g., SLA, SDA) among the parties involved in the risk assessment process (step 0) defines a set of security requirements (e.g., to reach internal organisation's security goals, or be compliant to regulatory security requirements, such as CRA, CSA cybersecurity requirements such as by identifying Protection Profile requirements for their ICT product or ICT SCS -see Chapter 7). These requirements shall be met by adopting optimal security strategies. To this aim, ICT stakeholders and business partners should:

- Explore various mitigation strategies
- Conduct Cost-Benefit Analysis
- Adopt security measures focusing on risk compliance with the specified security requirements (e.g., Protection Profile security requirements)
- Assess the risk levels estimates against specified security requirements

The vulnerability chains produced during the attack path construction (see step 3 and step 4) expose the risks embedded in the individual ICT assets and in the entire ICT supply chain service (ICT SCS). Thereupon, the ICT stakeholders and business partners require guidelines recommending the selection of the most appropriate security controls and indicating optimisation practices, to minimise the expected damage.

The methodology provides guidance for rational-decision making, enabling ICT stakeholders to determine which security controls must be implemented and which business partners need to implement them to encounter the identified security issues and cyber risks (in case an ICT SCS is the subject of security evaluation). The CyberICT risk assessment methodology provides the following recommendations for identifying the optimal mitigation strategies for ICT product owners and ICT supply chain operators [1]:

- For ICT products security evaluation to be prepared for a conformity assessment process:



- Review the risk assessment results and focus on assets with high individual risk; highlight the responsible vulnerabilities and the applicable security controls.
- Review the security requirements defined when setting the boundaries of the assessment (step 0) or the security requirements specified in a protection profile of the under evaluation ICT product if the aim is to get prepared for a cybersecurity certification evaluation process following an adopted scheme (e.g., the EUCC [14]), as described in Chapter 7.
- If a Protection Profile aims to be developed (see Section 7.1.2.2), explore interrelations of the specified security requirements with security objectives and the security problem defined and select strategies that mitigate security issues related to the corresponding threat categories. In addition, consult the CyberICT taxonomy that relates the security requirements with corresponding security controls
- In case rigorous and deep evaluation is needed (depending on the selected Assurance Level, see Sections 4.6 and Chapter 7), run attack path analysis scenarios, as indicated in the ICT SCS assessment case, described in the following
- For ICT SCS security evaluation:
  - Review the risk assessment results and focus on assets with high individual risk; highlight the responsible vulnerabilities and the applicable security controls.
  - Run attack path analysis scenarios setting:
    - high-risk assets as entry points (e.g., GIS web services, malware SCADA supervisory workstations, etc.)
    - cyberdependencies as targets. To determine the critical ICT assets and consider their cyberdependencies and their location to the network, the ICT stakeholder can consult the asset criticality rules defined in step 1.3.
  - Explore the attack paths and vulnerabilities that considerably contribute to the cumulative risk on the cyberdependencies. Mitigating these will limit the potential impact imposed on collaborating business partners. In addition, attack path analysis can be conducted by developing alternative scenarios of cyberdependencies as entry points and study the propagated sub-graph;
  - Mitigation Strategy Selection. Select the security controls of choice and build different defensive strategies. Since all defence strategies and the corresponding payoffs have been determined, use game-theoretic and Blue Team – Red Team approaches to evaluate the defence strategies and explore the optimal results. For instance, the game-theoretic algorithm implementations in [372]-[373] deliver optimal ways of selecting actions both of the attacker and defender. This equilibrium has a twofold notion:

- to protect the assets by adopting the proper proposed security measures that eliminate the damage;
- to identify the highest damage an adversary may cause to the business partner and indicate the defense strategy that deviates the attacker from this optimal solution providing the minimum business partner's loss.

To this end, to determine which mitigation strategies to adopt, the worst case scenario of damage within the ICT SCS shall be explored.

### **Step 6.2: Optimal Mitigation strategy selection and implementation**

Upon selecting mitigation strategies in step 6.1, the current step aims to guide the ICT stakeholder how to implement countermeasures and adopt the optimal mitigation strategy(-ies). The methodology provides the following indications to support the interested parties:

- Apply security controls after consulting the security requirements-controls taxonomy, presented in Section 7, which provides information on the security controls based on standardised approaches, such as the Common Criteria certification framework [58] and the security controls catalogue of NIST SP 800-53 [368].
- Re-assess the risk levels estimates against a set of security requirements (e.g., using security tools, code linting, dependency checking and pentesting techniques on ICT assets) to test the controls efficiency and effectiveness. Repeat the process until the specified requirements are met.
- Collect evidence of the cybersecurity risk assessment and security testing processes, additional documentation and material that justifies the security requirements satisfaction.
- Construct security reports of the outcomes.
- Request a self- or third party conformity assessment procedure to validate or attest, respectively, the security results.

### **6.2.3 CyberICT Risk Ontology**

Section 6.2.3.1 describes the foundational knowledge management framework used in the development of the CyberICT Risk Ontology. Section 6.2.3.2 presents the resulting ontology, while Section 6.2.3.3 outlines its validation. The work reported here builds upon the research presented in publication [84].

#### **6.2.3.1 Knowledge Formalisation Approach**

Chapter 3 discussed that Knowledge Management techniques can help organise and formalise knowledge when information becomes chaotic and difficult to capture and conceptualise, especially in cybersecurity topics where complexity can be rampant for complex ICT products and large-scale heterogeneous networks, such as the ICT supply chain networks. Chapter 4

discussed the value of Knowledge Management practices as an assisting structuring tool to create a cohesive, comprehensive and formalised body of cybersecurity knowledge.

Recognised knowledge management flows within the ICT ecosystem, analyses thoroughly the subject of evaluation (i.e., ICT products, associated ICT supply chain services) in a collaborative manner with the participation of all relevant ICT stakeholders. Depending on the type of analysis (holistic-technical or sectoral) the analysis can be either horizontal or vertical (see Section 3.2.3.2). Externalising cybersecurity information facilitates the analysis, promotes information sharing and expands the security knowledge (see Section 3.4.2.3).

The proposed CyberICT Risk Management Methodology is semantically represented into an ontology OWL 2 [130] based model of formal knowledge structures. The developed ontology serves a structural tool to externalise tacit security knowledge in the concepts included in the methodology, understand relations between threats, vulnerabilities, weaknesses and assets, create inferences and promote information sharing and organisational learning.

To model the intricate and often non-linear relationships between security ICT concepts, a hybrid methodology is adopted that bridges knowledge management theory with Semantic Web engineering. The Nonaka SECI model [114], described in Section 3.4.2.1, provides a historically validated, rigorous framework specifically optimised for capturing tacit security insights. In addition, it is used to identify, elicit, categorise, manage and obtain security concepts within the ICT SCS to construct a solid body of cybersecurity knowledge. The four tiers of the SECI model are utilised to the CyberICT Risk Management methodology to extract critical information and formalise it into the cybersecurity risk ontology using Semantic Web techniques, as described below. The SECI model [114] is applied as follows:

**Socialisation (Tacit to Tacit).** Mission-critical ICT SCS, such as the Maritime and Logistics Supply Chain (MLoSC) (see Section 3.3.2), are of a composite nature, engaging multiple ICT stakeholders and heterogeneous interconnected systems from downstream and upstream linkages with cooperating business domains and industries. Transferring security knowledge among individuals in a collaborative manner can help shareholders formulate best practice knowledge and better comprehend how cybersecurity events can be addressed in different supply-chain processes. **The creation of the cybersecurity risk ontology aims to serve the communication tool for transferring the ICT security knowledge.**

**Externalisation (Tacit to Explicit).** The digitalisation of modern supply chains increasingly attracts adversarial attention, amplifying the scale and complexity of cyberattacks. In this context, cybersecurity risks in composite ICT supply chain networks—comprising diverse, interdependent infrastructures with varying technical characteristics and security requirements—must be thoroughly identified, analysed, and understood. A critical prerequisite for this process is the acquisition of organisational knowledge, much of which resides tacitly in the minds of ICT supply chain stakeholders. Cybersecurity risk assessment is often bottlenecked by this unwritten expertise and heuristic judgment of human analysts. To address this challenge, systemic methods, mechanisms, and tools are employed to externalise and crystallise ICT stakeholders' tacit knowledge. In the current work, domain concepts were codified into an

explicit, standardised syntax using the Protégé platform [132], where relationships were represented as RD [129] triples (Subject-Predicate-Object) and strongly typed with OWL 2 [130] primitives. **This process establishes rigorous ontological classes, properties, and axioms for the cognitive transition into machine-readable context.** For instance, mapping how a specific weakness instantiates a vulnerability that compromises an asset transforms subjective intuition into structured, machine-interpretable knowledge.

**Combination (Explicit to Explicit).** ICT supply chain services are complex and interrelated, where failures such as cyberattacks on Critical Information Infrastructures (CII) can cascade across dependent assets, causing service disruptions and information leaks. Stakeholders need effective practices to elicit, collect, combine, and organise diverse cyber threat information. Once knowledge is formalised in RDF/OWL 2, **the Combination phase synthesises it into an inferential risk network** using the Pellet reasoner [135] for ontology consistency checking and inference of implicit risk relationships.

**Internalisation (Explicit to Tacit).** Once cybersecurity knowledge for ICT supply chains is formalised in the ontology, ICT stakeholders and business partners need to understand relationships between assets, vulnerabilities, threats and risks. To this end, SPARQL [131] is used to query the ontology and extract actionable, multi-layered cybersecurity intelligence. **This structured, machine-interpretable representation enables interested parties to transform explicit knowledge into practical understanding, supporting informed decision-making and effective risk management.**

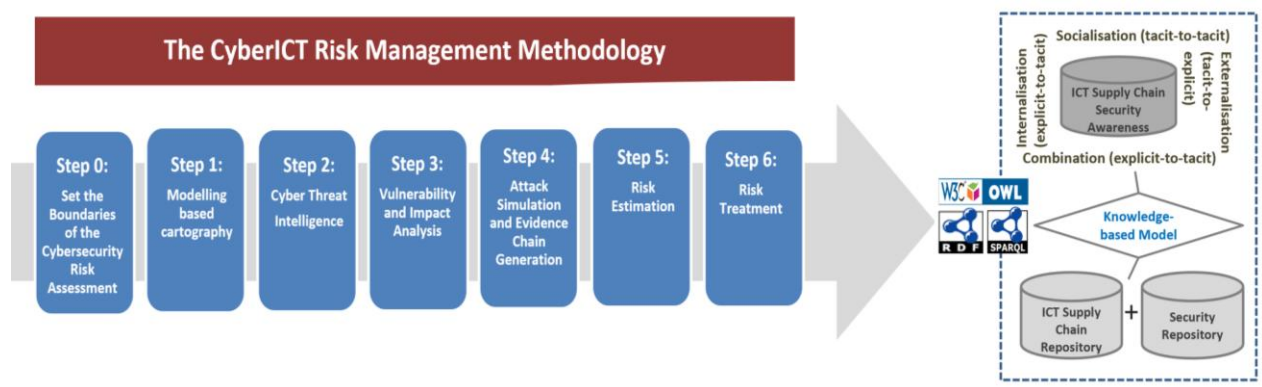


Figure 23: The CyberICT Risk Ontology.

#### 6.2.3.2 Cybersecurity Risk Ontology design

The CyberICT Risk ontology is generated according to the main concepts of the CyberICT Risk Management Methodology, i.e., the ICT SCS main elements, as identified in the ICT SCS analysis in Section 6.2.2.2 (Step 1) and corresponding security concepts of the methodology. The ontology structure is based on the work in [84], conducted as a part of this dissertation research.

The ontology is grounded in a real-life example, namely the Maritime and Logistics Supply Chain (MLoSC), which is analysed from business and security perspectives in Sections 3.3.2 and 4.5.3, respectively. This real-life example serves as the ICT supply chain environment through which

Section 6.4 demonstrates the applicability of the CyberICT Risk Management Methodology. The ontology integrates both process-centric and asset-centric views of the MLoSC. As discussed in Section 6.2.3.1, the ontology was developed using the Protégé platform [132] and employs the RDF standard [129], OWL 2 Description Logic (DL) [130], and the SPARQL [131] semantic query language.

The CyberICT Risk Ontology comprises the following main superclasses:

- **ICT SCS-related concepts:** Supply Chain Service (SCS), Process, Business Partner, Infrastructure, Network, Asset, and CyberDependency.
- **Security-related concepts:** Threat, Vulnerability, Risk, and SecurityControl.

These superclasses are further divided into subclasses where appropriate. For example, the superclass *Infrastructure* comprises six subclasses representing the critical infrastructures (CIs) of the Maritime and Logistics Supply Chain (MLoSC) used in the ICT processes analysed in the use cases of Section 6.4: Automatic Identification System (AIS), Electronic Data Interchange (EDI), Enterprise Resource Planning (ERP), Port Community System (PCS), Supervisory Control and Data Acquisition (SCADA), and Ship Information System (SIS).

Similarly, the superclass *Asset* comprises the subclass *AssetCartography*, which is further divided into *AssetCategory*, *AssetProduct*, and *AssetVendor*. The *AssetCategory* subclass is further specialised into *Application*, *Hardware*, and *OperatingSystem (OS)*.

Furthermore, the superclass *Vulnerability* is divided into the subclasses *Confirmed* and *ZeroDay\_Unknown*. Figure 24 depicts the main superclass hierarchy of the ontology structure.

The created ontology is a conceptualisation of both the BPMN models [93] and CyberICT Risk Management Methodology modules. It serves as an example of how MLoSC information is represented formally, according to the proposed methodology in which tacit knowledge is converted to explicit. Furthermore, the BPMN models have been semantically represented into the BPMN ontology, following the BPMN 2.0 normative in [92]-[93], developed as a part of this dissertation research. The ontology boosts the knowledge of the MLoSC in the following ways:

- *Recognising knowledge flows* among the MLoSC key-components. Semantic flows are identified among the classes of the ontology in order to expand the knowledge base information. For example, individual threats are mapped to cyber assets with the object property “effective threat” depending on the asset category and the vulnerabilities identified in the specific cyber assets, as shown in Figure 25. The image also depicts the asset characteristics for the Operating System of the Port Community System, which is represented with the class “PCSOS”. For example, neither asset classes nor cyber threat classes include information implying a relation between them, though assets are associated with specific security vulnerabilities, which are juxtaposed with corresponding cyber threats via the Common Weakness Enumeration (CWE) id listing characteristic.
- *Extracting new explicit knowledge using reasoning mechanisms and inference rules.* Reasoning automation mechanisms generate new explicit knowledge from the ontology. For example, the left window of Figure 26 shows on the “PCSOS” individual of class Assets

inverse semantic relations of other individual of this class. In addition, it shows the functions the PCS OS executes, derived from the BPMN ontology. Both are examples of useful new knowledge extracted from the ontology.

- *Extracting new explicit knowledge using ontological logical axioms that compose semantic assertions.* Figure 26 depicts the “CustomAsset” class, which is the complement of the class “IdentifiedAsset” (right window of Figure 26). This is another example of explicit-to-explicit conversion.
- *Extracting new explicit knowledge.* Using the SPARQL semantic query language [131], declared information can be retrieved from the ontology Figure 27. Additionally, using logic expressions, such as semantic relations of Figure 28, new knowledge can be created. Moreover, Figure 26 depicts the “CustomAsset” class, as the complement of the class “IdentifiedAsset” (Top-right window in Figure 26) (explicit-to-explicit conversion).
- *Storing, retrieving, and reusing articulated knowledge.* Using snapSPARQL query language, complex tacit information may be retrieved from the ontology, such as threats for assets of different organisations communicating to support a heterogeneous SCADA system (Figure 27-right window). Querying the ontology can help stakeholders internalise available knowledge (explicit-to-tacit conversion).
- *Extracting tacit knowledge using reasoning mechanisms and inference rules.* Reasoning automation mechanisms are able to extract tacit knowledge within the ontology. For example, the left window of xxx shows on the “PCSOS” individual of class “Assets” inverse semantic relations of other individual of this class. It also shows the functions the PCS OS executes, derived from the BPMN ontology approach. They are both data of tacit knowledge extracted from the execution of reasoning services using FACT++ reasoner.

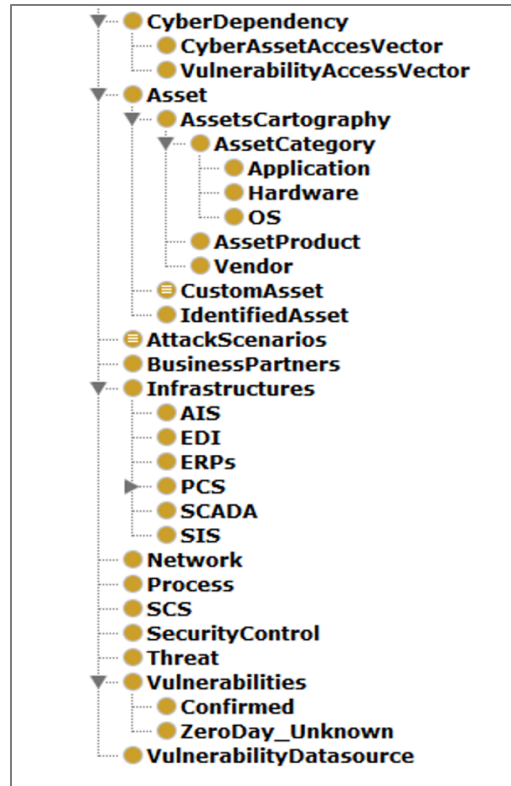


Figure 24. CyberICT Risk Ontology superclasses.

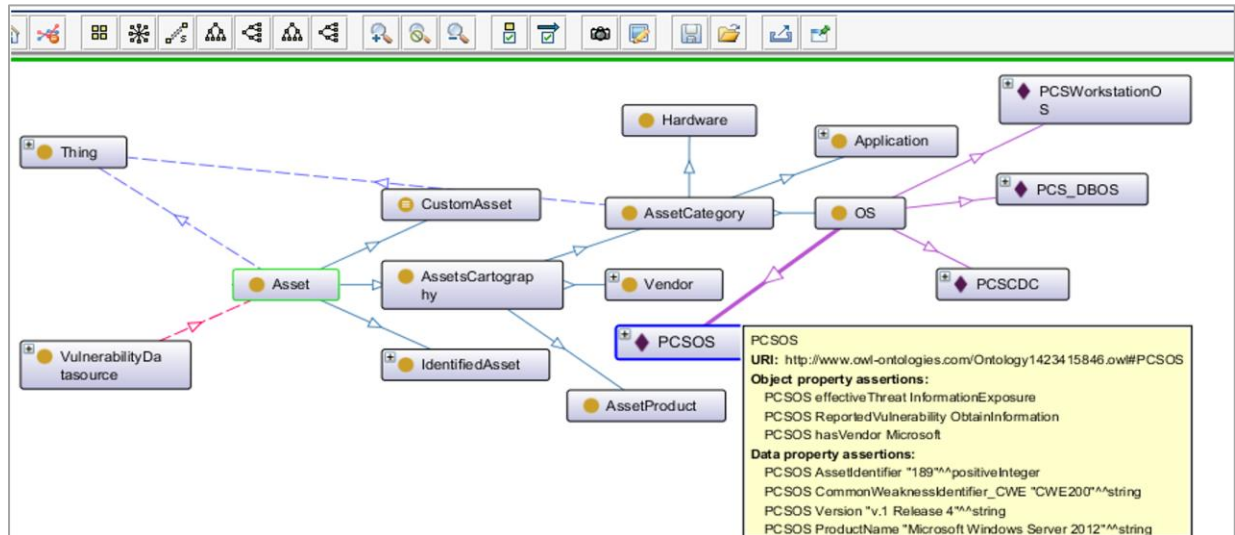


Figure 25. An example of identifying Knowledge Management flows to provide cyber asset characteristics.

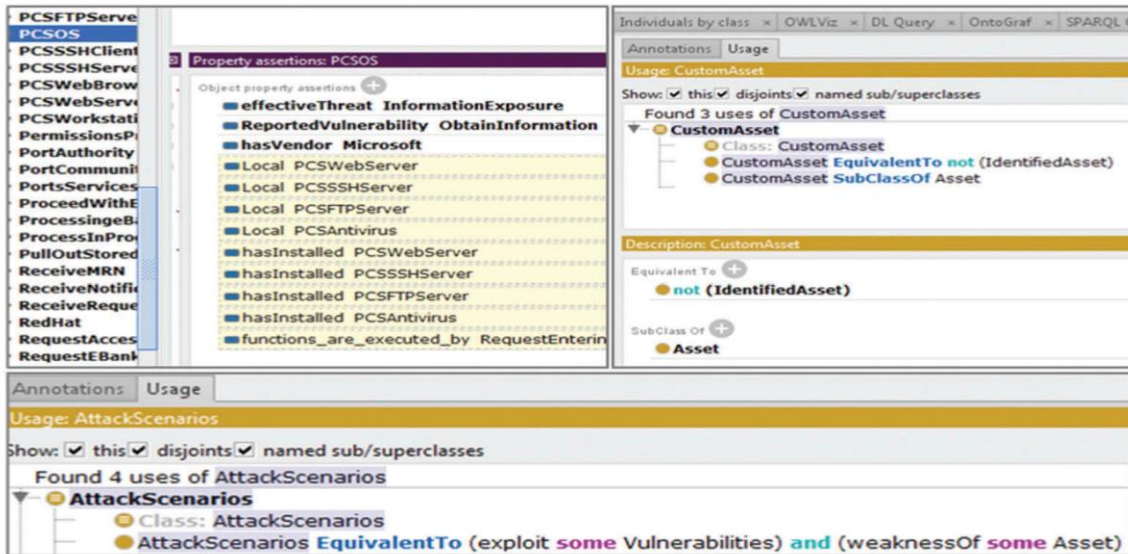


Figure 26. Examples of the semantic assertions usage: i) left window extracts tacit knowledge while reasoning, ii) right window uses semantic axioms.

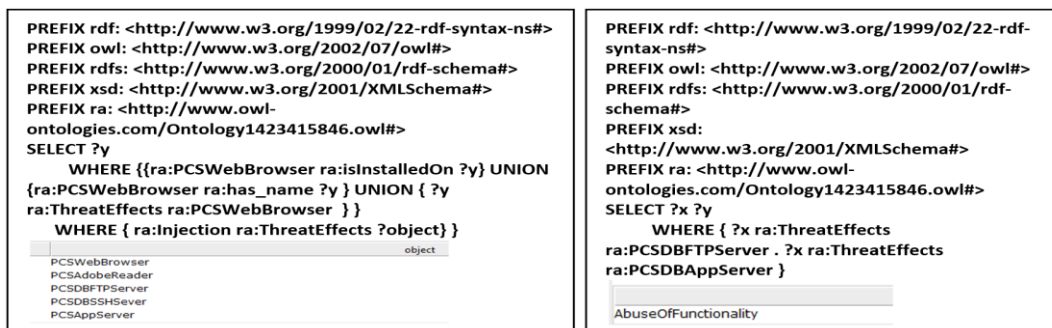


Figure 27. Outcomes from complex SPARQL queries: i) on the left window the results from extracting assets with specific characteristics, ii) on the right window security threat result for FTP Server and Application Server assets.





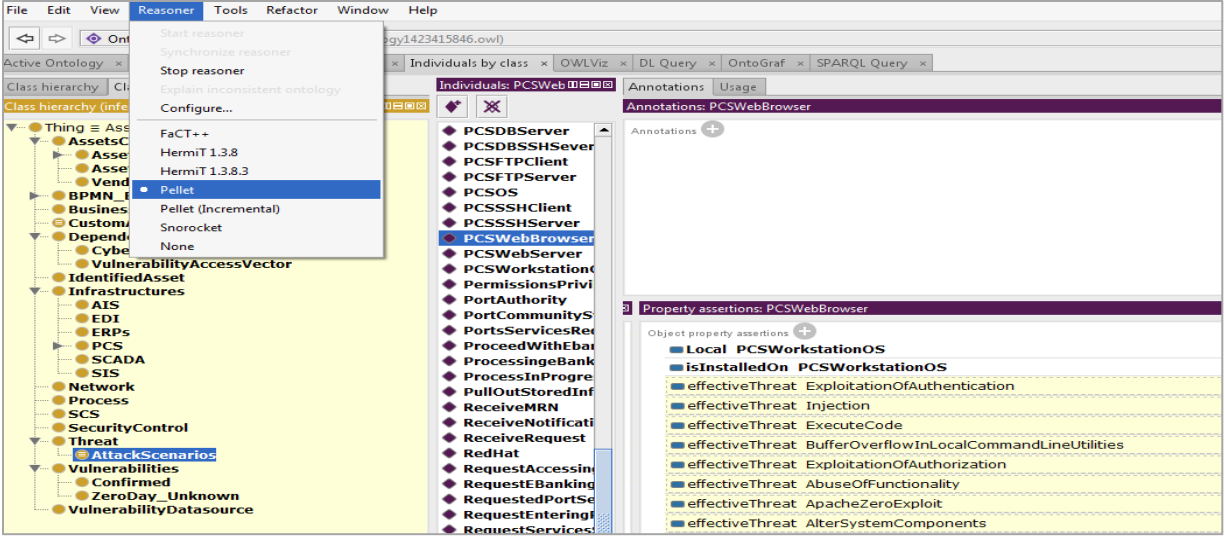


Figure 29. The reasoning for consistency checking of the CyberICT ontology. No logical errors were found. In the property assertions browser, the implicit information is highlighted.

## 6.2.4 Evaluation approach

As presented throughout the current doctoral thesis, this dissertation follows a Design Science Research (DSR) approach that developed a set of artefacts (see Chapters 1 and 5). The CyberICT Risk Management Methodology and the corresponding risk ontology are critical artefacts of this research. Their evaluation was conducted with a combination of approaches, explained in the following.

### 6.2.4.1 Evaluation of the CyberICT Risk Management Methodology

The CyberICT Risk Management methodology was evaluated from multiple perspectives described in the following.

#### Proof of concept demonstration

The proposed CyberICT Risk Management Methodology was demonstrated through real-world scenarios drawn from critical industry domains. Specifically, its applicability, utility, and effectiveness were evaluated through several use cases, each addressing either individual components of the methodology or its end-to-end application. The demonstration scenarios derive from three critical ICT supply chain services of the Maritime and Logistics Supply Chain (MLoSC): the Vehicle Transport Service, the LNG Transport Service, and the Container Management Service. The ICT supply chain service scenarios presented in Section 6.4 served as proof-of-concept demonstrations, providing evidence of the methodology's applicability in realistic operational environments. Furthermore, multiple research publications developed during this doctoral research present and evaluate different aspects of the proposed CyberICT Risk Management Methodology (see Chapter 8). Through rigorous cyberattack scenarios involving the three ICT supply chain services, the methodology was evaluated across its business, holistic-technical, and sector-specific dimensions, providing evidence of its applicability, utility, and effectiveness.

## **Practical adoption**

The proposed CyberICT Risk Management Methodology has been progressively adopted in the design of digital risk management platforms developed within the context of research projects (analysed in Section 6.3). The methodology informed the implementation of functionalities, such as supply chain process modelling and asset criticality, while its process-oriented risk assessment procedure provided both the conceptual and procedural framework for the design and evolution of the platforms' services and functionalities.

## **Questionnaire survey**

Questionnaire-based surveys involving ICT stakeholders from diverse industrial sectors were conducted within the context of research project activities. The participants evaluated digital risk management platforms whose design and functionalities were largely driven by the proposed CyberICT Risk Management Methodology.

In addition to assessing the technical capabilities of the risk management platform, the participants provided feedback on methodological aspects that informed their design. Specifically, the questionnaires included items related to the process-oriented supply chain modelling approach, the asset views, the supply chain journey supporting the risk assessment process, and the asset–vulnerability–threat interrelation model. By interacting with these services and functionalities, the participants indirectly evaluated key aspects of the proposed methodology and provided structured feedback (see Section 6.5.1). Furthermore, the surveys captured evidence regarding the methodology's applicability, perceived usefulness, usability, learnability, understandability, and overall user satisfaction within practical settings. To support the evaluation activities, hands-on training sessions were delivered to participants, accompanied by comprehensive documentation and user manuals describing the platform's functionalities. Although the surveys primarily evaluated the platform, their results provide indirect evidence of the proposed methodology's feasibility, usability, and practical utility.

## **CyberICT Risk Management Methodology analysis against domain-specific issues**

The proposed CyberICT Risk Management Methodology supports the assessment of threats, vulnerabilities, risks, and their cascading effects within ICT supply chain networks. To evaluate its applicability in realistic environments, the methodology was applied to representative cyberattack scenarios involving MLoSC domain-specific ICT infrastructures, including SCADA systems. In this context, the proposed methodology is systematically analysed against domain-specific issues, identified in Section 4.5.3.5. The analysis is presented in Section 6.5.2.

## **Analysis of CyberICT Risk Management Methodology calculation models**

Section 6.5.3 analyses the vulnerability exploitability and impact calculation models of the proposed CyberICT Risk Management Methodology. The analysis explains the rationale underpinning these models and discusses their design, assumptions, and contribution to the overall methodology, providing further evidence of their conceptual soundness and applicability.

#### 6.2.4.2 Evaluation of the CyberICT Risk Ontology

The proposed CyberICT Risk Ontology represents semantically the main concepts of the CyberICT Risk Management Methodology, i.e., the core elements of the ICT ecosystem and corresponding risk management concepts. The developed ontology was evaluated from diverse perspectives.

##### **Ontology verification and logical validation**

The CyberICT risk ontology was validated using semantic reasoning mechanisms, such as the Reasoner Pellet of W3C semantic web standards, applied in the semantic platform of Protégé . The successful outcome of the consistency checking on rational assertions, typology, and syntax was presented in Section 6.2.3.3 of this chapter.

The CyberICT Risk Ontology was verified through semantic reasoning mechanisms within the Protégé [132] ontology development environment. Reasoning services, including consistency checking, ontology classification, and logical inference, were used to validate the ontology. The detailed validation aspects are presented in sections 6.2.3.3, 6.5.2 and 8.1.

##### **Demonstration through case studies**

The CyberICT Risk Ontology was demonstrated through the semantic representation of realistic cyberattack scenarios involving actors, assets, and processes within the Maritime and Logistics Supply Chain (MLoSC). These proof-of-concept case studies, presented in Section 6.2.3.2 and in the related publications produced during this doctoral research (see Section 8.1), demonstrate the ontology's applicability in modelling ICT supply chain risk scenarios.

##### **Practical adoption**

As described in Section 6.2.3.2, the CyberICT Risk Ontology provided the conceptual foundation for the design and enhancement of research risk management platforms and their underlying data models. In particular, the semantic relationships among assets, threats, vulnerabilities, and Common Weakness Enumeration (CWE) identifiers informed the specification of asset–vulnerability–threat triplets used in the development of cyber-threat scenarios. This practical adoption provides additional evidence of the ontology's usefulness and applicability (for further details see Section 6.3.1.2).

### **6.3 Practical adoption in system**

Section 6.2 presented the development of the CyberICT Risk Management Methodology following a systematic and rigorous approach. As discussed in Chapter 5, this doctoral thesis adopts a Design Science Research (DSR) approach, in which the CyberICT Risk Management methodology constitutes one of the developed research artefacts. The methodology provided the foundational principles and processes that drove the design of risk management services and corresponding enhancements applied in research risk management platforms.

### 6.3.1 Design integration

Several parts of the proposed risk management methodology were adopted in the design of the services of the following research tool. The referred risk management tool is a dynamic, collaborative, standards-based tool applicable to ICT-based infrastructures for ICT product owners, supply chain operators, and other ICT stakeholders, including a wide variety of different sizes and types of entities, such as microenterprises (MEs), Small and Medium-sized Enterprises (SMEs), large enterprises, governmental agencies, and non-profit and research organisations. The tool is applicable to diverse industry sectors, such as Maritime Transport, Energy, Healthcare, Telecom and Automobile Industry. It provides asset technical characteristics based on the CPE MITRE structured naming scheme and package URL software identification. It obtains security-related information from open-source repositories (e.g., CVE MITRE, CAPEC MITRE, OSV, and GitHub Advisory) and promotes a rigorous, rational approach that gathers and critically appraises quality information gleaned from simulations or is available online. It supports supply chain risk management services by estimating vulnerabilities, threats, and risks to cyber assets and their cascading effects. In addition, the referred risk management tool supports risk management for complex ICT products and auditing capabilities based on prominent cybersecurity certification frameworks.

This research tool was evolved over time and incorporated aspects of the proposed methodology in the context of research EU projects. The following sections describe how the CyberICT Risk Management Methodology and the corresponding risk ontology contributed to the design of the evolved risk management platforms.

#### 6.3.1.1 CyberICT Risk Management Methodology contribution

In line with the principles of Design Science Research, the CyberICT Risk Management Methodology served as a conceptual framework to enhance existing services and guide the design of additional capabilities within the risk management tool. Its application provided instantiations of the methodology to demonstrate its utility and practical relevance in a real-world research context, specifically through EU Horizon projects. The application of the CyberICT Risk Management Methodology to the risk management tool was conducted solely for research purposes and does not imply commercial use.

Instantiations of the CyberICT Risk Management Methodology regarding cybersecurity risk assessment in ICT Supply Chain Services were provided in the following services of the risk management tool:

- Supply Chain Modeling service. Step 1 of the methodology, described in Section 6.2.2.2, guided the identification and analysis of the ICT Supply Chain Service. Furthermore the combined techniques of process-centric and asset-centric views (step 1), described in [84], which was developed and published in the context of the current dissertation research, were adopted [1]. The process-centric view defines the business processes and business partners' participation and collaboration in the provision of the supply chain service whereas the cyber-asset view identifies the cyber asset operation and their interrelation with processes within the supply chain service (Figure 31-Figure 33). In this regard, the

criticality service was added to assess the importance of supply chain services, processes and assets through a set of criticality rules (see step 1 and [15]).

- Threat Scenario Specification service. The idea of synchronising the CPE MITRE and CAPEC MITRE identifiers and associating the identified vulnerabilities with one or more weakness identifiers to declare statically the mapping of threats and vulnerabilities with assets was adopted. Specifically, the idea is conceptualised in the CyberICT Risk Ontology with semantic representations and adopted as explained in Section 6.3.1.2.
- Vulnerability/Threat/Risk Management services. These services were initially developed based on the research in [371]–[372]. The CyberICT Risk Management Methodology enhances these services using the process-centric approach (step 1) [1] which identifies dependencies and knowledge management flows between supply chain services, business partners, processes, assets, vulnerabilities, threats, and risks (Figure 34-Figure 39).
- Attack Path simulation service. The current service in the risk management platform was initially developed based on the vulnerability discovery and game theoretic methods presented in [276],[370]–[373]. The service was enhanced with the evidence chain generation approach, described in [9], developed during the current dissertation research, which was used to build the Attack Simulation and Evidence Chain Generation (ASECG) model, presented in Section 6.2.2.5 (step 4). Specifically, the Attack Paths Simulation service was enhanced by calculating all possible attack paths that an adversary could follow in relation to specific confirmed event(s)<sup>18</sup>. Based on the approach described in [9], the attack graph discovery was reconstructed to deliver results that match the predefined scenario and produce only the possible courses an attacker would follow, which are associated with the specific confirmed event(s) (Figure 40-Figure 41).

The enhancements and additions of the services described above were made, as previously stated, solely for research purposes and activities within EU research projects. Specifically, all the above contributions to the implementation of the services were provided during the MITIGATE EU [382] project research activities, apart from the updates in the attack simulation service, which were applied to the evolved risk management platform in the context of the CyberSane EU H2020 project [383] research activities.

#### 6.3.1.2 CyberICT Risk Ontology contribution

The CyberICT Risk Ontology informed the design of data structures and semantic relationships implemented within a risk management tool (see Section 6.3.1.1). In particular, the knowledge management flows identified in Section 6.2.3 guided the hierarchical organisation of the process-based assessment structure. Furthermore, the object properties and data properties defined in the

---

<sup>18</sup> The confirmed security event is identified from the log file analysis delivered from the tool's other modules.

CyberICT ontology informed the specification of classes, entities, and their interrelationships within the tool's data model.

More specifically, the ontology provided a conceptual basis for modelling the relationships between ICT supply chain services, business partners, business processes, and assets. In addition, the CyberICT ontology supports the semantic representation of asset–threat–vulnerability interrelations, leveraging the MITRE Common Platform Enumeration (CPE) naming scheme with the Common Weakness Enumeration (CWE) classification to establish consistent and structured knowledge associations.

In summary, the CyberICT Risk Management Methodology provided the conceptual and procedural framework for service design, while the CyberICT Risk Ontology informed the underlying data structures and semantic relationships, together enabling a rigorous and structured implementation of cybersecurity risk assessment functionalities of the risk management tool.

### 6.3.2 Visualisation of services in the risk management platforms

This section visualises the services of the risk management platforms, which integrate the updates described in Section 6.3.1.

The screenshot displays the MITIGATE web application interface. The top navigation bar is blue with the MITIGATE logo on the left and links for Dashboard, Documentation, and Logout (portauthority) on the right. A left sidebar menu lists various application sections: Dashboard, Risk Assessments, Supply chain services (highlighted), Pending actions, Business Partners, Assets, Sites, Networks, Vendors, Vulnerabilities, Threats, Threat Profiles, and Controls. The main content area shows the breadcrumb path / SUPPLYCHAINSERVICE and the title SupplyChainServices. Below the title is a 'Create New' button. The form for creating a new service includes a text input field labeled 'SupplyChainService Name' and a 'Save' button.

Figure 30. Creation of Supply Chain Service.

MITIGATE

v 1.2.3 Dashboard Documentation Logout (MitigatePortAuthority)

Dashboard

Supply chain services

Risk Assessments

Assets

Sites

Networks

Vendors

Products

Vulnerabilities

Threats

Attack Scenarios

Controls

SUPPLYCHAINSERVICE

SupplyChainService Management

SEARCH BY:

ID

ID

Name

Name

Initiator

Port Authority

Search

| ID | Name                                 | Initiator      |                                          |
|----|--------------------------------------|----------------|------------------------------------------|
| 20 | Bulk/General Cargo Transport Service | Port Authority | Edit SCS<br>List Processes<br>Delete SCS |
| 11 | Container Cargo Management Service   | Port Authority | Edit SCS<br>List Processes<br>Delete SCS |
| 12 | LNG Transport Service                | Port Authority | Edit SCS<br>List Processes<br>Delete SCS |

Figure 31. List of created Supply Chain Services.

MITIGATE

Dashboard Documentation Logout (portauthority)

Dashboard

Risk Assessments

Supply chain services

Pending actions

Business Partners

Assets

Sites

Networks

Vendors

Vulnerabilities

Threats

Threat Profiles

Controls

SUPPLYCHAINSERVICE / VEHICLES TRANSPORT SERVICE

Edit Process

SupplyChainService: Vehicles Transport Service

Process name

process name

Save

Figure 32. Create an ICT process in an ICT Supply Chain Service (ICT SCS).



MITIGATE

Dashboard
Documentation
Logout (portauthority)

MENU

Dashboard
Risk Assessments
Supply chain services
Pending actions
Business Partners
**Assets**
Sites
Networks
Vendors
Vulnerabilities
Threats
Threat Profiles
Controls

/ ASSETS

Assets

Asset Management

+ CREATE NEW
VISUALIZE

| ID  | Name               | Type        | Product                                      |  |
|-----|--------------------|-------------|----------------------------------------------|--|
| 62  | AdminOS            | OS          | cpe:/o:microsoft:windows_10:-::~~x64~        |  |
| 82  | BREPOS 3 OS        | OS          | cpe:/o:microsoft:windows_2003_server:-       |  |
| 81  | BREPOS 3 Server    | Hardware    | cpe:/h:lenovo:thinkserver_ts440:-            |  |
| 63  | Corporate Web Site | Application | cpe:/a:drupal:drupal:6.24                    |  |
| 74  | DomainController   | Application | cpe:/a:microsoft:active_directory:-          |  |
| 67  | IoTdevice1         | OS          | cpe:/o:microsoft:windows_10:-::~~x86~        |  |
| 71  | MyCustomApp        | Application | cpe:/a:wordpress:wordpress:3.1.4             |  |
| 70  | MyCustomOS         | OS          | cpe:/o:microsoft:windows_2008:r2:sp2::~~x64~ |  |
| 69  | MySampleHardware   | Hardware    | cpe:/h:dell:poweredge_2950                   |  |
| 103 | myTestApp          | Application | cpe:/a:skype_technologies:skype:3.6.0.216    |  |

1
2
3
4

Figure 33. ICT asset technical details.

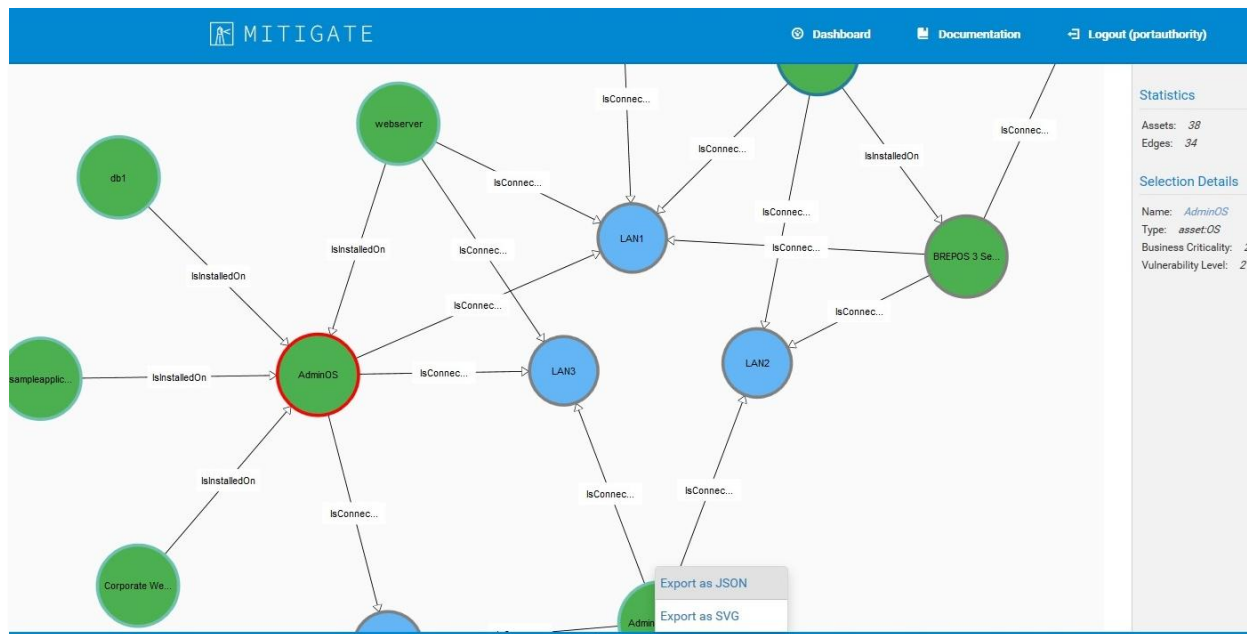


Figure 34. Visualisation of asset dependency graphs.

MITIGATE

Dashboard
Documentation
Logout (portauthority)

Dashboard

Supply chain services

Pending actions

Business Partners

Risk Assessments

Assets

Sites

Networks

Vendors

Vulnerabilities

Threats

Threat Profiles

Attack Scenarios

/ RISKASSESSMENT / RISKASSESSMENT2

← Risk Assessment - Controls Customization

Risk Assessment: riskassessment2  
Process: C.1 Portá??s Services Requested  
SupplyChainService: Vehicles Transport Service  
Initiator: Port Authority  
Asset: AdminOS [cpe:/o:microsoft:windows\_10:::~~~x64~]

CONFIRMED VULNERABILITIES

+/- THREAT

+/- CONTROL

| ID            | CVSS | Exploitability | Impact | Description                                           |
|---------------|------|----------------|--------|-------------------------------------------------------|
| CVE-2015-1769 | 7.20 | 3.90           | 10.00  | Mount Manager in Microsoft Windows Vista SP2, Wind... |
| CVE-2015-2423 | 4.30 | 8.60           | 3.00   | Microsoft Windows Vista SP2, Windows Server 2008 S... |
| CVE-2015-2433 | 2.10 | 3.90           | 3.00   | The kernel in Microsoft Windows Vista SP2, Windows... |
| CVE-2015-2435 | 9.30 | 8.60           | 10.00  | Microsoft Windows Vista SP2, Windows Server 2008 S... |

Figure 35. Identification of confirmed vulnerabilities in the ICT assets of an ICT process of an ICT SCS.

MITIGATE

v 1.2.3

Dashboard
Documentation
Logout (MitigatePortAuthority)

Dashboard

Supply chain services

Pending actions

Risk Assessments

Assets

Sites

Networks

Vendors

Products

Vulnerabilities

Threats

Attack Scenarios

Controls

Open Intelligence News

Open Intelligence Search

Open Intelligence Sources

Jobs

/ SCENARIOS

Scenarios

Scenario management

+ CREATE NEW

SEARCH BY:

Name

Search

| Name                                                        | Threat  | Vulnerability | Asset/CPE                                                |
|-------------------------------------------------------------|---------|---------------|----------------------------------------------------------|
| Exploitation of CVE-2015-0733 using common weakness CWE-113 | CWE-113 | CVE-2015-0733 | cpe:/o:cisco:headend_digital_broadband_delivery_system:- |
| Exploitation of CVE-2016-4993 using common weakness CWE-113 | CWE-113 | CVE-2016-4993 | cpe:/o:redhat:enterprise_linux:7.0                       |
| Exploitation of CVE-2016-4993 using common weakness CWE-113 | CWE-113 | CVE-2016-4993 | cpe:/a:redhat:boss_wildfly_application_server:10.0.0     |
| Exploitation of CVE-2016-4993 using common weakness CWE-113 | CWE-113 | CVE-2016-4993 | cpe:/o:redhat:enterprise_linux:6.0                       |
| Exploitation of CVE-2016-4993 using common weakness CWE-113 | CWE-113 | CVE-2016-4993 | cpe:/a:redhat:boss_enterprise_application_platform:7.0.1 |
| Exploitation of CVE-2016-5325 using common weakness CWE-113 | CWE-113 | CVE-2016-5325 | cpe:/a:nodejs:node.js:0.10.0                             |
| Exploitation of CVE-2016-5325 using common weakness CWE-113 | CWE-113 | CVE-2016-5325 | cpe:/a:nodejs:node.js:0.10.1                             |

Figure 36. Interrelations between assets, vulnerabilities and threats in an threat scenario.

Dashboard
Documentation
Logout (portauthority)

Dashboard
Supply chain services
Pending actions
Business Partners
Risk Assessments
Assets
Sites
Networks
Vendors
Vulnerabilities
Threats
Threat Profiles
Attack Scenarios

## Scenarios

Scenario management

CREATE NEW

| Name              | Threat                        | Vulnerability | Asset            |
|-------------------|-------------------------------|---------------|------------------|
| Attack1           | Abuse of Functionality        | CVE-2015-6933 | Hypervisor1      |
| Attack2           | Abuse of Functionality        | CVE-2016-5330 | Hypervisor1      |
| Attack4           | Manipulate Data Structures    | CVE-2014-8370 | OS1              |
| DoSAttack1        | Abuse of Functionality        | CVE-2009-1426 | HPServer         |
| injectionscenario | Injection                     | CVE-2014-3704 | CorporateWebSite |
| scenario1234      | newtypeofattack               | CVE-2016-7860 | AdminOS          |
| sshattack         | Exploitation of Authorization | CVE-2005-2771 | PPA SSH Server   |

1

Figure 37. Threat scenario management.

Dashboard
Documentation
Logout (portauthority)

MENU

Dashboard
Risk Assessments
Supply chain services
Pending actions
Business Partners
Assets
Sites
Networks
Vendors
Vulnerabilities
Threats
Threat Profiles

/ RISKASSESSMENT / SCADA RISK ASSESSMENT

← Risk Assessment - Threat Customization

Risk Assessment: SCADA Risk Assessment
Process: D.1 Vehicles Unloading
SupplyChainService: Vehicles Transport Service
Initiator: Port Authority
Asset: Microsoft Windows Server R2 (MTU) [cpe:/o:microsoft:windows\_server\_2012:r2]

CONFIRMED VULNERABILITIES

THREAT

CONTROL

Effective Threats

| Identifier | Name                                            | Threat Level (freq. of occurrence) |
|------------|-------------------------------------------------|------------------------------------|
| 210        | Abuse of Functionality                          | Very High                          |
| 9          | Buffer Overflow in Local Command-Line Utilities | Very High                          |
| 76         | Manipulating Web Input to File System Calls     | Very High                          |
| 474        | Signature Spoofing by Key Theft                 | Very High                          |
| 79         | Using Slashes in Alternate Encoding             | Very High                          |

Figure 38. Threat level estimation.

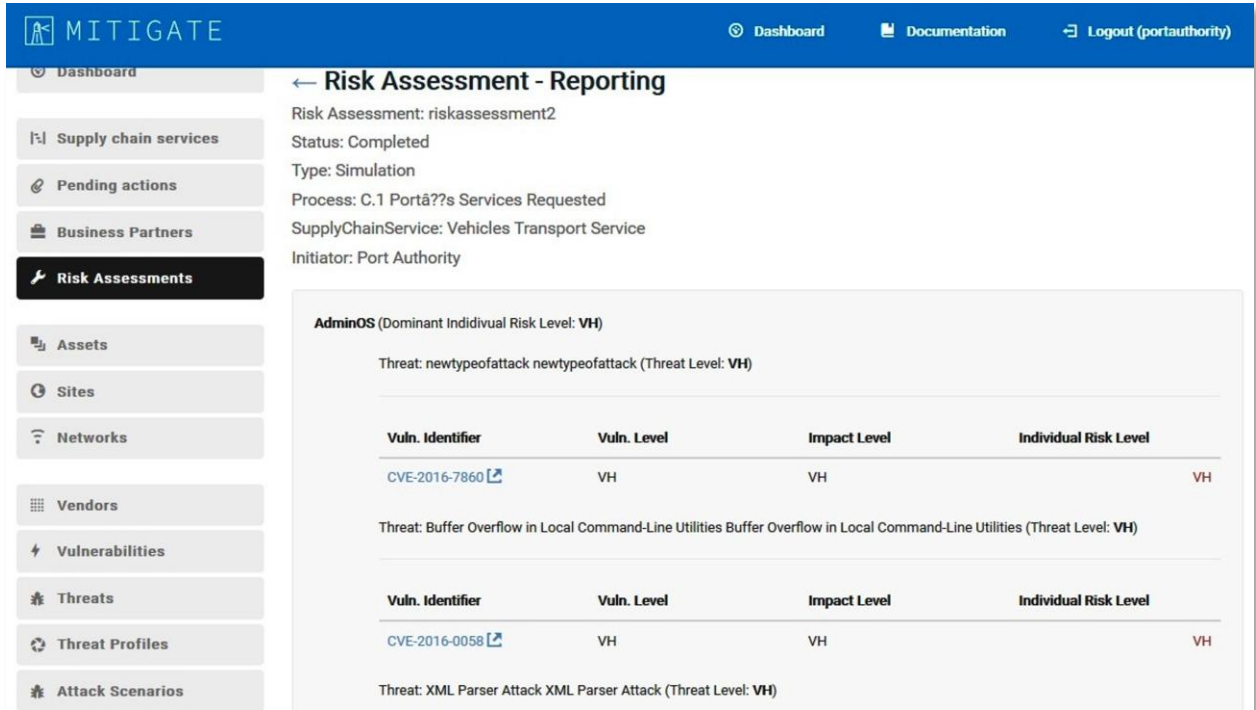


Figure 39. Risk Assessment results in an ICT process.

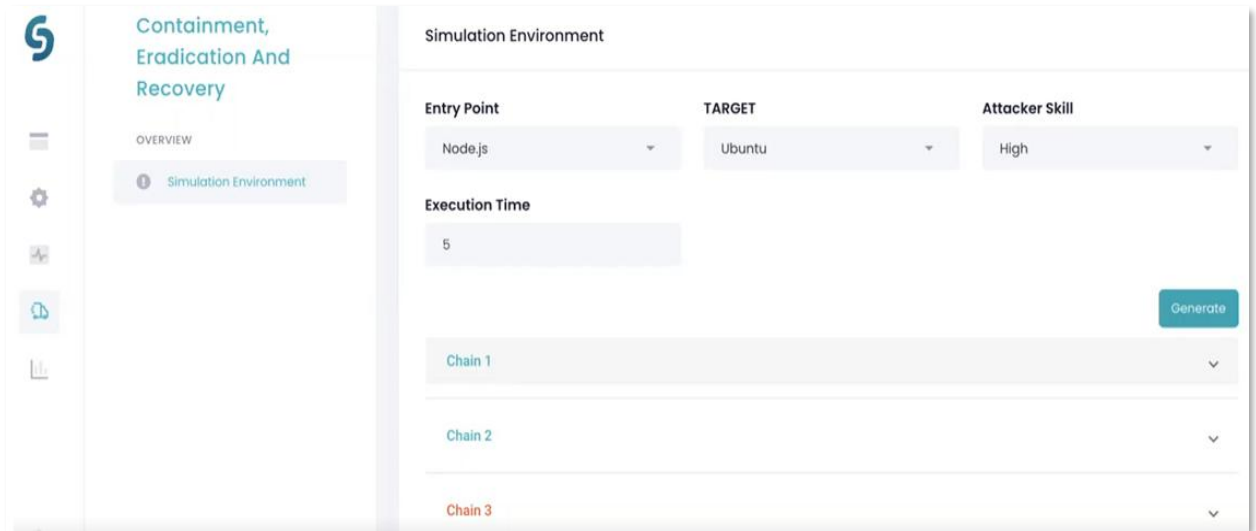


Figure 40. Credible vulnerability chains.

Figure 40 illustrates the attack path environments and attributes and the extracted vulnerability chains. The attack path results are provided upon creating an attack path query. The green-coloured chains are successful attack paths that might have occurred in the organisation's assets, according to the detected evidence (credible evidence chains). Attack path visualisations are depicted in Figure 41.

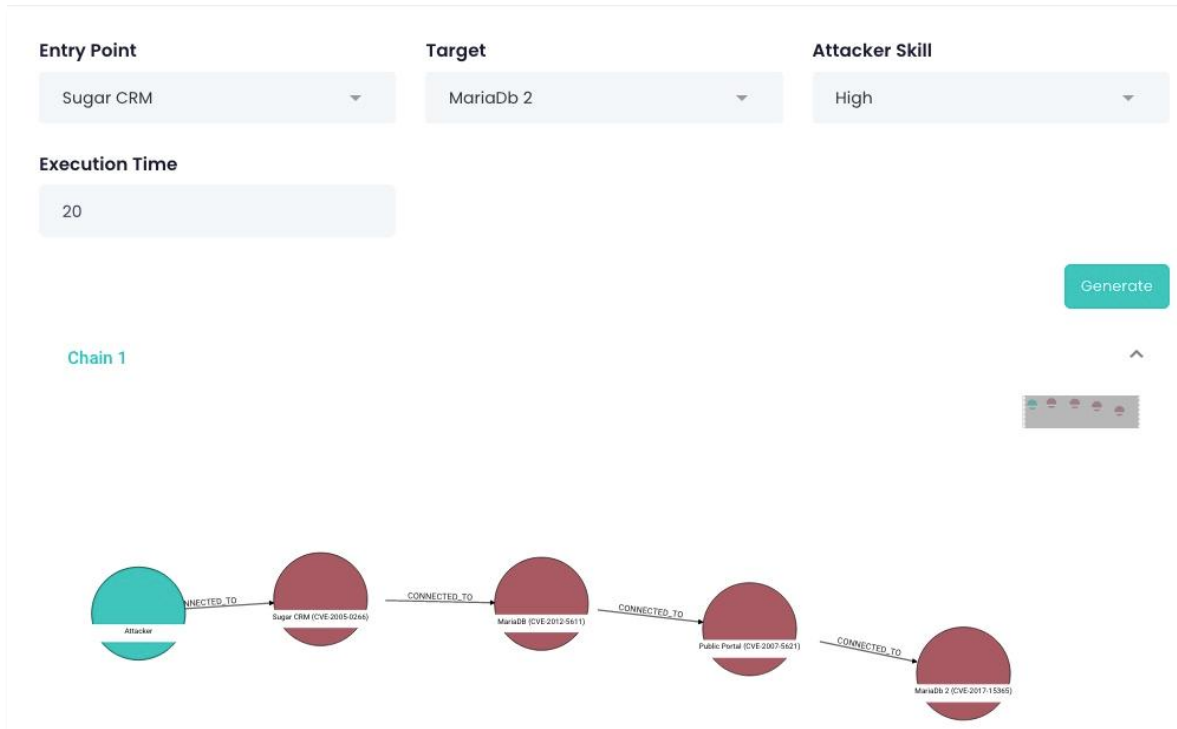


Figure 41. Credible vulnerability Attack graphs illustrate the potential attack paths between interdependent asset nodes upon specific query.

## 6.4 Demonstration and Applicability

This section presents the CyberICT Risk Management methodology and the corresponding CyberICT Risk Ontology applicability through real-life scenarios. The scenarios presented in this section refer to the risk assessment processes of ICT Supply Chain Services (ICT SCS). They were intentionally selected to reflect the applicability of the methodology by assessing an ICT SCS, as it is a more complex case than the risk assessment of a single ICT product. Nevertheless, a real-life scenario of a single ICT product, where the methodology is used to assess its risks, is presented in Chapter 7, to illustrate the applicability of the proposed CyberICT Protection Profile.

As presented in Chapter 3, the ICT SCS scenarios described in this section are related to the Maritime and Logistics Supply Chain (MLoSC). Specifically, three (3) ICT SCS services are used to demonstrate the applicability of the CyberICT Risk Management methodology through three (3) diverse real-life scenarios:

- The Vehicle Transport Service
- The Liquefied Natural Gas (LNG) Transport Service
- The Container Cargo Management Service

All of the above services fall in general to the MLoSC ecosystem (MLoSC stakeholders, infrastructure, systems, processes, and environments) because the services mainly reside in the

Maritime Transport. Nonetheless, the three (3) services engage the application of combined industries for their performance. For instance, the Vehicle Transport Service involves stakeholders and systems of the Automobile Industry sector, whereas the LNG Transport Service engages infrastructures from the Energy Industry Sector.

The selected services have been identified as critical to the Maritime Logistics Industry due to security and economic reasons (see NIS 2 Directive [12]). The criteria for selecting these Critical Services satisfy the following prerequisites:

- European level nature: implemented in large European commercial ports;
- Economic enablers: address the high economic impact across the EU Maritime Logistics; Industry and the entire European economy;
- Environmental value: meet EU environmental requirements and standards.

The selected MLoSC services can be subject to a number of possible threat scenarios that can be realised by conducting a combination/series of specific cyberattacks in various SCADA cyberphysical systems operating within the MLoSC. Hence, malicious users/adversaries can realise complex threat scenarios to disrupt MLoSCs' operations or facilitate illegal activities aimed at obtaining financial, political/military, or even ideological gain and benefits. For example, adversaries may manage to smuggle illegal material of any kind (e.g., drugs, weapons) or illegal immigrants or destroy a Critical Information Infrastructure (CII) of the MLoSC by interrupting and modifying its services, gaining access to it either locally or remotely to take advantage of the system's security-sensitive operations. Three credible cyberattack scenarios against the aforementioned critical MLoSC services are described sequentially in the following sections.

In the following real-life ICT SCS scenarios:

- the Vehicle Transport Service is used to demonstrate the business evaluation aspect (identifying processes, assets and related threat scenarios)
- the LNG Transport Service is utilised to demonstrate the holistic-technical evaluation aspect (end-to-end risk assessment)
- the Container Cargo Management Service supports the scenario to demonstrate the sector-specific evaluation (rigorous analysis of a specific business partner of the supply chain (sectoral perspective) and the application of the Attack Simulation and Evidence Chain Generation Model (ASECG).

Additional short scenario of the SCADA infrastructure architecture is presented in Section 6.4.1 to illustrate the ICT SCS analysis, including the process and asset modelling applicability of the CyberICT Risk Management methodology using the BPMN models of Step 1 of the methodology.

#### **6.4.1 The Vehicle Transport Service**

This ICT SCS aims to present the business evaluation aspect of the CyberICT Risk Management Methodology. It focuses on a rigor analysis of the first three steps of the methodology and creates business process and ontology models of the ICT elements and the identified threats.

## **Step 0. VT - Set the Risk Assessment Boundaries**

It is a mission-critical service of the maritime sector. The maritime logistics procedures regarding the Vehicle Transport Service can be divided into three main categories: shipping activities, port/terminal operations, and vehicles forwarding (see Section 3.3.2). Since the Ship Formalities Arrangement process has been presented as an example in Section 6.2 to facilitate the understanding, in the current case the following two critical maritime processes of the VehicleTransport Service are analysed:

- Port's Services Requested
- Vehicle Unloading

They will represent the key processes of the current ICT SCS. The ICT assets required for these three ICT processes of the Vehicle Transport Service and the involved business partners will be analysed. Moreover, ICT process analysis, vulnerabilities referred to these cyber assets and some threat identification will be provided. The expected outcome is the identification of threats to the ICT assets, processes and ICT infrastructures of the Vehicle Transport Service. The business partners involved in the ICT SCS sign an SDA (see Appendix C) to mutually agree on the conditions of the risk assessment and the security controls they promise to collaboratively implement after the risk assessment completion.

## **Step 1 VT – Modelling based cartography.**

The following steps apply to the modelling of the Vehicle Transport Service.

### **Step 1.1 Define Vehicle Transport Service criticality.**

The Vehicle Transport Service is a complex service, including domestic and international transportation, warehouse management, order and inventory control, materials handling, import/export facilitation, and information technology. It is operated by numerous players, including the automobile industry, shippers, transport agents, authorities, the importer, etc. The main objective of the Vehicle Transport Service is to deliver the vehicles from the initial port to the destination port and complete all the required shipping and logistics preparations. The participants of the current service are all EU members. Thus, according to Section 6.2.2.1, Table 14, which specifies the ICT SCS criticality, the Vehicle Transport Service is considered of medium criticality.

### **Step 1.2 ICT stakeholder and business partners identification**

The main entities participating in the Vehicle Transport Service are mentioned in the example in Section 6.2.2.2. Nevertheless, a brief description of the key entities participating in the selected ICT processes (see VT Step 0) is provided:

- Port authority (bp<sub>0</sub>) is a local authority which manages the areas where port operations take place. Furthermore, port authorities handle physical operations like stevedoring, storage, inspection, and data flow operations, such as forwarding, invoicing, and International Ship and Port Facility Security (ISPS) declaration.



- Customs (bp<sub>1</sub>) is a local authority responsible for overseeing the implementation of the customs clearance procedures for the clearance of the vehicles from customs control of an importer's consignment
- Ship agent (bp<sub>2</sub>) is responsible for the transports of the vehicles by the sea, via ships. Usually, the ship agent does not own ships and acts as a charterer to deal with vessel bookings.
- Local agent (bp<sub>3</sub>) is a business and/or individual intermediate who has the primary responsibility to fulfil shipping and logistics documentation required for the vehicles' transportation.
- Carrier agent (bp<sub>4</sub>) is a business and/or individual intermediate who aims to accomplish the arrangement for the vehicles' transportation and storage.

In the current assessment, the Port Authority initiates the procedure.

Table 41. Vehicle Transport Service processes.

| Vehicle Transport Service (VT) |                                                                                                                                                                            |                                                                                                                                                                 |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ICT process                    | ICT process description                                                                                                                                                    | Business partners involved in the identified processes                                                                                                          |
| Port's Services Requested      | The process aims to realise services for the vessel's arrival or departure via a Master Reference Number (MRN) verification.                                               | <b>ICT stakeholder:</b><br>Port authority (bp <sub>1</sub> )<br><b>Business Partners:</b><br>Ship Agent (bp <sub>2</sub> )                                      |
| Vehicles Unloading             | Deals with all the required logistics, stevedoring, transport, and forwarding procedures to unload the vehicles from the vessel and store them to the port's car terminal. | <b>ICT stakeholder:</b><br>Port authority (bp <sub>0</sub> )<br><b>Business Partners:</b><br>Local Agent (bp <sub>3</sub> )<br>Carrier Agent (bp <sub>4</sub> ) |

The two ICT processes are further analysed into its main elements and represented via business process models using the BPMN 2.2.0 Business Process Modelling Notation (ISO 19510:2013 [114]). The analysis of the two (2) Vehicle Transport Service processes (Figure 42 and Figure 43) is mostly focused on the bilateral interactions between the Port Authority and the Local Agent in the current case. Moreover, the primary actors involved in these processes are presented in Table 42



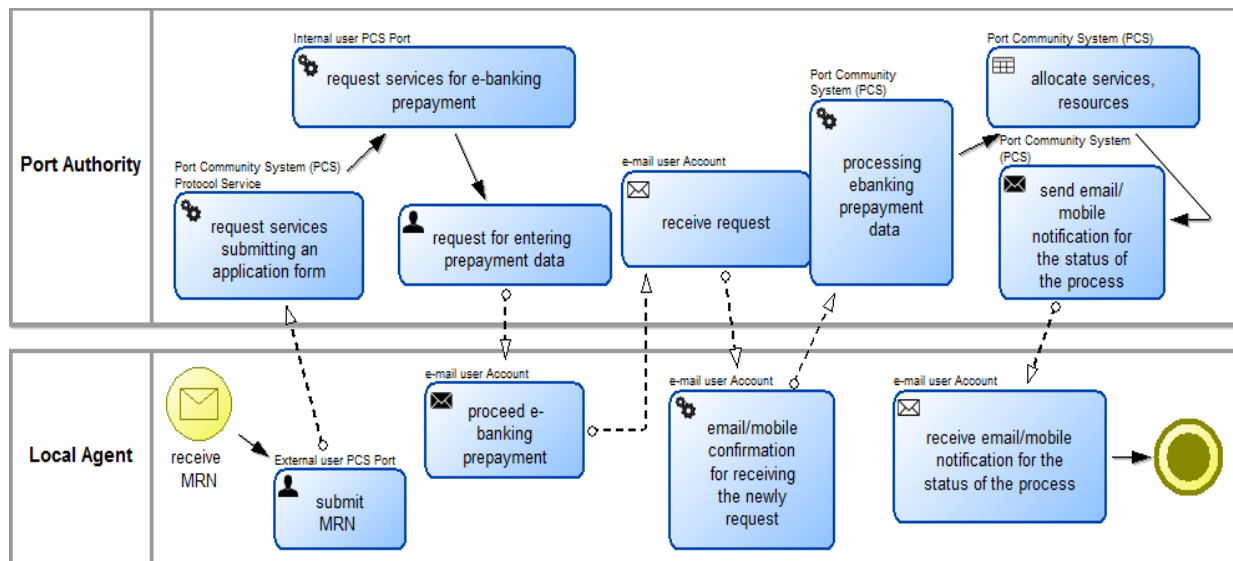


Figure 42. Port's Services Requested.

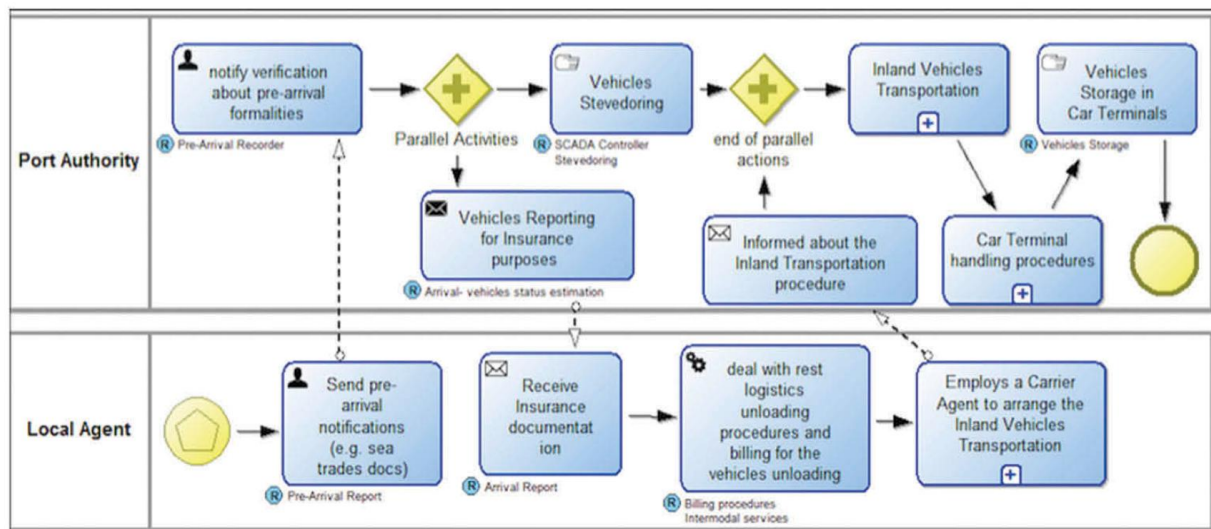


Figure 43. Vehicles Unloading process.

Table 42. Analysis of Vehicle Transport Service infrastructure in ICT processes.

| Vehicle Trasport Service (VT)                                   |                                                                    |
|-----------------------------------------------------------------|--------------------------------------------------------------------|
| Port's Services Requested                                       |                                                                    |
| Vehicles Unloading                                              |                                                                    |
| ICT stakeholder and Business partners involved in the processes | ICT infrastructure                                                 |
| Port Authority (bp <sub>0</sub> )                               | Port Community System (PCS), Automatic Identification System (AIS) |
| Customs (bp <sub>1</sub> )                                      | Customs' Network                                                   |

|                                  |                                                        |
|----------------------------------|--------------------------------------------------------|
| Ship Agent (bp <sub>2</sub> )    | Individual Electronic devices                          |
| Local Agent (bp <sub>3</sub> )   | Vessel's infrastructure, Ship Information System (SIS) |
| Carrier Agent (bp <sub>4</sub> ) | Individual Electronic devices                          |

Figure 44 depicts a detailed representation of the Port Community System (PCS), the most important system of the Port Authority and the interactions between the Customs Integrated Network.

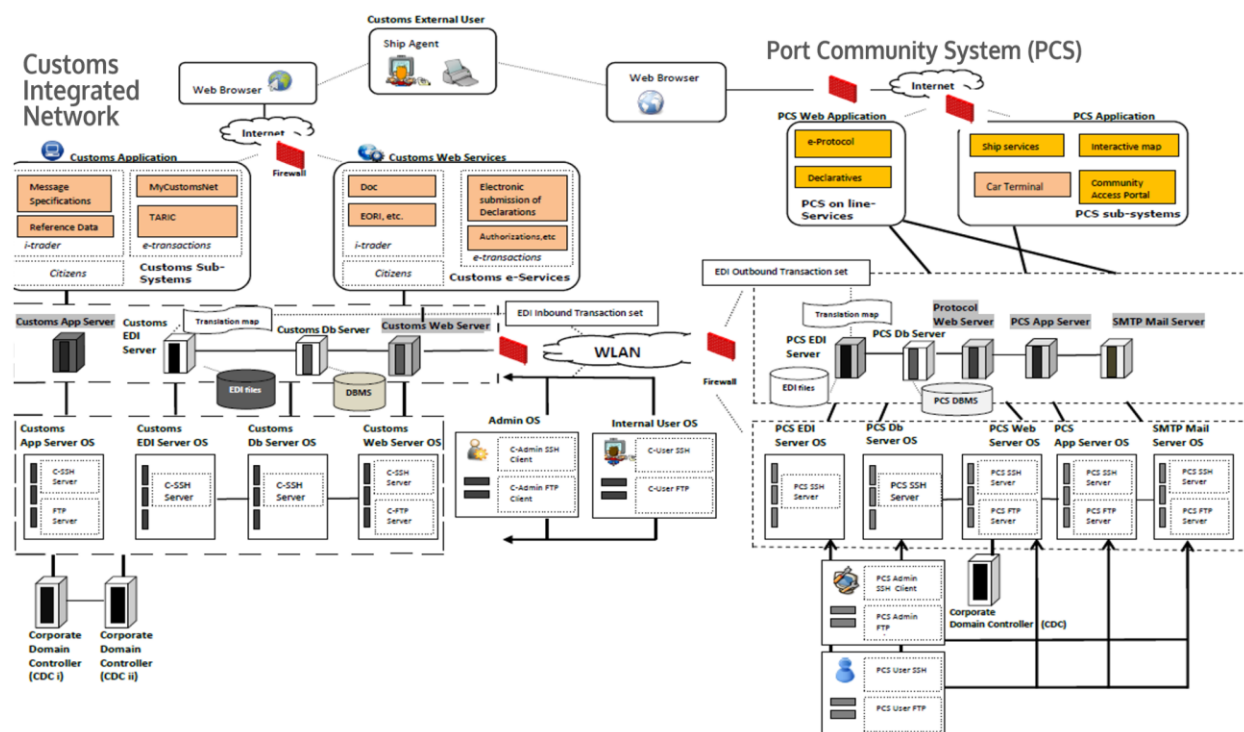


Figure 44. Interdependencies between Port's Community System and Custom's infrastructure.

An indicative analysis of interdependencies between assets of the Port Community System (PCS) is presented in Table 43. In addition, Table 44 presents a realistic threat scenario where an adversary can sequentially exploit the vulnerabilities starting from the PCS Database (Entry Point) and compromise the PCS Operating System (Target Point).

Table 43. Asset dependencies in the Port Community System.

| Asset Source        | Asset Destination    | Dependency type | Dependency access vector |
|---------------------|----------------------|-----------------|--------------------------|
| PCS Web Application | PCS Web Server       | 1. Hosting      | Local (L)                |
| PCS Web Server      | PCS Operating System | 7. installing   | Local (L)                |

|                      |                                   |                             |             |
|----------------------|-----------------------------------|-----------------------------|-------------|
| PCS Application      | PCS Database Server               | 2.Exchange data/information | Network (N) |
| PCS Operating System | Corporate Domain Controller (CDC) | 8.Trusted                   | Network (N) |

Table 44. Threat scenario for the Port Community System.

| Asset                | Threat ID  | Threat Description            | CWE ID  | CWE Name                      | Vulnerability ID | Vulnerability Name           | Threat Level     |
|----------------------|------------|-------------------------------|---------|-------------------------------|------------------|------------------------------|------------------|
| PCS Database         | CAPE C-66  | SQL injection                 | CWE-20  | Inproper input validation     | CVE-2025-10460   | Unauthenticated Web endpoint | Very High (0.90) |
| PCS Operating SYstem | CAPE C-233 | Overflow Privilege Escalation | CWE-269 | Improper Privilege Management | CVE-2024-38014   | Active Privilege Escalation  | Very High (0.75) |

Figure 45 provides an indicative example of a SCADA infrastructure architecture which operates in Port terminals for the vehicles unloading process. The work in [96] created within the current dissertation research presents a short threat scenario on SCADA systems and it is represented in a BPMN process model to illustrate how business modelling languages can be utilised to visualise security concepts.

### SCADA system architecture for vehicles unloading process

SCADA systems facilitate maritime and shipping operations, as they provide services referring to vessel control and monitoring, stevedoring and cargo warehousing. Thus, the SCADA model provides procedures within the MLoSCS to support the Vehicle Transport Service unloading services.. The SCADA model infrastructure is divided into four successive levels:

- the bottom level is known as field or technological level, including sensors, amplifiers
- the distribution level consists of remote control stations
- the supervision level, is the core of SCADA system, comprises of the Master Terminal Unit (MTU)
- the Human Machine Interface (HMI)
- the top level is the enterprise level communicating with the Port Community System (PCS) of Port Authority.

A SCADA system in a Port terminal can serve as a common process automation system, used to gather data from sensors and instruments located at remote points and to transmit them at a central point for either control or monitoring purposes. The system is, thus, able to analyse and display information improving the performance of vehicles shipping operations, reducing waste of time and providing cost saving. In order for a SCADA system to meet its objectives it incorporates a bundle of components (see Figure 45):

- The SCADA infrastructure comprises the Human-Machine Interface (HMI) for monitoring and control
- Programmable Logic Controllers (PLCs) for local automation and process control
- Remote Terminal Units (RTUs) for interfacing field devices with supervisory systems
- the Master Terminal Unit (MTU) for real-time data management
- a Data Historian for data storage, and supervisory stations for data acquisition and communication between RTUs/PLCs and the HMI.
- Supervisory stations which are responsible for communicating between SCADA equipment such as RTUs or PLCs and HMI software for data acquisition
- Trailer cranes and forklifts are monitored and controlled through sensors integrated into the SCADA system. Communications are performed via wired and wireless networks, with RTUs supporting geographically distributed operations and PLCs providing efficient local control.

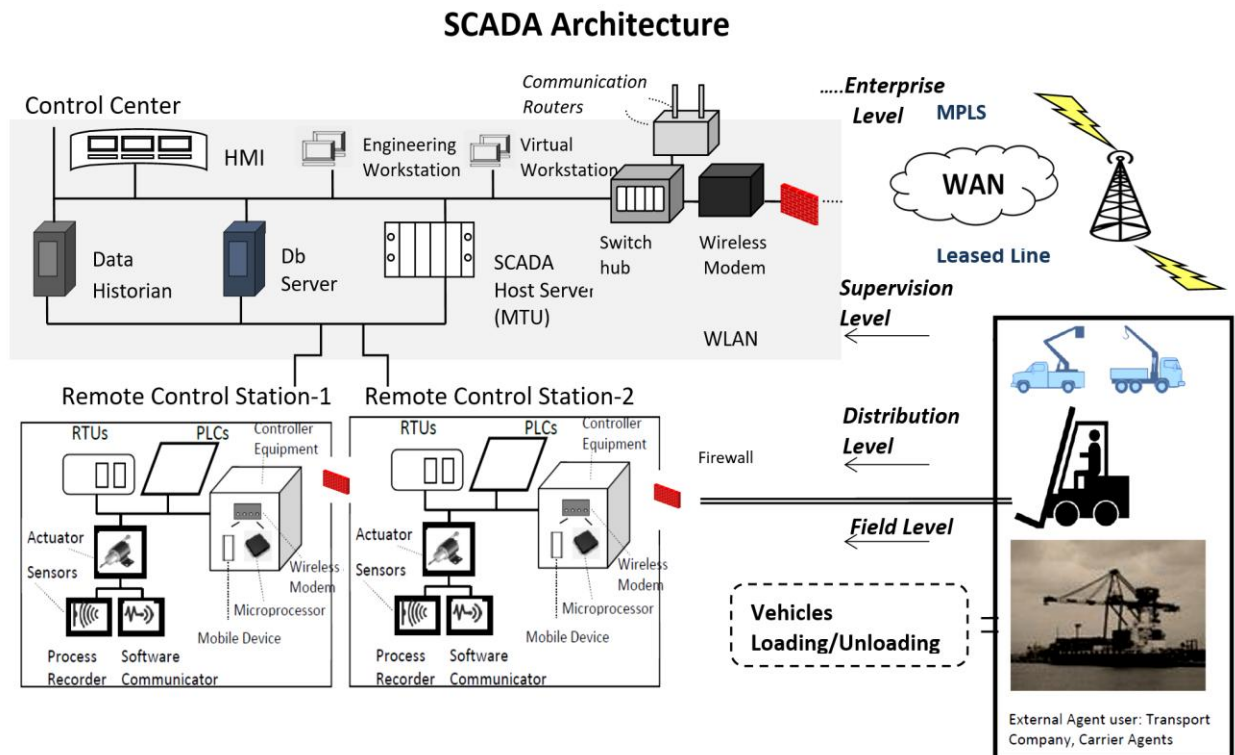


Figure 45. SCADA system for stevedoring; loading/unloading vehicles from vessels and their transportation to car terminals.

Using the BPMN 2.0.2 specification, a credible attack scenario is modelled, likely to occur in SCADA systems across maritime and shipping operations. As SCADA asset operations are composite and complex, the developed BPMN model includes some abstract representative functions. Current attack scenario occurs while the vessel unloading and vehicles' transportation to the car terminal are in progress. The attack scenario is described in the following.

## Modelling SCADA Attacks

The criminals manage to compromise some critical elements of the SCADA system by exploiting various vulnerabilities, one of which is especially interesting, as the MTU user is a domain administrator with elevated privileges to most SCADA assets at port. The criminals use the credentials of the MTU administrator to gain remote access to the SCADA system, and by exploiting the vulnerability that allows them to execute code, they penetrate the HMI system. As a consequence, they identify the precise location of the relevant vehicles within the port and some especially valuable truck-based transports. Then, the hackers send their location and delivery times to their drivers and change the relevant data to collect the vehicles.

The BPMN 2.0.2 developed model follows the four levels of the SCADA architecture (see Figure 45), represented as BPMN swimlanes. It illustrates the flow of control information from sensors and RTUs/PLCs to supervisory stations, remote control stations, and actuators, ultimately enabling the movement of trailer cranes and vehicles.

In the examined attack scenario (see Figure 46), attackers exploit privilege escalation and code execution vulnerabilities in the HMI system to alter vehicle geolocation data. These vulnerabilities are represented in the BPMN model as throwing escalation events. The attack creates two alternative process paths: (i) a normal path, where no attack occurs and vehicles are successfully delivered to the terminal, and (ii) an attack path, where the compromise of the HMI results in vehicle theft. Vulnerability types are mapped to BPMN boundary events according to their characteristics (e.g., directory traversal, denial-of-service, memory corruption, SQL injection). The attacker, assumed to be a terrorist in this scenario, is represented through BPMN annotations to highlight the effects of the attack on SCADA assets. The exploitation primarily affects the HMI and MTU, while additional impacts propagate to other SCADA components, including the Data Historian, PLCs, sensors, and actuators.

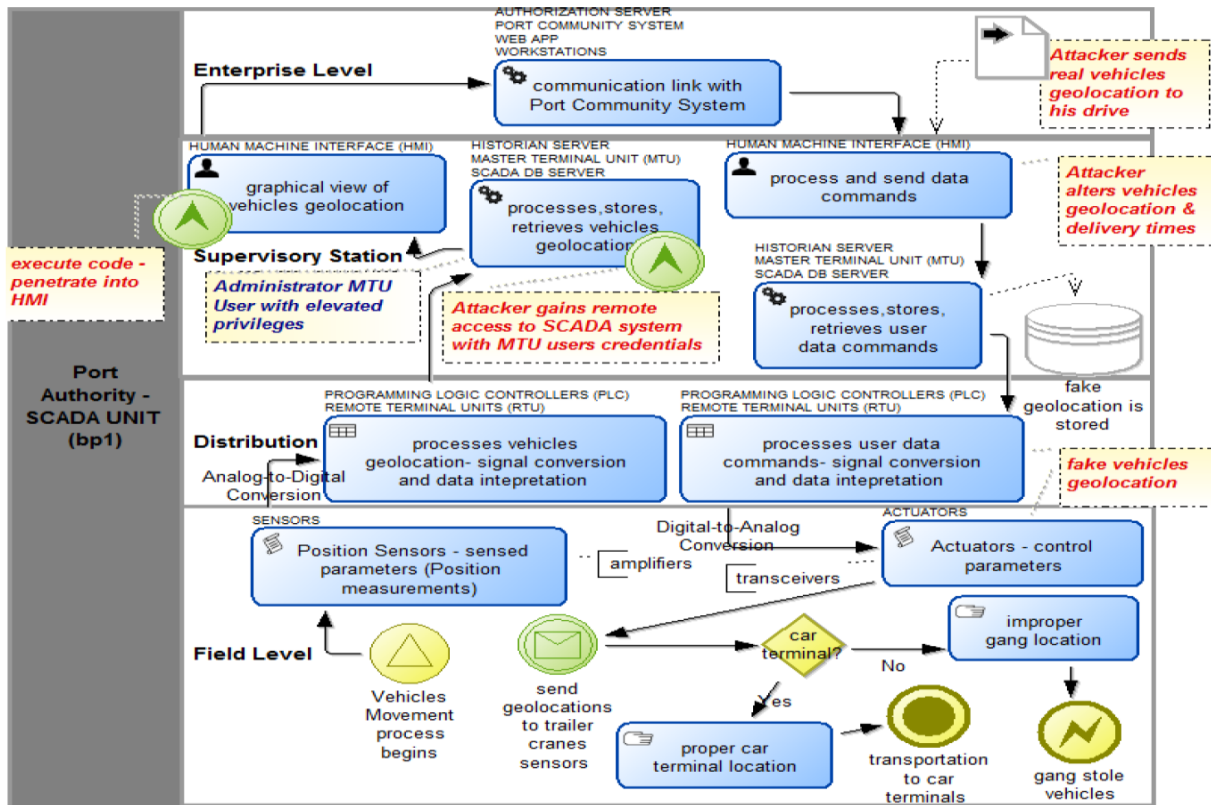


Figure 46. Visualisation of vehicles robbery attack during vessels unloading.

## 6.4.2 The LNG Transport Service

The section presents the holistic-technical evaluation aspect of CyberICT Risk Management Methodology. In the current ICT SCS case, an end-to-end cybersecurity risk assessment is performed (see Section 6.4.2.2) showcasing a realistic cyberattack scenario (see Section 6.4.2.1). The current section presents the research work described in [1] which aspects were additionally demonstrated through the risk management platform (see Section 6.2.4).

### 6.4.2.1 Intrusion Scenario on the Oil Monitoring System of the LNG Transport Service

The demonstration case is presented in two parts: i) the LNG cyberattack realistic scenario, and ii) the LNG Transport ecosystem.

#### The LNG cyberattack scenario

Liquefied Natural Gas (LNG) is a natural gas, predominantly methane (CH<sub>4</sub>), that has been converted to a liquid form for ease of storage or transport. It is odourless, colourless, nontoxic, and noncorrosive. Hazards include flammability after vaporisation into a gaseous state, freezing, and asphyxia. Considering that a tanker contains more than one hundred thousand cubic metres of LNG, it represents a potential explosive hazard comparable to a nuclear bomb.



A terrorist group seeks to cause significant human casualties, economic losses, and environmental damage by attacking the LNG land-based facilities of a port or an LNG tanker. For example, a possible cyberattack on LNG land-based infrastructure may cause catastrophic fires either inside the port or even in nearby populated areas, and an LNG tanker attack may result in a major spill that could pose a hazard to coastal communities along the tanker's route. Furthermore, a physical attack on LNG storage facilities, either in the form of bombing or by impacting a vehicle in the facility, may cause an explosion that leads to a widespread fire, jeopardising people's lives within the port.

Assuming that a terrorist group commits a cyberattack during LNG shipping. The scenario starts with a shipping company receiving an e-mail purportedly from an IT company that supports and maintains its ICT infrastructure, asking them to download and install software that improves the performance of their systems. In this way, the terrorists succeed in downloading and executing arbitrary code on the victims' systems to gain access to them. Accordingly, terrorists can leverage their access to go deep into the network by exploiting vulnerabilities in the oil company's monitoring software that provides remote tank monitoring, asset tracking, and data reporting services to break into the system. Therefore, they can empty the oil tank without detection.

### **The LNG Transport ecosystem**

The scenario involves several business partners: a Local Agent of a maritime logistics company; the Port Authority from the Port of origin located in a European country (e.g. in Greece); the Port Authority from the destination Port (e.g., in Qatar), and a Gas Shipping Company, collaborating for the provision of the LNG Transport Service, which is highly dependent on the combined use of the port's physical (i.e., facilities, buildings, cranes, pipelines, rail track, roads, and data centres) and cyber infrastructure (i.e., networks, ICT hardware equipment, communication systems, and access control/authentication of users and containers).

#### **6.4.2.2 Methodology implementation to the scenario**

The current section presents the CyberICT Risk Management Methodology applicability following its step-wised approach for the LNG Transport Service (LNGTS).

#### **Step 0. LNGTS - Set the risk assessment boundaries**

The four MLoSC business partners (Local Agent, two Port Authorities, and the Gas Shipping Company) signed a Security Declaration Statement, which is a documented commitment of each partner to exchange any security-related information and data concerning the LNG Transport Service and report any security risks or information related to the provision of this service. This information includes the security measures implemented on their infrastructures, how the ICT systems of LNG Transport are safeguarded, and how their accompanying information is protected. The security measures are demonstrated and verified. In particular, business partners use the CyberICT Risk Management Methodology to assess their SCADA components and identify individual cyber risks. The corresponding propagated and cascading effects with respect to the entire LNG Transport Service. The goal is to have a holistic treatment of threats, offering an enhanced understanding of the cyber interfaces for unidentified vulnerabilities, providing

decision-making with an improved assessment of the integrated risks containing the propagating and cascading effects of the entire ICT SCS.

### Step 1. LNGTS - Modelling based cartography

In this scenario the ICT stakeholder is the LNG Shipping Company, which is responsible for the Tanker and its technical operation, implemented by the LNG Carrier Vessel. The two Port Authorities and the Local Agent are considered the business partners collaborating in the LNG Transport Service.

According to Table 14, the criticality of LNG Transport Service is “High”, as the service resides in two critical industry sectors, i.e., Maritime Transport and Energy and one (1) of the business partners is a non-European member.

The under-examination ICT process is the LNG Monitoring Service process, as prescribed in Table 45. The current example presents indicative SCADA components, presented in Table 46

Table 45. Analysis of “LNG Monitoring Service” ICT process.

| LNGTransport Service (LNGTS) |                                                                                                                                                                                 |                                                                                                                                                                                                                                                                         |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ICT process                  | ICT process description                                                                                                                                                         | Business partners involved in the identified processes                                                                                                                                                                                                                  |
| LNG Monitoring Service       | It refers to the LNG handling functions of the LNG port terminal and the LNG carrier vessel operating during the LNG Transport (i.e., pipeline monitoring and fuel monitoring). | <b>ICT stakeholder:</b><br>LNG Shipping Company (bp <sub>0</sub> )<br><b>Business Partners:</b><br>LNG Carrier Vessel (bp <sub>1</sub> )<br>European Port Authority (bp <sub>2</sub> ),<br>Local Agent (bp <sub>3</sub> )<br>Port Authority of Qatar (bp <sub>5</sub> ) |

Table 46. High level LNG SCADA infrastructure analysis.

| LNG Trasport Service (ICT SCS)                                    |                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LNG Monitoring Service                                            |                                                                                                                                                                                                                                                                                                                                                                                 |
| ICT stakeholder and Business partners involved in the ICT process | ICT infrastructure                                                                                                                                                                                                                                                                                                                                                              |
| LNG Carrier Vessel (bp <sub>1</sub> )                             | SCADA infrastructure: <ul style="list-style-type: none"> <li>System for FUEL monitoring service: assets (i.e., software installed on an operating system) that deliver fuel consumption information for the LNG Carrier Vessel.</li> <li>PLCs handling the LNG Tanker capacity</li> <li>A MTU which controls the PLCs using the Modbus TCP/IP communication protocol</li> </ul> |



|                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                            | <ul style="list-style-type: none"> <li>• A Historian Data Server which records historical data upon LNG Tanker capacity and stores in the LNG Database Server</li> <li>• The LNG Database Server</li> <li>• a HMI which is considered an input-output device with a panel view for depicting graphically the process data to human operators of the engineering workstations</li> <li>• a SMTP mail server with each mail</li> <li>• Operating System for the e-mail communication across the interconnected SCADA assets operating within the LNG network</li> </ul> |
| European Port Authority (bp <sub>2</sub> ) | Port Authority mailing system Port Community System (PCS)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Local Agent (bp <sub>3</sub> )             | Local Agent mailing system                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

To this purpose the SCADA components are further decomposed into its primary assets, as shown in Table 47, indicating their types and cyberdependencies, according to the twofold dependency concept analysed in Section 6.2.2.2 Step 1.

Table 47. LNG Monitoring asset matrix.

| Asset Source     | Asset Destination                   | Dependency type              | Dependency access vector |
|------------------|-------------------------------------|------------------------------|--------------------------|
| LNG—PLC software | LNG—PLC OS                          | 7. installing                | Local (L)                |
| SMTP Mail Server | Local Agent Mail Server             | 2. exchange data/information | Network (N)              |
| LNG—PLC          | LNG Master Terminal Unit Connecting | 9. connecting                | Adjacent Network(A)      |

## Step 2. LNGTS – Cyber Threat Intelligence

Using the open repositories, described in Step 2.1 and Step 2.2 (e.g., CAPEC MITRE threat catalogue and MITRE CVE), threats, weaknesses and vulnerabilities are identified for the asset “PLC Software”(see Table 48). The threat level is also estimated. Indicative interrelations of asset-threat-vulnerability are provided in (Table 48).

Table 48. Threat scenario for PLC Software.

| Asset        | Threat ID  | Threat Description  | CWE ID | CWE Name       | Vulnerability ID | Vulnerability Name | Threat Level     |
|--------------|------------|---------------------|--------|----------------|------------------|--------------------|------------------|
| PLC Software | CAPEC -242 | Component injection | CWE-94 | Code Injection | CVE-2022-22965   | Spring4Shell       | Very High (0.82) |

|              |           |                  |         |                                                                         |               |                                      |                  |
|--------------|-----------|------------------|---------|-------------------------------------------------------------------------|---------------|--------------------------------------|------------------|
| PLC Software | CAPEC-100 | Overflow Buffers | CWE-119 | Improper Restriction of Operations within the Bounds of a Memory Buffer | CVE-2009-2502 | Critical remote code execution (RCE) | Very High (0.94) |
|--------------|-----------|------------------|---------|-------------------------------------------------------------------------|---------------|--------------------------------------|------------------|

### Step 3. LNGTS – Vulnerability and Impact Analysis

Following the CyberICT Risk Management Methodology formulas of step 3, the Individual vulnerability level and the impact level are calculated:

For example, concerning the CVE-2009-2502:

$$MESS_{v_{CVE-2009-2502}} = 8.22 \cdot 0.85 \cdot 0.44 \cdot 0.85 \cdot 0.85$$

$$MESS_v = 2.22$$

Then, the outcome is normalised:

$$IVL_{CVE-2009-2502_{norm}} = \frac{MESS_v - MESS_{Min}}{MESS_{Max} - MESS_{Min}}$$

$$IVL_{CVE-2009-2502_{norm}} = \frac{2.22 - 0.22}{3.89 - 0.22}$$

$$IVL_{CVE-2009-2502_{norm}} = 0.55 = \text{Moderate (M)}$$

To calculate the Exploitation Level of CVE-2009-2502 for the PLC software,

The Attacker's Capability is assumed High = 0.75

and the Attacker's location the Network = 1

Then, the Attacker's Profile is:

$$P_c = 0.5 \times 0.75 + 0.5$$

$$P_c = 0.875$$

To calculate the EL using equal weights:

$$EL_{CVE-2009-2502} = 0.5 \times 0.55_v + 0.5 \times 0.875$$

$$EL_{CVE-2009-2502} = 0.7125 = \text{High}$$

To calculate the Impact Level for CVE-2009-2502,

It is assumed that the criticality of the PLC software is Very High. Then, according to Table 32 of Step 3.3,  $C_{mod} = I_{mod} = A_{mod} = 0.56$  and  $CR = IR = AR = 1.5$

Thus,

$$MISS_{CVE-2009-2502} = \min(1 - (1 - 0.84) \times (1 - 0.84) \times (1 - 0.84), 0.915)$$

$$MISS_{CVE-2009-2502} = \min(0.995904, 0.915)$$

$$MISS_{CVE-2009-2502} = 0.915$$

Assuming that the scope in the current scenario is unchanged, then:

$$IL_{\text{CVE-2009-2502}} = 6.42 \times 0.915$$

$$IL_{\text{CVE-2009-2502}} = 5.87$$

Now the value is normalised using the formula:

$$IL_{\text{CVE-2009-2502}} = \frac{5.87 - 0}{5.8743}$$

$$IL_{\text{CVE-2009-2502}} = 0.9993 = \text{Very High (VH)}$$

Respectively, following the formulas of step 3 and the current scenario assumptions, for CVE-2022-22965:

IVL<sub>CVE-2022-22965</sub> = Very High (VH)

EL<sub>CVE-2022-22965</sub> = 0.71875 = High (H)

IL<sub>CVE-2022-22965</sub> = Very High (H)

#### Step 4. LNGTS – ASECG Model

Since the current scenario has not detected any abnormal activity or unusual traffic or any other issue yet, there is no security event confirmed; the current step does not apply.

#### Step 5. LNGTS – Risk Estimation

To estimate the Individual Risk Level, considering the TL, Els, ILs from the previous steps, the formula of Step 5 is used:

$$RL_{s,A_{i,j}} = TL_s \times EL_v \times IL_v$$

Then, for CAPEC 100 and CVE-2009-2502 scenario:

$$RL_{1,PLC_{\text{software}}} = 0.94 \times 0.7125 \times 0.9993$$

$$RL_{1,PLC_{\text{software}}} = 0.6693 = \text{High (H)}$$

Moreover for CAPEC 242 and CVE-2022-22965 scenario:

$$RL_{2,PLC_{\text{software}}} = 0.82 \times 0.71875 \times 0.9993$$

$$RL_{2,PLC_{\text{software}}} = 0.5890 = \text{Moderate (M)}$$

To estimate the cumulative risk, alternative attack path scenarios were run setting:

- high-risk assets as entry points, such as the LNG Database and the SMTP Mail Server and review the attack path analysis results
- cyberdependency assets either as entry or target points and study the attack path sub-graphs.

The cumulative risk for each attack path, according to the qualitative scale of Table 87, is estimated and shown in Table 49. For instance, the risk exposure of reaching the specific asset

“Fuel Monitoring Software” is “Very High” in case the adversary succeeds to enter into the LNG Transport Network by attacking the “LNG-SMTP Mail Server”.

Table 49. Attack path scenarios in LNG Transport Service.

| Scenario Description                 | Asset nodes                                                                                                                                                                           | Cumulative Risk |
|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| LNG spill (Locally)                  | <b>LNG – Database</b><br><i>(LNG Transport Network) -&gt;</i><br><b>LNG – mailstation DesktopApp1</b><br><i>(LNG Transport Network) -&gt;</i><br><b>LNG – Fuel Monitoring Softwar</b> | H               |
| LNG spill (Network)                  | <b>LNG – SMTP Mail Server</b><br><i>(LNG Transport Network) -&gt;</i><br><b>LNG – Fuel Monitoring Software</b>                                                                        | VH              |
|                                      | <b>LNG – SMTP Mail Server</b><br><i>(LNG Transport Network) -&gt;</i><br><b>LNG – HMI software</b><br><i>(LNG Transport Network) -&gt;</i><br><b>LNG – Fuel Monitoring Software</b>   | H               |
| Attack on Control Stations (Network) | <b>LNG – mailstation DesktopApp1</b><br><i>(LNG Transport Network) -&gt;</i><br><b>LNG – HMI software</b><br><i>(LNG Transport Network) -&gt;</i><br><b>LNG – PLC OS</b>              | H               |
|                                      | <b>LNG – mailstation DesktopApp1</b><br><i>(LNG Transport Network) -&gt;</i><br><b>LNG – Engineering workstation</b><br><i>(LNG Transport Network) -&gt;</i><br><b>LNG – PLC OS</b>   | H               |

## Step 6. LNGTS - Risk Management and Treatement

To identify potential mitigation strategies, the above simulation scenarios can be reconsidered upon implementing security controls on assets that may mitigate vulnerabilities or threats and reassess the scenario based on the asset interdependencies. Moreover, additional practices can be adopted, as described in Section 6.2.2.7.

### 6.4.3 The Container Cargo Management Service

The section presents the sector-specific evaluation aspect of CyberICT Risk Management Methodology. In the Container Cargo Management Service case, the Attack Simulation and Evidence Chain Genaration (ASECG) model was performed, showcasing a realistic cyberattack scenario (see Section 6.4.3.2). This section is based on aspects of the work in [9] created as part of this dissertation research, which was updated over time to enhance the vulnerability

exploitability calculation model. The terrorist scenario, presented in Section 6.4.3.1, is considered to have at least one successful attack to apply the ASECG model to calculate the attack paths related to the specific confirmed security event.

#### 6.4.3.1 Cyber-Attack on SCADA Systems of the Container Cargo Management Service

The demonstration case is presented in two parts: i) the Container Cargo terrorist attack scenario, and ii) the Cargo Management ecosystem.

##### **The Container Cargo terrorist attack**

According to Eurostat 184/2016 statistics, the containerised freight represents almost the third part of total trade exchanges measured in monetary value. However, the percentage of maritime transport in relation to the total transported is even higher when kilometres or tonne-kilometres are measured. Consequently, these references highlight the important role of container terminals in the international carriage of goods. Uniform boxes that can be easily moved between lorries, train,s and ships have reshaped global trade over the past few decades.

A terrorist group wants to carry out a terrorist attack at a port to inflict wide-scale death and destruction by placing a bomb in a container, shipping it to the target port, and detonating it before it can be inspected. The terrorist group is aware that a name-brand company ships containers of products and other cargo to this port. The containers on any given ship are packed at the factories of the company; the container doors are shut, and a mechanical seal is placed into the door pad eyes. A transportation company has undertaken the responsibility of picking up the container and transferring it to a container vessel. However, the containers are not delivered directly from the name-brand company's premises to the port terminal; rather, they go through a third party, a container-packing warehouse. The terrorists are aware that deliveries are managed through an IT system at the container packing warehouse; thus, they cooperate with skilled hackers who can infiltrate the IT environment of the third party and gain access to the container management system. The terrorists change the information of the shipping container to replace it with another one carrying a bomb, which has already been placed by the terrorist group in the container packing warehouse.

Alternatively, hackers can target any RFID tags and sensors attached to the container to monitor goods. Such RFID kits are usually used to monitor various: (i) safety-oriented features, such as whether the container door is opened or closed and the temperature inside the container, or (ii) national security concerns, such as the illegal transportation of radioactive material and/or chemicals used in bomb construction. Each container's RFID tag transmits its ID number and sensor data to an RFID reader, which then forwards that information (e.g., via a GSM base station) to an onboard control system and finally to the system administrator. Hackers can remotely exploit these RFID tags and sensors by injecting their own malware so that they transmit falsified information for the cargo of the targeted container. Worse, they can manipulate the tags of other legitimate containers to make them look as if they hold suspicious cargo instead of the actual malevolent container. At the target port, the security authorities inspect containers that the

screening identifies as suspicious, based on Ports of call, manifest data, shipping companies, etc. To circumvent the authorities and bypass the inspection process, terrorists compromise the IT infrastructure of the port and gain access to the container shipping system that maintains the routing or scheduling of the containers. Hence, they can change the container's details in the system and place the container in the desired location so that the detonation of the bomb can cause the maximum number of injuries and deaths.

### **The Container Cargo Management ecosystem**

The scenario refers to the maritime transport industry. It implements a process that is executed during the performance of the General Cargo Transport Service. The Service relies on the transportation of general cargo from a port of origin to the destination port, including loading/unloading procedures and inbound/outbound logistics to deliver the cargo to the final consumer. A critical document used during cargo transportation is the Standard Cargo Manifest, which contains detailed information about the vessel and the cargo being transported onboard. Suppose a Ship Agent sends a Standard Cargo Manifest request to the Port Authority.

These communications are accomplished using the Port Community System (PCS), which provides users with a client application to launch the service rapidly and fulfil the requirements of sending documentation electronically to the involved entities. In addition, the port operator of the Port Authority, who handles the current transaction with the Ship Agent (through the PCS), uses other web services to implement port activities (i.e., Customs Clearance).

#### **6.4.3.2 Application of the Evidence Chain Generation Approach**

This section applies the ASECG, described in Section 6.2.2.5, via a simplified realistic terrorist scenario. The scenario is considered a confirmed security event aiming to demonstrate the proposed model and validate the approach of estimating how an attacker has moved into a network by checking its applicability.

The Port Authority's assets, operating in the Container Management Service (MCS) scenario, are the following:

- A Web Application for the Standard Cargo Manifest request ( $A_1$ ) hosted on a Web Server ( $A_2$ ), which is installed on the PCS Operating System ( $A_3$ ). Customs Clearance is supported by another Web Service ( $A_4$ ) of the Port Authority, which is also hosted on the Web Server ( $A_2$ ).
- A Database Server ( $A_5$ ) stores the PCS data and is installed on the PCS Operating System ( $A_3$ ). The Database Server ( $A_5$ ) exchanges information with the Standard Cargo Manifest request Web Application ( $A_1$ ). When the Ship Agent sends the Standard Cargo Manifest request, relevant data are stored on the Database Server ( $A_5$ ).
- The Port Authority assets communicate with various port stakeholders (e.g., Ship Agent, Vessels, Customs, etc.).

Assuming the Port Authority has activated the presented risk assessment process, during the vulnerability assessment, the proposed model is implemented to assess vulnerabilities and their

exploitation. The steps of the proposed approach are implemented subsequently, utilising tasks and rules presented in Table 50 and described in the following.

#### Step 4.1 CCMS - Generation of Vulnerability Chains

In the current step, the Vulnerability Chains Discovery method is activated (see steps 4.1.1–4.1.5) to generate all possible vulnerability chains, considered as potential attack paths. To generate vulnerability chains, the first and third steps of the Cybersecurity Risk Assessment methodology must be implemented (Asset Cartography and Modelling and the Vulnerability Assessment in terms of generating vulnerability chains).

##### Step 4.1.1 CCMS - Identify Asset Dependency Graphs

According to the first step of the methodology, asset modelling is performed. The engaged assets are presented in Table 50 along with their cyberdependency types in asset pairs (cf. Step 4.1, Section **Error! Reference source not found.**).

Table 50. Assets and their cyberdependencies of the current scenario.

| Asset Source   |                 | Asset Destination |                  | Cyber-dependency Type                                                                                                                       |
|----------------|-----------------|-------------------|------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| Asset          | Asset Category  | Asset             | Asset Category   | 1. Hosting; 2. Exchange Data/Information; 3. Storing; 4. Controlling; 5. Processing; 6. Accessing; 7. Installing; 8. Trusted; 9. Connecting |
| A <sub>1</sub> | Web Application | A <sub>2</sub>    | Web Server       | hosted_by                                                                                                                                   |
| A <sub>2</sub> | Web Server      | A <sub>3</sub>    | Operating System | installed_on                                                                                                                                |
| A <sub>4</sub> | Web Service     | A <sub>2</sub>    | Web Server       | hosted_by                                                                                                                                   |
| A <sub>5</sub> | Database Server | A <sub>3</sub>    | Operating System | installed_on                                                                                                                                |
| A <sub>1</sub> | Web Application | A <sub>5</sub>    | Database Server  | exchange_data                                                                                                                               |

A visualisation of the ICT assets cyberdependencies are depicted in Figure 47 asset dependency graph.

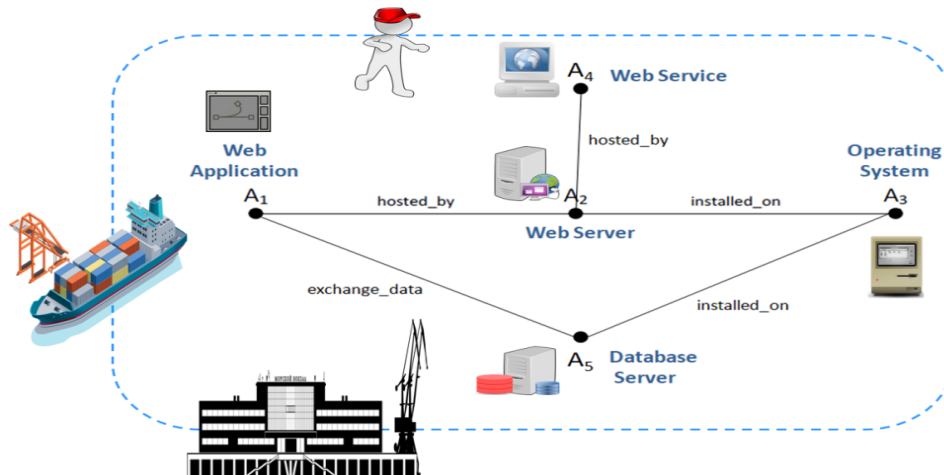


Figure 47. Cyberdependency graph of Port Authority assets.

### Steps 4.1.2-4.1.3 CCMS - Define Entry Points – Define Target Points

According to the asset cyberdependencies developed, CII operators of the Port Authority define potential Asset Entry Points (Step 4.1.2) and Asset Target Points (Step 4.1.3) that are considered critical to be examined.

### Step 4.1.4 CCMS - Perform Individual Vulnerability Assessment

In the current scenario, thirteen vulnerabilities (confirmed and unconfirmed) are detected among those assets as follows:

- three vulnerabilities (V<sub>1</sub>,V<sub>2</sub>,V<sub>3</sub>) are identified on asset A<sub>1</sub>
- two vulnerabilities (V<sub>4</sub>,V<sub>5</sub>) are identified on asset A<sub>2</sub>
- three vulnerabilities (V<sub>6</sub>,V<sub>7</sub>,V<sub>8</sub>) are identified on asset A<sub>3</sub>
- three vulnerabilities (V<sub>9</sub>,V<sub>10</sub>,V<sub>11</sub>) are identified on asset A<sub>4</sub>
- two vulnerabilities (V<sub>12</sub>,V<sub>13</sub>) are identified on asset A<sub>5</sub>.

According to the CVSS 3.1 score metrics related to technical exploitability of vulnerabilities [139] (see Step 4.1.4), the thirteen identified vulnerabilities (V<sub>1</sub>, V<sub>2</sub>, ..., V<sub>13</sub>) along with their attributes are presented in Table 51 with respect to the corresponding assets.

Table 51. Vulnerabilities identified on assets and corresponding CVSS 3.1 metrics.

| Asset          | Vulnerability  |                    | CVSS Exploitability                                  |                                  |                                    |                                 | CVSS Impact                   |                               |                               |
|----------------|----------------|--------------------|------------------------------------------------------|----------------------------------|------------------------------------|---------------------------------|-------------------------------|-------------------------------|-------------------------------|
|                | ID             | Vulnerability Name | Modified Attack Vector (MAV)                         | Modified Attack Complexity (MAC) | Modified Privileges Required (MPR) | Modified User Interaction (MUI) | Modified Confidentiality (MC) | Modified Integrity (MI)       | Modified Availability (MA)    |
|                |                |                    | (Physical (P), Local (L), Adjacent (A), Network (N)) | (Low (L), High (H))              | (None (N), Low (L), High (H))      | (None (N), Required (R))        | (None (N), Low (L), High (H)) | (None (N), Low (L), High (H)) | (None (N), Low (L), High (H)) |
| A <sub>1</sub> | V <sub>1</sub> | CVE-2025-55182     | N                                                    | L                                | N                                  | N                               | H                             | H                             | H                             |
| A <sub>1</sub> | V <sub>2</sub> | CVE-2026-23738     | A                                                    | L                                | N                                  | R                               | L                             | N                             | N                             |
| A <sub>1</sub> | V <sub>3</sub> | CVE-2026-29000     | N                                                    | L                                | N                                  | N                               | H                             | H                             | N                             |



|    |     |                |   |   |   |   |   |   |   |
|----|-----|----------------|---|---|---|---|---|---|---|
| A2 | V4  | CVE-2017-5638  | N | L | N | N | H | H | H |
| A2 | V5  | CVE-2024-26295 | N | L | L | N | H | H | H |
| A3 | V6  | CVE-2025-24991 | L | L | N | R | H | N | N |
| A3 | V7  | CVE-2026-41096 | N | L | N | N | H | H | H |
| A3 | V8  | CVE-2026-20824 | L | L | N | R | H | N | N |
| A4 | V9  | CVE-2022-22965 | N | L | N | N | H | H | H |
| A4 | V10 | CVE-2022-22963 | N | L | N | N | H | H | H |
| A4 | V11 | CVE-2024-22271 | N | L | N | N | H | L | N |
| A5 | V12 | CVE-2019-10130 | N | L | L | N | L | L | N |
| A5 | V13 | CVE-2022-1552  | N | L | L | N | H | H | H |

Then, the Individual Vulnerability Level (IVL) is estimated upon these asset/vulnerability combinations, according to what has been described in Step 4.1.4. Moreover, considering the Modified Attack Vector (MAV), Modified Attack Complexity (MAC), Modified Privileges Required (MPR) and Modified User Interaction (MUI) policy vulnerability attributes of Table 51 the  $IVL_v$  formula, defined in Step 5.1.4, is used to calculate the Individual Vulnerability Level for reach vulnerability  $v$  identified in numeric values which are normalised using the normalisation technique, described in Step 4.1.4.

Figure 48 illustrates the asset graph of asset/vulnerability combinations for the Port Authority assets scenario. The asset graph illustrates the asset/vulnerability combinations only for vulnerabilities of asset entry points that have the MAC “Network” attribute (see “Produce Vulnerability Chains”, Step 4.1.5 in the following). This is because, in the current scenario, it is assumed that the attacker’s location is in another country. Thus, the attacker can reach the asset only through the Web. Moreover, it is assumed for the current scenario that the attacker does not have the advanced capacity to access the adjacent network as MAV. For instance, an attacker’s

employment with advanced options in reaching the Port Authority’s adjacent network by connecting through the company’s VPN, gaining access to the same cloud VPC/subnet, pivoting through another internal host, or controlling a device already on the same Wi-Fi is considered not possible for the current scenario. In this regard, dependencies of  $A_1V_2$  are excluded from the graph. For each asset/vulnerability combinations depicted in Figure 48, the IVL is calculated, presented in Table 52, and depicted in the asset/vulnerability graph of Figure 49. For instance, the IVL of vulnerability  $V_{10}$  of asset  $A_4$  is “Very High”. The IVL is calculated following the approach presented in step 4.1.4. The analysis of the IVL calculations are presented in Table 100 of Appendix D6.

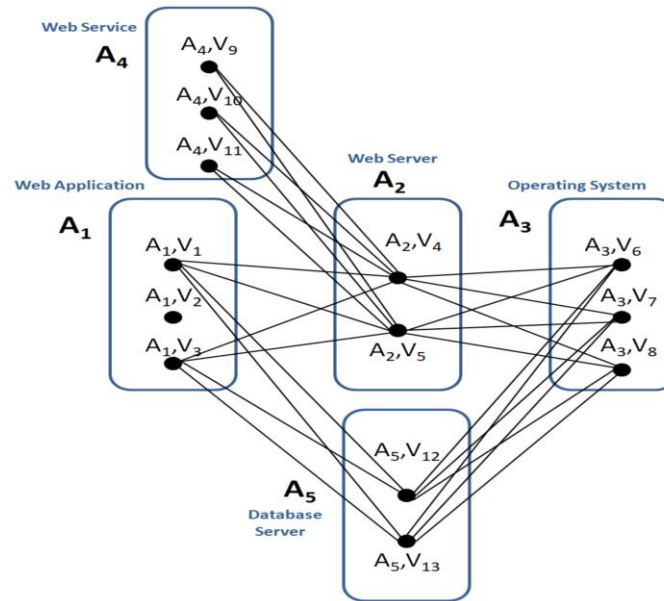


Figure 48. Combinations of assets and vulnerabilities developed, according to the current scenario.

Table 52. Estimation of the Individual Vulnerability Level (IVL) for each identified asset/ vulnerability combination.

| Vulnerability | Asset | Individual Vulnerability Level |
|---------------|-------|--------------------------------|
| $V_1$         | $A_1$ | $VL_{V1} = VH$                 |
| $V_3$         | $A_1$ | $VL_{V3} = VH$                 |
| $V_4$         | $A_2$ | $VL_{V4} = VH$                 |
| $V_5$         | $A_2$ | $VL_{V5} = H$                  |
| $V_6$         | $A_3$ | $VL_{V6} = M$                  |
| $V_7$         | $A_3$ | $VL_{V7} = VH$                 |
| $V_8$         | $A_3$ | $VL_{V8} = M$                  |
| $V_9$         | $A_4$ | $VL_{V9} = VH$                 |
| $V_{10}$      | $A_4$ | $VL_{V10} = VH$                |
| $V_{11}$      | $A_4$ | $VL_{V11} = VH$                |
| $V_{12}$      | $A_5$ | $VL_{V12} = H$                 |
| $V_{13}$      | $A_5$ | $VL_{V13} = H$                 |

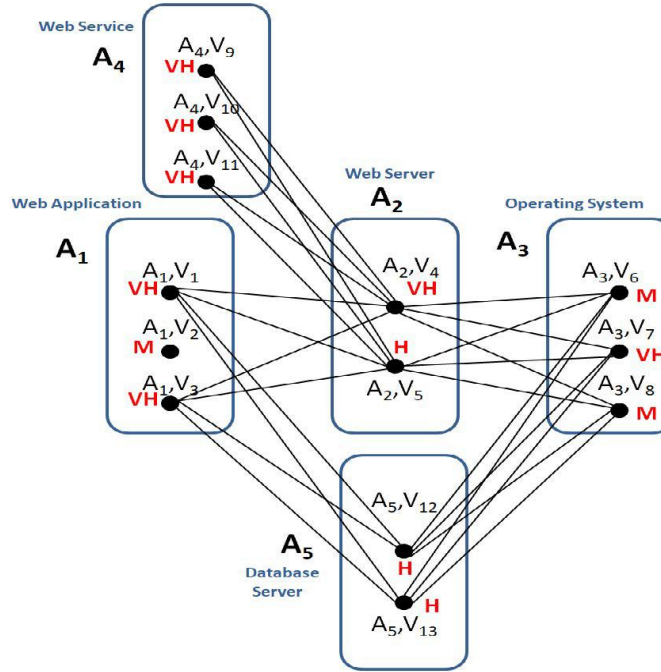


Figure 49. The Individual Vulnerability Level is calculated on asset/vulnerability combinations.

#### Step 4.1.5 CCMS - Produce Vulnerability Chains

At this point, considering the graph of Figure 49, a great number of possible sequential vulnerability chains can be generated. For instance:

- the  $V_1 \rightarrow V_5 \rightarrow V_6$  vulnerability chain for  $A_1, V_1 \rightarrow A_2, V_5 \rightarrow A_3, V_6$  asset/vulnerability combinations
- the  $V_5 \rightarrow V_7$  vulnerability chain for  $A_2, V_5 \rightarrow A_3, V_7$  sequence of asset/vulnerability combinations
- the  $V_9 \rightarrow V_4 \rightarrow V_6$ , vulnerability chain for  $A_4, V_9 \rightarrow A_2, V_4 \rightarrow A_3, V_6$  asset interdependency chain, etc.

The Vulnerability Chains Discovery algorithm [370] (see Step 4.1) is executed, and all vulnerability chains are developed to illustrate potential attack paths. The generated vulnerability chains of the current scenario are depicted in Figure 49, and the exhaustive list of these chains is shown in Table 99 of Appendix D6. After reviewing Table 99, from the 13 vulnerabilities that have been identified, 84 vulnerability chains are generated, which can be potential attack paths in case of being exploited by an adversary.

#### Step 4.2 CCMS - Recurring Process Activation

##### Step 4.2.1 CCMS - Points of Compromise – Indicators of Compromise

Within this step, cyber threats are detected on the defined asset network and the IoC is analysed. In particular, in the current scenario, an unauthorised access to the Database Server (asset A5) was detected from an analysed log file. The log file reported the specific IoC, i.e., IoC<sub>1</sub>, that uncovered

the threatening activity that evidenced the specific Database Server (A<sub>5</sub>) compromise for which the specific PoC has been identified.

This case involves a confirmed event of a cyberattack. To discover and produce potential cyberattack paths for the compromised asset A<sub>5</sub>, a simulated scenario will run only for assets that are cyberdependent on the PCS Database Server (A<sub>5</sub>).

Following the current scenario, all potential cyberdependencies associated with the compromised asset A<sub>5</sub> are identified. According to Table 53. the PCS Database Server has a cyberdependency with the Standard Cargo Manifest Application (A<sub>1</sub>) and the Operating System (A<sub>3</sub>). Figure 50 presents all potential cyberattack paths that link the compromised PCS Database Server (A<sub>5</sub>) with the Standard Cargo Manifest Web Application (A<sub>1</sub>) and the PCS Operating System (A<sub>3</sub>) concerning the specific identified IoC<sub>1</sub>. The A<sub>5</sub>,IoC<sub>1</sub> combination symbolises the PoC on the PCS Database Server (A<sub>5</sub>).

Table 53. Assets cyberdependencies linked to the detected compromised asset A<sub>5</sub>.

| Asset Source   |                 | Asset Destination |                  | Cyber-dependency Type                                                                                                                       |
|----------------|-----------------|-------------------|------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| Asset          | Asset Category  | Asset             | Asset Category   | 1. Hosting; 2. Exchange Data/Information; 3. Storing; 4. Controlling; 5. Processing; 6. Accessing; 7. Installing; 8. Trusted; 9. Connecting |
| A <sub>5</sub> | Database Server | A <sub>3</sub>    | Operating System | installed_on                                                                                                                                |
| A <sub>1</sub> | Web Application | A <sub>5</sub>    | Database Server  | exchange_data                                                                                                                               |

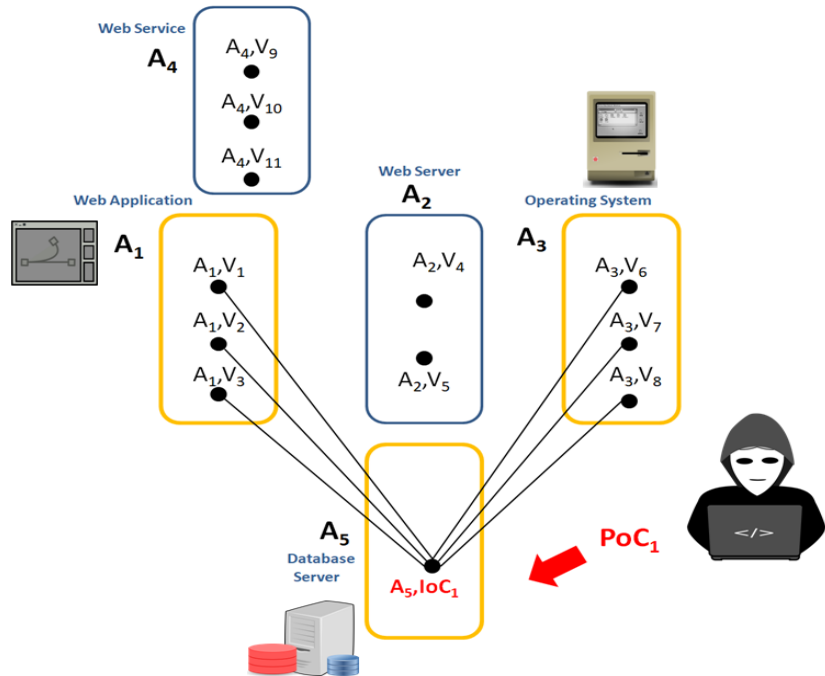


Figure 50. Potential attack paths related to the compromised PCS Database Server (A<sub>5</sub>) given the specific PoC<sub>1</sub> derived from the analysed IoC<sub>1</sub>.

### Step 4.2.2 CCMS - Reconstruction of Potential Attack Paths

The potential attack paths are reconstructed according to the received evidence of the compromised PCS Database Server (A5). In particular, all redeveloped attack paths related to the PoC<sub>1</sub>, where PoC<sub>1</sub> = A5,IoC<sub>1</sub>, are presented in Figure 50 and listed in Table 54.

Table 54. Attack paths are reconstructed according to the confirmed security event and potential evidence chains.

| Asset interdependency Chains                            | Attack Paths                                           | Evidence Chains                         |
|---------------------------------------------------------|--------------------------------------------------------|-----------------------------------------|
| $A_1, V_1 \rightarrow A_5, V_{12} \rightarrow A_3, V_6$ | $A_1, V_1 \rightarrow A_5, IoC_1 \rightarrow A_3, V_6$ | $V_1 \rightarrow IoC_1 \rightarrow V_6$ |
| $A_1, V_1 \rightarrow A_5, V_{13} \rightarrow A_3, V_6$ |                                                        |                                         |
| $A_1, V_1 \rightarrow A_5, V_{12} \rightarrow A_3, V_7$ | $A_1, V_1 \rightarrow A_5, IoC_1 \rightarrow A_3, V_7$ | $V_1 \rightarrow IoC_1 \rightarrow V_7$ |
| $A_1, V_1 \rightarrow A_5, V_{13} \rightarrow A_3, V_7$ |                                                        |                                         |
| $A_1, V_1 \rightarrow A_5, V_{12} \rightarrow A_3, V_8$ | $A_1, V_1 \rightarrow A_5, IoC_1 \rightarrow A_3, V_8$ | $V_1 \rightarrow IoC_1 \rightarrow V_8$ |
| $A_1, V_1 \rightarrow A_5, V_{13} \rightarrow A_3, V_8$ |                                                        |                                         |
| $A_1, V_1 \rightarrow A_5, V_{12}$                      | $A_1, V_1 \rightarrow A_5, IoC_1$                      | $V_1 \rightarrow IoC_1$                 |
| $A_1, V_1 \rightarrow A_5, V_{13}$                      |                                                        |                                         |
| $A_1, V_2 \rightarrow A_5, V_{12} \rightarrow A_3, V_6$ | $A_1, V_2 \rightarrow A_5, IoC_1 \rightarrow A_3, V_6$ | $V_2 \rightarrow IoC_1 \rightarrow V_6$ |
| $A_1, V_2 \rightarrow A_5, V_{13} \rightarrow A_3, V_6$ |                                                        |                                         |
| $A_1, V_2 \rightarrow A_5, V_{12} \rightarrow A_3, V_7$ | $A_1, V_2 \rightarrow A_5, IoC_1 \rightarrow A_3, V_7$ | $V_2 \rightarrow IoC_1 \rightarrow V_7$ |
| $A_1, V_2 \rightarrow A_5, V_{13} \rightarrow A_3, V_7$ |                                                        |                                         |
| $A_1, V_2 \rightarrow A_5, V_{12} \rightarrow A_3, V_8$ | $A_1, V_2 \rightarrow A_5, IoC_1 \rightarrow A_3, V_8$ | $V_2 \rightarrow IoC_1 \rightarrow V_8$ |
| $A_1, V_2 \rightarrow A_5, V_{13} \rightarrow A_3, V_8$ |                                                        |                                         |
| $A_1, V_2 \rightarrow A_5, V_{12}$                      | $A_1, V_2 \rightarrow A_5, IoC_1$                      | $V_2 \rightarrow IoC_1$                 |
| $A_1, V_2 \rightarrow A_5, V_{13}$                      |                                                        |                                         |
| $A_5, V_{12} \rightarrow A_3, V_6$                      | $A_5, IoC_1 \rightarrow A_3, V_6$                      | $IoC_1 \rightarrow V_6$                 |
| $A_5, V_{13} \rightarrow A_3, V_6$                      |                                                        |                                         |
| $A_5, V_{12} \rightarrow A_3, V_7$                      | $A_5, IoC_1 \rightarrow A_3, V_7$                      | $IoC_1 \rightarrow V_7$                 |
| $A_5, V_{13} \rightarrow A_3, V_7$                      |                                                        |                                         |
| $A_5, V_{12} \rightarrow A_3, V_8$                      | $A_5, IoC_1 \rightarrow A_3, V_8$                      | $IoC_1 \rightarrow V_8$                 |
| $A_5, V_{13} \rightarrow A_3, V_8$                      |                                                        |                                         |
| $A_1, V_3 \rightarrow A_5, V_{12}$                      | $A_1, V_3 \rightarrow A_5, IoC_1$                      | $V_3 \rightarrow IoC_1$                 |
| $A_1, V_3 \rightarrow A_5, V_{13}$                      |                                                        |                                         |
| $A_1, V_3 \rightarrow A_5, V_{12} \rightarrow A_3, V_6$ | $A_1, V_3 \rightarrow A_5, IoC_1 \rightarrow A_3, V_6$ | $V_3 \rightarrow IoC_1 \rightarrow V_6$ |
| $A_1, V_3 \rightarrow A_5, V_{13} \rightarrow A_3, V_6$ |                                                        |                                         |
| $A_1, V_3 \rightarrow A_5, V_{12} \rightarrow A_3, V_7$ | $A_1, V_3 \rightarrow A_5, IoC_1 \rightarrow A_3, V_7$ | $V_3 \rightarrow IoC_1 \rightarrow V_7$ |
| $A_1, V_3 \rightarrow A_5, V_{13} \rightarrow A_3, V_7$ |                                                        |                                         |
| $A_1, V_3 \rightarrow A_5, V_{12} \rightarrow A_3, V_8$ | $A_1, V_3 \rightarrow A_5, IoC_1 \rightarrow A_3, V_8$ | $V_3 \rightarrow IoC_1 \rightarrow V_8$ |
| $A_1, V_3 \rightarrow A_5, V_{13} \rightarrow A_3, V_8$ |                                                        |                                         |

The Asset interdependency chains, shown in Table 54, are considered asset/vulnerability combinations that involve the compromised PCS Database Server (A5) as evidenced by the IoC findings. If the results of Table 99 (Appendix D6), retrieved from Step 4.1.5, and the results of Table 54 derived from Step 4.2.2 are compared, it is noted that the previously developed 84 asset

interdependency chains are now limited to 30. On this account, the 84 potential attack paths identified in Table 99 (Appendix D6) have been redeveloped into 15 potential attack paths, displayed in Table 99. This means that 69 attack paths have left, considering the results of Table 99, some of which were erased as they were not related to the infected PCS Database Server (A5), and some others were shrunk/merged because the vulnerability exploitability that reside in the infected asset is 1 (exploitability PIOC = 1), as the asset has already been compromised. Hence, the two potential attack paths  $A1, V1 \rightarrow A5, V12 \rightarrow A3, V6$  and  $A1, V1 \rightarrow A5, V13 \rightarrow A3, V6$  engaging 2 different vulnerabilities V12, V13 are now shrunk into one attack path:  $A1, V1 \rightarrow A5, IoC_1 \rightarrow A3, V6$ . In addition, all potential attack paths associated with  $IoC_1$  are generated and displayed in Table 54.

### Step 4.2.3 CCMS - Attacker's Profile Identification

The attacker's profile is recognised based on the location and capability. Considering the location, as described in step 4.1.4, it is assumed that the attacker is an outsider and can initiate an attack on the Port Authority assets only remotely through the Web. Accordingly, the asset-vulnerability combination graph, developed in Figure 48, represents asset entry points associated with vulnerabilities that have a "Network" Attack Vector. In addition, in the current Port Authority scenario the attacker's capability is considered low, as described in step 4.1.4 of the current section. In this context, the Attacker' Profile score is estimated using the formula presented in Section **Error! Reference source not found.** and the attacker's capability and attacker's location values, presented in Table 96 and Table 97 (Appendix D5):

$$P_i = 0.5 \text{ Capability}_i + 0.5 \text{ Location}_i$$

$$P_i = 0.5 \times 0.25 + 0.5 \times 1$$

$$P_i = 0.5 \times 0.25 + 0.5 \times 1$$

$$P_i = 0.625$$

To compute the Exploitability Level (EL) for each asset per specific vulnerability, the IVLs already calculated (see Table 52; Table 100-Appendix D6) and the attacker's profile score must be considered using the following formula, analysed in Section 6.2.2.5:

$$EL_{vi} = w_1 IVL_v + w_2 P_i$$

where

$$w_1 = 0.7, w_2 = 0.3$$

As IVL refers to technical severity values of CVSS 3.1 [139] and the attacker's Profile refines operational feasibility, higher weighting is assigned to IVL for the specific Port Authority scenario. This is because IVL represents the intrinsic technical characteristics of the vulnerability, whereas the attacker profile acts as a contextual operational modifier influencing exploitation feasibility under specific attack conditions. Thereby,  $w_1=0.7$  ensures that exploitability remains primarily vulnerability-centric and  $w_2=0.3$  allows attacker-dependent adaptation without overwhelming technical severity.

The EL for each asset per specific vulnerability of Figure 48 is presented in Table 55, whereas the calculation analysis is provided in

Table 101 of Appendix D6.

Table 55. Exploitation Level (EL) calculation for each asset/vulnerability combination, according to the attacker's profile identified.

| Vulnerability   | Asset          | Exploitation Level (EL)<br>(Attacker's Capability = Low,<br>Attacker's Location = Network) |
|-----------------|----------------|--------------------------------------------------------------------------------------------|
| V <sub>1</sub>  | A <sub>1</sub> | EL <sub>V1</sub> = VH                                                                      |
| V <sub>3</sub>  | A <sub>1</sub> | EL <sub>V3</sub> = VH                                                                      |
| V <sub>4</sub>  | A <sub>2</sub> | EL <sub>V4</sub> = VH                                                                      |
| V <sub>5</sub>  | A <sub>2</sub> | EL <sub>V5</sub> = H                                                                       |
| V <sub>6</sub>  | A <sub>3</sub> | EL <sub>V6</sub> = M                                                                       |
| V <sub>7</sub>  | A <sub>3</sub> | EL <sub>V7</sub> = VH                                                                      |
| V <sub>8</sub>  | A <sub>3</sub> | EL <sub>V8</sub> = M                                                                       |
| V <sub>9</sub>  | A <sub>4</sub> | EL <sub>V9</sub> = VH                                                                      |
| V <sub>10</sub> | A <sub>4</sub> | EL <sub>V10</sub> = VH                                                                     |
| V <sub>11</sub> | A <sub>4</sub> | EL <sub>V11</sub> = VH                                                                     |
| V <sub>12</sub> | A <sub>5</sub> | EL <sub>V12</sub> = H                                                                      |
| V <sub>13</sub> | A <sub>5</sub> | EL <sub>V13</sub> = H                                                                      |

To estimate the EL per vulnerability, with respect to the analyzed IoC<sub>1</sub>, only vulnerabilities of the assets interconnected with the IoC<sub>1</sub>, namely, vulnerabilities of the Web Application and Operating System assets, are considered.

Considering the attacker's profile, identified in the current scenario, and the rationale with MAV and attacker's location explained in Section 6.2.2.4, vulnerability chains starting with a vulnerability of "Adjacent Network" or "Local" MAV attribute of CVSS 3.1 are excluded (according to the current scenario 4 vulnerability chains are excluded, i.e., V<sub>2</sub> → IoC<sub>1</sub> → V<sub>6</sub>, V<sub>2</sub> → IoC<sub>1</sub> → V<sub>7</sub>, V<sub>2</sub> → IoC<sub>1</sub> → V<sub>8</sub>, and V<sub>2</sub> → IoC<sub>1</sub>). Thus, from the 15 reconstructed potential attack paths, 11 potential attack paths are now included and depicted in Table 56 along with their corresponding evidence chains. From the ELs calculated previously in Table 55 per asset/vulnerability, the Exploitation Level Chains (ELCs) are created and depicted in Table 56. Considering the results of Table 55 and using the APEL formula, shown below and described in Section 6.2.2.5 **Error! Reference source not found.**, the Attack Path Exploitability Level quantitative value is calculated (see Table 56):

$$APEL = ELC_k = EL_{v_1} \times EL_{v_2} \times EL_{IOC_k} \times \dots \times EL_{v_n}$$

Then, the APEL is estimated in a qualitative value, according to the CyberICT propability scale (see Table 87 of Appendix D1), as presented in Table 56.

Table 56. The exploitability levels of the 11 potential attack paths is estimated according to the detected IoC1.

| Attack Paths                                           | Evidence Chains                         | Exploitation Level Chain (ELC)        | Attack Path Exploitability (APEL)  |                   |
|--------------------------------------------------------|-----------------------------------------|---------------------------------------|------------------------------------|-------------------|
|                                                        |                                         |                                       | Quantitative value                 | Qualitative value |
| $A_1, V_1 \rightarrow A_5, IoC_1 \rightarrow A_3, V_6$ | $V_1 \rightarrow IoC_1 \rightarrow V_6$ | $VH \rightarrow IoC_1 \rightarrow M$  | $0,89 \times 1 \times 0,50 = 0,45$ | <b>M</b>          |
| $A_1, V_1 \rightarrow A_5, IoC_1 \rightarrow A_3, V_7$ | $V_1 \rightarrow IoC_1 \rightarrow V_7$ | $VH \rightarrow IoC_1 \rightarrow VH$ | $0,89 \times 1 \times 0,89 = 0,79$ | <b>H</b>          |
| $A_1, V_1 \rightarrow A_5, IoC_1 \rightarrow A_3, V_8$ | $V_1 \rightarrow IoC_1 \rightarrow V_8$ | $VH \rightarrow IoC_1 \rightarrow M$  | $0,89 \times 1 \times 0,50 = 0,45$ | <b>M</b>          |
| $A_1, V_1 \rightarrow A_5, IoC_1$                      | $V_1 \rightarrow IoC_1$                 | $VH \rightarrow IoC_1$                | $0,89 \times 1 = 0,89$             | <b>VH</b>         |
| $A_5, IoC_1 \rightarrow A_3, V_6$                      | $IoC_1 \rightarrow V_6$                 | $IoC_1 \rightarrow M$                 | $1 \times 0,50 = 0,50$             | <b>M</b>          |
| $A_5, IoC_1 \rightarrow A_3, V_7$                      | $IoC_1 \rightarrow V_7$                 | $IoC_1 \rightarrow VH$                | $1 \times 0,89 = 0,89$             | <b>VH</b>         |
| $A_5, IoC_1 \rightarrow A_3, V_8$                      | $IoC_1 \rightarrow V_8$                 | $IoC_1 \rightarrow M$                 | $1 \times 0,50 = 0,50$             | <b>M</b>          |
| $A_1, V_3 \rightarrow A_5, IoC_1$                      | $V_3 \rightarrow IoC_1$                 | $VH \rightarrow IoC_1$                | $0,89 \times 1 = 0,89$             | <b>VH</b>         |
| $A_1, V_3 \rightarrow A_5, IoC_1 \rightarrow A_3, V_6$ | $V_3 \rightarrow IoC_1 \rightarrow V_6$ | $VH \rightarrow IoC_1 \rightarrow M$  | $0,89 \times 1 \times 0,50 = 0,45$ | <b>M</b>          |
| $A_1, V_3 \rightarrow A_5, IoC_1 \rightarrow A_3, V_7$ | $V_3 \rightarrow IoC_1 \rightarrow V_7$ | $VH \rightarrow IoC_1 \rightarrow VH$ | $0,89 \times 1 \times 0,89 = 0,79$ | <b>H</b>          |
| $A_1, V_3 \rightarrow A_5, IoC_1 \rightarrow A_3, V_8$ | $V_3 \rightarrow IoC_1 \rightarrow V_8$ | $VH \rightarrow IoC_1 \rightarrow M$  | $0,89 \times 1 \times 0,50 = 0,45$ | <b>M</b>          |

#### Step 4.2.4 CCMS - Prioritisation of Potential Attack Paths

Within this step, the 11 remaining attack paths are prioritised regarding their APEL with the worst case scenario, namely, from the highest probability to the lowest to occur (see Table 57).

Table 57. Attack Path prioritisation from highest to lowest exploitability.

| Attack Paths                                           | Evidence Chains                         | Exploitation Level Chain (ELC)        | Attack Path Exploitability (APEL)  |                   |
|--------------------------------------------------------|-----------------------------------------|---------------------------------------|------------------------------------|-------------------|
|                                                        |                                         |                                       | Quantitative value                 | Qualitative value |
| $A_1, V_1 \rightarrow A_5, IoC_1$                      | $V_1 \rightarrow IoC_1$                 | $VH \rightarrow IoC_1$                | $0,89 \times 1 = 0,89$             | <b>VH</b>         |
| $A_5, IoC_1 \rightarrow A_3, V_7$                      | $IoC_1 \rightarrow V_7$                 | $IoC_1 \rightarrow VH$                | $1 \times 0,89 = 0,89$             | <b>VH</b>         |
| $A_1, V_3 \rightarrow A_5, IoC_1$                      | $V_3 \rightarrow IoC_1$                 | $VH \rightarrow IoC_1$                | $0,89 \times 1 = 0,89$             | <b>VH</b>         |
| $A_1, V_1 \rightarrow A_5, IoC_1 \rightarrow A_3, V_7$ | $V_1 \rightarrow IoC_1 \rightarrow V_7$ | $VH \rightarrow IoC_1 \rightarrow VH$ | $0,89 \times 1 \times 0,89 = 0,79$ | <b>H</b>          |
| $A_1, V_3 \rightarrow A_5, IoC_1 \rightarrow A_3, V_7$ | $V_3 \rightarrow IoC_1 \rightarrow V_7$ | $VH \rightarrow IoC_1 \rightarrow VH$ | $0,89 \times 1 \times 0,89 = 0,79$ | <b>H</b>          |
| $A_5, IoC_1 \rightarrow A_3, V_6$                      | $IoC_1 \rightarrow V_6$                 | $IoC_1 \rightarrow M$                 | $1 \times 0,50 = 0,50$             | <b>M</b>          |
| $A_5, IoC_1 \rightarrow A_3, V_8$                      | $IoC_1 \rightarrow V_8$                 | $IoC_1 \rightarrow M$                 | $1 \times 0,50 = 0,50$             | <b>M</b>          |
| $A_1, V_1 \rightarrow A_5, IoC_1 \rightarrow A_3, V_6$ | $V_1 \rightarrow IoC_1 \rightarrow V_6$ | $VH \rightarrow IoC_1 \rightarrow M$  | $0,89 \times 1 \times 0,50 = 0,45$ | <b>M</b>          |
| $A_1, V_1 \rightarrow A_5, IoC_1 \rightarrow A_3, V_8$ | $V_1 \rightarrow IoC_1 \rightarrow V_8$ | $VH \rightarrow IoC_1 \rightarrow M$  | $0,89 \times 1 \times 0,50 = 0,45$ | <b>M</b>          |
| $A_1, V_3 \rightarrow A_5, IoC_1 \rightarrow A_3, V_6$ | $V_3 \rightarrow IoC_1 \rightarrow V_6$ | $VH \rightarrow IoC_1 \rightarrow M$  | $0,89 \times 1 \times 0,50 = 0,45$ | <b>M</b>          |
| $A_1, V_3 \rightarrow A_5, IoC_1 \rightarrow A_3, V_8$ | $V_3 \rightarrow IoC_1 \rightarrow V_8$ | $VH \rightarrow IoC_1 \rightarrow M$  | $0,89 \times 1 \times 0,50 = 0,45$ | <b>M</b>          |

#### Step 4.2.5 CCMS - Pruning Process Activation



Considering that, in the current scenario, the attacker's capability is classified as "Low", and according to the attacker's exploitation capacity defined in Table 36, the adversary is only capable of executing attack paths composed of vulnerabilities with higher exploitability levels. Therefore, in the Port Authority scenario, only attack paths with High (H) or Very High (VH) Attack Path Exploitability Levels (APELs) are considered feasible for the attacker. In this vein, after reviewing Table 57, only 5 out of 11 potential attack paths are considered as *credible evidence chains*.

Table 58. Credible Evidence Chains of the current Port Authority scenario.

| Attack Paths                                           | Evidence Chains                         | Exploitation Level Chain (ELC)        | Attack Path Exploitability (APEL)  |                   |
|--------------------------------------------------------|-----------------------------------------|---------------------------------------|------------------------------------|-------------------|
|                                                        |                                         |                                       | Quantitative value                 | Qualitative value |
| $A_1, V_1 \rightarrow A_5, IoC_1$                      | $V_1 \rightarrow IoC_1$                 | $VH \rightarrow IoC_1$                | $0,89 \times 1 = 0,89$             | <b>VH</b>         |
| $A_5, IoC_1 \rightarrow A_3, V_7$                      | $IoC_1 \rightarrow V_7$                 | $IoC_1 \rightarrow VH$                | $1 \times 0,89 = 0,89$             | <b>VH</b>         |
| $A_1, V_3 \rightarrow A_5, IoC_1$                      | $V_3 \rightarrow IoC_1$                 | $VH \rightarrow IoC_1$                | $0,89 \times 1 = 0,89$             | <b>VH</b>         |
| $A_1, V_1 \rightarrow A_5, IoC_1 \rightarrow A_3, V_7$ | $V_1 \rightarrow IoC_1 \rightarrow V_7$ | $VH \rightarrow IoC_1 \rightarrow VH$ | $0,89 \times 1 \times 0,89 = 0,79$ | <b>H</b>          |
| $A_1, V_3 \rightarrow A_5, IoC_1 \rightarrow A_3, V_7$ | $V_3 \rightarrow IoC_1 \rightarrow V_7$ | $VH \rightarrow IoC_1 \rightarrow VH$ | $0,89 \times 1 \times 0,89 = 0,79$ | <b>H</b>          |

Figure 51 reflects the final results from the application of the proposed approach to the current threat scenario of the Cargo Transportation Service. Five Evidence Chains are generated colored in green, blue, light blue, purple and orange to show how the attacker could have moved inside the network:

- Option a: The attacker used the Standard Cargo Manifest Web Application (entry point) to reach the PCS Database Server (target point) by exploiting the corresponding vulnerabilities ( $V_1 \rightarrow IoC_1, V_3 \rightarrow IoC_1$ );
- Option b: The attacker used the Standard Cargo Manifest Web Application as an entry point to reach the PCS Database Operating System (target point) by exploiting the corresponding vulnerabilities ( $V_1 \rightarrow IoC_1 \rightarrow V_7, V_1 \rightarrow IoC_1 \rightarrow V_7$ );
- Option c: The attacker used the PCS Database Server (entry point) to reach the PCS Operating System (target point) by exploiting the corresponding vulnerabilities ( $IoC_1 \rightarrow V_7$ ).

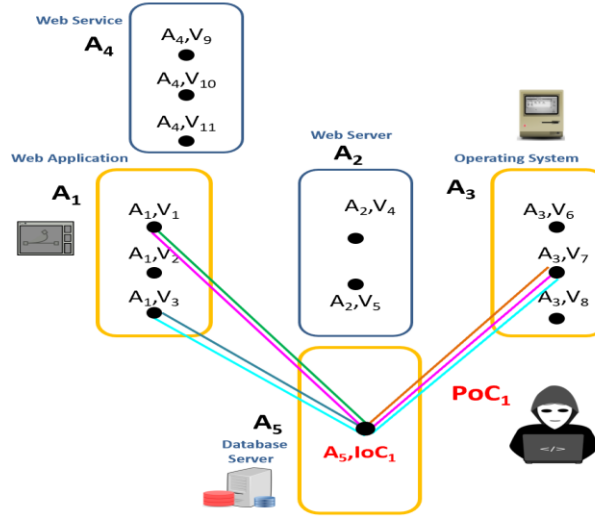


Figure 51. The Credible Evidence Chains of the General Cargo Transportation scenario.

## 6.5 Evaluation of the CyberICT Risk Management and risk ontology

The evaluation approach of the CyberICT Risk Management and the corresponding ontology is described in this section.

### 6.5.1 Questionnaire survey

Two questionnaire-based surveys, presented in this section, were conducted to evaluate the risk management platform, described in Section 6.3. As the design of many platform services and functionalities was driven by the proposed CyberICT Risk Management Methodology, the platform evaluation also provided indirect evidence regarding the methodology. Consequently, this section presents only the results of the questionnaires items that specifically assessed methodological aspects. The evaluation activities included the organisation of pilot testing sessions, hands-on training, and structured evaluation procedures involving ICT stakeholders. The resulting stakeholder feedback constitutes a complementary evaluation mechanism alongside the analytical case studies, proof-of-concept demonstrations, and real-world applications presented in this dissertation.

#### 6.5.1.1 Evaluation objectives and participants

The Questionnaire survey aimed to evaluate the research risk management platform in the context of the EU H2020 project MITIGATE [382] activities (see Section 6.3). Internal and external tests were conducted for a period of 15 months, which were divided into two phases and carried out simultaneously in four European countries. During the internal phase, the system and its services were initially evaluated by port operators. In the external phase, the system was demonstrated to external professionals, experts from Transport and Logistics enterprises and security consultants, who evaluated the platform and its corresponding services. Their comments and suggestions have been collected. The feedback and experience gained were communicated to the technical team to elaborate on improvements where possible.

The test sites reported in total the involvement of 235 internal and 452 external participants, mostly representatives from maritime, transport and logistics sectors.

The questionnaire results reported in sections 6.5.1.3 and 6.5.1.4, were derived from two surveys conducted during this period. During the evaluation process, pilot end-users conducted an evaluation from a technical, technological, usability and business perspective. Specifically, the first survey was related to more technical and UI/UX characteristics, whereas the second survey mostly concerned evaluating business aspects. The first survey involved 70 respondents in total, whereas the second survey involved 113 respondents in total.

The pilot operations were organised and coordinated by maritime and logistics stakeholders, including, additionally, IT vendors, research centres, and business initiators to satisfy technical support and business consultancy requirements.

#### 6.5.1.2 Structure of the questionnaires utilised

The evaluation was conducted through predefined online questionnaires.

##### **First Questionnaire survey**

The questionnaire is divided into the distinguished units shown in Table 59 to mostly address the creation of the supply chain service and its components, according to the methodology and the identification of threats and vulnerabilities. Respondents provided their assessment using a five-point Likert scale: A. Very Easy, B. Easy, C. Difficult to understand, D. Complex, and E. Very difficult. The units, depicted in Table 59, incorporate only the questions which are related to the aspects of the CyberICT Risk Management Methodology, including the creation of an ICT supply chain service, an ICT process, the association of business partners in a process, asset creation and management in a process, and vulnerability and threat identification and management on assets.

Table 59. Questionnaire utilised in the survey.

| Unit                                                      | Question                                                                                                                                                                                                                                                                     |
|-----------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Unit 2: Business Process analysis                         | Q1. How easy was to create a new Supply Chain Service?<br>Q2. How easy is to edit an existing Supply Chain Service?<br>Q3. How easy is to declare a process for a specific Supply Chain Services?<br>Q4. How easy is to edit a process for a specific Supply Chain Services? |
| Unit 3: Business partners and participants identification | Q1. How easy is to associate a business partner to a given process?<br>Q2. How easy is to confirm the involvement of a business partner to a given process?<br>Q3. How easy is to review the Business Partners involved in a defined SCS process?                            |
| Unit 4: Business Partners Infrastructure                  | Q1. How easy is to declare the assets associated with a process?<br>Q2. How easy is to explore the assets associated with the process?                                                                                                                                       |

|                                                          |                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Unit 5: Assets analysis and vulnerabilities              | Q1. How easy is to edit an asset?<br>Q2. How easy is to declare a new Vendor?<br>Q3. How easy is to declare a new vulnerability?<br>Q4. How easy is the editing of published vulnerabilities?<br>Q5. How easy is the browsing of published vulnerabilities?<br>Q6. How easy is to explore the Asset Related Information (e.g. Vulnerabilities)? |
| Unit 6: Assets interdependencies                         | Q1. How easy is to declare a new network?<br>Q2. How easy is to manage the list of Asset Networks?                                                                                                                                                                                                                                              |
| Unit 7: Supply Chain Service Cyber Threat Identification | Q1. How easy is to declare a new threat?<br>Q2. How easy is to manage the list of the declared threats?<br>Q3. How easy is the association of an asset with a threat profile?<br>Q4. How easy is to manage the list of threats applied to an asset?                                                                                             |

## Second Questionnaire survey

The second non-technical questionnaire, included aspects related to usability, efficiency and effectiveness of the system and its methodology. The questionnaire was disseminated online, a sample question from the non-technical user questionnaire is shown in Figure 52.

**The MITIGATE system provides important decision support for improving the organizations risk situation. \***

Please choose only one of the following:

☐ strongly agree  
☐ agree  
☐ disagree  
☐ strongly disagree  
☐ I'm unable to answer this question.

Make a comment on your choice here:

Figure 52. Sample question of the second survey.

### 6.5.1.3 Evaluation Results from the first survey

The evaluation results are shown in the following figures. In total, 70 participants responded to the questionnaire. Information is expressed as average percentage values for every single question per unit.

Figure 53 shows that most respondents found it very easy to declare or edit a process for a specific ICT supply chain service.

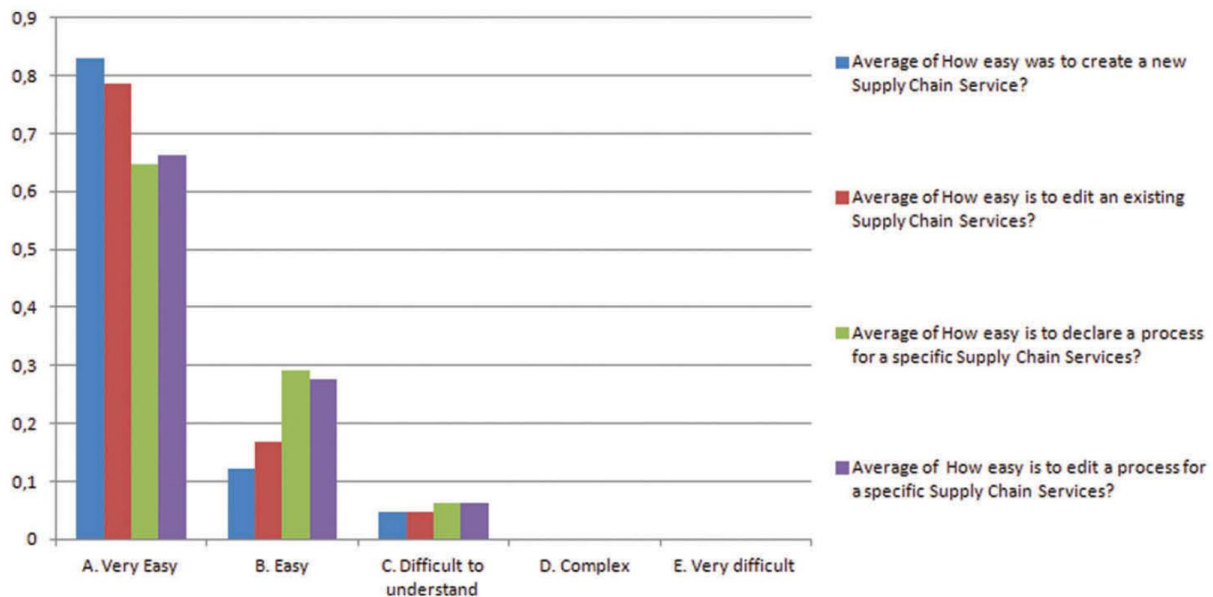


Figure 53. ICT process analysis capacity.

Figure 54 depicts the response on the capacity to identify business partners (left image of Figure 54) and declare assets in processes of the supply chain service (right image of Figure 54). It is shown that declaring assets is slightly easier than defining business partners, as the 23,08% and 24,61% of respondents have given a negative answer, respectively.

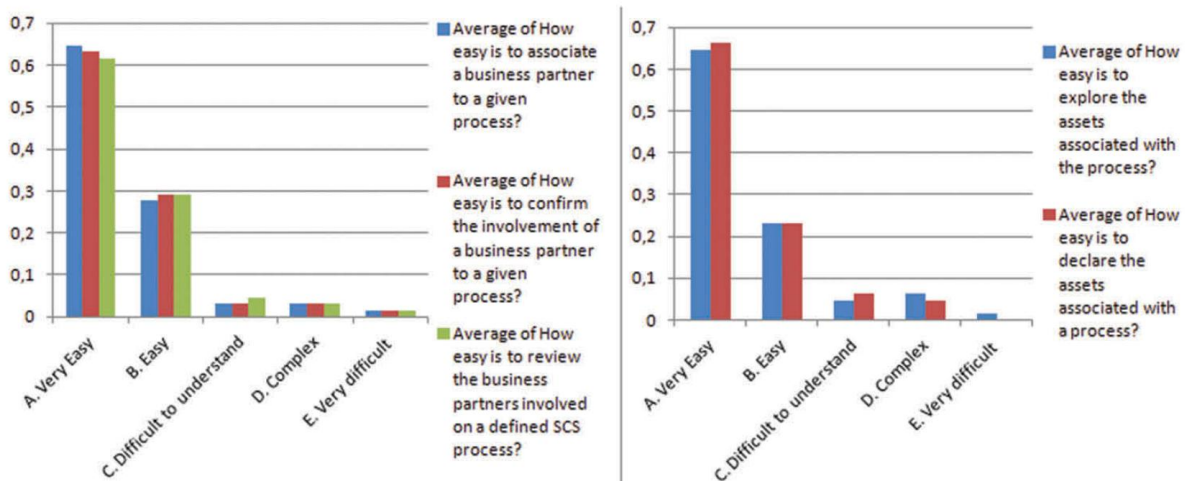


Figure 54. Business partners and participants' identification (left image) and business partners' infrastructure (right image).

Figure 55 displays the answers of the ability to edit vendors and vulnerabilities and associate them with assets. As presented in Figure 55, identifying vulnerabilities in assets, asset editing and asset browsing is slightly more difficult (approximately 27%) than managing networks and associating them with cyber-assets (approximately 29%).

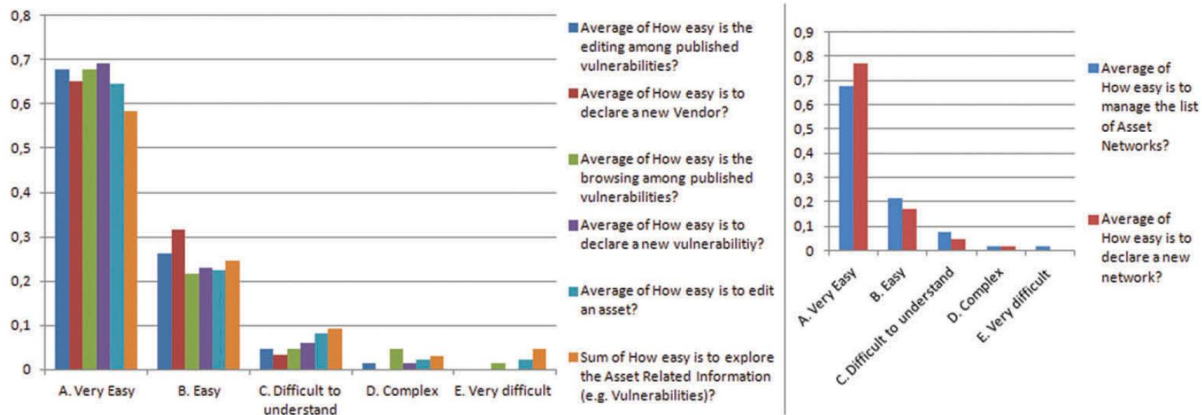


Figure 55. Analysis and vulnerabilities identification (left image) and assets' interdependencies declaration (right image).

Figure 56 shows threats identification. Declaring a new threat is the easiest task for almost 77%, though, associating an asset with a threat profiled is the hardest task, as 25% of people is the percentage of the most negative answer.

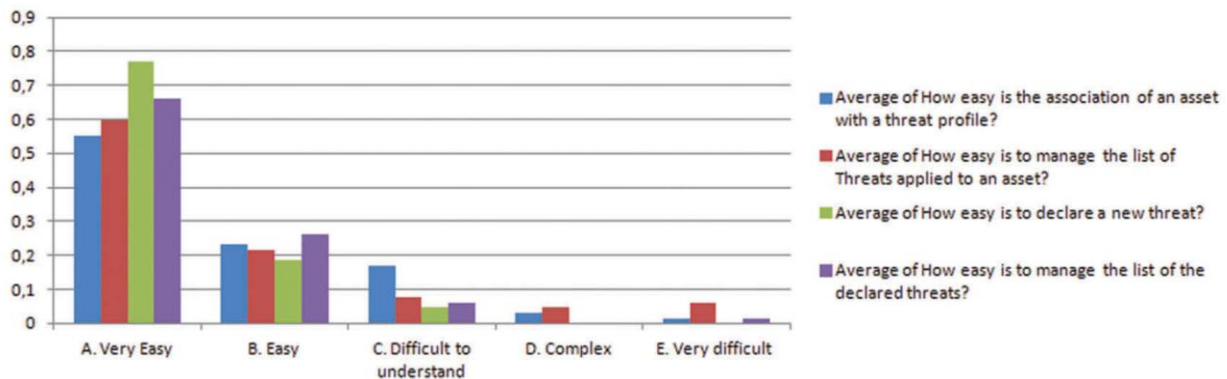


Figure 56. Threats' identification cyber assets.

Finally, Figure 57 shows the overall response from the evaluation of the methodology. Every unit is totally estimated on the average amount of its questions.

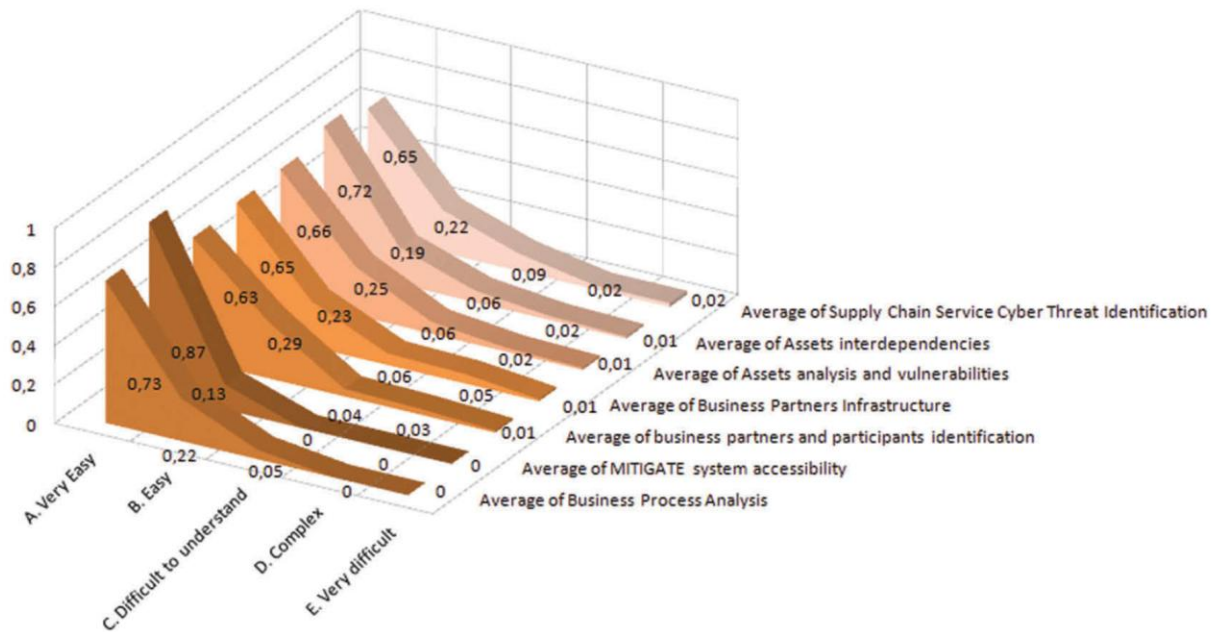


Figure 57. Overall evaluation results of the methodology.

#### 6.5.1.4 Evaluation Results from the second survey

Overall, 113 non-technical questionnaires have been collected. Eighteen (18) of the respondents had an IT background deriving from positions such as SCADA/EMS Operator, Senior Software Architect or Manager Network, Security and Infrastructure IT. At least 16 respondents can be assumed to have a security-related background, holding positions such as Port Facility Security Officer (PFSO), Chief Security Officer or Head of Safety and Security. In summary, 34 out of 113 have IT or Security related knowledge. Respondents answered questionnaires and provided their assessment using a 4-point Likert scale; A. Strongly disagree; B. Disagree; C. Agree; D. Strongly agree.

The respondents were asked whether the system fulfils its purpose **of mapping the general characteristics of the methodology**. In addition, they were asked if the system enables a collaborative approach for supply chain participants, and whether it provides convenient possibilities to exchange data (Figure 58) with other software. Most respondents agreed that the system can successfully exchange data, **satisfies the methodology-characteristics mapping and is easy to learn, enabling a collaborative approach for supply chain participants to take care of their Critical Infrastructure**.



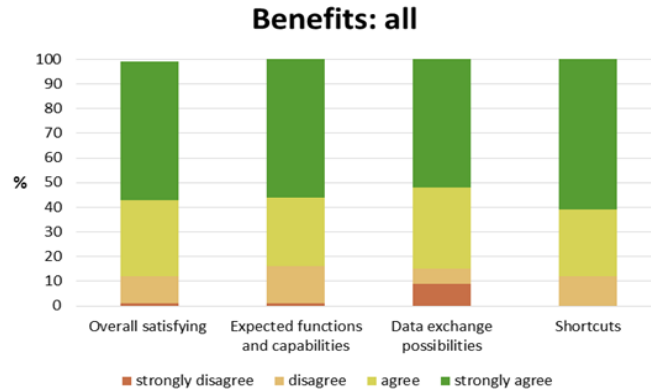


Figure 58. Overall impression of the respondents regarding the benefits of the MITIGATE security assessment services

The majority of the responders either strongly agreed (52%) or agreed (44%) that the system provides important decision support for improving the organisations' risk situation (Figure 59).

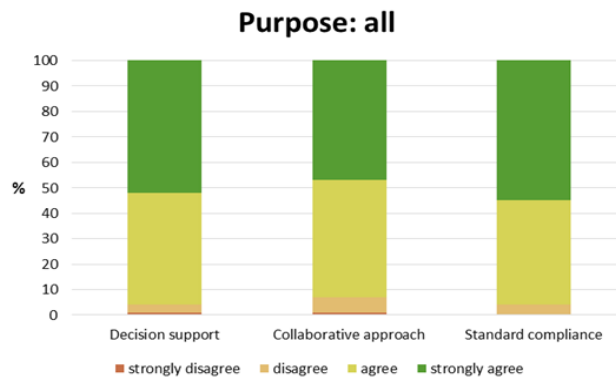


Figure 59. Overall impression of the respondents concerning the utilization of the MITIGATE system services.

Concerning the overall impression of the system utility, as shown in Figure 60: Over 78% of the test users responded positively that the required time for the risk assessment is reasonable, and over 87% of the test users implied that they felt comfortable using the-system, while 19% responded negatively that the system is easy to learn. Moreover, 64% strongly agreed and 23% agreed that the system can facilitate them in becoming more productive.

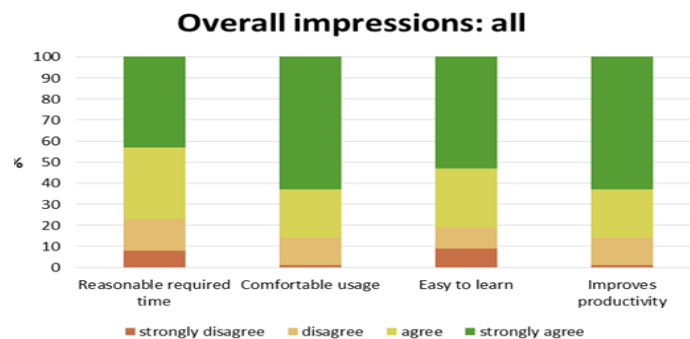


Figure 60. The impressions of the overall respondents for the system.



Apart from the multiple-choice responses, some respondents added useful comments and remarks regarding problems and barriers during the evaluation process. Specifically, respondents comment that the most important business issue is that a list of cyber assets is required to be manually registered, which is cost-consuming for a business partner. Nevertheless, an automated import method could be introduced. The option of adding metadata like a description or specification of supply chain service components would be very convenient. Besides, additional data like who the process owner or initiator is would be useful. These comments fostered the update of identifying the automated SBOM scanning approach to declare assets in a system apart from the CPE identifier approach (see product analysis in step 1 of Section 6.2.2.2).

#### 6.5.1.5 Overall evaluation outcomes from the two surveys

The findings from both surveys were largely positive. In the first survey, the majority of respondents gave favourable responses to all questions that were indirectly associated with the CyberICT Risk Management Methodology, suggesting that the methodology is comprehensible and supports the effective creation and management of supply chain services, processes, and assets together with the identification of their interrelationships, vulnerabilities, and threats.

Regarding the second questionnaire survey, the majority of respondents (above 70%) showed user satisfaction with the methodology from aspects such as learnability, effectiveness, time to execute the steps and its collaborative activity. Some comments referred to further automating the identification of assets and were considered to enhance the asset analysis aspect of the methodology, which led to refining, respectively, the relevant system service.

### 6.5.2 CyberICT Risk Management Methodology against domain-specific issues

The current section describes the contribution of the proposed methodology compared to domain-specific issues identified for the Maritime and Logistics Supply Chain (MLoSC) (see Section 4.5.3.5).

The state-of-the-art security analysis provided in Chapter 4 showed that existing risk management policies insufficiently consider the composite nature of ICT-empowered infrastructures (i.e., SCADA and AIS systems) and forget to take into account the global supply chain interdependent environment to define the security processes. An effective risk assessment approach for ICT SCS, including complex infrastructures, such as SCADA systems, may reflect the characteristics presented in Section 4.5.3.5. Considering the recommendations on risk management for MLoSC infrastructures, the proposed methodology supports them, as follows:

- **Domain-specific recommendation #1: A structured body of cybersecurity knowledge using knowledge management practices can leverage organisational learning**

The CyberICT Risk Management Methodology utilises ontology models and rule-based mechanisms to elicit implicit knowledge, articulate, store it and externalise it to enhance organisational learning.

- **Domain-specific recommendation #2: Modelling and simulation techniques can facilitate the development of diverse real-world cyberattack scenarios and results interpretation.**

The CyberICT Risk Management Methodology uses knowledge management models (see Section 6.1.4) and recommends open-source intelligence techniques and social engineering to provide accurate and updated information for vulnerabilities and threats. Moreover, it provides a set of approaches to estimate attack paths in terms of cumulative and propagated vulnerabilities based on approaches described in Section 6.1.5 and develops the Attack Simulation and Evidence Chains Generation (ASECG) model, which estimates attack paths based on a confirmed security event.

- **Domain-specific recommendation #3: Risk assessment methods should provide rational decision and probabilistic-based techniques to scrutinise complex cyberattack scenarios.**

Regarding risk assessment methods on SCADA systems, few approaches provide system-asset analysis, vulnerabilities and countermeasures [222] (see Section 4.5.3.5). The proposed methodology applies a comprehensive and systematic asset-centric analysis in supply chain processes that defines assets' interdependencies, addresses vulnerabilities, threats, individual, cumulative and propagated risks and their cascading effects and indicates how to identify mitigation strategies and payoffs.

- **Domain-specific recommendation #4: Identify common or cross-border scenarios throughout national and regional limits.**

The ICT SCS scenarios demonstrated in Section 6.4 are real-life examples of the global supply chain which show the applicability of the methodology in cross-border environments and complex infrastructures, such as SCADA and AIS systems. The three evaluation aspects of the proposed methodology (business, holistic-technical, and sectorial) provide a thorough analysis of the ICT SCS, considering the supply chain complexity and infrastructure interdependencies and system-wide assessment.

- **Domain-specific recommendation #5: Be compliant with regulations and directives or international standards applying to the supply chain.**

The proposed methodology provides a standards-based harmonised hybrid evaluation framework based on international risk management standards and cybersecurity certification frameworks (i.e., ISO 27k, ISO 28k family standards and ISO/IEC 15408 [44], [59]) Common Criteria-based IT Evaluation; see Chapter 7).

- **Domain-specific recommendation #6: Introduce collaborative practices to facilitate the sharing and transfer of risk-related information across supply chain operators.**

The CyberICT Risk Management Methodology is based on a collaborative approach [371]-[372] engaging ICT stakeholders and business partners to cooperate in a process-wise approach to estimate threats, vulnerabilities and risks and their cascading effects across the ICT network and undertake mutually agreed security controls.

### 6.5.3 Analysis of CyberICT Risk Management Methodology calculation models

The research work in [323] illustrates the need for a well-defined definition of risk and its dependent factors (i.e., threat, vulnerability, and impact) in risk assessment approaches. Risk assessment approaches, often confuse the likelihood of a potential cyberattack with the likelihood of successfully exploiting a vulnerability [323]. The proposed methodology supports the assessment of potential attack paths without evidence of a confirmed intrusion, relying on pruning unreasonable attack paths following a set of rules based on the models [276], [370] described in Section 6.1.5. In addition, it develops the Attack Simulation and Evidence Chain Generation (ASECG) model (see Section 6.2.2.5) that estimates credible vulnerability chains upon a confirmed security event. The vulnerability exploitability and ASECG calculation models are analysed below, according to the following evaluation criteria: conceptual consistency, non-redundancy of variables, coherence with established standards (CVSS and NIST), logical behaviour under representative attack conditions and interpretability of the resulting scores.

The proposed methodology introduces dedicated vulnerability exploitability and impact calculation models that integrate technical vulnerability characteristics with attacker-source attributes. These models are analysed with respect to their conceptual completeness, internal consistency, and design rationale. The vulnerability exploitability calculation model combines technical vulnerability characteristics derived from CVSS with attacker-specific characteristics adapted from NIST SP 800-30, including capability, expertise, intention, motivation, interest, and operational location. From a conceptual perspective, CVSS exploitability metrics and NIST SP 800-30 threat-source characteristics both contribute to the exploitation complexity and attacker capability. However, CVSS evaluates the technical conditions required for successful exploitation, whereas NIST assesses attributes of the threat actor. Consequently, the variables are considered complementary rather than redundant. The combination of CVSS and NIST characteristics for the vulnerability exploitability calculation are explained in the following regarding the specific concerns mentioned above:

**Elimination of Additive Inflation.** Because the core formula relies on a linear addition (+), an advanced threat actor  $P_i \approx 0.93$  targeting an air-gapped system ( $MAV = 0.20$ ) from the internet would mathematically yield an artificially high exploitability score. The rule of a vulnerability exploitation is not applicable when it is known that an attacker is in a location not applicable to exploit concerning the MAV (see Table 98 of Appendix D5) acts as a hard logical constraint, dropping the score to exactly 0 when physical/logical boundaries cannot be breached.

**Preservation of Attacker's Profile quantisation.** By avoiding a fractional pivoting multiplier at the entry point, the model natively preserves the integrity of the semi-quantitative scales based on NIST attacker's characteristics (see Appendix D5), e.g., 0.93 for "Very High", 0.75 for "High", without dampening them prematurely.

**Clean Separation of Concerns.** This design enforces that the Exploitability Level ( $EL_v$ ) handles the technical gatekeeping at the perimeter, while any subsequent network lateral movement or pivoting is offloaded to the Modified Impact Subscore (MISS) via CVSS Scope metrics.

# PART V:

## PROTECTION PROFILE FOR ICT PRODUCTS

---

## 7. CyberICT Protection Profile

This section presents an evaluation approach for preparing ICT stakeholders and organisations to security compliance processes either required, according to existing regulation mandates, such as the Cyber Resilience Act (CRA) [11] or to meet cybersecurity certification requirements of the Cybersecurity Act (CSA) [13] and its recent proposal for Cybersecurity Act 2 (CSA 2) [49], considering the adoption of the only officially released Common Criteria-based European Cybersecurity Certification Scheme (Eucc) [14].

This CyberICT Protection Profile aims to help ICT stakeholders create the Protection Profile of composite ICT products, and it is driven by:

- The Protection Profile taxonomy (data model) of the Composite Target of Evaluation (PP<sub>CTOE</sub>)
- The Composite Target of Evaluation structure (CToE) for a given ICT product (CToE<sub>ICT Product</sub>) which is embedded in the Protection Profile taxonomy.

As explained in Chapter 5, the CyberICT hybrid evaluation framework of this dissertation incorporates the CyberICT Risk Management Methodology, presented in Chapter 6, and the current CyberICT Protection Profile. The CyberICT hybrid evaluation framework integrates risk and conformity assessments into a unified framework based on the enhanced security model, described in Section 2.2.2.

### 7.1 CyberICT Protection Profile preparation of composite ICT products

This section presents the building blocks of the proposed CyberICT Protection Profile for composite products (Section 7.1.1) and describes the evaluation approach (Section 7.1.2).

#### 7.1.1 Building Blocks

The foundational elements for the design of the CyberICT Protection Profile for composite ICT products are presented in this section.

##### 7.1.1.1 Scope and Objectives

The CyberICT Protection Profile preparation, as mentioned above, is to provide a holistic view of an end-to-end evaluation approach to help ICT stakeholders define measurable and actionable sets of security requirements and corresponding security controls to meet their security needs.

Considering the technical complexity of ICT products, as described in Chapter 3, and Section 6.2.2.2, the framework is designed to evaluate composite ICT products that can be decomposed into their constituent ICT assets. The CyberICT Protection Profile further addresses the following lower-level objectives, which rely on the global Dissertation Objectives #1 and #2, specified in Section 5.1:

- Provide a dual-use evaluation mechanism that ICT stakeholders can use to define the protection profile (PP) of composite ICT products and self- or third-party assessors can use to examine whether the security requirements of an adopted cybersecurity certification schema are satisfied.
- Guide ICT stakeholders to identify a measurable and actionable set of security requirements and apply effective controls. This will also facilitate the ICT stakeholders managing their cybersecurity risks and implementing effective countermeasures that establish efficient defence strategies.
- Guide ICT stakeholders to prepare the documentation required for supporting the claims of the Protection Profile of composite ICT products.
- Support a cybersecurity and privacy evaluation approach of different types of evaluations, including
  - Self-assessment when a non-rigorous and deep evaluation is needed for an ICT product security compliance (no cybersecurity certification purpose) or when the procedure aims just to prepare and train the ICT stakeholder for the actual cybersecurity certification evaluation, which adopts the EUCC.
  - Third-party assessment, where an independent accredited entity, a Conformity Assessment Body (CAB) performs the assessment either for reaching compliance with the CRA or cybersecurity certification requirements based on the EUCC
- Apply to different levels of assurance which determine the rigor and depth of the vulnerability analysis and the evaluation conditions.
- Bring together practices from diverse research fields, such as risk assessment, conformity assessment and cybersecurity certification evaluation mechanism.
- Comply with standards relevant to risk assessment, conformity assessment, and security resilience (i.e., ISO 28000 [70], [59], ISO/IEC 27001 [55], ISO/IEC 15048 [44], and ISO/IEC 18045 [59] standards).
- Enhance cybersecurity certification and compliance knowledge.
- Assess the security and resilience of ICT products, and their ICT Supply Chain Services (ICT SCS).
- Contribute to the implementation of EU regulations, such as CRA [11], CSA [13], NIS 2 Directive [12] and GDPR [161].
- Identify interrelations of existing security classifications and aggregates best practices for developing a Composite ToE and its respective Protection Profile of complex ICT products and their embedded elements.
- Guide to develop a Protection Profile of different types of composite ICT products.

#### 7.1.1.2 Regulatory Background, standards and best practices

CyberICT Protection Profile preparation approach relies on the ICT product, ICT service, ICT process and ICT supply chain definitions of the EU CSA regulation [13] and its recent CSA 2 proposal [49]. It adopts the concepts of Common Criteria evaluation and security assurance of ISO/IEC 15408 [44]–[46] that establish the evaluation criteria. It is related to ISO/IEC 18045 [59], which outlines the mandatory actions and procedures that independent, accredited testing labs

must follow to evaluate the ICT product against the ISO/IEC 15408 requirements. The CyberICT Protection Profile preparation adopts the European Cybersecurity Certification Scheme (EUCC) and the structure of its elements, regulated by the Commission Implementing Regulation (EU) 2024/482 EUCC [14]. Furthermore, for the criticality of Products with Digital Elements (PDEs), the CRA's PDEs classification classes [11] are considered (see Section 6.2.2.2)

The requirements for the evaluation of the claims of the Protection Profile by Testing and Calibration Laboratories and by the accredited authorised bodies (CABs) are based on ISO/IEC 17025 [201] and ISO/IEC 17065 [204], respectively. Moreover, the generic concepts of the conformity assessment process rely on the ISO/IEC 17065.

#### 7.1.1.3 The CyberICT Risk Management Methodology

The CyberICT Risk Management Methodology is applied to assess the risk, threats, vulnerabilities and their cascading effects on ICT products (or PDEs) wherever required (see Chapter 6).

#### 7.1.1.4 Protection Profile for Composite ICT Products taxonomies

The Protection Profile for Composite ICT products taxonomy embeds the following data models, as defined in Section 7.2:

- The Composite Target of Evaluation (CToE) structure for ICT products
- A security classification supporting elements of the Protection Profile (i.e, threat categories, security objectives, security functional requirements and security controls.

#### 7.1.1.5 Users of the CyberICT Protection Profile

The CyberICT Protection Profile for composite products is primarily used by ICT Product Owners, ICT Manufacturers, ICT Vendors, ICT Service Providers, IT Security Experts, Risk Assessors, Users of Certificates, Auditors, Testing Laboratories, Pentesters, DevSecOps Engineers, and Conformity Assessors.

It can be adopted by organisations of any type or size—SMEs, microenterprises, military/ defence, governmental agencies, and academic or research institutions—that manufacture, commercialise, or use products in any CRA [11] class with priority determined by its class hierarchy (Class II, Class I, Default Class).

For assessments aimed at EUCC [14] cybersecurity certification [13], primary users are those whose products are evaluated at higher Common Criteria Assurance Levels (EAL 4+), while other users may have secondary interest in reaching the cybersecurity certification requirements. The approach also benefits additional ICT stakeholders, such as policymakers, and standardisation bodies.

### 7.1.2 CyberICT Protection Profile preparation of composite ICT products

Section 7.1.2.1 provides an overview of the CyberICT Protection Profile, whereas Section 7.1.2.2 analyses the steps of the approach.

#### 7.1.2.1 Overview of the CyberICT Protection Profile preparatory framework

The CyberICT Protection Profile preparatory framework is divided into 8 high-level steps, as depicted in Figure 61. The hybrid evaluation framework of this dissertation is depicted in Figure 61. The methodology structural template of Table 11 in Chapter 6 is provided to present the steps of the approach.

The evaluation approach engages three main actors:

- the ICT Product Owner (or CToE Owner) who initiates the assessment of the ICT product's compliance
- the Risk Assessor who conducts the risk assessment of the ICT product (it can be the same entity with the ICT Product Owner)
- the Conformity Assessor who is requested to conduct the Conformity Assessment upon completion of the Composite Protection Profile of the ICT Product.



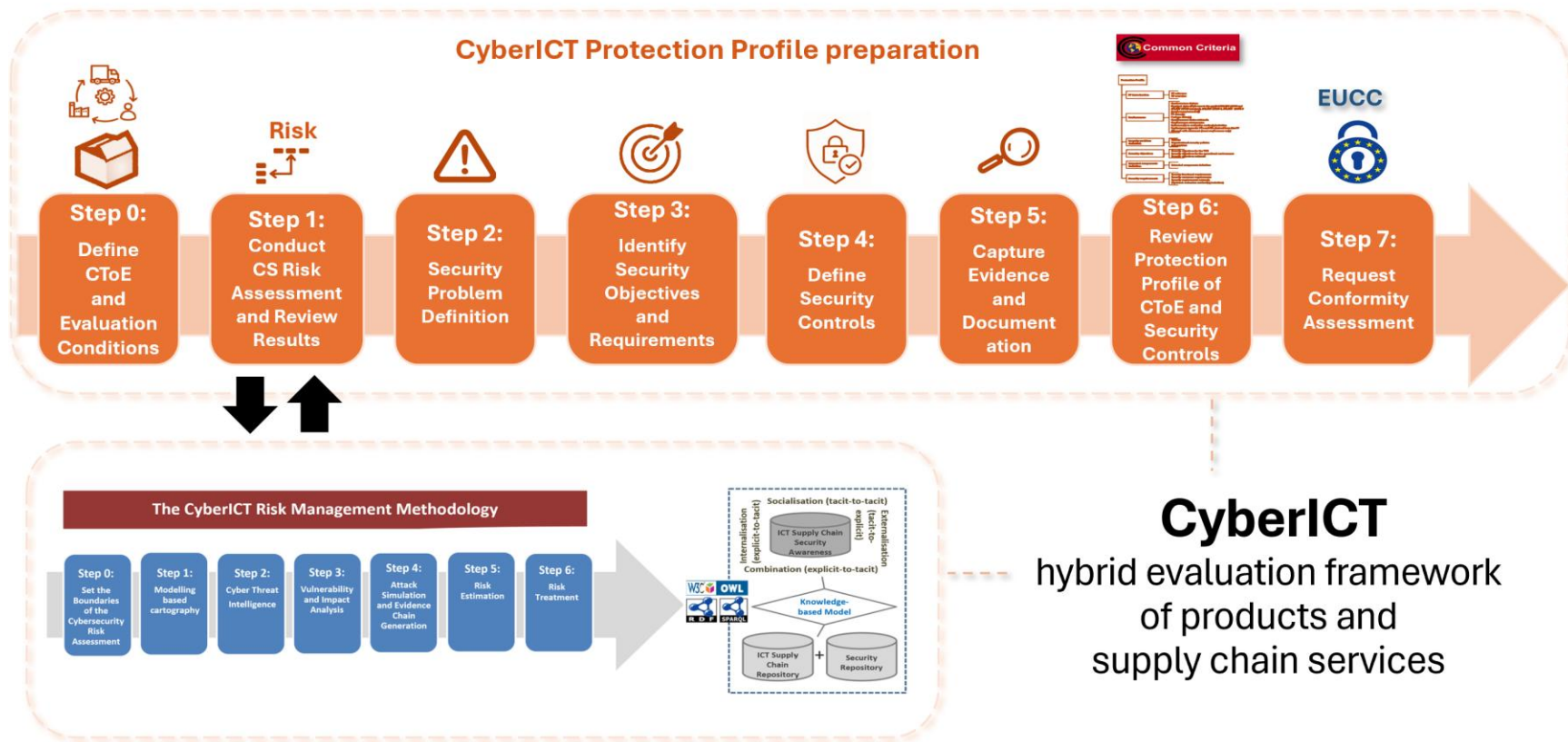


Figure 61. The CyberICT hybrid valuation framework embedding the Risk Management Methodology and the Protection Profile preparatory framework.

### 7.1.2.2 Composite Protection Profile Preparation analysis

This section analyses the steps of the CyberICT Protection Profile preparatory framework.

#### Step 0. Define the CToE and Evaluation Conditions

In this initial step the ICT product or the parts of the ICT product that will be subject of evaluation are considered as the Composite Target of Evaluation (CToE). Evaluation boundaries, the CToE and its embedded assets are characterised. In case a more rigor and deep analysis is needed and a higher Evaluation Assurance Level is adopted (EAL4+), the ICT Product Owner can analyse and assess the ICT products, supply chain service(s). For instance, for the mobile client product the shipping supply chain service of the product may be analysed.

Table 60. Define the CToE and Evaluation Conditions.

| <b>Step 0. Define the CToE and Evaluation Conditions</b><br>Step 0.1 Set the Boundaries of the Evaluation<br>Step 0.2 ICT product analysis into its main elements<br>Step 0.3 Composite Target of Evaluation creation |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Input</b>                                                                                                                                                                                                          | The ICT product to be evaluated (CToE)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Activity</b>                                                                                                                                                                                                       | <p><b>Step 0.1: The perimeter of evaluation is defined.</b> The CToE and the Common Criteria Evaluation Assurance Level that will be selected for the current evaluation (Level of Assurance to be achieved (grounds of confidence). How rigor and deep will be the evaluation, depends on the ICT product's criticality</p> <p>The CToE owner selects an EAL from the 7-level Common Criteria framework to define evaluation boundaries. The choice depends on the CToE's criticality and intended use—for example, <b>EAL4+</b> is used for high-security systems like smartcards and encryption mechanisms or a configured operating system by a governmental agency (cf. EUCC Implementing Regulation (EU) 2024/482, Annex I). Typical use cases vary by EAL level.</p> <p><b>Step 0.2 ICT product analysis into its main elements.</b> The aim of this step is to identify the evaluation boundaries, by defining the CToE, its primary assets following the CPE identifier or SBOM approach, presented in Step 1 of CyberICT Risk Management Methodology.</p> <p><b>Step 0.3 Composite Target of Evaluation creation.</b></p> <p>Upon selecting the CC EAL, additional evaluation conditions, such as the EUCC certificate level and the depth of vulnerability analysis that shall be conducted (CC AVA Assurance Class) are presented automatically through mapping procedures (see Table 102. The CToE Owner identifies CToE specific characteristics,i.e, a brief description of the CToE including details, CToE usage, etc, according to the CToE structure (see Section 1567.2.1).</p> |
| <b>Output</b>                                                                                                                                                                                                         | Step 0.1: Evaluation boundaries, Step 0.2: list of CPE assets or SBOMs, Step0.3: CToE description and relevant details.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

|                |                                                                                                                                                                                                                                                                                                                                                              |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Example</b> | <p>Step 0.1: CToE Mobile Client, EAL: 3 – AVA.VAN:2 , Attack Potential: Basic, EUCC Assurance Level: Substantial</p> <p>Step 0.2: list of mobile assets or SBOMs , e.g., Asset 1: Mobile Web Server, Asset 2: Mobile Web Application, Asset 3: Mobile Operating System, 4.Mobile libraries (SBOM)</p> <p>Step0.3: CToE description and relevant details.</p> |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Table 61. Evaluation Assurance Assessment Scale.

| CC Evaluation Assurance Level (EAL) | Name                                     | Description                                                                                                                                                                                                                                                                           | Typical Use Case                                               |
|-------------------------------------|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|
| EAL1                                | Functionally Tested                      | <b>Basic</b> assurance through functional testing. Evaluates basic system documentation and operates on independent testing of specified security functions. Used when data risks are low.                                                                                            | Low-risk applications, general IT products.                    |
| EAL2                                | Structurally Tested                      | <b>Security features tested</b> at a more structured level, including <b>design review</b> . Requires design information, vulnerability searches, and developer testing results. Ideal for legacy systems or low-risk commercial software.                                            | Commercial security software (e.g., VPN, database).            |
| EAL3                                | Methodically Tested & Checked            | Security testing with a <b>formalized development process</b> and vulnerability assessment. Introduces systematic testing across the product's life cycle and configuration management. Commonly applied to general enterprise networks and systems.                                  | Network security appliances, enterprise software.              |
| EAL4                                | Methodically Designed, Tested & Reviewed | Includes <b>penetration testing</b> and <b>formalised design specifications</b> . The highest level commercially viable for retrofitted systems. Involves rigorous code inspection and detailed source engineering analysis. Standard for mainstream firewalls and operating systems. | Commercial security appliances, government-certified products. |
| EAL5                                | Semi-Formally                            | Advanced <b>formal design documentation</b> , <b>independent testing</b> , and <b>resistance to attacks</b> . The system must be explicitly                                                                                                                                           | Smartcards, banking security modules, cryptographic systems.   |

|      |                                        |                                                                                                                                                                                                                                                                                     |                                                                                            |
|------|----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
|      | Designed & Tested                      | architected for high security from inception. Employs semi-formal evidence and strict modular design analysis. Used for banking chips and smart cards.                                                                                                                              |                                                                                            |
| EAL6 | Semi-Formally Verified Design & Tested | Rigorous <b>security validation</b> , advanced penetration testing, and <b>formal verification</b> of design. Structured for high-protection environments containing highly sensitive assets. Demands comprehensive engineering verification to counteract advanced threat vectors. | High-security environments (e.g., military systems, high-assurance cryptographic systems). |
| EAL7 | Formally Verified Design & Tested      | <b>Highest level of assurance</b> , with <b>mathematical proofs</b> for security properties and advanced attack resistance. The maximum tier of assurance. Reserved for ultra-secure tactical or infrastructure components.                                                         | Defence-grade cryptographic systems, high-assurance hardware security modules.             |

### Step 1. Conduct Cybersecurity Risk Assessment on CToE's asset

In this initial step the ICT product (or a part of the ICT product) that will be subject of evaluation is considered as the Composite Target of Evaluation (CToE). Evaluation boundaries, the CToE and its embedded assets are characterised. In case the EAL is high and a more rigorous and deep analysis is needed, the ICT Product Owner can analyse and assess the ICT products, supply chain service. For instance, for the mobile client product if owned to a governmental agency, the shipping supply chain service of the product may be analysed, as described in CyberICT Risk Management methodology, Step 1.

Table 62. Conduct Cybersecurity Risk Assessment on CToE's assets and review the results.

| Step 1. Conduct Cybersecurity Risk Assessment |                                                                                                                                                                                                                                                                               |
|-----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Input</b>                                  | CToE and relevant asset analysis.                                                                                                                                                                                                                                             |
| <b>Activity</b>                               | The aim of the current step is to use assess threats, vulnerabilities and risks on the CToE's asset. The CToE Owner may use the Cyber ICT Risk Management Methodology to conduct the Risk Assessment. Upon completing the risk assessment the CToE Owner reviews the results. |
| <b>Output</b>                                 | List of threats, vulnerabilities, risks per asset and relevant details.                                                                                                                                                                                                       |
| <b>Example</b>                                | Mobile application vulnerabilities, threats and risks.                                                                                                                                                                                                                        |

### Step 2. Security Problem Definition

In this step, the CToE Owner selects the details to define the security problem for the CToE evaluation:

- Cyber threat categories
- Identification of Organisation's Security Policy (OSP)

- Identification of assumptions and further security considerations for the evaluation.

Table 63. Define the Security Problem.

| Step 2. Security Problem Definition |                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Input</b>                        | CToE risk assessment results.                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Activity</b>                     | The aim of the current step is to define the security problem of the evaluation. The Security problem definition is a Protection Profile element including cyber threat categories, OSPs and evaluation assumptions (optionally). The CToE Owner may consult the risk assessment results, provided by the Cyber ICT Risk Management methodology, to identify the threat categories that match to the current evaluation. |
| <b>Output</b>                       | List of threat categories, list of OSPs, list of assumptions (optionally)                                                                                                                                                                                                                                                                                                                                                |
| <b>Example</b>                      | Mobile threat categories: UnauthorisedAccess, Repudiation                                                                                                                                                                                                                                                                                                                                                                |

### Step 3. Identify Security Objectives and Security Requirements.

In this step the security objectives and security requirements are identified.

Table 64. Security objectives and security Requirements identification.

| Step 3. Identify Security Objectives and Requirements |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Input</b>                                          | Information from the security problem definition                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Activity</b>                                       | The CToE Owner reviews the information specified in the security problem. The CyberICT Protection Profile taxonomy embeds security classifications (see Apendix D7) that map the identified threats with related security objectives and security functional requirements (SFRs or extended SFRs see Section 7.2). The CToE Owner or Security Expert defines the security objectives and security requirements that will be considered in the current evaluation according to the ICT product configurations, etc. |
| <b>Output</b>                                         | Lists of assets mapped with threat categories, relevant security objectives and corresponding SFRs.                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Example</b>                                        | Asset 1: Mobile Web Application Security Objective: TOE.ACCESS<br>SFR1: FDP_ACC.1 (Access Control Policy), SFR2: FIA_ATD.1 (User Attribute Definition) (Threat category: UnauthorisedAccess)                                                                                                                                                                                                                                                                                                                       |

### Step 4. Define Security Controls.

In this step, the CToE Owner declares the security controls implemented for the specified security requirements.

Table 65. Define Security Controls.

| Step 4. Define Security Controls |                                                                                                                                                                                                                                                                                                                                   |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Input</b>                     | Asset mapping with threat category, relevant security objective, corresponding SFR.                                                                                                                                                                                                                                               |
| <b>Activity</b>                  | For each specified requirements the CToE Owner declares the security control(s) implemented and to which specific asset correspond. The selected security control are not included in the Protection Profile. They are given separately to the conformity assessor to review when assessing the claims of the Protection Profile. |
| <b>Output</b>                    | Lists of asset-requirement-security control statements.                                                                                                                                                                                                                                                                           |

|                |                                                                                                                                                                                                                                                                          |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Example</b> | Asset 1: Mobile Web Application – SFR1: FDP_ACC.1 (Access Control Policy) – AC-3 (Access Enforcement-Mandatory Access Control)<br>Asset 1: Mobile Web Application – SFR2: FIA_ATD.1 (User Attribute Definition) – IA-2 (Identification and Authentication (Mobile User)) |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Step 5. Capture Evidence and Documentation.

In this step, the CToE Owner collects all the evidence required to justify the security requirement-security control statements, defined in the previous step.

Table 66. Capture Evidence and Documentation.

| Step 5. Capture Evidence and Documentation |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Input</b>                               | Lists of asset-requirement-security control statements.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Activity</b>                            | The CToE Owner collects all the evidence to prove that the asset-requirement-security control statements, defined in the previous step are correct. The evidence can be multiple material, such as an asset documentation, the product manual, asset architecture, pentest results, result after using a security tool to test a code – e.g., dependency check testing or code linting test or secret scanning result. The output of this activity is not included in the Protection Profile. It is provided as an additional material to the conformity assessor to be considered for the Security Laboratory testing upon initiating a conformity assessment process after the Protection Profile is prepared. |
| <b>Output</b>                              | All evidence captured to justify the product's requirement-security control statements.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Example</b>                             | Mobile pentest results.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

### Step 6. Review Protection Profile and Security Controls.

The CToE Owner reviews the developed Protection Profile and the Security Controls before finalising the process.

Table 67. Review Protection Profile and Security Controls.

| Step 6 Define Security Controls |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Input</b>                    | CToE and relevant asset analysis.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Activity</b>                 | After defining all security controls and collecting all the required evidence to justify that the defined security requirements of the ICT product are satisfied, the CToE Owner reviews at last the created Protection Profile compared to the implemented security control. This can be an iterative procedure in case he/she detects that the implemented controls do not satisfy the identified requirements. In that case the CToE Owner reconsiders the adopted control policy and applies additional controls if needed until the requirements are satisfied. Correspondingly, reviews the evidence and in case it is incomplete, he/she adds additional material. This relies on the subjective opinion of the CToE Owner or the Security Experts that manages this activity. The final verdict will be determined by the conformity assessor (self-assessor if a certification process is not the case and the EAL is Low or CAB for a certification evaluation process and an upper EAL evaluation). |
| <b>Output</b>                   | All security requirements stated in the Protection Profile are satisfied by the defined security controls (upon CToE Owners opinion)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Example</b>                  | Mobile application vulnerabilities, threats and risks.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |



## Step 7. Request Conformity Assessment.

In this final step, the CToE Owner either conducts a self-conformity assessment or requests a third-party assessment by an authorised body (i.e., a CAB for the EUCC evaluation).

Table 68. Request Conformity Assessment.

| Step 7. Request Conformity Assessment |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Input</b>                          | Protection Profile of composite ICT product.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Activity</b>                       | Upon completing the Protection Profile of the CToE, the CToE Owner can request either for a third-party conformity assessment or for self-conformity assessment depending on the type of evaluation. In a EUCC certification evaluation procedure a third-party conformity assessment is required by an accredited body (CAB) no matter the level of Assurance adopted (EAL). For a conformity assessment to check compliance with the CRA requirements, a third party assessment by a notified party, such as a CAB and the EUCC evaluation approach described herein, is required for products of important Class II and conditionally for products of important class I. Otherwise, a self conformity assessment can be adopted. |
| <b>Output</b>                         | Protection Profile of composite ICT product assessed, assessor's verdict.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Example</b>                        | Mobile Client Protection Profile assessed by a CAB by adopting the EUCC scheme, Passed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

## 7.2 CyberICT Protection Profile Taxonomy for Composite Product

This section presents the Protection Profile taxonomy. The Protection Profile taxonomy of a composite ICT product is a data model that embeds the Composite Target of Evaluation structure (Section 7.2.1), which presents the ICT product or the part of the ICT product that is subject to evaluation. Moreover, the Protection Profile taxonomy (Section 7.2.2) embeds a security classification of Protection Profile elements.

### 7.2.1 Composite Target of Evaluation structure

The Composite Target of Evaluation (CToE) structure is based on aspects of the Common Criteria (CC) certification scheme [44]. The CToE provides a 3-level structure with the features presented in Table 69. The features marked with a star (\*) are mandatory, namely, the corresponding information is required to be provided. Features without a star (\*) are non-mandatory features, namely, the corresponding information may be optionally provided. The structure of the CToE is analysed below and an indicative example is given to illustrate its application.

Table 69. Composite Target of Evaluation (CToE).

| CToE 1 <sup>st</sup> level | CToE 2 <sup>nd</sup> level | CToE 3 <sup>rd</sup> level | Example                    |
|----------------------------|----------------------------|----------------------------|----------------------------|
| CToE Content *             | CToE Reference *           | CToE Name*                 | <i>Worskstation User A</i> |
|                            |                            | CToE ID*                   | <i>CToE_1</i>              |
|                            |                            | CToE Version*              | <i>v1.1</i>                |
|                            |                            | CToE Owner (Author)*       | <i>Product Owner_x</i>     |

|  |                                      |                                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | (Informative content of the CToE)    | The entity that created the CToE and acts as the representative in the process (Administrator)                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|  |                                      | CToE Product*                                                                                                                                                                                                                                                                              | A maritime company's workstation for user A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|  | CToE Overview *                      | CToE Description and usage*<br>(It describes the CToE and its embedded assets, the operational environment its intended use and clarifies whether a part of the ICT product is excluded from the evaluation. If additional documentation is provided to explain the CToE is referred here) | This workstation is used to connect the user through the navigation system application of the maritime company. The operational environment of the mobile connected with the navigation system is described in the "Architecture" file.                                                                                                                                                                                                                                                                                                                                                                                                                   |
|  |                                      | CToE Technical Details*<br>(The assets/building blocks composing the CToE and their technical characteristics, ie., CPE-defined assets or SBOMs)                                                                                                                                           | Asset 1: Mobile Database CPE:<br>pe:2.3:a:mariadb:mariadb:10.6.7<br>Asset 2: Management Server Jetty10,<br>SBOM: org.eclipse.jetty:jetty-bom:11.0.16<br>+--- org.eclipse.jetty:jetty-webapp:11.0.16 (c)<br>+--- org.eclipse.jetty:jetty-servlet:11.0.16 (c)<br>+--- org.eclipse.jetty:jetty-xml:11.0.16 (c)<br>+--- org.eclipse.jetty:jetty-security:11.0.16 (c)<br>+--- org.eclipse.jetty:jetty-util:11.0.16 (c)<br>+--- org.eclipse.jetty:jetty-server:11.0.16 (c)<br>+--- org.eclipse.jetty:jetty-http:11.0.16 (c)<br>+--- org.eclipse.jetty:jetty-io:11.0.16 (c)<br>Asset 3: Java Enterprise Application<br>cpe:2.3:a:eclipse:jetty:11.0.16:*:*:*:*:* |
|  |                                      | CToE asset interdependencies                                                                                                                                                                                                                                                               | The Java Enterprise Application is hosted by the Java Application Server Maria DB is connected with the Enterprise Application                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|  | Certification - related information* | Certification Status*<br>(Clarify whether a certification was given in the past and if so, provide its ID and duration of validity)                                                                                                                                                        | No certification was obtained in the past                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|  |                                      | Related standards and frameworks<br>(describe whether any standards apply in the CToE)                                                                                                                                                                                                     | ISO/IEC 27001                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|  |                                      | Cybersecurity certification scheme*<br>(The Certification scheme adopted in this evaluation)                                                                                                                                                                                               | Common Criteria based EUCC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |



## CToE elements structure

CToE Content\* (1<sup>st</sup> Level) mandatory element, including all features related to the CToE identification. CToE Content is further decomposed into the following lower level elements:

- CToE Reference\* (2<sup>nd</sup> Level)  
It includes the following elements (3<sup>rd</sup> level): CToE Name\*, CToE ID\*, CToE Version\*, CToE Owner (Author), CToE Product\*.
- CToE Overview\* (2<sup>nd</sup> Level)  
It includes the following elements (3<sup>rd</sup> level): CToE Description and usage\*, CToE technical details\*, CToE Asset interdependencies (defined according to step 1 of the CyberICT Risk Management Methodology)
- Certification-related information\* (2<sup>nd</sup> Level)  
It includes the following elements (3<sup>rd</sup> level): Certification status, Related standards and frameworks, Cybersecurity Certification Scheme

### 7.2.2 Protection Profile Taxonomy of Composite ICT Product

The CyberICT Protection Profile Taxonomy of Composite ICT product, depicted in Figure 62 is based on the Common Criteria [44]–[46] Protection Profile scheme.

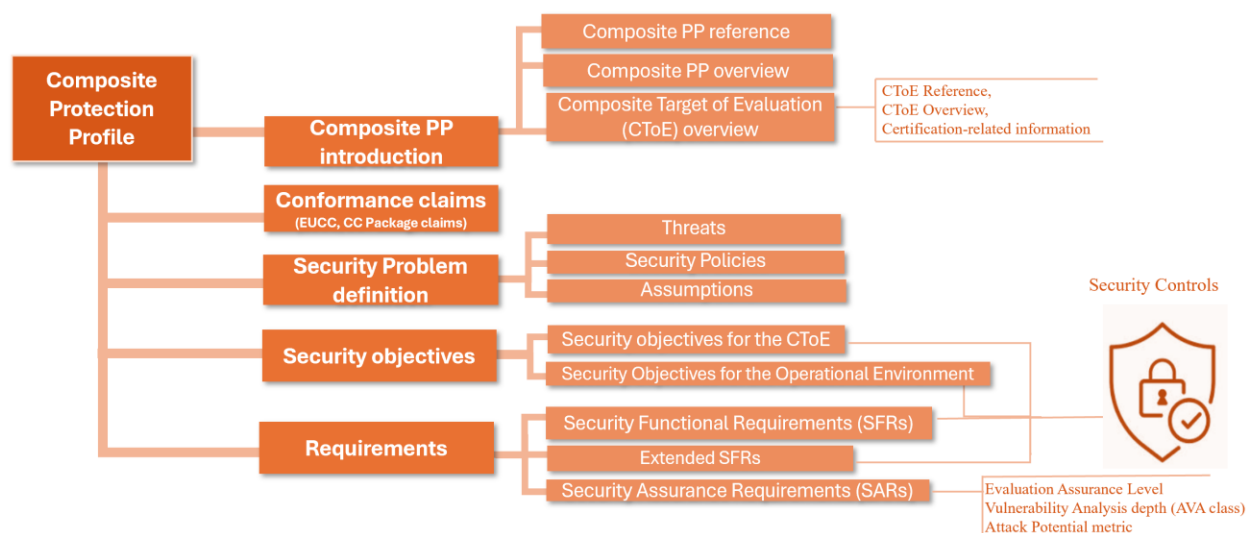


Figure 62. CyberICT Protection Profile for Composite Products.

The CyberICT Protection Profile incorporates the CToE structure, presented in Section 7.2.1.

The CyberICT Protection Profile taxonomy for composite ICT products considers a wide range of security objectives, the Common Criteria Security Functional Requirements (SFRs) [45] and several extended SFRs identified from approved Protection Profiles. The security objectives and the extended SFRs derived from prominent Protection Profile publications [384]–[394]. The Common Criteria SFRs and the extended SFRs are mapped with security and privacy controls of NIST SP 800-53 specification [125],[395]. A sample of the security classification that connects the

security functional requirements with security controls is depicted in Table 103 of Appendix D8, whereas the entire classification is found in [396].

The security objectives were mapped with the Common Criteria SFRs and the identified extended SFRs, according to the diverse technical specificities of ICT products they reflect, such for Operating System, application software, network devices and IoTs, databases, encryption modules and PKIs, VPNs, and Virtual Machines specificities. For example:

Table 70. Indicative relations between threats, security objectives, security requirements and security controls in diverse devices.

| <b>STRIDE Threat Categories</b> | <b>Security Objective</b>                                                                                            | <b>Device example</b>                                                                                                                          | <b>Security Functional Requirement (SFR) (CC or Extended)</b>       | <b>NIST Security Control</b>                       |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------|----------------------------------------------------|
| Elevation of Privilege          | OT.AUTHORIZED_USE                                                                                                    | 1. Privilege management in an Operating System<br>2. Encryption mechanism for electronic document                                              | FAU_GEN.1<br>(Security Audit Data Generation)                       | AU-3<br>(Content of Audit Records)                 |
| Information Disclosure          | OT.SECURE_COMMS<br>(To address both passive (eavesdropping) and active (packet modification) network attack threats) | 1. kernel networking stack protection in an operating System<br>2. end-to-end encryption in application,<br>3. VPN gateway in a network device | FIA_X509_EXT.1 (It defines the rules used to validate certificates) | IA-3<br>(Device Identification and Authentication) |

The classification of security objectives and SFRs is presented in Table 104.

To allow the ICT stakeholders easily define threats for the Security Problem Definition of the Protection Profile, the security objectives, presented in Table 104, are mapped with the threat categories of the widely known threat model of Microsoft “STRIDE” [260], presented in Table 105.

All these security classifications create a security taxonomy that interrelates product’s assets with threat categories, security objectives, security functional requirements and security controls. This security taxonomy is considered to identify the corresponding security concepts mentioned above in steps 2–4 of the CyberICT Protection Profile preparation.

The Protection Profile taxonomy and an indicative example to demonstrate its applicability is presented below. A detailed structure of the Protection Profile is presented in Table 71.

Table 71. CyberICT Protection Profile (PP) Taxonomy.

| PP 1 <sup>st</sup> level                | PP 2 <sup>nd</sup> level                                   | PP 3 <sup>rd</sup> level                       | Example                                                                                                                                                                                                                                                                  |
|-----------------------------------------|------------------------------------------------------------|------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Composite PP Intro*</b>              | <b>Composite PP Reference*</b>                             | Composite PP Name*                             | <i>Protection Profile Workstation A</i>                                                                                                                                                                                                                                  |
|                                         |                                                            | Composite PP ID*                               | <i>PW-A</i>                                                                                                                                                                                                                                                              |
|                                         |                                                            | Composite PP Version*                          | <i>v0.1</i>                                                                                                                                                                                                                                                              |
|                                         |                                                            | Composite PP Owner* (Author)                   | <i>Product Owner_x</i>                                                                                                                                                                                                                                                   |
|                                         |                                                            | Composite PP Publication Date*                 | <i>March 1, 2026</i>                                                                                                                                                                                                                                                     |
|                                         | <b>Composite PP Overview*</b>                              | -                                              | <i>The scope of PP WorkstationA is to describe the workstation and its assets connected to the Navigation System of the Maritime Company in terms of [CC] and to define functional and assurance requirements The current PP corresponds to CToE "Worsktation_UserA"</i> |
|                                         | <b>CToE Overview* / Certification-related information*</b> | <i>CToE as presented in Section 7.1.2.1</i>    | <i>CToE as presented in Section 7.1.2.1</i>                                                                                                                                                                                                                              |
| <b>Composite PP Conformance Claims*</b> | <b>EUCC Conformance claim*</b>                             | EUCC Assurance Level* (Basic/Substantial/High) | <i>Substantial</i>                                                                                                                                                                                                                                                       |
|                                         | <b>CC Conformance claim*</b>                               | -                                              | <i>Common Criteria Part I, Part II, Part III</i>                                                                                                                                                                                                                         |
|                                         | <b>CC Package claim*</b>                                   | EAL claim*                                     | <i>EAL 3</i>                                                                                                                                                                                                                                                             |
|                                         |                                                            | Assurance Package claim*                       | <i>AVA_COMP, AVA_Class</i>                                                                                                                                                                                                                                               |
|                                         |                                                            | Functional Package claim*                      | <i>FAU_STG</i>                                                                                                                                                                                                                                                           |
|                                         |                                                            | CC Package claim description*                  | <i>Assurance Package EAL3, follows AVA_VAN.2, Functional Requirements package extended</i>                                                                                                                                                                               |
|                                         | <b>PP Conformance claim*</b>                               | -                                              | <i>The "PP Workstation A" does not claim conformance to any PP.</i>                                                                                                                                                                                                      |
| <b>Security Problem Definition*</b>     | <b>Assumptions</b>                                         | Assumption ID                                  | <i>A.SECURE_SETTINGS</i>                                                                                                                                                                                                                                                 |
|                                         |                                                            | Assumption Description                         | <i>Administrators apply and maintain secure configuration settings</i>                                                                                                                                                                                                   |
|                                         | <b>Organisational Security Policies*</b>                   | Policy ID*                                     | <i>OSP.1</i>                                                                                                                                                                                                                                                             |
|                                         |                                                            | Policy ID Description                          | <i>The authorised users of the CToE shall be held accountable for their actions within the CToE.</i>                                                                                                                                                                     |
|                                         | <b>Threat Categories*</b>                                  | Description* (STRIDE)                          | <i>Denial of Service, InformationDisclosure</i>                                                                                                                                                                                                                          |
|                                         |                                                            | Security Objective ID*                         | <i>OT.AUDIT_LOSS_RESPONSE, OT.KEY_ESCROW</i>                                                                                                                                                                                                                             |

|                                     |                                                           |                                                                           |                                                                                                                                                                                                                               |
|-------------------------------------|-----------------------------------------------------------|---------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Security Objectives*                | Security Objectives for the CToE*                         | Security Objective Description*                                           | OT.AUDIT_LOSS_RESPONSE<br>:The TOE will respond to possible loss of audit records when audit trail storage is full or nearly full by alerting administrators and inviting them to save audit files.                           |
|                                     | Security Objectives for the CToE Operational Environment* | Security Objective ID*                                                    | OE.REQUIRE_AUTH                                                                                                                                                                                                               |
|                                     |                                                           | Security Objective Description*                                           | The operational environment will protect assets in a manner that requires authentication commensurate with the sensitivity of the assets.                                                                                     |
| Security Controls*<br>(NIST 800-30) | Security Control ID*                                      | -                                                                         | SC-13, AU-5(2)                                                                                                                                                                                                                |
|                                     | Security Control Family Name*                             | -                                                                         | Cryptographic Protection, Response To Audit Processing Failures-Real-Time Alerts                                                                                                                                              |
|                                     | Security Control Description*                             | -                                                                         | Conformant TOE has the ability to perform either symmetric encryption and decryption or cryptographic hashing or keyed-hash message authentication or cryptographic signing using NSA-approved and FIPS-validated algorithms. |
| Security Requirements*              | Security Functional Requirements (SFRs)*                  | SFR ID Details* (SFR ID/ Name/ Description/ Family/ Class)                | FAU_STG.3 (Security Audit Data Storage, Protected Audit Trail Storage), FCS_CKM.1 (Cryptographic Key Management-Cryptographic Key Generation)                                                                                 |
|                                     |                                                           | SFR Dependencies* (Direct/ Indirect/Hierarchical)                         | FAU_STG.3: Direct: FAU_GEN.1, FTP_ITC.1, Indirect: FPT_STM.1                                                                                                                                                                  |
|                                     |                                                           | Extended SFRs Details (Extended SFR ID/ Name/ Description/ Family/ Class) | FTA_TAH_EXT.1 (CToE Access information )/FMT_SMF_EXT.1 (Specification of Management Functions)                                                                                                                                |
|                                     |                                                           | Extended SFR Dependencies                                                 | FTA_TAH_EXT.1: FTA_TAH_EXT.1: FTA_TAH.1                                                                                                                                                                                       |
|                                     | Security Assurance Requirements (SARs)*                   | Composite CC EAL*(EAL1/ EAL2/ EAL3/ EAL4/ EAL5/ EAL6/ EAL7)               | EAL3                                                                                                                                                                                                                          |
|                                     |                                                           | Attack Potential Level* (Basic/ Enhanced Basic/ Moderate/ High)           | Basic                                                                                                                                                                                                                         |
|                                     |                                                           | SAR Details* (SAR ID/ Name/ Description/ Family/ Class)                   | AVA_COMP.1                                                                                                                                                                                                                    |
|                                     |                                                           |                                                                           |                                                                                                                                                                                                                               |
| Extended Package                    | Extended Components                                       | Description                                                               | The extended Family FTA_TAH ToE Access History defines requirements for the TSF to display to a user (a history of successful and unsuccessful attempts to access the user's account).                                        |

The elements marked with a star (\*) are mandatory, whereas elements without a star (\*) are non-mandatory elements.

### **Composite PP Intro**

- Composite PP Reference\* (2<sup>nd</sup> Level)  
It includes the following elements (3<sup>rd</sup> level): Composite PP ID\*, Composite PP Version\*, Composite PP Owner (Author)\*, Publication Date\*, ID\_Version\*.
- Composite PP Overview\* (2<sup>nd</sup> Level)
- CToE Overview\*/Certification Related Information

### **Composite PP Conformance Claims feature and sub-features**

- EUCC Conformance claim\*(2<sup>nd</sup> Level)  
It includes the following elements (3<sup>rd</sup> level): EUCC Assurance level
- CC Conformance claim\*(2<sup>nd</sup> Level)
- CC package claim\*(2<sup>nd</sup> Level)  
It includes the following elements (3<sup>rd</sup> level): EAL claim\*, Assurance package claim\*, Functional package claim\*, CC package claim description
- PP Conformance claim\* (2<sup>nd</sup> Level)

### **Security Problem Definition**

- Assumptions (2<sup>nd</sup> Level)  
It includes the following elements (3<sup>rd</sup> level): Assumption ID, Assumption Description
- Organisational Security Policies\* (2<sup>nd</sup> Level)  
It includes the following elements (3<sup>rd</sup> level): Policy ID, Description.
- Threat Categories\* (2<sup>nd</sup> Level)  
It includes the following elements (3<sup>rd</sup> level): Description.

### **Security Objectives**

- Security Objectives for the CToE\* (2<sup>nd</sup> Level)  
It includes the following elements (3<sup>rd</sup> level): Security Objective ID\*, Security Objective Description\*
- Security Objectives for the CToE Operational Environment\* (2<sup>nd</sup> Level)  
It includes the following elements (3<sup>rd</sup> level): Security Objective ID\*, Security Objective Description\*

### **Security Controls**

- Security Control ID\* (2<sup>nd</sup> Level)
- Security Control Family Name\* (2<sup>nd</sup> Level)
- Security Control Description\* (2<sup>nd</sup> Level)

### **Security Requirements feature and sub-features**

- Security Functional Requirements (SFRs) (2<sup>nd</sup> Level)  
It includes the following elements (3<sup>rd</sup> level): SFR ID Details\* (SFR ID\*/ SFR Name\*/ SFR Description\*, SFR Family\*/ SFR Class), SFR Dependencies\*

(Direct\*/Indirect\*/Hierarchical), Extended SFRs Details (SFR ID\*/ SFR Name\*/ SFR Description\*, SFR Family\*/ SFR Class), Extended SFR Dependencies.

- Security Assurance Requirements (SARs)\* (2<sup>nd</sup> Level)  
It includes the following elements (3<sup>rd</sup> level): Composite CC EAL\*, Attack Potential Level\*, SAR Details\*

#### **Extended Package feature and sub-features**

- Extended Components (2<sup>nd</sup> Level)  
It includes the following elements (3<sup>rd</sup> level): Description

### **7.3 Practical Adoption in System**

The CyberICT Protection Profile preparatory framework and the corresponding Protection Profile Taxonomy for composite products are research artefacts, developed in the current dissertation. These artefacts facilitated the design of cybersecurity certification evaluation services in a certification platform implemented in the context of EU Horizon research project [397].

#### **7.3.1 Design integration**

The proposed CyberICT Protection Profile was adopted in the design of a cybersecurity certification platform. Specifically, the CToE structure and the Protection Profile taxonomy informed the design of the CToE (Figure 63) and Protection Profile management services (Figure 67- Figure 69), which were developed from scratch (i.e., the “Product” management service and the “Composite Protection Profile Details” environment). Furthermore, the security classification interrelating assets, threats, security objectives, security requirements, and security controls was incorporated into the platform's certification services (Figure 64 and Figure 66). In addition, the mapping between the Common Criteria (CC) Evaluation Assurance Level (EAL), the EUCC Assurance Level, AVA\_VAN, and Attack Potential was implemented to support the identification of evaluation conditions during the conformity assessment process Figure 65. These platform enhancements were developed within the context of the CUSTODES HE research project [397].

#### **7.3.2 Visualisation of service in the cybersecurity certification platform**

This section presents visualisations of the cybersecurity certification platform services implemented based on the design of the proposed CyberICT Protection Profile, as described in Section 7.3.1.

Add Product

Name

Description \*

Describe your Product...

Used Scheme of Standards \*

Used Scheme of Standards

Figure 63. Service related to the CToE creation.

Controls

| Security Requirement | Applied NIST Controls |
|----------------------|-----------------------|
| SSM-2                | SC-28                 |
| SSM-1                | SC-28                 |
| SCM-2                | IA-3                  |
| FMT_MTD.1            | AC-3(7)               |

View 10 Rows

« 1 »

Figure 64. Security controls applied to the identified security functional requirements.

|                                       |                                                                                                                                                                            |
|---------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Conformance Claims                    |                                                                                                                                                                            |
| Conformance Statement:                | The composite Protection Profile of the current product claims conformance to Common Criteria assurance packages AVA , EAL (CC Part 3, CC Part 5)                          |
| Common Criteria Assurance Level:      | EAL2: Structurally Tested                                                                                                                                                  |
| Vulnerability Analysis Level:         | AVA_VAN.2: Vulnerability analysis                                                                                                                                          |
| Vulnerability Analysis Description:   | Assessment against simple, low-skill attacks. Ensures basic protection measures are in place                                                                               |
| Attack Potential:                     | Basic                                                                                                                                                                      |
| EUCC Assurance Level:                 | Substantial                                                                                                                                                                |
| Used scheme or standards:             | EUCC                                                                                                                                                                       |
| Assumptions:                          | The tablet is operated in a physically secure environment. The user is assumed to be non-hostile and properly trained. The network environment is assumed to be untrusted. |
| Organizational Security Policies:     | All data stored on the device must be encrypted at rest. Access to the device requires user authentication. Software updates must be applied within 30 days of release.    |
| Protection Profile conformance claim: | The composite Protection Profile of the current product does not claim conformance to any Protection Profile                                                               |

Figure 65. Evaluation criteria details.

About

Assets 2

Security Objectives 2

Security Requirements 5

Assessment 36

Certification Sharing

Search

| Name                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Id        | Appliance     |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|---------------|
| Appropriate integrity and authenticity protection for secure communication mechanisms                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | SCM-2     | Fully Applied |
| Management of Functions in TSF                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | FMT_MOF.1 | Fully Applied |
| <div> <div>Security Family</div> <div>Management of functions in TSF</div> </div> <div> <div>Name</div> <div></div> </div> <div> <div>Security Family Id</div> <div>FMT_MOF</div> </div> <div> <div>Security Family Description</div> <div>This family allows authorized users to control over the management of functions in the TSF.</div> </div> <div> <div>Description</div> <div>Management of Security Functions Behavior</div> </div> <div> <div>Security Objectives</div> <div>OT.CONFIGURATION_MANAGEMENT</div> </div> <div> <div>Threat Categories</div> <div>ElevationOfPrivilege</div> </div> |           |               |

Figure 66. Use of Protection Profile’s security classification to identify threat categories, relevant security objectives and security requirements of product’s assets.

Information for Security Problem Definitions

Assumptions:

Organizational Security Policies:

Figure 67. Assumptions and Organisational Security Policies for the Security Problem Definition.

Threats for Security Problem Definitions

Search

| Name                  | Framework |
|-----------------------|-----------|
| Tampering             | STRIDE    |
| InformationDisclosure | STRIDE    |

View 10 Rows

« 1 »

Figure 68. Threat categories for the Security Problem Definition.



| Security Requirements                                                                                         |                  |            |
|---------------------------------------------------------------------------------------------------------------|------------------|------------|
| <input type="text" value="Search"/> <input type="button" value="Filter"/> <input type="button" value="List"/> |                  |            |
| Name                                                                                                          | Id               | Compliance |
| ✓ EAP-TLS specification for TSF                                                                               | FCS_EAPTLS_EXT.1 | Positive   |
| ✓ User Authentication                                                                                         | FIA_UAU.5        | Positive   |
| ✓ Authentication Failure                                                                                      | FIA_AFL.1        | Positive   |
| ✓ Inter-TSF Trusted Channel                                                                                   | FTP_ITC.1        | Positive   |
| ✓ Certificate validation                                                                                      | FIA_X509_EXT.1   | Positive   |
| ✓ TSF Testing (extended)                                                                                      | FPT_TST_EXT.1    | Positive   |
| ✓ Integrity for Installation and Update package                                                               | FPT_TUD_EXT.2    | Positive   |
| ✓ Cryptographic Operation                                                                                     | FCS_COP.1        | Positive   |

Figure 69. Security Functional Requirements and Extended Requirements visualisation deriving from the security classification.

## 7.4 Demonstration and Applicability of CyberICT Protection Profile preparatory framework

This section presents a real-life scenario of a composite ICT product and how its Protection Profile can be prepared using the proposed Protection Profile preparation approach.

### 7.4.1 Step 0: Define the CToE and Evaluation Conditions

The ICT product which is evaluated is an ICT enterprise solution of a company. The ICT product embeds the following assets (Table 72) and CToE's details (Table 73):

Table 72. CToE assets

| CToE Asset Name                          | CToE Asset Technical Details             | CToE Asset Description                                                                                                                                                 |
|------------------------------------------|------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Operating System for Server Applications | Vendor: Canonical, Type: Ubuntu Linux    | This is a system software, i.e., an Ubuntu Server Operating System, designed to support server environments. It provides the platform for running server applications. |
| Database Management Server               | Vendor: RedHat<br>Type: Enterprise Linux | OS which runs the company's database management system.                                                                                                                |
| Database Management App                  | Vendor: Oracle MySQL                     | DBMS app provides all features for the company's database management system. It supports a set of utilities for database                                               |

|                    |                                                       |                                                                                 |
|--------------------|-------------------------------------------------------|---------------------------------------------------------------------------------|
|                    |                                                       | administration and interacts with end-users, applications, and databases.       |
| Application Server | Vendor:<br>Apache_software_foundation<br>Type: tomcat | Apache is an application server that serves content to the company's web users. |

Table 73. CToE details

| CToE 1: ICT Enterprise SCADA Solution   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>CToE Description</b>                 | <p>The current Composite Target of Evaluation (CTOE) is the company's ICT system for managing all businesses and enabling communication with all enterprise's networking devices in a secure manner.</p> <p>CTOE operational environment: A stand-alone information system running the DBMS server application and DBMS (server and client(s)) (ToE_4, ToE_3) serving one, or more than one, online user at a given time. It supports a network of workstations or terminals running DBMS clients and communicating with a DBMS server simultaneously. The network of workstations communicates with the company's application server (Asset_2), which in turn interacts with the DBMS (Asset_4) on behalf of the workstation. It operates a set of web services supported by an application server (via ToE_2) run on ToE_1 OS. The system accepts requests from web users and sends desired information in the form of files and Web pages. In addition, these procedures are supported by Asset_2 and Asset_4 communication enabled by a DBI Purl module integrated on Asset_2.</p> |
| <b>Evaluation Assurance Level</b>       | EAL 3: Methodically Tested and Checked<br>AVA_VAN.2 Attack Potential: Basic, EUCC: Sunstantial                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Certiciation related information</b> | None                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Application Server</b>               | EUCC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

#### 7.4.2 Step 1: Conduct Cybersecurity Risk Assessment on CToE's asset

After using the CyberICT Risk Management methodology, the following risk assessment results are identified (indicative examples):

Table 74. Risk Assessment results

| CToE Asset Name            | CVE Vulnerability                                                            | CAPEC MITRE                                                                                        | Risk Level |
|----------------------------|------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|------------|
| Database Management Server | CVE-2025-3155, CVE-2025-2784, CVE-2025-26601, CVE-2025-26601, CVE-2025-26598 | OS which runs the company's database management system.                                            | 99.8%      |
| Database Management App    | CVE-2024-21247<br>CVE-2024-21239                                             | CAPEC-97 Cryptanalysis, CAPEC-9 Buffer Overflow in Local Command-Line Utilities, CAPEC-87 Forceful | 99.9%      |

|  |                                  |                                                                      |  |
|--|----------------------------------|----------------------------------------------------------------------|--|
|  | CVE-2024-21238<br>CVE-2024-21230 | Browsing, CAPEC-85 AJAX<br>Footprinting, CAPEC-83 XPath<br>Injection |  |
|--|----------------------------------|----------------------------------------------------------------------|--|

#### 7.4.3 Step 2: Security Problem Definition

The security problem definition is presented below:

Table 75. Security Problem Definition.

| CToE 1: ICT Enterprise SCADA Solution |                                                                                                                                                            |
|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| OSP                                   | P. ACCESS_CONTROL: Authority shall only be given to the users who are permitted by the maritime company and they are trusted to perform actions correctly. |
| Assumption                            | A.SECURE_CONFIGURATION: The current solution is configured according to a secure baseline defined by the product owner (A.SECURE_CONFIGURATION).           |
| Threat Category                       | Elevation of Privilege                                                                                                                                     |

#### 7.4.4 Step 3: Identify Security Objectives and Security Requirements

The following security objectives have been identified along with the SFRs apply to all assets.

Table 76. Security objectives and security requirements.

| CToE 1: ICT Enterprise SCADA Solution |                                     |
|---------------------------------------|-------------------------------------|
| Security Objective                    | OT.ACCOUNTABILITY, OT.INTEGRITY     |
| Security Requirement                  | FAU_GEN.1, FTP_ITC_1, SFR FCS_CKM.1 |
| Threat Category                       | Repudiation, Tampering              |

#### 7.4.5 Step 4: Define Security Controls

The security controls implemented, are presented below.

Table 77. Security Controls definition.

| CToE 1: ICT Enterprise SCADA Solution |                                                                                                                      |
|---------------------------------------|----------------------------------------------------------------------------------------------------------------------|
| Security Objective                    | OT.ACCOUNTABILITY, OT.INTEGRITY                                                                                      |
| Security Requirement                  | FAU_GEN.1, FTP_ITC.1 , SFR FCS_CKM.1                                                                                 |
| Security Control                      | AU-2 (Event Logging), IA-3(1) (Device Identification and Authentication, Cryptographic Bidirectional Authentication) |
| Threat Category                       | Repudiation, Tampering                                                                                               |

#### 7.4.6 Step 5: Capture Evidence and Documentation

The appropriate evidence which justifies the security requirement-security control statement is provided in this step.

Table 78. Evidence and documentation.

| CToE 1: ICT Enterprise SCADA Solution |                                                                                                                                                  |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| Security Objective                    | OT.ACCOUNTABILITY, OT.INTEGRITY                                                                                                                  |
| Security Requirement                  | FAU_GEN.1, FTP_ITC_.1, FCS_CKM.1                                                                                                                 |
| Security Control                      | AU-2 (Event Logging), IA-3(1) (Device Identification and Authentication, Cryptographic Bidirectional Authentication)                             |
| Threat Category                       | Repudiation, Tampering                                                                                                                           |
| Evidence                              | SCADA solution pentest result, Secret Scanning findings: Reduced “Exposed Secrets” after adoption of vaulting, but residual weak patterns remain |

#### 7.4.7 Step 6: Review Protection Profile

Since the Secret scanning result detected an issue, the CToE Owner reviews once more the Protection Profile. Then, the CToE Owner realises that the SFR FCS\_CKM.1 “Enforce centralised secrets management” has not been satisfied. Thus, he/she decides to implement the additional control SC-12(3) “Cryptographic Key Establishment and Management - Assymetric Keys”. Afterwards, he repeats the security test and eventually delivers no findings.

#### 7.4.1 Step 7: Request Conformity Assessment

According to the CToE Owner’s opinion, all defined security requirements have been satisfied by appropriate security controls. Thus, the CToE Owner proceeds with the final step to request a third-party conformity assessment from an accredited body (CAB). The verdict of the CAB will determines if the current Protection Profile can receive the EUCC certification.

### 7.5 Evaluation of CyberICT Protection Profile

This section describes the evaluation approach used to assess the CyberICT Protection Profile.

#### 7.5.1 Evaluation approach

The CyberICT Protection Profile preparatory framework and its corresponding taxonomy were evaluated through proof-of-concept demonstrations and their practical adoption within a cybersecurity certification platform.

#### 7.5.2 Proof of concept demonstration

The CyberICT Protection Profile was demonstrated through a proof-of-concept involving a real-world scenario of maritime SCADA product. The case study evaluated the applicability and usefulness of the proposed Protection Profile preparatory framework and taxonomy for the specification of composite ICT products and their associated threat categories, security objectives,

security requirements, and security controls. The demonstration, presented in Section 7.4, provides evidence of the framework's applicability within realistic cybersecurity certification scenarios.

### 7.5.3 Practical adoption

As discussed in Section 7.3, the proposed CyberICT Protection Profile was adopted in the design of services supporting the creation of Protection Profiles for composite ICT products, including Security Objective, Security Requirement, and Security Control management services. Furthermore, the Protection Profile taxonomy was used to structure the composite Protection Profile environment, while the process-oriented preparatory framework provided both the conceptual and procedural foundation for the design and evolution of these services.

### 7.5.4 Comparative analysis of the CyberICT Protection Profile with respect to the Common Criteria and EUCC

This section provides a comparative analysis of the CyberICT Protection Profile with respect to the Common Criteria (CC) [44] certification framework and the European Cybersecurity Certification Scheme (EUCC) [14].

#### Target of Evaluation (ToE)

The EUCC relies on the CC structure to identify the Target of Evaluation (ToE). The proposed CyberICT Protection Profile extends the Common Criteria ToE structure by introducing the Composite Target of Evaluation (CToE), enabling complex ICT products to be represented as collections of interconnected assets. Specifically, *the CyberICT CToE structure provides additional information on the product's technical details* (vendor, version, etc.) and *the asset's dependencies with other product assets*. This information facilitates the risk assessment process (see certification challenges in Section 4.6.7). Although the Common Criteria recognises composite evaluations, it does not provide a detailed representation of composite ICT products and their constituent assets. Moreover, the *proposed CToE structure includes further information concerning whether the specific product has received a cybersecurity certification in the past*, requiring ID and duration validity details. This additional information supports *the auditing process* and potential *reuse of certification-related information* that can further simplify the evaluation process and *strengthens the information sharing within the certification ecosystem*.

#### Protection Profile

The EUCC is based on the CC Protection Profile (PP) structure. The CC PP provides several protection profile types in the CC portal which may create uncertainty for the product which is proper to adopt. The EUCC identifies technical domains and recommended Protection Profiles only for higher assurance levels (AVA\_VAN 4,5). Consequently, a harmonised approach to defining and classifying CToEs and Protection Profiles is required (see certification challenges in Section 4.6.7). To this aim, the CyberICT Protection Profile *harmonises the evaluation of prominent technical domains of ICT products*, (e.g., OS, application software, network devices and IoTs, databases, encryption modules and PKIs, VPNs, Virtual Machines) with a set of standards-based security concepts. In addition, based on the EUCC [14], CC [44] and CRA [11], it

provides indications on types of products for each specific Assurance Level. Moreover, the CyberICT Protection Profile, based on several Protection Profile-approved templates from prominent certification bodies [385]–[395], *identifies interrelations of security concepts between assets, threat categories, security objectives, security requirements and security controls and introduces a unified security classification* (see Appendix D7, D8 and [396]) to drive the Product Owners corresponding definitions of their PPs. Furthermore, based on the above PP templates, the *proposed Protection Profile extends the approximately 300 Security Functional Requirements (SFRs), defined by the Common Criteria, with eighty-six (86) additional domain-specific SFRs* [396].

Protection Profile preparation. The existing regulatory certification background may provide ToE and PP structures and generic methodologies for the evaluation process [59], [152]; nevertheless, they lack adopting a unique and standards-harmonised approach indicating how to develop the Protection Profile of complex ICT products and analyse/decompose the CToE into its primary assets. The proposed Protection Profile preparatory framework presents *a stepwise approach guiding the Product Owners comprehensively on how to create the PP of composite products and assess their claims*. Furthermore, the CC and the EUCC do not apply an evaluation for ICT supply chains, as the recently proposed CSA 2 [49] initially recommends in relation to the NIS 2 Directive [12] and its amendments.

The recently published CSA 2 proposal [49] introduces a *trusted ICT supply chain framework*, intended to address ICT supply chain security, particularly for sectors covered by the NIS 2 Directive [12] (ICT security toolbox [398]). Neither the Common Criteria nor the EUCC explicitly address the evaluation of ICT supply chains. In contrast, the proposed CyberICT Protection Profile preparatory framework incorporates the model-driven and evidence-based CyberICT Risk Management Methodology (Chapter 6) to assess the security of ICT Supply Chain Services (ICT SCSs) associated with an ICT product. The risk assessment results of ICT SCS provide additional evidence that can support conformity assessment activities for composite ICT products, especially where rigorous evaluation is needed.

Table 79. Protection Profile templates analysis.

| Evaluation aspect              | Common Criteria / EUCC        | CyberICT Protection Profile                                                                                                                                                                    |
|--------------------------------|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Target of Evaluation (ToE)     | Conventional ToE              | CToE with asset decomposition                                                                                                                                                                  |
| Protection Profile (PP)        | Several existing PP templates | Harmonised taxonomy, unified security classification ( +86 extended SFRs)                                                                                                                      |
| Protection Profile preparation | Generic guidance              | Stepwise preparation framework, comprehensive ICT product risk assessment, including corresponding ICT SCS generating additional evidence to support rigorous conformity assessment processes. |

# PART VI:

## EVALUATION OUTCOMES, CONCLUSIONS, AND CONTRIBUTION TO SCIENCE

---

## 8. Overall Evaluation

This research has created a set of interconnected artefacts grounded in the Design Science Research (DSR) framework presented in Section 1.3. Specifically, the research delivers the CyberICT Risk Management Methodology together with its supporting risk ontology; the CyberICT Protection Profile preparatory framework, complemented by a structured taxonomy for composite ICT products; and a comprehensive ontology for cybersecurity standards.

### 8.1 Ontologies evaluation

The developed ontologies (CyberICT Standards Ontology and CyberICT Risk Ontology) were evaluated through reasoning-based mechanisms validation (HermiT, FaCT++, Pellet reasoners) [133]-[135], as mentioned in sections 5.3.4 and 6.2.3. For instance, the Pellet reasoner is a formal, widely recognised method for validating Semantic Web ontologies, well-suited for extracting actionable cybersecurity intelligence from complex ontologies. The reasoning mechanisms use logical inference rules to assess the correctness, consistency, and integrity of data or software models against the predefined knowledge framework. Particularly: i) they conduct consistency checking by scanning the entire ontology to verify there are no logical contradictions, ii) they check the class hierarchy classification of the ontology based on their property constraints, iii) they analyse existing axioms to deduce new facts (infer new knowledge), and iv) they provide axiom pinpointing with debugging justifications<sup>19</sup> when a logical error or contradiction occurs. The validation outcomes from the reasoning mechanisms showed no conflicts, overlaps or any other logical errors or inconsistencies in the structure and syntax of the two (2) taxonomies. SPARQL [131] queries were used in conjunction with Description Logic (DL) reasoning to retrieve knowledge inferred from the ontologies.

The two (2) ontologies served as the formal representation of security knowledge in machine-readable formats for i) cybersecurity standards classification (CyberICT Standards Ontology) and ii) risk management concepts classification within the ICT ecosystem (CyberICT Risk Ontology). The developed ontology models helped to recognise knowledge flows from these topics and extract new knowledge and store, retrieve and reuse articulated knowledge.

Cybersecurity risk assessment is constrained by intuition and tacit expertise, while existing models assume fully codified data. The SECI model [114] is a golden knowledge management framework used to systematically externalise unwritten, hidden knowledge into structured, reproducible concepts. Moreover, the application of the CyberICT Risk ontology was used to introduce how security knowledge converts between tacit (non-externalised, unknown) and explicit (externalised, known) forms through socialisation, externalisation, combination, and internalisation in the ICT ecosystem. The CyberICT Risk Ontology and SECI model application are supported in the publications [84],[97] created during this dissertation research. The publications present the ontology's applicability with scenario-based analysis of two (2) MLoSC

---

<sup>19</sup> built in full explanation support in Pellet Reasoner, partial explanation support in HermiT and FaCT++.



services, i.e., the Vehicle Transport Service and the Vessel Traffic Service, respectively (see Section 6.4). The CyberICT Risk Ontology formalises security knowledge of the ICT ecosystem by enabling the generation of new insights through inference mechanisms and effective utilisation of organisational knowledge across the ecosystem. The ontology was instantiated using actors, processes and assets of the Maritime and Logistics Supply Chain (MLoSC).

The CyberICT Standards Ontology organises cybersecurity standards by objective, usage, and sector perspectives. This structured knowledge base helps stakeholders better understand the purpose of each standard and make informed decisions about which to adopt based on their specific needs. The ontology was instantiated using cybersecurity standards, best practices for AI/ML-based infrastructure security, and cybersecurity guidelines applicable to the maritime transport sector. The application of the ontology through this scenario is presented in the [18] research publication, which was created as part of this dissertation's research.

Furthermore, the EduSor ontology [109], introduced in Section 3.4.2.1, was developed as an initial effort to gain experience in semantic knowledge representation and ontology engineering. The research works presented in [92]-[93] describe the BPMN ontology [110], discussed in Section 3.4.2.2, which was developed to combine the Business Process Model and Notation (BPMN) [114] with Semantic Web technologies [130] through the semantic representation of BPMN 2.0.2 concepts. This ontology subsequently informed the development of concepts of the CyberICT Risk Ontology, as described in Section 6.2.3. Both ontologies were applied to realistic scenarios within the educational public sector, as presented in the aforementioned publications. The ontologies were validated using the HermiT, FaCT++, and Pellet reasoners [133]-[135], which confirmed that they were logically consistent, correctly classified, and without logical inconsistencies. SPARQL queries were also developed to retrieve knowledge inferred by the reasoners from both ontologies. Therefore, the EduSor and BPMN ontologies served as preliminary ontology engineering efforts that supported the development of expertise in business process modelling and Semantic Web technologies during the early stages of this doctoral research.

## **8.2 CyberICT Risk Management Methodology evaluation**

This dissertation follows a Design Science Research approach and evaluates the proposed CyberICT Risk Management Methodology through multiple complementary methods, presented in sections 6.2.4, 6.3, 6.4 and 6.5.

These include: (i) proof-of-concept demonstrations using real-world ICT Supply Chain Service (SCS) scenarios, (ii) adoption in the design of risk management platforms, (iii) stakeholder surveys providing indirect evidence of user acceptance, (iv) analysis against domain-specific challenges, and (v) examination of the vulnerability and impact calculation models. Collectively, these evaluation activities provide evidence of the methodology's applicability, usefulness, and conceptual soundness.

Demonstration scenarios were derived from real-world ICT Supply Chain Services (SCSs) within the Maritime and Logistics Supply Chain (MLoSC), namely the Vehicle Transport Service, the LNG Transport Service, and the Container Management Service. As described in Section 6.4 and in the state-of-the-art presented in Chapters 3 and 4, the MLoSC integrates multiple industrial sectors, including the maritime, automotive, energy, and logistics sectors.

The applicability of the proposed methodology was demonstrated through these MLoSC services by applying its business, holistic-technical, and sectoral dimensions to realistic cyber-threat scenarios. The scenario-based analysis is supported by publications [1],[9],[84] produced as part of this doctoral research. Publications [2],[15],[95]-[97],[322] also produced during this doctoral research, further supported the ICT supply chain service and threat-modelling analyses.

Furthermore, a case study derived from Healthcare industry sector, presented in publication [274] and developed during this doctoral research, demonstrates the application of the attack-path generation aspects of the proposed methodology.

The proposed methodology was evaluated through two (2) questionnaire-based surveys, as presented in Section 6.5.1, primarily capturing ICT stakeholders' perceptions regarding the methodology's usefulness, applicability, and overall satisfaction. The research publications [1],[9] describe the evaluation results.

### **8.3 CyberICT Protection Profile evaluation**

The CyberICT Protection Profile is another artefact of the CyberICT hybrid evaluation framework. The CyberICT Protection Profile was evaluated through three complementary activities: (i) a proof-of-concept demonstration using a real-world ICT scenario involving a maritime SCADA product from the maritime sector, presented in Section 7.4, (ii) its adoption in the design of a cybersecurity certification management platform, presented in Section 7.3, and iii) a comparative analysis of the CyberICT Protection Profile versus the CC versus the EUCC certification schemes (see Section 7.5). The CyberICT Protection Profile enhancements are presented in Section 7.5.4.

These evaluation activities provide evidence of the Protection Profile's applicability and feasibility within realistic cybersecurity and certification contexts. Furthermore, the proposed CyberICT Protection Profile has subsequently been applied in the research reported in publications [357]-[358], providing additional evidence of its practical relevance.

### **8.4 Contribution to identified challenges and requirements coverage from the CyberICT hybrid evaluation approach.**

Section 5.2 established the mapping between the identified challenges, requirements, dissertation objectives of Section 5.1, and the developed artefacts. The following tables summarise the contributions of the developed artefacts (Dissertation Contribution: DC#) towards addressing the identified challenges CH#), fulfilling the specified requirements (Req#), and achieving the corresponding dissertation objectives (DO#).

Table 80. An integrated framework of Risk Management and Conformity Assessment.

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>CH#1: An integrated framework of Risk Management and Conformity Assessment</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Req#1.1: Need for measurable and actionable security requirements linked with appropriate security controls</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>DO #1.1 Develop an approach that creates a measurable and actionable set of security requirements and corresponding security controls that are capable of meeting EU digital market's needs</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <p><b>DC #CyberICT Protection Profile taxonomy for composite ICT products</b></p> <p>The literature review revealed that no existing approaches can systematically guide the Product Owners how to define security concepts of a composite product during the development of its Protection Profile. Furthermore, the availability of several Protection Profile publications [359] may create uncertainty regarding the selection of the most appropriate Protection Profile for a particular ICT product. To address this gap, the proposed CyberICT Protection Profile taxonomy for composite ICT products (see Section 7.2) introduces a unified security classification that interrelates threat categories, security objectives, security requirements, and security controls. This classification (Table 103-Table 105) provides structured guidance to ICT stakeholders in selecting appropriate security controls to satisfy the identified security requirements during the preparation of Protection Profiles for composite ICT products.</p>                                                                                                                                                                                                                                                                        |
| <b>Req#1.2: The synergy of risk assessment and conformity assessment procedures is required to provide an end-to-end evaluation for attesting the security, according to specified criteria and guide ICT stakeholders how to create the Protection Profile of composite ICT products</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>DO#1.2: Develop an approach that integrates both risk management and conformity assessment procedures guiding ICT stakeholders how to conduct an end-to-end evaluation to facilitate readiness for cybersecurity certification and security compliance procedures and create the Protection Profile of composite ICT products</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <p><b>DC #CyberICT hybrid evaluation framework for products and supply chain services (CyberICT Risk Management Methodology; Protection Profile preparatory framework and taxonomy)</b></p> <p>The CyberICT hybrid evaluation framework integrates risk management and conformity assessment processes into a unified evaluation approach. ICT stakeholders can first apply the CyberICT Risk Management Methodology to assess threats, vulnerabilities, and risks affecting ICT products, their constituent assets, and the associated ICT Supply Chain Services (ICT SCSs). Thereby, they can identify appropriate security controls and mitigation strategies. Subsequently, they can apply the CyberICT Protection Profile preparatory framework to progressively develop the Protection Profile for their ICT products and assess the conformity of the corresponding security claims. The preparatory framework guides ICT stakeholders throughout the Protection Profile development process while supporting the generation of evidence required for conformity assessment. Furthermore, the Protection Profile security classification, described in Section 7.2, provides structured guidance for verifying that the identified security requirements are adequately addressed by the selected security controls.</p> |

Table 81. Harmonisation of cybersecurity standards.

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>CH#2: Harmonisation of cybersecurity standards</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Req#2.1: Reduce fragmentation of cybersecurity standards</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>DO #2.1 Develop an ontology that classifies cybersecurity standards and enhances comprehension</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <p><b>DC #CyberICT standards ontology</b></p> <p>The developed CyberICT standards ontology classifies cybersecurity standards based on their objective, usage, and sector and thereby guides ICT stakeholders understand their purpose and decide which they should adopt to cover their organisational needs.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Req#2.2: Need for harmonised standards-based approaches for assessing ICT products security</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>DO#2.2: Develop a standards-based approach that combines and harmonises risk management and conformity assessment concepts.</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <p><b>DC #CyberICT hybrid evaluation framework for products and supply chain services</b></p> <p>The CyberICT hybrid evaluation framework integrates the risk management and conformity assessment concepts based on an enhanced security model (Figure 2) that addresses the interplay of the EU CSA, CRA and NIS 2 Directive. Moreover, it harmonises the risk assessment concepts of ISO/IEC 27k, the supply chain security and resilience concepts of ISO 28000, 28001 and 28004 and the evaluation criteria and approach for conformity assessment procedures, based on ISO/IEC 15408 and ISO/IEC 18045. An interested party can use the cybersecurity risk management methodology of the CyberICT hybrid evaluation framework to assess threats, vulnerabilities and risks either in composite ICT products or in their ICT supply chain service environments. In addition, the framework supports conformity assessment preparation through the CyberICT Protection Profile framework, enabling interested parties to prepare for cybersecurity certification evaluations and to demonstrate compliance with the security requirements of legal frameworks, such as the EU Cyber Resilience Act (CRA).</p> |

Table 82. Address the complex nature of large-scale environments.

|                                                                                                                                                                                                                                                                                   |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>CH#3: Address the complex nature of large-scale environments</b>                                                                                                                                                                                                               |
| <b>Req#3.1: Need for identifying asset interdependencies</b>                                                                                                                                                                                                                      |
| <b>DO #3.1: Develop a cybersecurity risk management methodology for ICT products and ICT supply chain services which identifies interdependencies between interconnected ICT assets</b>                                                                                           |
| <p><b>DC #CyberICT Risk Management methodology</b></p> <p>The CyberICT Risk Management methodology identifies diverse types of cyberdependencies between ICT assets (see Section 6.2.2.2) and estimates the length of the path between two assets across the ICT SCS network.</p> |
| <b>Req#3.2: Need for identifying criticality on ICT products</b>                                                                                                                                                                                                                  |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>DO#3.2: Develop a cybersecurity risk management methodology which analyses ICT products and identifies their criticality</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Req#3.3: Need for identifying criticality on ICT supply chain services, ICT processes and ICT assets</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>DO#3.3: Develop a cybersecurity risk management methodology which estimates criticality on ICT supply chain services, ICT processes and ICT assets</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>DC #CyberICT Risk Management methodology</b><br><br>The CyberICT Risk Management Methodology supports an extensive analysis for ICT products and ICT SCS. In the case of ICT SCS, the methodology provides a set of criticality rules considering the ICT assets relation to the ICT processes and their location in the ICT network. Regarding the assessment of ICT products, the methodology recommends the interested party to use the product's criticality scales of the EU CRA.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Req#3.4: Need for analysing ICT supply chain services from business-oriented, horizontal and vertical evaluation aspects.</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>DO#3.4: Develop a cybersecurity risk management methodology which provides diverse evaluation aspects on ICT supply chain services, i.e., business, holistic-technical, and sector-specific.</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>DC #CyberICT Risk Management methodology</b><br><br>The CyberICT Risk Management Methodology supports three complementary evaluation perspectives for ICT Supply Chain Services (ICT SCSs). The business perspective focuses on analysing the business context and modelling ICT SCSs to improve the understanding of supply chain processes and stakeholder interactions. The holistic-technical perspective provides a comprehensive assessment of ICT assets, their interdependencies, and their cybersecurity posture across the supply chain. The sectoral perspective focuses on assessing the systems and assets operated by an individual business partner within the ICT SCS. These three evaluation perspectives were demonstrated through rigorous scenario-based testing: the Vehicle Transport Service scenario demonstrated the business perspective, the LNG Transport Service scenario demonstrated the holistic-technical perspective, and the Container Management Service scenario demonstrated the sectoral perspective. |

Table 83. Lack of security typology.

|                                                                                                                                                                                             |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>CH#4: Lack of security typology</b>                                                                                                                                                      |
| <b>Req#4.1: Need for improving comprehension of ICT processes and their embedded actors and elements.</b>                                                                                   |
| <b>DO #4.1: Develop a cybersecurity risk management methodology which uses business process models to visualise business partners participating and assets operating in an ICT process.</b> |
| <b>DC #CyberICT Risk Management methodology</b>                                                                                                                                             |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>The CyberICT Risk Management methodology supports a business evaluation aspect which guides the ICT stakeholder how to use business process models (e.g., BPMN models) to represent the ICT processes of the ICT SCS, the actors involved and the assets operating.</p>                                                                                                                                                                                                                                    |
| <p><b>Req#4.2: Need for enhancing organisational learning and security knowledge flows within the ICT supply chain environment.</b></p>                                                                                                                                                                                                                                                                                                                                                                       |
| <p><b>DO#4.2: Develop a cybersecurity risk management methodology that adopts Knowledge Management practices to recognise knowledge management flows and externalise tacit security knowledge within the ICT ecosystem.</b></p>                                                                                                                                                                                                                                                                               |
| <p><b>DC #CyberICT Risk Ontology</b></p> <p>The CyberICT Risk Ontology relies on the SECI model, which is an historical globally accepted knowledge management framework, to identify knowledge flows within the ICT ecosystem and systematically capture tacit internalised knowledge. The ontology was developed based on OWL2 and RDF specifications and utilised inference and reasoning mechanisms (e.g., SPARQL, Pellet) to identify tacit inferences and externalise them to create new knowledge.</p> |
| <p><b>Req#4.3: Create a structured body of cybersecurity knowledge in machine-readable format</b></p>                                                                                                                                                                                                                                                                                                                                                                                                         |
| <p><b>DO#4.3.1: Develop a risk ontology to semantically represent ICT supply chain service elements and relevant security concepts.</b></p> <p><b>DO#4.3.2: Develop an ontology that classifies cybersecurity standards from diverse perspectives.</b></p>                                                                                                                                                                                                                                                    |
| <p><b>DC #CyberICT ontologies (Cybersecurity standards Ontology; Risk Ontology)</b></p> <p>The two ontologies have been developed during the dissertation research and presented in this doctoral thesis. They were validated using reasoning mechanisms (e.g., Reasoner Pellet) and instantiated real-world examples to check their applicability.</p>                                                                                                                                                       |

Table 84. Siloed risk measurements lacking holistic view.

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>CH#5: Siloed risk measurements lacking holistic view</b></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <p><b>Req#5.1: Need for estimating the impact of potential cyberattacks in ICT supply chain networks</b></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <p><b>DO #5.1: Develop a cybersecurity risk management methodology that uses calculation models to estimate threats, vulnerabilities, risks and their cascading effects.</b></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <p><b>DC #CyberICT Risk Management methodology</b></p> <p>The CyberICT Risk Management methodology, based on the models described in Section 6.2.2.4, supports cumulative assessment to estimate accordingly individual, cumulative risk/vulnerability/impact levels. Furthermore, it estimates the cascading effects from different perspectives considering: i) the individual vulnerability chain relying on a specific asset entry point to specific asset target point, ii) the Entry's vulnerability chains, namely, all vulnerability chains originated from a specific asset entry point and iii) the cumulative vulnerability chains, namely, all vulnerability chains from all possible asset entry points to a specific asset target point.</p> |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Req#5.2: Need for estimating risk propagation in ICT supply chain networks</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>DO#5.2: Develop a cybersecurity risk management methodology that uses calculation models for propagated assessment of vulnerabilities, impact and risks.</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <p><b>DC #CyberICT Risk Management methodology</b></p> <p>The CyberICT Risk Management methodology, based on the models described in Section 6.2.2.4, supports propagated assessment to estimate how deep an attacker can penetrate the network with corresponding estimations of vulnerability, impact and risks propagated levels.</p>                                                                                                                                                                                                                                                                        |
| <b>Req#5.3: Need for enhancing attack modelling techniques</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>DO#5.3: Develop an attack simulation and evidence-based generation model for estimating attack paths in complex ICT networks associated with a confirmed security event.</b>                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <p><b>DC #CyberICT Risk Management Methodology</b></p> <p>Within the current dissertation research, the Attack Simulation Evidence Chain Generation (ASECG) model was developed (see Section 6.2.2.5), which estimates all possible and meaningful attack paths associated with a specific confirmed event (an attack not as potential, as known security event) that was identified in a specific asset node. It creates credible vulnerability chains by investigating how an attacker has moved inside the network to create the attack and how he/she could proceed launching additional chain attacks.</p> |

## 9. Conclusions and contribution to science

Chapter 9 concludes the dissertation by highlighting the outcomes of this dissertation, the scientific contributions of the proposed CyberICT hybrid evaluation framework, and identifying its novel aspects.

### 9.1 Conclusions and future work

Chapter 2 analyses that the integration of risk and conformity assessment procedures is a pathway to raise the security resilience in the EU single market, as recommended by the European Cyber Resilience Act [11], the Cybersecurity Act [13] and the NIS 2 Directive [12]. The state-of-the-art (Chapter 4) demonstrates poor effort in integrating risk and conformity assessment processes into a unique hybrid approach.

The main objective of this dissertation is to contribute to this challenge by creating a hybrid evaluation approach that integrates risk and conformity assessment procedures, which guides the ICT stakeholder in identifying actionable and measurable requirements for composite ICT products associated with security controls. It provides an end-to-end evaluation process to train the ICT stakeholders on how to prepare the Protection Profile of their composite ICT product for cybersecurity certification under the Common Criteria-based EU Cybersecurity Certification Scheme (EUCC).

The developed Protection Profile preparation approach drives the ICT stakeholder to evaluate the conformity of an ICT product by assessing the claims specified in the Protection Profile. Thereby, ICT stakeholders, such as ICT product owners, ICT manufacturers or ICT providers, can familiarise themselves with the conformity assessment process to obtain a pre-auditing experience that will help them to raise preparedness in such conformance. In addition, the Protection Profile preparation approach can assist ICT stakeholders in assessing the conformity of a composite ICT product with the CRA requirements in relation to its level of criticality.

The literature reviewed fragmentation of cybersecurity standards, including those related to cybersecurity certification (Chapter 4). The proliferation of Protection Profiles confuses ICT stakeholders in determining which one is the most appropriate for their intended use (see Section 4.6). The CyberICT Profile preparatory framework is accompanied by a complementary Protection Profile taxonomy (data model), developed to incorporate a combined set of security classifications that map threat categories with security objectives, security requirements and controls. The taxonomy helps ICT stakeholders identify actionable and measurable security requirements for their composite ICT products and improves decision-making regarding the selection of security controls that best meet their organisational needs. Moreover, this dissertation developed an ontology of cybersecurity standards that classifies them according to their objective, usage, and sector in light of helping ICT stakeholders understand their purpose and determine which they should adopt to cover their security needs.

The proposed hybrid evaluation approach incorporates a cybersecurity risk management methodology, designed to guide ICT stakeholders in assessing vulnerabilities, threats, and risks



associated with the composite ICT product under evaluation. Furthermore, it assists them in identifying and implementing appropriate technical mitigation measures prior to preparing the corresponding Protection Profile. The proposed Protection Profile taxonomy can subsequently be used during the Protection Profile preparation process to verify that the selected security controls are appropriate for addressing the identified security requirements and their associated security objectives. Moreover, the risk assessment results can help ICT stakeholders define the security problem during the development of the Protection Profile by identifying relevant threat categories and establishing appropriate security assumptions. This, in turn, facilitates the selection of security objectives and requirements for the composite ICT product evaluation that are aligned with the entity's specific security needs.

The developed cybersecurity risk management methodology supports the assessment of composite ICT products and ICT supply chain services. Thereby, the methodology provides the option to the ICT stakeholder to assess the security of ICT supply chain services connected to the ICT product (e.g., assessing the security of a CCTV and the supply chain service for manufacturing its components). According to the NIS 2 Directive [12], ICT supply chain service risk assessment is mandatory and legally binding for Operators of essential or Important Services.

In the context of ICT product evaluation, the assessment of ICT supply chain services is necessary to support rigorous and in-depth security evaluations, particularly at higher evaluation assurance levels. Such assessments are especially relevant when (i) integrating third-party code, such as open-source libraries, commercial software components, or proprietary external APIs, and (ii) generating Software Bills of Materials (SBOMs) to identify dependencies and facilitate the mapping of vulnerabilities throughout the supplier ecosystem [354]. In this context, the NIS Cooperation Group has recently adopted the EU ICT Supply Chain Security Toolbox [354], which was developed by the Member States with the support of the European Commission and the European Union Agency for Cybersecurity (ENISA).

The proposed cybersecurity risk management methodology considers a composite assessment which scrutinises the technical complexity either of a composite ICT product, considered a product which can be further analysed into primary elements, or of a large-scale heterogeneous supply chain network, such as SCADA or AIS or Satellite networks. The cybersecurity risk management methodology supports a stepwise, thorough analysis of ICT elements, relying on asset interdependencies and ICT element criticality assessment (asset, process, and ICT supply chain services). This contributes to the challenge of adequately analysing the complex nature of large-scale environments identified through the literature analysis. To facilitate comprehension of the analysis, it utilises business process modelling techniques and knowledge management practices to visualise complicated information, such as complex SCADA architectures, and extracts new knowledge from implicit and tacit information. This contributes to the challenge of raising the security awareness in the ICT ecosystem. The reviewed literature suggests that incorporating knowledge management practices into the risk management processes of complex ICT supply chain environments can improve risk awareness, promote the development of organisational knowledge, and facilitate the efficient retrieval of information (see Section 5.1).

The proposed cybersecurity risk management methodology provides an in-depth assessment of threats, vulnerabilities, and risks, considering ICT asset cyberdependencies and enabling the estimation of cascading effects and risk propagation. This addresses limitations of existing risk assessment approaches in providing a holistic risk analysis (see Section 5.1). Moreover, the estimation of vulnerability exploitability incorporates complementary aspects of both intrinsic vulnerability characteristics and attacker-specific attributes.

This dissertation addresses the challenges abovementioned through the creation of a hybrid evaluation framework that incorporates a set of artefacts following the Design Science Research (DSR) model presented in Chapter 1:

- the CyberICT Risk Management methodology for composite ICT products and ICT supply chain services
- the CyberICT Protection Profile preparatory framework of composite ICT products
- the CyberICT standards ontology
- the CyberICT Risk Ontology
- the CyberICT Protection Profile taxonomy (data model)

The interrelationships between these artefacts are presented in Section 5.2. In addition, a comprehensive glossary of terms has been developed (see Appendix A) which integrates terms of risk assessment, supply chain security, conformity assessment, cybersecurity certification and additional domain research topics based on prominent standards and best practices.

Each artefact was developed systematically, motivated by challenges and open issues identified in the literature review, founded on established frameworks and relevant standardised approaches and practices, and iteratively refined and subjected to conceptual validation (see Chapter 8). For the development of the artefacts a set of requirements was defined, which were elicited from the challenges derived from the literature review. Relevant dissertation objectives were defined. An assessment of whether the artefacts satisfy the identified requirements and objectives and how they contribute to the challenges is analysed in Section 8.4.

The developed artefacts were validated through proof of concept demonstration by checking their applicability, efficacy and efficiency through real-life examples of critical industry sectors (scenario-based testing), such as Maritime Transport, Logistics and Energy, and their practical adoption in risk and certification management platforms' conceptual design, as described in Chapters 6 and 7. In addition, the evaluation of the CyberICT Risk Management methodology included the pilot testing and training activities and two (2) ICT stakeholder questionnaire-based surveys associated with the risk management platform evaluation, which incorporates steps of the proposed methodology, as described in Chapter 6. The questionnaire results related to the practical application of the methodology provide additional evidence of its feasibility and usability.

The ontology-based models were created to provide explicit semantics and traceable reasoning, which is deemed essential for the current security evaluation purposes. The ontologies were validated through the typical verification and validation approach for ontology artefacts, which

elaborates on semantic validation using ontology reasoning mechanisms, as described in Section 8.1. No errors and inconsistencies were identified.

The dissertation adopts knowledge management and ontology-based models to address the requirement for formal semantics, interpretability, and traceable reasoning within ICT supply chain risk assessment.

Nevertheless, AI-based methods present valuable opportunities for advancing risk analysis through learning-based and predictive capabilities. In this context, collaborative research conducted during this dissertation [357]-[358] explored an initial hybrid AI framework for risk and conformity assessment processes of composite ICT products within the EUCC certification scheme. The proposed framework combined the CyberICT Protection Profile approach developed in this dissertation with ensemble learning techniques for vulnerability exploitation prediction and Explainable AI (XAI) mechanisms to support risk level estimation. These collaborative research outcomes indicate the potential of integrating AI with the proposed framework. Thus, AI-based techniques constitute a promising direction for the future evolution and enhancement of the CyberICT hybrid evaluation framework.

## **9.2 Novelty and Contribution to Science**

The novelty of this dissertation mainly relies on the integration of risk and conformity assessment practices and the development of a coherent ecosystem of artefacts addressing multiple interdisciplinary perspectives, as presented in the following.

### **9.2.1 Contribution to cybersecurity certification**

The integration of risk and conformity assessment in a hybrid approach is a key novelty in the evaluation procedures related to the European cybersecurity certification. The dissertation provides an approach of assessing the security of ICT products for preparing ICT stakeholders on the evaluation process either for EUCC-based cybersecurity certification or to assess their compliance with the Cyber Resilience Act requirements.

The CyberICT hybrid evaluation framework:

- meaningfully integrates the processes of risk and conformity assessment to structure the Protection Profile of a composite ICT product, whereas limited research work that currently exists mostly treats them separately
- bridges cybersecurity risk management with Protection Profile preparation objectives based on the adopted Common Criteria based EUCC scheme
- supports pre-audit preparation and enhances stakeholders' readiness for EUCC certification procedures
- facilitates the accurate definition, evaluation and classification of composite ICT products and their corresponding ToEs and Protection Profiles

- harmonises the evaluation of prominent technical domains of ICT products (including operating systems, application software, databases, encryption modules and PKIs) through a standards-based set of security concepts
- establishes interrelationships among existing security classifications through the development of a security classification that maps threat categories to security objectives, security requirements, and security controls. Thereby, it enables ICT stakeholders to identify actionable, measurable, and verifiable requirements and select appropriate security controls during Protection Profile preparation
- provides methodological guidance for the development of Protection Profiles for composite ICT products
- introduces a stepwise and systematic process for conducting risk and conformity assessment that simplifies the complexity of traditional tedious, time-consuming, multi-level evaluation procedures
- recognises the need to assess ICT supply chain services associated with an ICT product (supply chain – aware assessment) to achieve rigorous security evaluations and support higher Evaluation Assurance Levels (EALs), and provides a methodology for conducting cybersecurity risk management in ICT supply chain environments.
- contributes to the advancement of standards-harmonised approaches for cybersecurity certification.

### **9.2.2 Contribution to cybersecurity standardisation**

Considering the open issues in the fragmentation of several existing cybersecurity standards, this dissertation developed the CyberICT standards ontology, which:

- contributes to the harmonisation of cybersecurity standards efforts by identifying relationships between EU regulation and prominent cybersecurity standards
- raises awareness of the role and purpose of cybersecurity standards and assists ICT stakeholders in selecting the most appropriate standards according to their needs
- aids government and business organisations in assessing their security policy and best practices;
- provides a robust foundation for the cybersecurity standards taxonomy by developing a semantic ontology.
- contributes to the cybersecurity standardisation work of EU delegates, such as the JRC and ENISA.

Moreover, the CyberICT hybrid evaluation framework contributes to the advancement of harmonised approaches addressing the interplay of CRA [11], CSA [13] and NIS 2 Directive [12] regulations.

### **9.2.3 Contribution to Supply Chain security**

The literature reviewed a research gap in providing holistic risk analysis of ICT supply chain environments. Several existing approaches fail to estimate the asset interdependencies and consider the technical complexity of the heterogeneous ICT supply chain networks when evaluating risks. The proposed CyberICT Risk Management Methodology:

- identifies a set of sequential procedures to thoroughly analyse the ICT supply chain services by guiding how to decompose it into its main elements, identifying criticalities on ICT elements and defining cyberdependencies between ICT assets considered for the assessment. The methodology supports diverse supply chain evaluation aspects of business, holistic-technical and sector-specific to support diverse evaluation objectives. This is an additional novelty of the dissertation
- supports risk assessment for heterogeneous, multi-modal, interdependent infrastructures of the global supply chain, such as SCADA infrastructures and AIS
- using business process modelling, knowledge management techniques and ontology models, it enhances the organisational learning within the ICT supply chain
- contributes to the advancement of supply chain management practices to improve the hands-on implementation and security assessment.

### **9.2.4 Contribution to Cybersecurity Risk Management**

The CyberICT Risk Management Methodology:

- contributes to the multi-factor calculation of risk, including the asset technical complexity and asset criticality rules, and estimates the vulnerability exploitability based on complementary vulnerability intrinsic and attacker-specific attributes.
- delivers an applicable risk management methodology which can be easily integrated into a conformity assessment procedure. This is another novelty of the dissertation.
- contributes to attack modelling research by:
  - combining multifarious security-related information, including IoCs and vulnerability assessment results to model attack paths
  - goes beyond traditional risk matrices by capturing ICT behaviours and interdependent failure dynamics.

### **9.2.5 Contribution to Knowledge Management and Ontology Engineering**

This dissertation contributes to the fields of Knowledge Management and Ontology Engineering through the development of ontology-based approaches for cybersecurity risk management and ICT supply chain security. It introduces two original ontologies, namely the CyberICT Risk Ontology and the CyberICT Standards Ontology, which formalise cybersecurity knowledge using Semantic Web technologies (OWL 2 and RDF) and support semantic reasoning and inference for dynamic knowledge extraction and decision support. Furthermore, the dissertation

extends Knowledge Management research by applying the SECI model to ICT supply chain security, providing a systematic approach for capturing, externalising, and reusing cybersecurity knowledge. Collectively, these contributions demonstrate how ontology engineering and knowledge management techniques can improve the representation, sharing, and utilisation of cybersecurity knowledge in complex ICT environments. Furthermore, the dissertation developed a BPMN ontology that provides a semantic representation of the BPMN 2.0.2 process model as a formal ontology. This work contributes to the specific field of Ontology Engineering of Semantic Business Process Modelling which integrates business process modelling with Semantic Web technologies and constitutes an additional ontology-based contribution of this dissertation.

#### **9.2.6 Contribution to Maritime and Logistics Supply Chain security and Critical Infrastructure Protection**

This dissertation contributes to the field of Maritime and Logistics Supply Chain (MLoSC) security by proposing a cybersecurity risk management methodology specifically designed for complex, heterogeneous ICT supply chain environments. The methodology addresses the security of interconnected maritime ICT infrastructures, including SCADA systems, AIS networks, and other Critical Information Infrastructures (CIIs) of the MLoSC, by modelling asset interdependencies, vulnerabilities, attack propagation, and cascading effects across ICT Supply Chain Services (ICT SCSs). Its applicability was demonstrated through representative maritime and logistics scenarios, providing evidence of its suitability for risk assessment in realistic operational environments. Beyond the maritime domain, the proposed approach contributes to Critical Infrastructure Protection by offering a generalisable framework for assessing cyber risks in interconnected ICT ecosystems across multiple sectors. Furthermore, the methodology considers aspects of the NIS 2 Directive and the Cyber Security Act (CSA), by supporting ICT supply chain risk assessment and ICT supply chain service criticality assessment for operators of essential and important services.

#### **9.2.7 Design Science Research**

This dissertation develops a coherent ecosystem of artefacts rather than a single model. The ecosystem relies on the CyberICT hybrid evaluation framework that consists of the CyberICT Risk Management Methodology, and the CyberICT Protection Profile preparatory framework, including the complementary artefacts of the CyberICT risk ontology and CyberICT Protection Profile data model. The developed artefacts are highly connected to address the dissertation objectives in a complementary manner. This creates a multi-layered framework with interlinked components, which can be more comprehensive than isolated approaches.

## References<sup>20</sup>

- [1] E.-M. Kalogeraki, S. Papastergiou, H. Mouratidis, and N. Polemi, "A novel risk assessment methodology for SCADA maritime logistics environments," *Applied Sciences*, vol. 8, no. 9, p. 1477, 2018, [doi: 10.3390/app8091477](https://doi.org/10.3390/app8091477).
- [2] S. Schauer, E.-M. Kalogeraki, S. Papastergiou, and C. Douligeris, "Detecting Sophisticated Attacks in Maritime Environments using Hybrid Situational Awareness," in *Proc. 2019 International Conference on Information and Communication Technologies for Disaster Management (ICT-DM)*, Paris, France, 2019, pp. 1–7. [doi: 10.1109/ICT-DM47966.2019.9032900](https://doi.org/10.1109/ICT-DM47966.2019.9032900)
- [3] European Union Agency for Cybersecurity (ENISA), "ENISA Threat Landscape 2024", ENISA, *Publications Office of the European Union*, September 2024. [doi: 10.2824/0710888](https://doi.org/10.2824/0710888)
- [4] S. Papastergiou, H. Mouratidis, and E. Kalogeraki, "Handling of advanced persistent threats and complex incidents in healthcare, transportation and energy ICT infrastructures," *Evolving Systems*, Vol.12, pp. 91–108, 2020. [doi: 10.1007/s12530-020-09335-4](https://doi.org/10.1007/s12530-020-09335-4).
- [5] A. Sharma, B. B. Gupta, A. K. Singh, and V. K. Saraswat, "Advanced persistent threats (APT): Evolution, anatomy, attribution and countermeasures", *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, no.7, pp. 9355–9381, 2023. [doi: 10.1007/s12652-023-04603-y](https://doi.org/10.1007/s12652-023-04603-y)
- [6] S. Papastergiou, E.-M. Kalogeraki, N. Polemi, and C. Douligeris, "Challenges and issues in risk assessment in modern maritime systems", In *Advances in Core Computer Science-Based Technologies*, G. Tsihrintzis and M. Virvou, Eds. Cham, Switzerland: Springer, 2021, pp. 129–156, [https://doi.org/10.1007/978-3-030-41196-1\\_7](https://doi.org/10.1007/978-3-030-41196-1_7).
- [7] T. Mauer and A. Nelson, "The Global Cyber Threat", *International Monetary Fund (IMF), Finance and Development*, March 2021. [Online]. Available: <https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm> [Accessed June 8, 2026]
- [8] Cyber Management Alliance, "Top 10 Biggest Cyber Attacks of 2024 & 25". Other Attacks to Know About!", Cyber Management Alliance, January 2025. [Online]. Available: <https://www.cm-alliance.com/cybersecurity-blog/top-10-biggest-cyber-attacks-of-2024-25-other-attacks-to-know-about> [Accessed June 8, 2026]
- [9] E.M. Kalogeraki, S. Papastergiou, T. Panayiotopoulos, "An Attack Simulation and Evidence Chains Generation Model for Critical Information Infrastructures", *Electronics, AI-Based Knowledge Management*, 11(3), 404, January 2022, MDPI, <https://doi.org/10.3390/electronics11030404>.
- [10] European Commission, "The EU's cybersecurity strategy for the digital decade," *The EU's Cybersecurity Strategy for the Digital Decade* Directorate-General for Communications Networks, Content and Technology, Joint Communication to the European Parliament and the Council (JOIN2020)18 Final, Brussels, Belgium, 2020. [Online]. Available: <https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0>.
- [11] European Union, Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act). *Official Journal of the European Union*, 32024R2847, Nov. 20, 2024. <http://data.europa.eu/eli/reg/2024/2847/oj>.

---

<sup>20</sup> References in bold are research works conducted in the context of this dissertation.

- [12] European Union, Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive). *Official Journal of the European Union*, 32022L2555, Dec. 27, 2022. <http://data.europa.eu/eli/dir/2022/2555/oj>.
- [13] European Union, Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). *Official Journal of the European Union*, 32019R0881, Feb. June 7, 2019. <http://data.europa.eu/eli/reg/2019/881/oj>.
- [14] European Union, Commission Implementing Regulation (EU) 2024/482 EUCC of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC). *Official Journal of the European Union*, 32024R0482, January 31, 2024. [http://data.europa.eu/eli/reg\\_impl/2024/482/oj](http://data.europa.eu/eli/reg_impl/2024/482/oj).
- [15] D. Boberic Krsticev, E. M. Kalogeraki, S. Karagiorgou, and D. Tesendic, "Risk and conformity assessment platform for supply chains" In M. Trajanović, N. Filipović, and M. Zdravković (eds), *Disruptive Information Technologies for a Smart Society, ICIST 2024, Lecture Notes in Networks and Systems*, vol. 860. Cham, Switzerland: Springer, 2024, ch. 32. [https://doi.org/10.1007/978-3-031-71419-1\\_32](https://doi.org/10.1007/978-3-031-71419-1_32).
- [16] S. Papastergiou *et al.*, "Composite Inspection and Certification (CIC) System for Cybersecurity Assessment of ICT Products, Services, and Processes" In *2024 IEEE International Conference on Cyber Security and Resilience (CSR)*, London, UK, 2024, pp. 833–838, [doi: 10.1109/CSR61664.2024.10679467](https://doi.org/10.1109/CSR61664.2024.10679467).
- [17] M. Ekstedt, Z. Afzal, P. Mukherjee, S. Hacks, and R. Lagerström, "Yet another cybersecurity risk assessment framework," *International Journal of Information Security*, vol. 22, pp. 1713–1729, 2023. [Online]. Available: [doi:org/10.1007/s10207-023-00713-y](https://doi.org/10.1007/s10207-023-00713-y).
- [18] E. M. Kalogeraki and N. Polemi, "A taxonomy for cybersecurity standards" *Journal of Surveillance, Security and Safety*, vol. 5, pp. 95–115, 2024, [doi: 10.20517/jsss.2023.50](https://doi.org/10.20517/jsss.2023.50).
- [19] European Union Agency for Cybersecurity (ENISA), "Network and Information Security Investments 2025", ENISA Publications, December, 2025. [Online]. Available: <https://www.enisa.europa.eu/publications/nis-investments-2025> [Accessed June 8, 2026]
- [20] D.-W. Song and P. Panayides, Eds., *Maritime Logistics: A Guide to Contemporary Shipping and Port Management*, 2nd ed. London, U.K.: Kogan Page Publishers, 2015.
- [21] UN Trade and Development, "Global trade to hit record \$35 trillion despite slowing momentum", *UNCTAD annual report*, December, 2025. [Online]. Available: <https://unctad.org/news/global-trade-hit-record-35-trillion-despite-slowing-momentum>. [Accessed June 8, 2026].
- [22] J. vom Brocke, A. Hevner, and A. Maedche, "Introduction to Design Science Research" In *Design Science Research. Cases*, J. vom Brocke, A. Hevner, and A. Maedche, Eds. Cham, Switzerland: Springer, 2020, pp. 1–13, [doi: 10.1007/978-3-030-46781-4\\_1](https://doi.org/10.1007/978-3-030-46781-4_1).
- [23] A. Benali and B. El Asri, "Towards Rigorous Selection and Configuration of Cloud Services: Research Methodology" In *IJCSI International Journal of Computer Science Issues*, Volume 17, Issue 6, November 2020, [doi:org/10.5281/zenodo.4431076](https://doi.org/10.5281/zenodo.4431076).
- [24] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A design science research methodology for information systems research," *Journal of Management Information Systems*, vol. 24, no. 3, pp. 45–77, 2007, [doi: 10.2753/MIS0742-1222240302](https://doi.org/10.2753/MIS0742-1222240302).



- [25] P. Kotler, *Marketing Management: Analysis, planning, implementation and control*. 9<sup>th</sup> Edition, Prentice Hall International, Upper Saddle River, New Jersey, 1997.
- [26] D. Ivanov, "Predicting the impacts of epidemic outbreaks on global supply chains: A simulation-based analysis on the coronavirus outbreak (COVID-19/SARS-CoV-2) case", *Transportation Research Part E: Logistics and Transportation Review*, vol.136, 101922, pp. 1-14, April 2020. ISSN 1366-5545, <https://doi.org/10.1016/j.tre.2020.101922>.
- [27] D. Li, K.H. Tan, J. Alias, N. Mat, "Global image of countries in international wars: A scoping review of influencing factors". *PLoS One*, 20(10), e0334095, October 2025, <https://doi.org/10.1371/journal.pone.0334095>.
- [28] R. Rame, P. Purwanto, and S. Sudarno, "Industry 5.0 and sustainability: An overview of emerging trends and challenges for a green future", *Innovation and Green Development*, 3(4), 100173, December 2024, Elsevier, <https://doi.org/10.1016/j.igd.2024.100173>.
- [29] I. Vietrov, "Generative AI Trends: Transforming Business and Shaping Future", master.of.code global, March 21, 2026. [Online]. Available: <https://masterofcode.com/blog/generative-ai-trends> [Accessed June 8, 2026]
- [30] V. Ignat, "Digitalization and the global technology trends" In *IOP Conference Series: Materials Science and Engineering* , Vol. 227, No. 1, p. 012062, Nov. 2017, IOP Publishing, <https://doi.org/10.1088/1757-899X/227/1/012062>.
- [31] F. Di Franco, "Analysis of the European R&D priorities in cybersecurity – Strategic priorities in cybersecurity for a safer Europe". ENISA. December, 2018. ISBN: 978-92-9204-278-3 doi:10.2824/14357. [Online]. Available: <https://www.enisa.europa.eu/publications/analysis-of-the-european-r-d-priorities-in-cybersecurity/> [Accessed June 8, 2026]
- [32] M.H. Zafar,, E.F. Langås, and F. Sanfilippo, "Exploring the synergies between collaborative robotics, digital twins, augmentation, and industry 5.0 for smart manufacturing: A state-of-the-art review". *Robotics and Computer-Integrated Manufacturing*, Vol. 89, 102769, October 2024, ISSN: 0736-5845, <https://doi.org/10.1016/j.rcim.2024.102769>.
- [33] Cisco and/or its affiliates, "The Internet of Everything. IoE", Cisco IoE Value Index Study, pp. 1-14, 2013. [Online]. Available: [https://www.cisco.com/c/dam/en\\_us/about/business-insights/docs/ioe-value-index-faq.pdf](https://www.cisco.com/c/dam/en_us/about/business-insights/docs/ioe-value-index-faq.pdf). [Accessed June 8, 2026]
- [34] Information Technology Laboratory. "Glossary". *Computer Security Resource Center (CSRS), National Institute of Standards and Technology (NIST)*, updated March 10, 2026. [Online]. Available: [https://csrc.nist.gov/glossary/term/security\\_requirement](https://csrc.nist.gov/glossary/term/security_requirement). [Accessed June 8, 2026]
- [35] S.S. Shafin, *et al.*, "Obfuscated Memory Malware Detection In Resource-Constrained IoT Devices for Smart City Applications". *Sensors*, 23(11), 5348. June 2023, <https://doi.org/10.3390/s23115348>
- [36] I. Kara and M. Aydos, "The rise of ransomware: Forensic analysis for windows-based ransomware attacks". *Expert Systems with Applications*, 190, 116198, March 2022, <https://doi.org/10.1016/j.eswa.2021.116198>.
- [37] Council of the EU and the European Council. "Cyber threats in the EU: facts and figure"s EU Consilium, June 30, 2025. [Online]. Available: <https://www.consilium.europa.eu/en/policies/top-cyber-threats/> [Accessed June 8, 2026]
- [38] G. Moschetta, *et al.*, "Global Security Outlook 2026", World Economic Forum in collaboration with Accenture. Insight Report, January, 2026 [Online]. Available: [https://reports.weforum.org/docs/WEF\\_Global\\_Cybersecurity\\_Outlook\\_2026.pdf](https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2026.pdf) [Accessed June 8, 2026]
- [39] European Commission, "Commission responds to cyber-attack on its Europa web platform", *Press release*, March 2026 [Online]. Available:

- [https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip\\_26\\_748/IP\\_26\\_748\\_EN.pdf](https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_26_748/IP_26_748_EN.pdf)  
[Accessed June 8, 2026]
- [40] R. Chandramouli, "Implementation of DevSecOps for a Microservices-based Application with Service Mesh", *National Institute of Standards and Technology, Gaithersburg, MD, NIST Special Publication (SP) 800-204C*, 2022, <https://doi.org/10.6028/NIST.SP.800-204C>.
  - [41] ISO/IEC/IEEE 32675:2022, "Information technology – DevOps – Building reliable and secure systems including application build, package and deployment", International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), and Institute of Electrical and Electronics Engineers (IEEE), Geneva, Switzerland, Edition 1, 2022. [Online]. Available: <https://www.iso.org/standard/83670.html>.
  - [42] European Commission. "Shaping Europe's digital future. Cyber Resilience Act", Directorate - General for Communications Networks, Content and Technology, December 3, 2025. [Online]. Available: <https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act> [Accessed June 8, 2026]
  - [43] European Commission. "Shaping Europe's digital future. Cybersecurity Act", Directorate - General for Communications Networks, Content and Technology, January 20, 2026. [Online]. Available: <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act> [Accessed June 8, 2026]
  - [44] ISO/IEC 15408-1: 2026, "Information security, cybersecurity and privacy protection — Evaluation criteria for IT security – Part 1: Introduction and general model". International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), Geneva, Switzerland, Edition 5, May 2026. [Online]. Available: <https://www.iso.org/obp/ui/en/#iso:std:iso-iec:15408:-1:ed-5:v1:en> [Accessed May 30, 2026]
  - [45] ISO/IEC 15408-2: 2026, "Information security, cybersecurity and privacy protection — Evaluation criteria for IT security Part 2: Security functional components". International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), Geneva, Switzerland, Edition 5, May 2026. [Online]. Available: <https://www.iso.org/standard/15408-2> [Accessed May 30, 2026]
  - [46] ISO/IEC 15408-3: 2026, "Information security, cybersecurity and privacy protection — Evaluation criteria for IT security Part 3: Security assurance components". International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), Geneva, Switzerland, Edition 5, May 2026. [Online]. Available: <https://www.iso.org/standard/15408-3> [Accessed May 30, 2026]
  - [47] European Union, Regulation (EU) 2025/37 of the European Parliament and of the Council of 19 December 2024 amending Regulation (EU) 2019/881 as regards managed security services. *Official Journal of the European Union*, 32025R0037, Dec. 19, 2024. <http://data.europa.eu/eli/reg/2025/37/oj>
  - [48] European Union Cybersecurity Certification, "EUMSS - EU Cybersecurity certification for Managed Security Services", ENISA. [Online]. Available: [https://certification.enisa.europa.eu/browse-topic/eumss\\_en?prefLang=da](https://certification.enisa.europa.eu/browse-topic/eumss_en?prefLang=da) [Accessed June 8, 2026]
  - [49] European Commission, "Shaping Europe's digital future. Proposal for a Regulation for the EU Cybersecurity Act". Directorate - General for Communications Networks, Content and Technology (DG-CONNECT), January 20, 2026. <https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-eu-cybersecurity-act> [Accessed June 8, 2026]
  - [50] European Union, Regulation (EU) 2016/1148 of the European Parliament and of the Council of (EU) concerning measures for a high common level of security of network and information systems across the Union. *Official Journal of the European Union*, 32016L1148, July 6, 2016. <http://data.europa.eu/eli/dir/2016/1148/oj>
  - [51] European Commission, "Shaping Europe's digital future. NIS 2 Directive: securing network and information systems", Directorate - General for Communications Networks, Content and Technology (DG-CONNECT), January 20, 2026. [Online]. Available: <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive> [Accessed June 8, 2026]

- [52] European Commission, “Shaping Europe’s digital future. Proposal for a Directive as regards simplification measures and alignment with the Cybersecurity Act”. *Directorate - General for Communications Networks, Content and Technology (DG-CONNECT)*, January 20, 2026. [Online]. Available: <https://digital-strategy.ec.europa.eu/en/library/proposal-directive-regards-simplification-measures-and-alignment-cybersecurity-act>. [Accessed June 8, 2026]
- [53] ISO/IEC 27000:2018, “Information technology – Security techniques – Information security management systems – Overview and vocabulary”. International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), 5<sup>th</sup> Edition 2018-02, Geneva, Switzerland, 2018. [Online]. Available: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en>. [Accessed June 8, 2026]
- [54] ISO/IEC 27000 family, “Information Security Management”. [Online]. Available: <https://www.iso.org/standard/iso-iec-27000-family> [Accessed June 8, 2026]
- [55] ISO/IEC 27001:2022, “Information security, cybersecurity and privacy protection — Information security management systems — Requirements”. International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), 3<sup>rd</sup> Edition, Geneva, Switzerland, 2022. [Online]. Available: <https://www.iso.org/standard/27001>. [Accessed June 8, 2026]
- [56] ISO/IEC 27005:2022, “Information technology – Security techniques – Information security risk management”. International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), 4<sup>th</sup> Edition, 2022-10, Geneva, Switzerland, 2022. [Online]. Available: <https://www.iso.org/standard/80585.html>. [Accessed June 8, 2026]
- [57] ISO/IEC 17000:2020, “Conformity assessment Vocabulary and general principles”. International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), 2<sup>nd</sup> Edition, 2020-12, Geneva, Switzerland, 2020. [Online]. Available: <https://www.iso.org/standard/73029.html> [Accessed June 8, 2026]
- [58] Common Criteria Development Board, “Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model”, *Common Criteria*, CCMB-2022-11-001, Rev.1, Nov. 2022 [Online]. Available: <https://www.commoncriteriaportal.org/files/ccfiles/CC2022PART1R1.pdf>. [Accessed June 8, 2026]
- [59] ISO/IEC 18045-1:2026. “Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Methodology for IT security evaluation”. International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), 4<sup>th</sup> Edition, 2026-05, Geneva, Switzerland, 2026. [Online]. Available: <https://www.iso.org/standard/18045> [Accessed June 8, 2026].
- [60] S. Taubenberger, “Vulnerability identification errors in security risk assessments”. PhD thesis, Open University (United Kingdom), *ProQuest LLC*, 10059762, 2014. [Online]. Available: <https://www.proquest.com/openview/4af133416397b06b5d7c8bac3acc452b/1?pq-origsite=gscholar&cbl=51922> [Accessed June 8, 2026]
- [61] R. Breu, F. Innerhofer-Oberperfler, and A. Yautsiukhin, “Quantitative assessment of enterprise security system,” in *Proc. IEEE 3rd Int. Conf. Availability, Reliability and Security (ARES 2008)*, Mar. 2008, pp. 921–928.
- [62] E. Andrukiewicz and J. M. Batalla, “Methodology for Sectoral Cybersecurity Assessments”. *European Union Agency for Cybersecurity (ENISA)*, Heraklion, Greece, 2021.
- [63] P. Kyranoudi, E. M. Kalogeraki, A. Michota, and N. Polemi, “Cybersecurity certification requirements for supply chain services,” In *Proc. 26<sup>th</sup> IEEE Symposium on Computers and Communications (ISCC)*, Athens, Greece, Sep. 5–8, 2021, pp. 1–7. <https://doi.org/10.1109/ISCC53001.2021.9631467>
- [64] European Commission, “Single market, Internal Market, Industry, Entrepreneurship and SMEs”, Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs (n.d.). [Online]. Available: [https://single-market-economy.ec.europa.eu/single-market\\_en](https://single-market-economy.ec.europa.eu/single-market_en). [Accessed June 8, 2026]

- [65] M. Hogan and E. Newton, "Supplemental Information for the Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity". Cybersecurity Standardization Working Group of the National Security Council's Cyber Interagency Policy Committee, NIST, NISTIR 8074, Vol.2. <http://dx.doi.org/10.6028/NIST.IR.8074v2>
- [66] ISO/IEC 27002:2022, "Information security, cybersecurity and privacy protection — Information security controls". International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), 3<sup>rd</sup> Edition, Geneva, Switzerland, 2022. [Online]. Available: <https://www.iso.org/standard/75652.html> . [Accessed June 8, 2026]
- [67] ISO/IEC 22300:2025, "Security and Resilience – Vocabulary". International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), 4<sup>th</sup> Edition, Geneva, Switzerland, 2025. [Online]. Available: <https://www.iso.org/standard/85749.html> [Accessed June 8, 2026]
- [68] T. H. Davenport, "Process Innovation: Reengineering Work through Information Technology". Harvard Business School Press, Boston, MA, USA, 1993.
- [69] J. T. Mentzer *et al.*, "Defining supply chain management," *Journal of Business Logistics*, vol. 22, no. 2, pp. 1–25, 2001, <https://doi.org/10.1002/j.2158-1592.2001.tb00001.x>
- [70] ISO 28001:2007, "Security management systems for the supply chain — Best practices for implementing supply chain security, assessments and plans — Requirements and guidance". International Organization for Standardization (ISO), 1<sup>st</sup> Edition, Geneva, Switzerland, 2007. [Online]. Available: <https://www.iso.org/standard/45654.html> . [Accessed June 8, 2026]
- [71] R. K. Oliver and M. D. Webber, "Supply-chain management: Logistics catches up with strategy," in *The Roots of Logistics*, Springer, Berlin, Heidelberg, 2012, pp. 183–194. [https://doi.org/10.1007/978-3-642-27922-5\\_15](https://doi.org/10.1007/978-3-642-27922-5_15)
- [72] D. Ivanov, A. Tsipoulanis, and J. Schönberger, "Supply Chain Risk Management and Resilience, in Global Supply Chain and Operations Management", *Springer Texts in Business and Economics*. Springer, Cham, Switzerland, 2021, [https://doi.org/10.1007/978-3-030-72331-6\\_15](https://doi.org/10.1007/978-3-030-72331-6_15)
- [73] T. Y. Choi and Y. Hong, "Unveiling the structure of supply networks: case studies in Honda, Acura, and DaimlerChrysler," *Journal of Operations Management*, vol. 20, no. 5, pp. 469–493, 2002, [https://doi.org/10.1016/S0272-6963\(02\)00025-6](https://doi.org/10.1016/S0272-6963(02)00025-6).
- [74] J. H. Han, Y. Wang, and M. Naim, "Reconceptualization of information technology flexibility for supply chain management: An empirical study," *International Journal of Production Economics*, vol. 187, pp. 196–215, 2017, <https://doi.org/10.1016/j.ijpe.2017.02.018>.
- [75] D. Power, "Supply chain management integration and implementation: A literature review," *Supply Chain Management*, vol. 10, no. 4, pp. 252–263, 2005. Online ISSN:1758-6852, <https://doi.org/10.1108/13598540510612721>.
- [76] J. Boyens, C. Paulsen, N. Bartol, K. Winkler, J. Gimbi, "Key Practices in Cyber Supply Chain Risk Management: Observations from Industry", *NISTIR 8276*, Gaithersburg, MD, USA, 2021. <https://doi.org/10.6028/NIST.IR.8276>.
- [77] S. Cadzow *et al.*, "Supply Chain Integrity: An Overview of the ICT Supply Chain Risks and Challenges, and Vision for the Way Forward", ENISA, Heraklion, Greece, v.1.1, Aug. 2015.
- [78] J. Boyens, A. Smith, N. Bartol, K. Winkler, A. Holbrook, and M. Fallon, "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations", *National Institute of Standards and Technology*, Gaithersburg, NIST Special Publication (SP) 800-161r1-upd1, May 2022, including updates as of 11 Jan., 2024. <https://doi.org/10.6028/NIST.SP.800-161r1-upd1>

- [79] United Nations Industrial Development Organization (UNIDO), "Building Sustainable Supply Chains for Developing Economies: Pathways to 2050 – Summary", *UNIDO Foresight Study Report*, Vienna, Austria, Aug. 2025. [Online]. Available: <https://www.unido.org/sites/default/files/unido-publications/2025-11/Building%20Sustainable%20Supply%20Chains%20for%20Developing%20Economies%20-%20Pathways%20to%202050%20-%20Summary.pdf>. [Accessed June 8, 2026]
- [80] M. A. Saeed and W. Kersten, "Drivers of sustainable supply chain management: Identification and classification," *Sustainability*, vol. 11, no. 4, p. 1137, 2019, doi: [10.3390/su11041137](https://doi.org/10.3390/su11041137).
- [81] E. Koberg and A. Longoni, "A systematic review of sustainable supply chain management in global supply chains," *Journal of Cleaner Production*, vol. 207, pp. 1084–1098, 2019, <https://doi.org/10.1016/j.jclepro.2018.10.033>
- [82] ISO 22301:2019, "Security and resilience—Business continuity management systems—Requirements". International Organization for Standardization (ISO), 2<sup>nd</sup> Edition, Geneva, Switzerland, 2019 [Online]. Available: <https://www.iso.org/standard/75106.html>. [Accessed June 8, 2026].
- [83] M. F. Blos, S. L. Hoeflich, P. E. Miyagi, "A general supply chain continuity management framework". *Procedia Computer Science*, vol. 55, pp.1160-1164, 2015, doi: [10.1016/j.procs.2015.07.087](https://doi.org/10.1016/j.procs.2015.07.087).
- [84] E.-M. Kalogeraki, D. Apostolou, N. Polemi, and S. Papastergiou, "Knowledge management methodology for identifying threats in maritime/logistics supply chains", In *Knowledge Management Research & Practice, Special Issue on "Logistics Knowledge Management: State of the Art and Future Perspectives,"* S. Durst and P. Evangelista, Eds., vol. 16, no. 4, pp. 508–524, June, 2018, ISSN: 1477-8238 (Print) 1477-8246, doi: [10.1080/14778238.2018.1486789](https://doi.org/10.1080/14778238.2018.1486789).
- [85] H. L. Lee, "The Triple-A Supply Chain," *Harvard Business Review*, vol. 82, no. 10, pp. 102–112, 2004. [Online]. Available: <https://hbr.org/2004/10/the-triple-a-supply-chain>. [Accessed June 8, 2026]
- [86] C. Cai, L. Pan, X. Li, S. Luo, and Z. Wu, "A risk identification model for ICT supply chain based on network embedding and text encoding," *Expert Systems with Applications*, vol. 228, p. 120459, Oct. 2023, doi: [10.1016/j.eswa.2023.120459](https://doi.org/10.1016/j.eswa.2023.120459)
- [87] N. Kailash, R. Saha, and S. Goyal, "Systematic literature review of classification and categorisation of benchmarking in supply chain management", *International Journal of Process Management and Benchmarking*, vol. 7, no. 2, pp. 183–205, 2017. doi: [10.1504/IJPMB.2017.083105](https://doi.org/10.1504/IJPMB.2017.083105).
- [88] J. Pennekamp *et al.*, "An interdisciplinary survey on information flows in supply chains," *ACM Computing Surveys*, vol. 56, no. 2, pp. 1–38, 2023, doi: [10.1145/3606693](https://doi.org/10.1145/3606693).
- [89] G. Büyüközkan and F. Göçer, "Digital Supply Chain: Literature review and a proposed framework for future research," *Computers in Industry*, vol. 97, pp. 157-177, May 2018, doi: [10.1016/j.compind.2018.02.010](https://doi.org/10.1016/j.compind.2018.02.010).
- [90] F. Farajpour, A. Hassanzadeh, S. Elahi, and M. Ghazanfari, "Digital supply chain blueprint via a systematic literature review," *Technological Forecasting and Social Change*, vol. 184, p. 121976, Nov. 2022, doi: [10.1016/j.techfore.2022.121976](https://doi.org/10.1016/j.techfore.2022.121976).
- [91] T. Baltacioglu, E. Ada, M. D. Kaplan, O. Yurt, and Y. C. Kaplan, "A new framework for service supply chains", *The Service Industries Journal*, vol. 27, no. 2, pp. 105–124, 2007, doi: [10.1080/02642060601122629](https://doi.org/10.1080/02642060601122629).
- [92] E.-M. Kalogeraki, T. Panayiotopoulos, and D. Apostolou, "Semantic queries in BPMN 2.0: A contemporary method for information retrieval", In *2015 6th International Conference on Information, Intelligence, Systems and Applications (IISA)*, 2015, pp. 1–6, doi: [10.1109/IISA.2015.7388061](https://doi.org/10.1109/IISA.2015.7388061).
- [93] E.-M. Kalogeraki, S. Theocharis, D. Apostolou, G. Tsihrintzis, and T. Panayiotopoulos, "Semantic concepts in BPMN 2.0", In *Proceedings of the 5th IEEE International Conference on Information, Intelligence, Systems and Applications (IISA)*, 2014, pp. 207–209, doi: [10.1109/IISA.2014.6878791](https://doi.org/10.1109/IISA.2014.6878791).



- [94] E. Yahia, M. Bigand, J. P. Bourey, and E. Castelain, "Supply chain business patterns definition for process interoperability", In *Proc. 13th IFAC Symp. Information Control Problems in Manufacturing (INCOM)*, Moscow, Russia, Jun. 2009, pp. 169–174, [doi: 10.3182/20090603-3-RU-2001.0359](https://doi.org/10.3182/20090603-3-RU-2001.0359).
- [95] E. M. Kalogeraki, N. Polemi, and S. Papastergiou, "A modeling approach for maritime supply chain services", In *Proc. 12th Int. Forum on Knowledge Asset Dynamics (IFKAD), Knowledge Management in the 21st Century: Resilience, Creativity and Co-creation*, J. C. Spender, G. Schiuma, and T. Gavrilova, Eds., St. Petersburg, Russia, 2017, pp. 1612–1627, ISSN: 2280-787X.
- [96] E.-M. Kalogeraki, N. Polemi, S. Papastergiou, and T. Panayiotopoulos, "Modeling SCADA attacks" In *Smart Trends in Systems, Security and Sustainability*, X.-S. Yang, A. Nagar, and A. Joshi, Eds., Lecture Notes in Networks and Systems, vol. 18. Singapore: Springer, 2018, pp. 47–55, 2017, [doi: 10.1007/978-981-10-6916-1\\_5](https://doi.org/10.1007/978-981-10-6916-1_5).
- [97] E.-M. Kalogeraki, S. Papastergiou, N. Polemi, C. Douligeris, and T. Panayiotopoulos, "Exploring cyber-security issues in vessel traffic services", In *Knowledge Science, Engineering and Management, Lecture Notes in Computer Science (LNAI)*, vol. 11061, Springer, Cham, Switzerland, 2018, pp. 442–451, [doi: 10.1007/978-3-319-99247-9\\_39](https://doi.org/10.1007/978-3-319-99247-9_39).
- [98] UN Trade and Development, "Review of Maritime Transport", *UNCTAD*, Transport, logistics and trade facilitation. [Online]. Available: <https://unctad.org/topic/transport-and-trade-logistics/review-of-maritime-transport>. [Accessed June 8, 2026].
- [99] European Union, "Maritime transport dominates international trade", Eurostat, September 2025. [Online]. Available: <https://ec.europa.eu/eurostat/web/products-eurostat-news/w/edn-20250925-1>.
- [100] S. Gülmez, G. Denктаş Şakar, and S. Baştuğ, "An overview of maritime logistics: Trends and research agenda", *Maritime Policy & Management*, vol. 50, no. 1, pp. 97–116, 2023, [doi: 10.1080/03088839.2021.1962557](https://doi.org/10.1080/03088839.2021.1962557).
- [101] J. An, "Maritime logistics and digital transformation with big data: Review and research trend", *Maritime Business Review*, vol. 9, no. 3, pp. 229–242, 2024, [doi: 10.1108/MABR-10-2023-0069](https://doi.org/10.1108/MABR-10-2023-0069).
- [102] A. Drougkas, A. Sarri and P. Kyranoudi, "Guidelines – Cyber Risk Management for Ports", *European Union Agency for Cybersecurity (ENISA)*, 2020, ISBN: 978-92-9204-403-9. [Online]. Available: <https://www.enisa.europa.eu/publications/guidelines-cyber-risk-management-for-ports>. [Accessed June 8, 2026].
- [103] N. Polemi, *Port Cybersecurity: Securing Critical Information Infrastructures and Supply Chains*. Elsevier, 2017, pp.1–193.
- [104] L. M. Ascencio, R. G. González-Ramírez, L. A. Bearzotti, N. R. Smith, and J. F. Camacho-Vallejo, "A Collaborative Supply Chain Management System for a Maritime Port Logistics Chain," *Journal of Applied Research and Technology*, vol. 12, no. 3, pp. 444–458, 2014. ISSN: 1665-6423. [https://doi.org/10.1016/S1665-6423\(14\)71625-6](https://doi.org/10.1016/S1665-6423(14)71625-6).
- [105] C. Zhou, H. Li, W. Liu, A. Stephen, L. H. Lee, and E. P. Chew, "Challenges and opportunities in integration of simulation and optimization in maritime logistics" In *Proc. 2018 Winter Simulation Conf. (WSC)*, Dec. 2018, pp. 2897–2908. [doi: 10.1109/WSC.2018.8632202](https://doi.org/10.1109/WSC.2018.8632202).
- [106] J. Shi, J. Chen, L. Xu, Z. Di, and Q. Qu, "Improving the resilience of maritime supply chains: The integration of ports and inland transporters in duopoly markets", *Engineering Management*, vol. 10, pp. 51–66, 2023. [doi: 10.1007/s42524-022-0231-3](https://doi.org/10.1007/s42524-022-0231-3).
- [107] L. Feng, X. Wang, Q. Wang, P. Jia, and A. K. Ng, "Robust optimization of port logistics service supply chain under demand uncertainties," *Ocean & Coastal Management*, vol. 271, p. 107935, 2026, [doi: 10.1016/j.ocecoaman.2025.107935](https://doi.org/10.1016/j.ocecoaman.2025.107935).

- [108] C. Durán, A. K. Yazdi, I. Derpich, and Y. Tan, "Leveraging blockchain for maritime port supply chain management through multicriteria decision making," *Mathematics*, vol. 12, no. 10, p. 1511, 2024. [doi: 10.3390/math12101511](https://doi.org/10.3390/math12101511).
- [109] E.-M. Kalogeraki, C. Troussas, D. Apostolou, M. Virvou, and T. Panayiotopoulos, "Ontology-based model for learning object metadata" In *Proc. 7th Int. Conf. Information, Intelligence, Systems and Applications (IISA)*, 2016, Art. no. 7785383. [doi: 10.1109/IISA.2016.7785383](https://doi.org/10.1109/IISA.2016.7785383).
- [110] E.-M. Kalogeraki, D. Apostolou, T. Panayiotopoulos, G. Tsihrintzis, and S. Theocharis, "A semantic approach for representing and querying business processes," in *Intelligent Computing Systems: Emerging Application Areas, Studies in Computational Intelligence*, vol. 627, pp. 87–114, Springer, 2016. [doi:10.1007/978-3-662-49179-9\\_4](https://doi.org/10.1007/978-3-662-49179-9_4)
- [111] B. L. MacCarthy and D. Ivanov, Eds., *The Digital Supply Chain*. Amsterdam, The Netherlands: Elsevier, 2022. [doi: 10.1016/C2020-0-03788-6](https://doi.org/10.1016/C2020-0-03788-6).
- [112] P. Grefen and I. Vanderfeesten, Eds., *Handbook on Business Process Management and Digital Transformation*. Cheltenham, U.K.: Edward Elgar Publishing, 2024, [doi: 10.4337/9781802206098](https://doi.org/10.4337/9781802206098).
- [113] S. Somabutr, S. Pandian, and S. Roh, "Conceptualizing a resilient supply chain paradigm in service industry," in *Proc. 4th Int. Conf. on Computers in Management and Business (ICCMB)*, Jan. 2021, pp. 53–57. [doi:10.1145/3450588.3450598](https://doi.org/10.1145/3450588.3450598)
- [114] ISO/IEC 19510:2013, "Information technology — Object Management Group Business Process Model and Notation". International Organization for Standardization (ISO), 1<sup>st</sup> Edition, Geneva, Switzerland, 2013 [Online]. Available: <https://www.iso.org/standard/62652.html>. [Accessed June 8, 2026].
- [115] P. Bergener, P. Delfmann, B. Weiss, and A. Winkelmann, "Detecting potential weaknesses in business processes: An exploration of semantic pattern matching in process models," *Business Process Management Journal*, vol. 21, no. 1, pp. 25–54, 2015 [doi:10.1108/BPMJ-07-2013-0103](https://doi.org/10.1108/BPMJ-07-2013-0103)
- [116] T. R. Gruber, "A translation approach to portable ontology specifications," *Knowledge Acquisition*, vol. 5, no. 2, pp. 199–220, 1993. [doi:10.1006/knac.1993.1008](https://doi.org/10.1006/knac.1993.1008)
- [117] I. Nonaka, "A dynamic theory of organizational knowledge creation," *Organization Science*, vol. 5, no. 1, pp. 14–37, 1994. [doi: 10.1287/orsc.5.1.14](https://doi.org/10.1287/orsc.5.1.14)
- [118] ISO 30401:2018, "Knowledge management systems — Requirements". Organization for Standardization (ISO), 1<sup>st</sup> Edition, Geneva, Switzerland, 2018-11. [Online]. Available: <https://www.iso.org/standard/68683.html#amendment> [Accessed June 8, 2026].
- [119] American Productivity & Quality Center, Knowledge Management Strategic Framework, APCW. [Online]. Available: <https://www.apqc.org/expertise/knowledge-management/interactive-km-framework> [Accessed June 8, 2026].
- [120] Z. Wahl, "Top Knowledge Management Trends – 2026", Enterprise Knowledge, January 29 , 2026. [Online]. Available: <https://enterprise-knowledge.com/top-knowledge-management-trends-2026/> [Accessed June 8, 2026].
- [121] J. Harper, "The Next Generation of Knowledge Management", Knowledge Management World, November 10, 2025. [Online]. Available: <https://www.kmworld.com/Articles/Editorial/Features/The-Next-Generation-of-Knowledge-Management-172132.aspx> [Accessed June 8, 2026].
- [122] N. Fteimi and K. Hopf, "Knowledge management in the era of artificial intelligence: Developing an integrative framework" In *Proc. ECIS 2021 Research-in-Progress Papers*, Marrakesh, Morocco, 2021, pp. 1–10.

- [123] Smitrex, “AI-Powered Knowledge Management: The Real State of Play in 2026” , May16, 2026 [Online]. Available: <https://smritex.com/ai-knowledge-management/> [Accessed June 8, 2026].
- [124] J. Burrell and N. Jones, “Knowledge management and technology for enhanced cybersecurity effectiveness,” *Online Journal of Applied Knowledge Management*, vol. 12, no. 1, pp. 54–72, 2024, doi: 10.36965/OJAKM.2024.12(1)54-72
- [125] National Institute of Standards and Technology, “Guide for Conducting Risk Assessments”, NIST Special Publication 800-30 Rev. 1, Gaithersburg, MD, USA, September 2012, doi: [10.6028/NIST.SP.800-30r1](https://doi.org/10.6028/NIST.SP.800-30r1).
- [126] R. Cerchione, P. Centobelli, E. Borin, A. Usai, and E. Oropallo, “The WISED knowledge-creating company: Rethinking SECI model in light of the digital transition,” *Journal of Knowledge Management*, vol. 28, no. 10, pp. 2997–3022, 2024, doi: [10.1108/JKM-02-2024-0133](https://doi.org/10.1108/JKM-02-2024-0133).
- [127] A. B. M. M. Hasan, L. Brankovic, D. Paul, and C. Sanin, “A systematic literature review on cybersecurity ontology,” *Procedia Computer Science*, vol. 270, pp. 3598–3607, 2025, doi: [10.1016/j.procs.2025.09.485](https://doi.org/10.1016/j.procs.2025.09.485).
- [128] B. Thalheim, “The science and art of conceptual modeling,” in *Lecture Notes in Computer Science*, vol. 7600, pp. 76–105, Springer, 2012. doi:[10.1007/978-3-642-34179-3\\_3](https://doi.org/10.1007/978-3-642-34179-3_3)
- [129] W3C Semantic Web standards, “Resource Description Framework (RDF)”, W3C, 2026. [Online]. Available: <https://www.w3.org/RDF/> [Accessed June 8, 2026].
- [130] World Wide Web Consortium (W3C), “OWL 2 Web Ontology Language - Document Overview”, W3C Recommendation, 2<sup>nd</sup> Edition, 11 December 2012 [Online]. Available: <https://www.w3.org/TR/owl2-overview/> [Accessed June 8, 2026].
- [131] W3C Semantic Web standards, SPARQL 1.2, W3C, April 23, 2026. [Online]. Available: <https://www.w3.org/TR/sparql12-update/> [Accessed June 8, 2026].
- [132] Stanford University, “Protégé open-source OWL ontology editor” The Board of Trustees of the Leland Stanford Junior University, [Online]. Available: <https://protege.stanford.edu/> [Accessed June 8, 2026].
- [133] W3C Semantic Web standards, HermiT, W3C, 2011. [Online]. Available: <https://www.w3.org/2001/sw/wiki/Hermit> [Accessed June 8, 2026].
- [134] W3C Semantic Web standards, FaCT++, W3C, 2026. [Online]. Available: <https://www.w3.org/2001/sw/wiki/FaCT++> [Accessed June 8, 2026].
- [135] W3C Semantic Web standards, Pellet, W3C, 2026. [Online]. Available: <https://www.w3.org/2001/sw/wiki/Pellet> [Accessed June 8, 2026].
- [136] J. M. Pawlowski and M. Bick, “The global knowledge management framework: Towards a theory for knowledge management in globally distributed settings,” *Leading Issues in Knowledge Management*, vol. 2, no. 2, p. 134, 2015.
- [137] ISO/IEC 27032:2023, “Cybersecurity – Guidelines for internet security”. Organization for Standardization (ISO), International Electrotechnical Commission (IEC), 2<sup>nd</sup> Edition, Geneva, Switzerland, 2023. [Online]. Available: <https://www.iso.org/standard/76070.html>. [Accessed June 8, 2026]
- [138] ISO 28000:2022, “Security and resilience — Security management systems — Requirements”. Organization for Standardization (ISO), 2<sup>nd</sup> Edition, Geneva, Switzerland, 2022. [Online]. Available: <https://www.iso.org/standard/79612.html> [Accessed June 8, 2026]
- [139] Forum of Incident Response and Security Teams (FIRST), “Common Vulnerability Scoring System”, *FIRST*, Specification Document, v3.1, Rev.1, Jun. 2019. [Online]. Available: <https://www.first.org/cvss/v3.1/specification-document>. [Accessed June 8, 2026]



- [140] MITRE, Common Vulnerabilities and Exposures, *CVE Program Mission, The MITRE Corporation*. [Online]. Available: <https://www.cve.org/>. [Accessed June 8, 2026]
- [141] J. Slaughter, F. Gutierrez, and S. Imano, "MOVEit Transfer Critical Vulnerability (CVE-2023-34362) Exploited as a 0-day", Fortinet FortiGuard Labs, Jun. 8, 2023. [Online]. Available: <https://www.fortinet.com/blog/threat-research/moveit-transfer-critical-vulnerability-cve-2023-34362-exploited-as-a-0-day>. [Accessed June 8, 2026]
- [142] MITRE, "Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK)", *MITRE Corporation*, ATT&CK Knowledge Base v19, April 28, 2026. [Online]. Available: <https://attack.mitre.org/>. [Accessed June 8, 2026]
- [143] Microsoft, "What is an advanced persistent threat (APT)?" *Microsoft Security*. [Online]. Available: Microsoft Security APT Article. [Online]. Available: <https://www.microsoft.com/en-us/security/business/security-101/what-is-advanced-persistent-threat-apt> [Accessed June 8, 2026]
- [144] European Union Agency for Cybersecurity (ENISA), "ENISA Cybersecurity Threat Landscape Methodology", *ENISA, Publications Office of the European Union*, August 2025, [doi: 10.2824/1888892](https://doi.org/10.2824/1888892)
- [145] Lockheed Martin, "The Cyber Kill Chain", Lockheed Martin, 2025. [Online]. Available: <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html> [Accessed June 8, 2026]
- [146] J. Jacobs, S. Romanosky, O. Suci, B. Edwards, and A. Sarabi, "Enhancing vulnerability prioritization: Data-driven exploit predictions with community-driven insights", June 2023, *arXiv preprint* [arXiv:2302.14172](https://arxiv.org/abs/2302.14172), 2023.
- [147] T.-H. Yun and M. Min, "MITRE ATT&CK-driven threat analysis for edge-IoT environment and a quantitative risk scoring model," *Computer Modeling in Engineering & Sciences*, vol. 145, no. 2, pp. 2707–2731, 2025, [doi:10.32604/cmes.2025.072357](https://doi.org/10.32604/cmes.2025.072357)
- [148] J. Wang, M. Neil, and N. Fenton, "A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model," *Computers & Security*, vol. 89, p. 101659, Feb. 2020, [doi: 10.1016/j.cose.2019.101659](https://doi.org/10.1016/j.cose.2019.101659).
- [149] G. Zeller and M. Scherer, "A comprehensive model for cyber risk based on marked point processes and its application to insurance", *European Actuarial Journal*, vol. 12, no. 1, pp. 33–85, Jun. 2022, [doi: 10.1007/s13385-021-00290-1](https://doi.org/10.1007/s13385-021-00290-1).
- [150] C. Grigoriadis, R. Laborde, A. Verdier, and P. Kotzanikolaou, "An adaptive, situation-based risk assessment and security enforcement framework for the maritime sector", *Sensors*, vol. 22, no. 1, p. 238, 2022, [doi: 10.3390/s22010238](https://doi.org/10.3390/s22010238).
- [151] J. C. Muria-Tarazón, J. V. Oltra-Gutiérrez, R. Oltra-Badenes, and S. Escobar-Román, "Uncovering research trends on artificial intelligence risk assessment in businesses: A state-of-the-art perspective using bibliometric analysis", *Applied Sciences*, vol. 15, no. 3, p. 1412, 2025, [doi: 10.3390/app15031412](https://doi.org/10.3390/app15031412).
- [152] European Telecommunications Standards Institute, "CYBER; Methods and Protocols; Part 1: Method and Pro Forma for Threat, Vulnerability, Risk Analysis (TVRA)", *European Telecommunications Standards Institute*, ETSI TS 102 165-1 v5.2.5, Jan. 2022. [Online]. Available: [https://www.etsi.org/deliver/etsi\\_ts/102100\\_102199/10216501/05.02.05\\_60/ts\\_10216501v050205p.pdf](https://www.etsi.org/deliver/etsi_ts/102100_102199/10216501/05.02.05_60/ts_10216501v050205p.pdf) [Accessed June 8, 2026]
- [153] ISO/IEC 27035-1:2023, "Information technology — Information security incident management — Part 1: Principles and process". Organization for Standardization (ISO), International Electrotechnical Commission (IEC), 2<sup>nd</sup> Edition, Geneva, Switzerland, 2023. [Online]. Available: <https://www.iso.org/standard/78973.html> (Last Accessed: Dec. 10, 2024).

- [154] European Union, Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, *Official Journal of the European Union*, 32008L0114, vol. L 345, pp. 75–82, Dec. 23, 2008, <http://data.europa.eu/eli/dir/2008/114/oj>.
- [155] European Union, Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (CER Directive), *Official Journal of the European Union*, 32022L2557, vol. L 333, pp. 164–198, Dec. 27, 2022, <http://data.europa.eu/eli/dir/2022/2557/oj>.
- [156] European Parliament, “European Parliament resolution of 12 June 2012 on Critical Information Infrastructure Protection – achievements and next steps: towards global cyber-security (2011/2284(INI))”, *Official Journal of the European Union*, 32014L0053, vol. C 332 E, pp. 22–29, Nov. 15, 2013. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52012IP0237>. [Accessed June 8, 2026]
- [157] European Union, “Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of Regulation (EU) 2024/2847 of the European Parliament and of the Council as regards technical descriptions of the categories of important and critical products with digital elements”, *Official Journal of the European Union*, 32024R2690, Oct. 18, 2024, [http://data.europa.eu/eli/reg\\_impl/2024/2690/oj](http://data.europa.eu/eli/reg_impl/2024/2690/oj).
- [158] European Union, “Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector” *Official Journal of the European Union*, 32022R2554, vol. 65, pp. L333/1–L333/79, Dec. 27, 2022, <http://data.europa.eu/eli/reg/2022/2554/oj>.
- [159] European Union, “Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive” 1999/5/EC, *Official Journal of the European Union*, vol. L 153, pp. 62–106, May 22, 2014. <http://data.europa.eu/eli/dir/2014/53/oj>.
- [160] European Union, “Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products,” *Official Journal of the European Union*, 32008R0765, vol. L218, pp. 30–47, Jul. 13, 2008. <http://data.europa.eu/eli/reg/2008/765/oj>.
- [161] European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *Official Journal of the European Union*, 32016R0679, vol. L 119, pp. 1–88, May 4, 2016. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.
- [162] European Union, Regulation (EU) 2024/1183 of the European Parliament and of the Council of 24 May 2024 amending Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation),” *Official Journal of the European Union*, 32024R1183, L189, pp. 1–45, May 28, 2024, <http://data.europa.eu/eli/reg/2024/1183/oj>. [Accessed June 8, 2026]
- [163] European Union, Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS Regulation),” *Official Journal of the European Union*, 32014R0910, vol. 57, pp. L257/73–L257/114, Aug. 28, 2014, <http://data.europa.eu/eli/reg/2014/910/oj>.
- [164] European Union, “Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (ePrivacy Directive),” *Official Journal of the European Communities*, 32002L0058, vol. L201, pp. 37–47, Jul. 31, 2002, <http://data.europa.eu/eli/dir/2002/58/oj>.

- [165] European Parliament and Council of the European Union, Regulation (EU) 2022/868 of 30 May 2022 on European Data Governance and Amending Regulation (EU) 2018/1724 (Data Governance Act), *Official Journal of the European Union*, 32022R0868, L152, pp.1–44, June 3, 2022, <http://data.europa.eu/eli/reg/2022/868/oj>.
- [166] European Union, Regulation (EU) 2023/1781 of the European Parliament and of the Council of 13 September 2023 establishing a framework of measures for strengthening Europe’s semiconductor ecosystem and amending Regulation (EU) 2021/694 (Chips Act), *Official Journal of the European Union*, 32023R1781, vol. L 229, pp. 1–53, Sept. 18, 2023, <http://data.europa.eu/eli/reg/2023/1781/oj>.
- [167] European Commission, “Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act),” *Official Journal of the European Union*, 32024R1689, July. 12, 2024, <http://data.europa.eu/eli/reg/2024/1689/oj>.
- [168] European Commission. “Shaping Europe’s digital future. Blockchain-Legal and Regulatory Framework”, European Commission. July 8, 2025. [Online]. Available: <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-blockchain>. [Accessed June 8, 2026]
- [169] European Commission. “Shaping Europe’s digital future. Quantum Europe Strategy”, European Commission. July 2, 2025. [Online]. Available: <https://digital-strategy.ec.europa.eu/en/library/quantum-europe-strategy> [Accessed June 8, 2026]
- [170] European Parliament, “Quantum Act proposal”, *Legislative Train 04.2026*, April 20, 2026. [Online]. Available: <https://www.europarl.europa.eu/legislative-train/theme-a-new-plan-for-europe-s-sustainable-prosperity-and-competitiveness/file-quantum-act> [Accessed June 8, 2026]
- [171] Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act), *Official Journal of the European Union*, 32025R0038, vol. L, 2025/38, Jan. 15, 2025. [Online]. Available: <http://data.europa.eu/eli/reg/2025/38/oj>.
- [172] European Union, Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240, *Official Journal of the European Union*, 32021R0694, vol. L 166, pp. 1–34, May 11, 2021, <http://data.europa.eu/eli/reg/2021/694/oj>.
- [173] The European Cyber Defence Policy, Cyber Risk GmbH. [Online]. Available: <https://www.european-cyber-defence-policy.com/> [Accessed June 8, 2026]
- [174] S. S. Shafin *et al.*, “Obfuscated Memory Malware Detection in Resource-Constrained IoT Devices for Smart City Applications”, *Sensors*, vol. 23, no. 11, p. 5348, 2023, [doi: 10.3390/s23115348](https://doi.org/10.3390/s23115348).
- [175] I. Kara and M. Aydos, “The rise of ransomware: Forensic analysis for Windows-based ransomware attacks”, *Expert Systems with Applications*, vol. 190, p. 116198, 2022, [doi:10.1016/j.eswa.2021.116198](https://doi.org/10.1016/j.eswa.2021.116198)
- [176] T. Maurer and A. Nelson, “The Global Cyber Threat to Financial Systems,” *International Monetary Fund (IMF)*, 2021. [Online]. Available: <https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm>. [Accessed June 8, 2026]
- [177] European Commission, “European Standards”, *Internal Market, Industry, Entrepreneurship and SMEs*. [Online]. Available: [https://single-market-economy.ec.europa.eu/single-market/european-standards\\_en](https://single-market-economy.ec.europa.eu/single-market/european-standards_en). [Accessed June 8, 2026]
- [178] CEN and CENELEC, “Work Programme 2023”, Andreea Gulacs, CEN – European Committee for Standardization, CENELEC – European Committee for Electrotechnical Standardization, January 2023. [Online]. Available: <https://www.cencenelec.eu/media/CEN-CENELEC/News/Publications/2023/workprog2023.pdf>

- [179] Ralph Eckmaier, Walter Fumy, Stéfane Mouille, J.-P. Quemard, N. Polemi and R. Rumpel, “Risk Management Standards: Analysis of Standardisation Requirements in Support of Cybersecurity Policy”, European Union Agency for Cybersecurity (ENISA), *Publications Office of the European Union*, Mar. 2022. ISBN: 978-92-9204-569-2, [doi: 10.2824/001991](https://doi.org/10.2824/001991)
- [180] European Union Agency for Cybersecurity (ENISA), “European Cybersecurity Skills Framework (ECSF)”, ENISA, *Publications Office of the European Union*, 2022. ISBN: 978-92-9204-584-5, [doi: 10.2824/859537](https://doi.org/10.2824/859537)
- [181] F. I. Nai, R. Neisse, A. Lazari, G. Ruzzante, N. Polemi and M. Figwer, “European Cybersecurity Centres of Expertise Map—Definitions and Taxonomy”, *JRC Technical Reports*, JRC 111441, EUR 29332, 2018, ISBN 978-92-79-92956-4, [doi: 10.2760/622400](https://doi.org/10.2760/622400).
- [182] European Union, Regulation (EU) No 1025/2012 of the European Parliament and of the Council of (EU) of 25 October 2012 on European standardisation. *Official Journal of the European Union*, 32012R1025, October 25, 2012. [Online]. Available: <http://data.europa.eu/eli/reg/2012/1025/oj> [Accessed June 8, 2026]
- [183] CEN and CENELEC European Standards, “What is a standard?”, CEN – European Committee for Standardization, CENELEC – European Committee for Electrotechnical Standardization. [Online]. Available: <https://www.cencenelec.eu/european-standardization/european-standards/>. [Accessed June 8, 2026].
- [184] European Telecommunications Standards Institute (ETSI), ETSI platform. [Online]. Available: <https://www.etsi.org/>. [Accessed June 8, 2026].
- [185] CEN and CENELEC European Standards, “Types of Deliverables”, CEN – European Committee for Standardization, CENELEC – European Committee for Electrotechnical Standardization. Available: <https://www.cencenelec.eu/european-standardization/european-standards/types-of-deliverables/>. [Accessed June 8, 2026].
- [186] S. Ntalampiras, G. Misuraca, P. Rossel, “ENISA Research and Innovation Brief: Artificial Intelligence and Cybersecurity Research”, European Union Agency for Cybersecurity (ENISA), *Publications Office of the European Union*, 2023. ISBN: 978-92-9204-637-8, [doi: 10.2824/808362](https://doi.org/10.2824/808362).
- [187] J. Soler Garrido, D. Fano Yela, and C. Panigutti, “Analysis of the Preliminary AI Standardisation Work Plan in Support of the AI Act”, JRC Technical Report. *Publications Office of the European Union*, Luxembourg, 2023. ISBN: 978-92-68-03924-3. [doi: 10.2760/5847](https://doi.org/10.2760/5847).
- [188] ISO 31000:2018, “Risk management — Guidelines”, 2<sup>nd</sup> Edition, Geneva, Switzerland, 2018 [Online]. Available: <https://www.iso.org/standard/65694.html> [Accessed June 8, 2026].
- [189] ISO 31010:2019, “Risk management — Risk assessment techniques”, 2<sup>nd</sup> Edition, Geneva, Switzerland, 2019. [Online]. Available: <https://www.iso.org/standard/72140.html> [Accessed June 8, 2026].
- [190] National Institute of Standards and Technology, “Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy”, *NIST Special Publication 800-37 Rev. 2*, Dec. 2018. [Online]. Available: <https://csrc.nist.gov/pubs/sp/800/37/r2/final> [Accessed June 8, 2026].
- [191] National Institute of Standards and Technology, *The NIST Cybersecurity Framework (CSF) 2.0*, NIST Cybersecurity White Paper (CSWP) 29, Feb. 2024. [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf> [Accessed June 8, 2026].
- [192] ISO/IEC 27006-1:2024, “Information security, cybersecurity and privacy protection — Requirements for bodies providing audit and certification of information security management systems. Part 1: General”, 1<sup>st</sup> Edition, Geneva, Switzerland, 2024. [Online]. Available: <https://www.iso.org/standard/82908.html>. [Accessed June 8, 2026]

- [193] EN ISO/IEC 19790:2025, “Information security, cybersecurity and privacy protection — Security requirements for cryptographic modules”, 3<sup>rd</sup> Edition, Geneva, Switzerland, 2025. [Online]. Available: <https://www.iso.org/standard/82908.html>. [Accessed June 8, 2026]
- [194] EN ISO/IEC 29134:2023, “Information technology — Security techniques — Guidelines for privacy impact assessment”, 2<sup>nd</sup> Edition, Geneva, Switzerland, 2023. [Online]. Available: <https://www.iso.org/standard/86012.html>. [Accessed June 8, 2026]
- [195] European Telecommunications Standards Institute, “Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); NGN Security” (ISO/IEC 15408-2 application), ETSI TR 187 011 V2.1.1, Jul. 2008. [Online]. Available: [https://www.etsi.org/deliver/etsi\\_tr/187000\\_187099/187011/02.01.01\\_60/tr\\_187011v020101p.pdf](https://www.etsi.org/deliver/etsi_tr/187000_187099/187011/02.01.01_60/tr_187011v020101p.pdf). [Accessed June 8, 2026]
- [196] German Federal Office for Information Security (BSI), “IT-Grundschutz Compendium – International Edition 2022”, 2022. [Online]. Available: [https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi\\_it\\_gs\\_comp\\_2022.pdf?\\_\\_blob=publicationFile&v=2](https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi_it_gs_comp_2022.pdf?__blob=publicationFile&v=2). [Accessed June 8, 2026]
- [197] OWASP Foundation, “OWASP Application Security Verification Standard (ASVS)”. [Online]. Available: <https://owasp.org/www-project-application-security-verification-standard>. [Accessed June 8, 2026]
- [198] Cloud Security Alliance, *Cloud Controls Matrix (CCM)*. [Online]. Available: <https://cloudsecurityalliance.org/research/cloud-controls-matrix>. [Accessed June 8, 2026]
- [199] ISO/IEC TR 15446:2017 “Information technology — Security techniques — Guidance for the production of protection profiles and security targets”. Organization for Standardization (ISO), 3<sup>rd</sup> Edition, Geneva, Switzerland, 2017. [Online]. Available: <https://www.iso.org/standard/68904.html>. [Accessed June 8, 2026]
- [200] ISO/IEC 17020:2026 “Conformity assessment — Requirements for bodies performing inspection”. Organization for Standardization (ISO), 3<sup>rd</sup> Edition, Geneva, Switzerland, 2026. [Online]. Available: <https://www.iso.org/standard/17020> [Accessed June 8, 2026]
- [201] ISO/IEC 17021-1:2015 “Conformity assessment — Requirements for bodies providing audit and certification of management systems Part 1: Requirements”. Organization for Standardization (ISO), 1<sup>st</sup> Edition, Geneva, Switzerland, 2015. [Online]. Available: <https://www.iso.org/standard/61651.html> [Accessed June 8, 2026]
- [202] ISO/IEC 17024:2026 “Conformity assessment — General requirements for bodies operating certification of persons”. Organization for Standardization (ISO), 3<sup>rd</sup> Edition, Geneva, Switzerland, 2026. [Online]. Available: <https://www.iso.org/standard/17024> [Accessed June 8, 2026]
- [203] ISO/IEC 17025:2017 “General requirements for the competence of testing and calibration laboratories”. Organization for Standardization (ISO), 3<sup>rd</sup> Edition, Geneva, Switzerland, 2017. [Online]. Available: <https://www.iso.org/standard/66912.html>. [Accessed June 8, 2026]
- [204] ISO/IEC 17065:2012 “Conformity Assessment – Requirements for bodies certifying products, processes and services”. Organization for Standardization (ISO), 1<sup>st</sup> Edition, Geneva, Switzerland, 2012. [Online]. Available: <https://www.iso.org/standard/46568.html>. [Accessed June 8, 2026]
- [205] National Institute of Standards and Technology, “Framework for Improving Critical Infrastructure Cybersecurity”, Version 1.1, Gaithersburg, MD, USA, Apr. 16, 2018. [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>. [Accessed June 8, 2026]



- [206] ISO 28004-1:2007, "Security management systems for the supply chain — Guidelines for the implementation of ISO 28000 — Part 1: General principles", 1<sup>st</sup> Edition, Geneva, Switzerland, 2007 [Online]. Available: <https://www.iso.org/standard/44962.html>. [Accessed June 8, 2026].
- [207] European Telecommunications Standards Institute (ETSI), "Cyber Security (CYBER); Implementation of the Revised Network and Information Security (NIS2) Directive Applying Critical Security Controls", ETSI TR 103 866 V1.1.1, Feb. 2023. [Online]. Available: <https://cdn.standards.iteh.ai/samples/63989/c249c46a4f66419fbc0234515f29e319/ETSI-TR-103-866-V1-1-1-2023-02-.pdf>. [Accessed June 8, 2026].
- [208] CEN-CENELEC, *Security Standardization Matters*. Brussels, Belgium: CEN-CENELEC, Nov. 2020. [Online]. Available: [https://www.cencenelec.eu/media/CEN-CENELEC/News/Publications/2020/2020-11-23\\_brochure\\_security.pdf](https://www.cencenelec.eu/media/CEN-CENELEC/News/Publications/2020/2020-11-23_brochure_security.pdf). [Accessed June 8, 2026].
- [209] European Commission. Shaping Europe's digital future. "Proposal for the Cloud and AI Development Act (CADA)". European Commission, June 3 2026. [Online]. Available: <https://digital-strategy.ec.europa.eu/en/library/proposal-cloud-and-ai-development-act-cada>. [Accessed June 8, 2026].
- [210] European Union Agency for Cybersecurity (ENISA), "Public Consultation on Specifications for eUICC Certification Under the EU5G Cybersecurity Certification Scheme", June 26, 2024. [Online]. Available: [Specifications for eUICC certification under the EUCC scheme](https://www.enisa.europa.eu/publications/specifications-for-euicc-certification-under-the-eu5g-cybersecurity-certification-scheme). [Accessed June 8, 2026].
- [211] ISO/IEC 27404:2025, "Cybersecurity — IoT security and privacy — Cybersecurity labelling framework for consumer IoT", ISO/IEC, 1<sup>st</sup> Edition, Geneva, Switzerland, 2025. [Online]. Available: <https://www.iso.org/standard/80138.html>. [Accessed June 8, 2026].
- [212] European Telecommunications Standards Institute (ETSI), ETSI EN 303 645 V2.1.1: CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements, Sophia Antipolis, France: ETSI, Jun. 2020. [Online]. Available: [https://www.etsi.org/deliver/etsi\\_en/303600\\_303699/303645/02.01.01\\_60/en\\_303645v020101p.pdf](https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf). [Accessed June 8, 2026].
- [213] M. Fagan, K. Megas, P. Watrobski, J. Marron, and B. Cuthill, "Profile of the IoT Core Baseline for Consumer IoT Products", *NIST Interagency/Internal Report (NIST IR) 8425*. Gaithersburg, MD, USA: National Institute of Standards and Technology (NIST), Sep. 2022. <https://doi.org/10.6028/NIST.IR.8425>.
- [214] CEN EN 17529:2022, "Data protection and privacy by design and by default", European Committee for Standardization, 2025. [Online]. Available: <https://standards.iteh.ai/catalog/standards/cen/7988285e-71fa-4a6b-845c-71ddadb1e33f/en-17529-2022>. [Accessed June 8, 2026].
- [215] ISO/IEC 33001:2015, "Information technology - process assessment - concepts and terminology", ISO/IEC, 1<sup>st</sup> Edition, Geneva, Switzerland, 2015. [Online]. Available: <https://www.iso.org/standard/54175.html>. [Accessed June 8, 2026].
- [216] ISO/IEC 27701:2025, "Information security, cybersecurity and privacy protection — Privacy information management systems — Requirements and guidance", ISO/IEC, 2<sup>nd</sup> Edition, Geneva, Switzerland, 2025. [Online]. Available: <https://www.iso.org/standard/27701>. [Accessed June 8, 2026].
- [217] European Parliament and Council of the European Union, Regulation (EU) 2023/2854 of 13 December 2023 on Harmonised Rules on Fair Access to and Use of Data (Data Act), *Official Journal of the European Union*, 32023R2854, L2023/2854, Dec.22, 2023. <http://data.europa.eu/eli/reg/2023/2854/oj>.
- [218] DKE standards. "Trusted Chips – European Semiconductors: Cybersecurity Standardization and Certification", VDE Verband der Elektrotechnik Elektronik Informationstechnik e.V., Jan. 15, 2026. [Online]. Available: <https://www.dke.de/en/areas-of-work/components-technologies/trusted-chips>. [Accessed June 8, 2026].

- [219] European Committee for Standardization (CEN) and European Committee for Electrotechnical Standardization (CENELEC), CEN/CLC/JTC 21: Artificial Intelligence. [Online]. Available: <https://standards.iteh.ai/catalog/tc/clc/f2e11393-2c03-4a0a-9bc4-92326e0118fc/cen-clc-jtc-21>. [Accessed June 8, 2026].
- [220] K. Scarfone, M. Quinn, T. Benzel, T. Grance, and K. Stine, "Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile", *NIST Special Publication 800-61 Rev. 3*, Gaithersburg, MD, USA: National Institute of Standards and Technology, Apr. 2025. <https://doi.org/10.6028/NIST.SP.800-61r3>.
- [221] M. Theodoridou and G. Giannopoulos, "Risk Assessment Methodologies for Critical Infrastructure Protection. Part II: A New Approach", Report EUR 27332, Luxembourg: Publications Office of the EU, 2015 JRC96623. [doi:10.2788/621843](https://doi.org/10.2788/621843).
- [222] Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby, and K. Stoddart, "A review of cyber security risk assessment methods for SCADA systems," *Computers & Security*, vol. 56, pp. 1–27, 2016, [doi:10.1016/j.cose.2015.09.009](https://doi.org/10.1016/j.cose.2015.09.009).
- [223] A. Rutkowski, "Global standards collaboration: Is it possible?," CircleID, Feb. 3, 2023. [Online]. Available: <https://circleid.com/posts/20230203-global-standards-collaboration-is-it-possible>. [Accessed June 8, 2026]
- [224] N. Abdelkafi, R. Bekkers, R. Bolla, A. Rodriguez-Ascaso, and M. Wetterwald, "Understanding ICT Standardization: Principles and Practices". [Online]. Available: [https://pure.tue.nl/ws/portalfiles/portal/192511633/Slideset\\_Understanding\\_ICT\\_Standardization.pdf](https://pure.tue.nl/ws/portalfiles/portal/192511633/Slideset_Understanding_ICT_Standardization.pdf) [Accessed June 8, 2026]
- [225] H. Taherdoost, "Understanding cybersecurity frameworks and information security standards – A review and comprehensive overview," *Electronics*, vol. 11, no. 14, Art. no. 2181, 2022, [doi: 10.3390/electronics11142181](https://doi.org/10.3390/electronics11142181).
- [226] M. Syafrizal, S. R. Selamat, and N. A. Zakaria, "Analysis of cybersecurity standard and framework components", *International Journal of Communication Networks and Information Security (IJCNIS)*, UK Zhende Publishing Limited, Vol.12, No3, 2020, <https://doi.org/10.17762/ijcnis.v12i3.4817>
- [227] A. Tsohou, S. Kokolakis, C. Lambrinoudakis, and S. Gritzalis, "Information systems security management: A review and a classification of the ISO standards" In *Next Generation Society: Technological and Legal Issues*, A. B. Sideridis and C. Z. Patrikakis, Eds. Berlin, Germany: Springer, 2010, pp. 220–235, [doi:10.1007/978-3-642-11631-5\\_21](https://doi.org/10.1007/978-3-642-11631-5_21).
- [228] K. Stouffer et al., Guide to Operational Technology (OT) Security, NIST SP 800-82 Rev. 3, Sep. 2023. <https://dx.doi.org/10.2788/621843>.
- [229] Q. Zhou, L. Zhu, and Y. Deng, "Measure-based uncertainty with Dempster-Shafer structure," *Science China Information Sciences*, vol. 68, no. 10, 2025, Art. no. 202204. [doi:10.1007/s11432-024-4563-x](https://doi.org/10.1007/s11432-024-4563-x)
- [230] S. Zybin, O. Korchenko, O. Korystin, V. Shulha, S. Kazmirchuk, and S. Demediuk, "Method for the risk assessing of hybrid threats in cyber security based on fuzzy set theory," *SSRN*, 2025, [doi: 10.2139/ssrn.5143937](https://doi.org/10.2139/ssrn.5143937).
- [231] K.-S. Son, J.-G. Song, and J.-W. Lee, "Development of the framework for quantitative cyber risk assessment in nuclear facilities," *Nuclear Engineering and Technology*, vol. 55, no. 6, pp. 2034–2046, Jun. 2023, [doi:10.1016/j.net.2023.03.023](https://doi.org/10.1016/j.net.2023.03.023).
- [232] C. Lambrinoudakis, S. Gritzalis, C. Xenakis, et al., "Interoperable EU Risk Management Framework," European Union Agency for Cybersecurity (ENISA), Dec. 2022. [Online]. Available: [https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report-Interoperable%20EU%20Risk%20Management%20Framework\\_Updated.pdf](https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report-Interoperable%20EU%20Risk%20Management%20Framework_Updated.pdf). [Accessed June 8, 2026]

- [233] B. C. J. Alberts and A. Dorofee, *Managing Information Security Risks: The OCTAVE Approach*. Boston, MA, USA: Addison-Wesley Longman, 2002.
- [234] A. Tucker, *Advancing Risk Management Capability Using the OCTAVE FORTE Process*, 2020. [doi:10.1184/R1/13014266.v1](https://doi.org/10.1184/R1/13014266.v1)
- [235] O. J. Olaore and A. F. Alkhwaldi, "AI-Enhanced Multi-Criteria Decision Support for Cybersecurity Risk Framework Selection: A Machine-Learning Comparative Analysis of NIST CSF, ISO 27001, FAIR, OCTAVE and CRAMM," *Preprints.org*, preprint, Jun. 2026. [doi: 10.20944/preprints202606.0398.v1](https://doi.org/10.20944/preprints202606.0398.v1).
- [236] A. Ekelhart, S. Fenz, T. Neubauer "Automated Risk and Utility Management" In *Proc. 6th Int. Conf. Information Technology: New Generations (ITNG)*, Las Vegas, NV, USA, Apr. 27–29, 2009, pp. 393–399.
- [237] J. Wang, M. Neil, and N. E. Fenton, "A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model," *Computers & Security*, vol. 89, p. 101659, 2020, [doi: 10.1016/j.cose.2019.101659](https://doi.org/10.1016/j.cose.2019.101659).
- [238] J. V. Barraza de la Paz, L. A. Rodríguez-Picón, V. Morales-Rocha, and S. V. Torres-Argüelles, "A systematic review of risk management methodologies for complex organizations in Industry 4.0 and 5.0", *Systems*, vol. 11, no. 5, Art. no. 218, 2023. [doi: 10.3390/systems11050218](https://doi.org/10.3390/systems11050218).
- [239] E. Zambon, S. Etalle, R. J. Wieringa, and P. H. Hartel, "Model-based qualitative risk assessment for availability of IT infrastructures," *Software and Systems Modeling*, vol. 10, no. 4, pp. 553–580, 2011, [doi: 10.1007/s10270-010-0166-8](https://doi.org/10.1007/s10270-010-0166-8).
- [240] M. S. Hellas, R. Chaib, and A. Khabtane, "Risk Optimization With a New BOBTA Approach (Barrier and Operational Bow Tie Analysis) Combining the Bow Tie Method and Risk Influence Factors," *Quality and Reliability Engineering International*, first published Sep. 4, 2025, [doi: 10.1002/qre.70069](https://doi.org/10.1002/qre.70069).
- [241] B. Abdolhamidzadeh, T. Abbasi, D. Rashtchian, and S. A. Abbasi, "Application of the Bow-Tie Analysis Technique in Quantitative Risk Assessment of Gas Condensate Storage Considering Domino Effects," *International Journal of Environmental Science and Technology*, vol. 18, no. 12, pp. 3613–3624, 2021, [doi: 10.1007/s13762-020-02858-4](https://doi.org/10.1007/s13762-020-02858-4).
- [242] F. Khan, S. A. Abbasi, and T. Abbasi, "Bow-Tie Analysis: A Tool for Risk Assessment in Process Industries," *Process Safety and Environmental Protection*, vol. 139, pp. 1–10, 2020, [doi: 10.1016/j.psep.2020.03.001](https://doi.org/10.1016/j.psep.2020.03.001).
- [243] S. S. Arici, E. Akyuz, and O. Arslan, "Application of Fuzzy Bow-tie Risk Analysis to Maritime Transportation: The Case of Ship Collision During the STS Operation," *Ocean Engineering*, vol. 217, Art. no. 107960, 2020, [doi: 10.1016/j.oceaneng.2020.107960](https://doi.org/10.1016/j.oceaneng.2020.107960).
- [244] V. A. Dokuchaev, V. V. Maklachkova, D. V. Makarova, and L. V. Volkova, "Analysis of Data Risk Management Methods for Personal Data Information Systems," in *2020 Systems of Signals Generating and Processing in the Field of On Board Communications*, Moscow, Russia, Mar. 19–20, 2020, pp. 1–5, [doi: 10.1109/IEEECONF48371.2020.9078547](https://doi.org/10.1109/IEEECONF48371.2020.9078547).
- [245] S. Papastergiou, N. Polemi, and A. Karantjias, "CYSM: An innovative physical/cyber security management system for ports," in *Human Aspects of Information Security, Privacy, and Trust, HAS 2015*, T. Tryfonas and I. Askoxylakis, Eds., Lecture Notes in Computer Science, vol. 9190. Cham, Switzerland: Springer, 2015, pp. 219–230, [doi: 10.1007/978-3-319-20376-8\\_20](https://doi.org/10.1007/978-3-319-20376-8_20).
- [246] N. Polemi and P. Kotzanikolaou, "Medusa: A Supply Chain Risk Assessment Methodology", In *Cyber Security and Privacy*, F. Cleary and M. Felici, Eds. Cham, Switzerland: Springer, 2015, pp. 79–90, [doi: 10.1007/978-3-319-25360-2\\_7](https://doi.org/10.1007/978-3-319-25360-2_7).



- [247] M. ThamaraiSelvan and A. Ambikapathy, "Literature Review and Identification of Research Gaps in Cybersecurity Risk Management," *IAPQR Transactions*, pp. 89–95, 2025.
- [248] S. Carnovale, S. DuHadway, A. S. Patrucco, and S. Yeniyurt, "Balancing risk and resilience: how network structures and firm strategies mitigate supply chain disruptions," *International Journal of Physical Distribution & Logistics Management*, vol. 55, no. 7, pp. 761–790, 2025. [doi:10.1108/IJPDLM-08-2024-0310](https://doi.org/10.1108/IJPDLM-08-2024-0310)
- [249] D. J. Bodeau, R. D. Graubart, R. M. McQuaid, and J. Woodill, "Cyber resiliency metrics, measures of effectiveness, and scoring," MITRE Technical Report MTR180314, 2018.
- [250] G. Behzadi, M. J. O'Sullivan, and T. L. Olsen, "On metrics for supply chain resilience," *European Journal of Operational Research*, 2020, [doi: 10.1016/j.ejor.2020.04.040](https://doi.org/10.1016/j.ejor.2020.04.040).
- [251] D. Snyder, L. A. Mayer, G. Weichenberg, D. C. Tarraf, B. Fox, M. Hura, et al., "Measuring cybersecurity and cyber resiliency" RAND Corporation, 2020, ISBN: 978-1-9774-0437-4.
- [252] C. Sánchez-Zas, V. Villagra, M. Vega-Barbas, and X. Larriva-Novo, "Ontology-based approach to real-time risk management and cyber-situational awareness," *Future Generation Computer Systems*, vol. 141, no. 2, 2022, [doi: 10.1016/j.future.2022.12.006](https://doi.org/10.1016/j.future.2022.12.006)
- [253] P. Cheimonidis and K. Rantos, "Dynamic risk assessment in cybersecurity: A systematic literature review," *Future Internet*, vol. 15, no. 10, p. 324, 2023. [doi:10.3390/fi15100324](https://doi.org/10.3390/fi15100324)
- [254] A. Qazi and M. C. E. Simsekler, "Risk assessment of construction projects using Monte Carlo simulation," *International Journal of Managing Projects in Business*, vol. 14, no. 5, pp. 1202–1218, 2021, [doi: 10.1108/IJMPB-04-2020-0129](https://doi.org/10.1108/IJMPB-04-2020-0129).
- [255] A. Amro, V. Gkioulos, and S. Katsikas, "Assessing cyber risk in cyber-physical systems using the ATT&CK framework," *ACM Transactions on Privacy and Security*, vol. 26, no. 2, pp. 1–33, May 2023, [doi: 10.1145/3571733](https://doi.org/10.1145/3571733).
- [256] H. H. D. Nguyen, C. H. Song, and Y. T. Kim, "Semi-quantitative risk assessment: From rainfall-induced landslides to the risk of persons in buildings," *Bulletin of Engineering Geology and the Environment*, vol. 84, no. 9, p. 434, 2025. [doi:10.1007/s10064-025-04420-x](https://doi.org/10.1007/s10064-025-04420-x)
- [257] X. Diao, Y. Zhao, C. Smidts, P. K. Vaddi, R. Li, H. Lei, et al., "Dynamic probabilistic risk assessment for electric grid cybersecurity," *Reliability Engineering & System Safety*, vol. 241, p. 109699, 2024.
- [258] M. Jaikanth and V. K. Madiseti, "A comparative analysis of cybersecurity threat taxonomies for healthcare organizations," *Journal of Software Engineering and Applications*, vol. 17, no. 5, pp. 359–377, 2024, [doi: 10.4236/jsea.2024.175020](https://doi.org/10.4236/jsea.2024.175020).
- [259] OWASP Threat Modeling [Online]. Available: [https://owasp.org/www-community/Threat\\_Modeling](https://owasp.org/www-community/Threat_Modeling) Accessed May 31, 2026].
- [260] OWASP, STRIDE Threat List. [Online]. Available: [https://owasp.org/www-community/Threat\\_Modeling\\_Process#stride-threat-list](https://owasp.org/www-community/Threat_Modeling_Process#stride-threat-list) [Accessed June 8, 2026]
- [261] OASIS Cyber Threat Intelligence (CTI) STIX. [Online]. Available: [https://www.oasis-open.org/committees/tc\\_home.php?wg\\_abbrev=cti](https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti) [Accessed June 8, 2026].
- [262] European Union Vulnerability Database, Critical Vulnerabilities CSIRTs, ENISA, CiRAS. [Online]. Available: <https://euvd.enisa.europa.eu/> [Accessed June 8, 2026].
- [263] R. Auger, The WASC Threat Classification v2.0. [Online]. Available: <http://projects.webappsec.org/w/page/13246978/Threat%20Classification> [Accessed June 8, 2026].

- [264] OpenCTI platform, Github. [Online]. Available: <https://github.com/opencti-platform/opencti> [Accessed June 8, 2026].
- [265] Malware Information Sharing Platform (MISP). MISP Intelligence Sharing, MISP Project. [Online]. Available: <https://www.misp-project.org/>. [Accessed June 8, 2026]
- [266] MITRE, "Common Weakness Enumeration", MITRE Corporation, CWE catalogue v3.9., July 6, 2023. [Online]. Available: <https://cwe.mitre.org/index.html>. [Accessed June 8, 2026]
- [267] MITRE Common Weakness Enumeration, "Common Weakness Risk Analysis Framework (CWRAF)", MITRE v0.8.3, June 6, 2023 [Online]. Available: <https://cwe.mitre.org/cwraf/> [Accessed June 8, 2026]
- [268] MITRE, Common Platform Enumeration (CPE). MITRE Corporation, catalogue v3.9., July 6, 2023. [Online]. Available: <https://nvd.nist.gov/products/cpe> [Accessed June 8, 2026].
- [269] National Institute of Standards and Technology (NIST). "National Vulnerability Database" (NVD), NIST. [Online]. Available: <https://nvd.nist.gov/> [Accessed June 8, 2026]
- [270] Open Source Vulnerabilities (OSV) schema. [Online]. Available: <https://osv.dev/> [Accessed June 8, 2026]
- [271] Github Advisory Database. Security Vulnerability Database, Github. [Online]. Available: <https://github.com/advisories> [Accessed June 8, 2026]
- [272] MITRE, "Common Attack Pattern Enumeration and Classification (CAPEC). A Community Resource for Identifying and Understanding Attacks", MITRE Corporation, CAPEC catalogue v3.9. , July 6, 2023. [Online]. Available: <https://capec.mitre.org/>. [Accessed June 8, 2026]
- [273] The Vocabulary for Event Recording and Incident Sharing (VERIS ). The Vocabulary for Event Recording and Incident Sharing. [Online]. Available: <https://verisframework.org/> [Accessed June 8, 2026].
- [274] S. Islam, S. Papastergiou, E.-M. Kalogeraki, and K. Kioskly, "Cyberattack path generation and prioritisation for securing healthcare systems," *Applied Sciences*, vol. 12, no. 9, p. 4443, 2022, doi: 10.3390/app12094443.
- [275] E.-M. Kalogeraki, S. Papastergiou, N. Polemi, and C. Douligieris, "SAURON Real-life Scenario: A Terrorist Coordinated Attack in an EU Port," *Maritime Interdiction Operations Journal*, NATO Maritime Interdiction Operational Training Centre (NMIOTC), vol. 16, no. 1, pp. 22–27, 2018, ISSN: 2242-441X.
- [276] N. Polatidis, M. Pavlidis, and H. Mouratidis, "Cyber-attack path discovery in a dynamic supply chain maritime risk management system," *Comput. Stand. Interfaces*, vol. 56, pp. 74–82, 2018, doi:10.1016/j.csi.2017.09.006.
- [277] X. Liu, W. Jiang, Z. Li, X. Jin, Z. Ma, and Q. Li, "FuzzAGG: A fuzzing-driven attack graph generation framework for industrial robot systems," *Comput. Secur.*, vol. 150, Art. no. 104223, 2025, doi: 10.1016/j.cose.2024.104223.
- [278] S. Huang, C. M. Poskitt, and L. K. Shar, "Security modelling for cyber-physical systems: A systematic literature review", *ACM Transactions on Cyber-Physical Systems*, vol. 10, no. 2, Art. 20, pp. 1–29, 2026, doi: 10.1145/3776549.
- [279] I. Chochliouros, A. Spiliopoulou, and S. Chochliouros, "Methods for Dependability and Security Analysis of Large Networks" In *Encyclopedia of Multimedia Technology and Networking*, 2nd ed., M. Pagani, Ed. Hershey, PA, USA: IGI Global, 2009, pp. 921–929. doi: 10.4018/978-1-60566-014-1.ch125.
- [280] I. Ahmad, F. Rodriguez, J. Huusko, and K. Seppänen, "On the Dependability of 6G Networks," *Electronics*, vol. 12, no. 6, Art. no. 1472, Mar. 2023, doi: 10.3390/electronics12061472.
- [281] C. Zhang, X. Zhao, E. Tian, and Y. Zou, "Stochastic important-data-based attack model and defense strategies for cyber-physical system: A data-driven method", *International Journal of Robust and Nonlinear Control*, vol. 34, no. 8, pp. 5384–5398, 2024, doi:10.1002/rnc.7274.

- [282] I. Nai Fovino, M. Masera, and A. De Cian, "Integrating Cyber Attack within Fault Trees," in *Risk, Reliability and Social Safety: Proceedings of the European Safety and Reliability Conference (ESREL 2007)*, T. Aven and J. E. Vinnem, Eds. London, U.K.: CRC Press, 2007, pp. 1–6, JRC Publications, JRC36470.
- [283] K. Lai, M. Illindala, and K. Subramaniam, "A tri-level optimization model to mitigate coordinated attacks on electric power systems in a cyber-physical environment," *Appl. Energy*, vol. 235, pp. 204–218, 2019, doi: [10.1016/j.apenergy.2018.10.077](https://doi.org/10.1016/j.apenergy.2018.10.077).
- [284] R. Mofouet, A. Kouam, H. Ma, J. Fu, C. Kamhoua, and G. Deugoue, "A probabilistic attack graph-based model for coordinated attacks in sensor-defended networks," *J. Supercomput.*, vol. 82, no. 1, Art. no. 19, 2026, doi: [10.1007/s11227-025-08147-0](https://doi.org/10.1007/s11227-025-08147-0).
- [285] V. Zokarkar and K. Mathur, "A Survey of Attack Prediction Approaches in Cyber Security" In *Proc. Int. Conf. Recent Advancements and Modernisations in Sustainable Intelligent Technologies and Applications (RAMSITA 2025)*, *Advances in Intelligent Systems Research*, May 2025, pp. 1003–1016, doi: [10.2991/978-94-6463-716-8\\_75](https://doi.org/10.2991/978-94-6463-716-8_75).
- [286] H. Moudoud, Z. Mlika, L. Khoukhi, and S. Cherkaoui, "Detection and prediction of FDI attacks in IoT systems via hidden Markov model", *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 5, pp. 2978–2990, 2022, doi: [10.1109/TNSE.2022.3161479](https://doi.org/10.1109/TNSE.2022.3161479).
- [287] S. Abraham and S. Nair, "Exploitability analysis using predictive cybersecurity framework" In *Proc. IEEE 2nd Int. Conf. Cybernetics (CYBCONF)*, Coventry, U.K., Jun. 2015, pp. 317–323, doi: [10.1109/CYBConf.2015.7175923](https://doi.org/10.1109/CYBConf.2015.7175923).
- [288] M.A.R. Al Amin, S. Shetty, L. Njilla, D. K. Tosh, and C. Kamhoua, "Hidden Markov model and cyber deception for the prevention of adversarial lateral movement", *IEEE Access*, vol. 9, pp. 49662–49682, 2021, doi: [10.1109/ACCESS.2021.3069105](https://doi.org/10.1109/ACCESS.2021.3069105).
- [289] T. Chadza, K. G. Kyriakopoulos, and S. Lambouharan, "Analysis of hidden Markov model learning algorithms for the detection and prediction of multi-stage network attacks," *Future Gener. Comput. Syst.*, vol. 108, pp. 636–649, 2020, doi:
- [290] A. A. Ramaki, M. Amini, and R. E. Atani, "RTECA: Real time episode correlation algorithm for multi-step attack scenarios detection", *Comput. Secur.*, vol. 49, pp. 206–219, March 2015, doi: [10.1016/j.cose.2014.10.006](https://doi.org/10.1016/j.cose.2014.10.006).
- [291] A. Okutan, S. J. Yang, and K. McConky, "Predicting cyber attacks with Bayesian networks using unconventional signals" In *Proc. 12th Annu. Conf. Cyber and Information Security Research (CISR)*, Oak Ridge, TN, USA, April 2017, pp. 1–4, doi: [10.1145/3064814.3064823](https://doi.org/10.1145/3064814.3064823).
- [292] A. Singhal and X. Ou, "Security risk analysis of enterprise networks using probabilistic attack graphs" In *Network Security Metrics*, Springer, 2017, pp. 53–73. doi: [10.1007/978-3-319-66505-4\\_3](https://doi.org/10.1007/978-3-319-66505-4_3).
- [293] O. S. M. B. H. Almazrouei, P. Magalingam, M. K. Hasan, and M. Shanmugam, "A review on attack graph analysis for IoT vulnerability assessment: challenges, open issues, and future directions", *IEEE Access*, vol. 11, pp. 44350–44376, 2023, doi: [10.1109/ACCESS.2023.3272053](https://doi.org/10.1109/ACCESS.2023.3272053).
- [294] Y. Li and X. Li, "Research on multi-target network security assessment with attack graph expert system model", *Sci. Program.*, vol. 2021, pp. 1–11, May 2021, doi: [10.1155/2021/9921731](https://doi.org/10.1155/2021/9921731).
- [295] O. Stan, et al., "Extending attack graphs to represent cyberattacks in communication protocols and modern IT networks" In *IEEE Trans. Depend. Sec. Comput.*, vol. 19, no. 3, pp. 1936–1954, May 2022, doi: [10.1109/TDSC.2020.3041999](https://doi.org/10.1109/TDSC.2020.3041999).
- [296] M. L. Artz, "NetSPA: A network security planning architecture," Ph.D. dissertation, Massachusetts Institute of Technology, Cambridge, MA, USA, 2002.

- [297] K. Ingols, M. Chu, R. Lippmann, S. Webster, and S. Boyer, "Modeling modern network attacks and countermeasures using attack graphs" In Proc. 2009 Annu. Comput. Secur. Appl. Conf. (ACSAC), 2009. [doi: 10.1109/ACSAC.2009.21](https://doi.org/10.1109/ACSAC.2009.21).
- [298] H. Al-Mohannadi, I. Awan, and J. Al Hamar, "Analysis of adversary activities using cloud-based web services to enhance cyber threat intelligence", *Service Oriented Computing and Applications*, vol. 14, pp. 175–187, 2020. [doi:10.1007/s11761-019-00285-7](https://doi.org/10.1007/s11761-019-00285-7).
- [299] K. Kim, Y. Shin, J. Lee, and K. Lee, "Automatically attributing mobile threat actors by vectorized ATT&CK matrix and paired indicator", *Sensors*, vol. 21, p. 6522, 2021. [doi:10.3390/s21196522](https://doi.org/10.3390/s21196522).
- [300] S. Balhara, N. Gupta, A. Alkhayyat, I. Bharti, R. Q. Malik, S. N. Mahmood, and F. Abedi, "A survey on deep reinforcement learning architectures, applications and emerging trends", *IET Communications*, vol. 19, no. 1, Art. no. e12447, 2025. [doi: 10.1049/cmu2.12447](https://doi.org/10.1049/cmu2.12447).
- [301] S. H. Oh, J. Kim, and J. Park, "Dynamic cyberattack simulation: Integrating improved deep reinforcement learning with the MITRE-ATT&CK framework", *Electronics*, vol. 13, no. 14, Art. no. 2831, 2024. [doi: 10.3390/electronics13142831](https://doi.org/10.3390/electronics13142831).
- [302] L. Li, R. Fayad, and A. Taylor, "Cygil: A cyber gym for training autonomous agents over emulated network systems", *arXiv preprint arXiv:2109.03331*, 2021. [doi: 10.48550/arXiv.2109.03331](https://doi.org/10.48550/arXiv.2109.03331).
- [303] Z. Wang, M. Fei, Y. Xiong, and A. Wang, "Dynamic attack path prediction and visualization for industrial cyber-physical systems under cyber attacks", In Proc. 2024 43rd Chinese Control Conf. (CCC), Jul. 2024, pp. 9005–9010. [doi: 10.23919/CCC63176.2024.10662270](https://doi.org/10.23919/CCC63176.2024.10662270).
- [304] E. Iturbe, J. Arcas, E. Rios, and N. Toledo, "A multi-layer approach through threat modelling and attack simulation for enhanced cyber security assessment" In Proc. 19th Int. Conf. Availability, Reliability and Security (ARES), Jul. 2024, pp. 1–8. [doi: 10.1145/3664476.3670458](https://doi.org/10.1145/3664476.3670458).
- [305] S. Armenia, M. Angelini, F. Nonino, G. Palombi, and M. F. Schlitzer, "A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs", *Decision Support Systems*, vol. 147, Art. no. 113580, 2021. [doi: 10.1016/j.dss.2021.113580](https://doi.org/10.1016/j.dss.2021.113580).
- [306] A. Piplai, M. Anoruo, K. Fasaye, A. Joshi, T. Finin, and A. Ridley, "Knowledge guided two-player reinforcement learning for cyber attacks and defenses" In Proc. 21st IEEE Int. Conf. Machine Learning and Applications (ICMLA), Dec. 2022, pp. 1342–1349. [doi: 10.1109/ICMLA55696.2022.00213](https://doi.org/10.1109/ICMLA55696.2022.00213).
- [307] D. H. Shin, D. Qian, and J. Zhang, "Cascading effects in interdependent networks", *IEEE Network*, vol. 28, no. 4, pp. 82–87, 2014. [doi: 10.1109/MNET.2014.6863136](https://doi.org/10.1109/MNET.2014.6863136).
- [308] L. Tang, K. Jing, J. He, and H. E. Stanley, "Complex interdependent supply chain networks: Cascading failure and robustness", *Physica A: Statistical Mechanics and its Applications*, vol. 443, pp. 58–69, Feb. 2016, [doi: 10.1016/j.physa.2015.09.082](https://doi.org/10.1016/j.physa.2015.09.082).
- [309] A. Panda and A. Bower, "Cyber security and the disaster resilience framework", *International Journal of Disaster Resilience in the Built Environment*, vol. 11, no. 4, pp. 507–518, Aug. 2020, [doi: 10.1108/IJDRBE-07-2019-0046](https://doi.org/10.1108/IJDRBE-07-2019-0046).
- [310] H. Guo, C. Zheng, H. H. C. Iu, and T. Fernando, "A critical review of cascading failure analysis and modeling of power system", *Renewable and Sustainable Energy Reviews*, vol. 80, pp. 9–22, 2017. [doi: 10.1016/j.rser.2017.05.206](https://doi.org/10.1016/j.rser.2017.05.206).
- [311] P. Pochelu, H. Cartiaux, and J. Schleich, "What artificial intelligence can do for high-performance computing systems?", *Engineering Applications of Artificial Intelligence*, vol. 164, Art. no. 113248, 2026. [doi: 10.1016/j.engappai.2025.113248](https://doi.org/10.1016/j.engappai.2025.113248).

- [312] C. Sánchez-Zas, V. A. Villagrà, M. Vega-Barbas, X. Larriva-Novo, J. I. Moreno, and J. Berrocal, "Ontology-based approach to real-time risk management and cyber-situational awareness", *Future Generation Computer Systems*, vol. 141, pp. 462–472, 2023.
- [313] D. Preuveneers and W. Joosen, "An ontology-based cybersecurity framework for AI-enabled systems and applications", *Future Internet*, vol. 16, no. 3, Art. no. 69, 2024.
- [314] B. F. Martins, L. J. Serrano Gil, J. F. Reyes Román, J. I. Panach, O. Pastor, M. Hadad, and B. Rochwerger, "A framework for conceptual characterization of ontologies and its application in the cybersecurity domain", *Software and Systems Modeling*, vol. 21, no. 4, pp. 1437–1464, 2022.
- [315] Ì. Oliveira, T. P. Sales, R. Baratella, M. Fumagalli, and G. Guizzardi, "An ontology of security from a risk treatment perspective", In *Conceptual Modeling*, Cham, Switzerland: Springer, 2022, pp. 365–379, [doi: 10.1007/978-3-031-17995-2\\_26](https://doi.org/10.1007/978-3-031-17995-2_26).
- [316] A. N. Talet and M. Z. Talet, "The role of knowledge management with risk management for information technology projects risk assessment", *International Journal of Environment and Sustainability*, vol. 6, no. 2, pp. 1–18, 2018.
- [317] A. Kovačević and S. D. Radenković, "SAWIT—Security awareness improvement tool in the workplace", *Applied Sciences*, vol. 10, no. 9, Art. no. 3065, 2020. [doi: 10.3390/app10093065](https://doi.org/10.3390/app10093065).
- [318] A. Neto, M. Perkusich, E. Dantas, F. Ramos, A. Costa, H. Almeida, and A. Perkusich, "Knowledge-based risk management: A systematic literature review" In Proc. XXXV Brazilian Symp. Software Engineering, Sep. 2021, pp. 320–329. [doi: 10.1145/3474624.3474635](https://doi.org/10.1145/3474624.3474635).
- [319] L. Chen and H. L. Lee, "Bullwhip effect measurement and its implications", *Operations Research*, vol. 60, no. 4, pp. 771–784, Jul.–Aug. 2012, doi:10.1287/opre.1120.1044. [doi: 10.1287/opre.1120.1074](https://doi.org/10.1287/opre.1120.1074).
- [320] E.-M. Kalogeraki and S. Papastergiou, "Self-Organized Artificial Swarm Intelligence Solution for Security and Privacy Threats in Healthcare ICT Infrastructures", *Maritime Interdiction Operations Journal*, NATO Maritime Interdiction Operational Training Centre (NMIOTC), vol. 23, no. 2, 2021, ISSN: 2241-438X.
- [321] S. Elvin, "EasyJet hackers access information of 9,000,000 customers", METRO, May 19, 2020. [Online]. Available: <https://metro.co.uk/2020/05/19/easyjet-hackers-accessed-information-9000000-customers-12726139> [Accessed June 8, 2026]
- [322] E.-M. Kalogeraki, K. D. Boberić, S. Karagiorgou, P. Gimenez, and G. Vivo, "Assessing the Security and Resilience of ICT Supply Chain Services", *Maritime Interdiction Operations Journal*, NATO Maritime Interdiction Operational Training Centre (NMIOTC), vol. 25, no. 1, pp. 28–34, 2023, ISSN: 2241-438X.
- [323] C. Martinie, C. Grigoriadis, E.-M. Kalogeraki, and P. Kotzanikolaou, "Modelling human tasks to enhance threat identification in critical maritime systems", in *Proc. 25th Pan-Hellenic Conf. Informatics*, 2021, pp. 375–380.
- [324] A. AlHarmali, S. Ali, W. Aman, and O. Hussain, "Cyber Risk Assessment for Cyber-Physical Systems: A Review of Methodologies and Recommendations for Improved Assessment Effectiveness," *arXiv preprint*, arXiv:2408.16841, 2024. [doi: 10.5121/csit.2024.141608](https://doi.org/10.5121/csit.2024.141608).
- [325] K. H. Kim, K. Kim, and H. K. Kim, "STRIDE-based threat modeling and DREAD evaluation for the distributed control system in the oil refinery," *ETRI Journal*, vol. 44, no. 6, pp. 991–1003, 2022. [doi: 10.4218/etrij.2021-0181](https://doi.org/10.4218/etrij.2021-0181).
- [326] M. A. S. P. Dayarathne, M. S. M. Jayathilaka, R. M. V. A. Bandara, V. Logeeshan, S. Kumarawadu, and Chathura Wanigasekara. 2025. Mitigating cyber risks in smart cyber-physical power systems through deep learning and hybrid security models. *IEEE Access* 13 (2025), 37474–37492.



- [327] Z. Zhou, H. Yang, H. Li, J. Zhang, S. Li, X. Gao, and P. Gong, "A dynamic cyber-attack approach for real-time hardware-in-the-loop simulation of power grid," in *Proc. 2022 24th Int. Conf. Advanced Communication Technology (ICACT)*, Feb. 2022, pp. 212–217.
- [328] Mohit, "15 Major Oil Spills Of The Maritime World", Marine insight, February 11, 2024. [Online]. Available: <https://www.marineinsight.com/environment/11-major-oil-spills-of-the-maritime-world/>. [Accessed June 8, 2026]
- [329] P. Wintour, "A visual guide to the Gulf tanker attack", The Guardian, June 14, 2019. [Online]. Available: <https://www.theguardian.com/world/2019/jun/13/a-visual-guide-to-the-gulf-tanker-attacks>. [Accessed June 8, 2026]
- [330] S. Writer, "Resecurity Warns Maritime Sector Faces Rising Cyber Threats", The Defense Post, 2026. [Online]. Available: <https://thedefensepost.com/2026/06/26/maritime-sector-cyber-threats-resecurity/>. [Accessed June 8, 2026]
- [331] S. Chambers, "Maersk hit by another cyber attack", Splash247, March 19, 2018. [Online]. Available: <https://splash247.com/maersk-hit-another-cyber-attack/>. [Accessed June 8, 2026]
- [332] The Maritime Executive, "Vard Hit by Cyberattack", The Maritime Executive, June 10, 2020. [Online]. Available: <https://maritime-executive.com/article/vard-hit-by-cyberattack>. [Accessed June 8, 2026]
- [333] European Commission, Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security, European Commission, 02004R0725-20090420, Apr. 20, 2009, <http://data.europa.eu/eli/reg/2004/725/2009-04-20>.
- [334] D. Bisht, "MARPOL Convention: All Six Annexes, Certificates, and 2026 Compliance Updates Explained", Shipfinex, June 2, 2026. [Online]. Available: <https://www.shipfinex.com/blog/marpol>. [Accessed June 8, 2026]
- [335] European Parliament and the Council of the European Union, "Directive 2002/84/EC of the European Parliament and of the Council of 5 November 2002 amending the Directives on maritime safety and the prevention of pollution from ships", *Official Journal of the European Communities*, L 324, pp. 53–58, Nov. 29, 2002. <http://data.europa.eu/eli/dir/2002/84/oj>.
- [336] International Maritime Organisation, "Amendments to IMO instruments: upcoming and recent entry into force/effective dates", IMO [Online]. Available: <https://www.imo.org/en/about/conventions/pages/amendments-to-imo-instruments.aspx>. [Accessed June 8, 2026]
- [337] International Maritime Organisation, "Maritime cyber risk", IMO, 2025. [Online]. Available: <https://www.imo.org/en/ourwork/security/pages/cyber-security.aspx>. [Accessed June 8, 2026]
- [338] European Parliament and the Council of the European Union, Regulation (EU) 2025/2434 of the European Parliament and of the Council of 26 November 2025 on the European Maritime Safety Agency and repealing Regulation (EC) No 1406/2002, *Official Journal of the European Union*, L 2025/2434, Dec. 29, 2025 <http://data.europa.eu/eli/reg/2025/2434/oj>.
- [339] European Commission "Commission Delegated Directive (EU) 2025/811 of 19 February 2025 amending Annex I to Directive 2002/59/EC of the European Parliament and of the Council as regards information to be notified to ship reporting systems", *Official Journal of the European Union*, April 30, 2025. [http://data.europa.eu/eli/dir\\_del/2025/811/oj](http://data.europa.eu/eli/dir_del/2025/811/oj).
- [340] European Commission and High Representative of the Union for Foreign Affairs and Security Policy, Joint Communication to the European Parliament and the Council on the update of the EU Maritime Security Strategy and its Action Plan: "An enhanced EU Maritime Security Strategy for evolving maritime threats", *JOIN(2023) 8 final*, Brussels, Belgium, Mar. 10, 2023. [Document 52023JC0008](#).

- [341] International Organization for Standardization, ISO 28005-1:2024, Ships and Marine Technology — Electronic Port Clearance (EPC)—Part 1: Message Structures. Geneva, Switzerland: ISO, 2024. [Online]. Available: <https://www.iso.org/standard/83881.html>. [Accessed June 8, 2026]
- [342] International Organization for Standardization, ISO 20858:2007, Ships and Marine Technology — Maritime Port Facility Security Assessments and Security Plan Development. Geneva, Switzerland: ISO, 2007. [Online]. Available: <https://www.iso.org/standard/46051.html>. [Accessed June 8, 2026]
- [343] International Organization for Standardization, ISO 28007-1:2015, Ships and Marine Technology — Guidelines for Private Maritime Security Companies (PMSC) Providing Privately Contracted Armed Security Personnel (PCASP) on Board Ships (and Pro Forma Contract)—Part 1: General. Geneva, Switzerland: ISO, 2015. [Online]. Available: <https://www.iso.org/standard/63166.html>. [Accessed June 8, 2026]
- [344] European Union Agency for Cybersecurity (ENISA), "Port Cybersecurity: Good Practices for Cybersecurity in the Maritime Sector". Heraklion, Greece: ENISA, Nov. 2019. [Online]. Available: <https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector>. [Accessed June 8, 2026]
- [345] S. Durst and P. Evangelista, "Exploring knowledge management practices in third-party logistics service providers", *VINE Journal of Information and Knowledge Management Systems*, vol. 48, no. 2, pp. 162–177, 2018, doi: [10.1108/VJIKMS-05-2016-0030](https://doi.org/10.1108/VJIKMS-05-2016-0030).
- [346] A. Kuznetsov, J. Dinwoodie, D. Gibbs, M. Sansom, and H. Knowles, "Knowledge capture to inform sustainable maritime operations," *International Journal of Operations & Production Management*, vol. 37, no. 7, pp. 882–897, 2017, doi: [10.1108/IJOPM-10-2015-0657](https://doi.org/10.1108/IJOPM-10-2015-0657).
- [347] I. Bondareva, A. Khanova, and M. A. August, "Cargo port risk management ontological model" In *Human-Centric Cyber-Society*, J. Rak, L. Bellatreche, M. T. Thai, and A. Khoumsi, Eds. Cham, Switzerland: Springer Nature Switzerland, 2026, pp. 65–75, doi: [10.1007/978-3-032-06787-6\\_6](https://doi.org/10.1007/978-3-032-06787-6_6).
- [348] D. Sumić, L. Maleš, T. Marušić and M. Rosić, "Ontology-Based Information Infrastructure for Autonomous Ships", *Transactions on Maritime Science*, vol. 13, no. 1, 2024, Art. no. 008, doi: [10.7225/toms.v13.n01.008](https://doi.org/10.7225/toms.v13.n01.008).
- [349] H. Hutschenreuter, S. D. Çakmakçı, C. Maeder, and T. Kemmerich, "Ontology-based cybersecurity and resilience framework" In *Proc. 7th Int. Conf. on Information Systems Security and Privacy (ICISSP)*, Feb. 2021, pp. 458–466, doi: [10.5220/0010240204580466](https://doi.org/10.5220/0010240204580466).
- [350] C. Arrigan, R. Emmitt, and D. Singer, "Ontologies in the marine domain and use cases for autonomous vessel design and other novel designs" In *Proc. SNAME International Marine Design Conference (IMDC)*. Alexandria, VA, USA: Society of Naval Architects and Marine Engineers (SNAME), Jun. 2022, Paper D021S002R003, doi: [10.5957/IMDC-2022-342](https://doi.org/10.5957/IMDC-2022-342).
- [351] F. Martínez, L. E. Sánchez, A. Santos-Olmo, D. G. Rosado, and E. Fernández-Medina, "Maritime cybersecurity: protecting digital seas", *International Journal of Information Security*, vol. 23, no. 2, pp. 1429–1457, 2024, doi: [10.1007/s10207-023-00800-0](https://doi.org/10.1007/s10207-023-00800-0).
- [352] M. H. Larsen and M. S. Lund, "Cyber Risk Perception in the Maritime Domain: A Systematic Literature Review", *IEEE Access*, vol. 9, pp. 144895–144905, 2021, doi: [10.1109/ACCESS.2021.3122433](https://doi.org/10.1109/ACCESS.2021.3122433).
- [353] S. Ali, "Security in SCADA System: A Technical Report on Cyber Attacks and Risk Assessment Methodologies," in *Data Analytics in System Engineering*, R. Silhavy and P. Silhavy, Eds., CoMeSySo 2023, *Lecture Notes in Networks and Systems*, vol. 935. Cham, Switzerland: Springer, 2024], doi: [10.1007/978-3-031-54820-8\\_35](https://doi.org/10.1007/978-3-031-54820-8_35).

- [354] Common Criteria. Request to establish an International Technical Community (iTC) for the creation of Common Criteria Collaborative Protection Profiles and Supporting Documents relating to the security evaluation and certification of USB Portable Storage Devices. [Online] Available: <https://www.commoncriteriaportal.org/files/communities/UK-%20SG-%20USB%20WG%20iTC%20letter%20v1.6.pdf> [Accessed June 8, 2026]
- [355] SOG-IS portal. Senior Officials Group – Information Systems Security, February 27, 2026. [Online]. Available: <https://www.sogis.eu/> [Accessed June 8, 2026]
- [356] SOG-IS. Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, January 2010. [Online]. Available: <https://www.sogis.eu/documents/mra/20100107-sogis-v3.pdf> [Accessed June 8, 2026]
- [357] S. Islam, B. Sardar, E.-M. Kalogeraki *et al.*, “Hybrid AI-based dynamic risk assessment framework with explainable AI practices for composite product cybersecurity certification”, *International Journal of Information Security*, vol. 25, p. 51, 2026, [doi: 10.1007/s10207-026-01218-0](https://doi.org/10.1007/s10207-026-01218-0).
- [358] N. Basheer, S. Islam, S. Papastergiou, and E. M. Kalogeraki, “Composite Product Cybersecurity Certification Using Explainable AI Based Dynamic Risk Assessment” In *2025 IEEE International Conference on Cyber Security and Resilience (CSR)*, Chania, Crete, Greece, 2025, pp. 476–481, [doi: 10.1109/CSR64739.2025.11130134](https://doi.org/10.1109/CSR64739.2025.11130134).
- [359] Common Criteria portal, Official CC/CEM versions, Protection Profiles, Common Criteria. [Online]. Available: <https://www.commoncriteriaportal.org/pps/index.cfm> [Accessed June 8, 2026]
- [360] R. Tillu, M. Muthusubramanian, and V. Periyasamy, “From data to compliance: The role of AI/ML in optimizing regulatory reporting processes”, *Journal of Knowledge Learning Science and Technology*, vol. 2, 2023. [doi: 10.60087/jklst.vol2.n3.p391](https://doi.org/10.60087/jklst.vol2.n3.p391).
- [361] A. Folorunso, T. Adewumi, A. Adewa, R. Okonkwo, and T. N. Olawumi, “Impact of AI on cybersecurity and security compliance”, *Global Journal of Engineering Technology Advances*, vol. 21, 2024. [doi: 10.30574/gjeta.2024.21.1.0193](https://doi.org/10.30574/gjeta.2024.21.1.0193).
- [362] C. James, “Regulatory implications of explainable AI in cybersecurity frameworks”, Stanford University, Research Publication, 2022.
- [363] D. Gaspar, P. Silva, C. Silva, “Explainable AI for intrusion detection systems: LIME and SHAP applicability on multi-layer perceptron”, *IEEE Access* 12, 2024. [doi: 10.1109/ACCESS.2024.3368377](https://doi.org/10.1109/ACCESS.2024.3368377).
- [364] S. Ahmed, M. Al-Shareeda, and F. Alturjman, “Explainable AI-based innovative hybrid ensemble model for intrusion detection”, *Journal of Cloud Computing*, vol. 13, 2024. [doi:10.1186/s13677-024-00712-x](https://doi.org/10.1186/s13677-024-00712-x).
- [365] ISO/IEC 42001 “Artificial Intelligence — Management System”, 1<sup>st</sup> Edition, Geneva, 2023. [Online]. Available: <https://www.iso.org/standard/42001>. [Accessed June 8, 2026].
- [366] National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework (AI RMF 1.0), Gaithersburg, MD, USA, 2023. [doi:10.6028/NIST.AI.100-1](https://doi.org/10.6028/NIST.AI.100-1).
- [367] ISO/IEC/IEEE 21841:2019 international standard. “Systems and software engineering - taxonomy of systems of systems”. ISO/IEC/IEEE, 1<sup>st</sup> Edition, 2019.[Online]. Available: <https://www.iso.org/standard/71957.html>.
- [368] National Institute of Standards and Technology (NIST), “Security and Privacy Controls for Information Systems and Organizations”, *NIST*, Special Publication 800-53 Rev. 5 (5.2.0), Gaithersburg, MD, USA: NIST, Dec. 2020. [Online]. Available: <https://doi.org/10.6028/NIST.SP.800-53r5>.
- [369] P. Cichonski, T. Millar, T. Grance, K. Scarfone, “Computer Security Incident Handling Guide”, National Institute of Standards and Technology, Revision 2, August 2012.



- [370] N. Polatidis, E. Pimenidis, M. Pavlidis, S. Papastergiou, and H. Mouratidis, "From product recommendation to cyber-attack prediction: Generating attack graphs and predicting future attacks", *Evolving Systems*, vol. 11, no. 2, pp. 479–490, 2020, [doi: 10.1007/s12530-018-9234-z](https://doi.org/10.1007/s12530-018-9234-z).
- [371] S. Papastergiou and N. Polemi, "MITIGATE: A Dynamic Supply Chain Cyber Risk Assessment Methodology" In *Smart Trends in Systems, Security and Sustainability*, X. S. Yang, A. Nagar, and A. Joshi, Eds., vol. 18, Lecture Notes in Networks and Systems. Singapore: Springer, 2018, pp. 1–9, [doi: 10.1007/978-981-10-6916-1\\_1](https://doi.org/10.1007/978-981-10-6916-1_1).
- [372] Schauer, S., N. Polemi, and H. Mouratidis, "MITIGATE: A dynamic supply chain cyber risk assessment methodology," *Journal of Transportation Security*, vol. 12, no. 1–2, pp. 1–35, 2018, [doi: 10.1007/s12198-018-0195-z](https://doi.org/10.1007/s12198-018-0195-z).
- [373] S. Rass, S. König, and S. Schauer, "Uncertainty in games: Using probability-distributions as payoffs", In *Decision and Game Theory for Security*, M. H. R. Khouzani, E. Panaousis, and G. Theodorakopoulos, Eds. Cham, Switzerland: Springer, 2015, pp. 346–357, [doi: 10.1007/978-3-319-25594-1\\_20](https://doi.org/10.1007/978-3-319-25594-1_20).
- [374] ISO/SAE 21434:2021 "Road vehicles — Cybersecurity engineering". International Organization for Standardization (ISO), Society of Automotive Engineers (SAE), 1<sup>st</sup> Edition, Geneva, Switzerland, 2021. [Online]. Available: <https://www.iso.org/standard/70918.html> [Accessed June 8, 2026].
- [375] ISO 20000-1:2018, "Information technology — Service management — Part 1: Service management system requirements". Organization for Standardization (ISO), 3<sup>rd</sup> Edition, Geneva, Switzerland, 2018. [Online]. Available: <https://www.iso.org/standard/70636.html> [Accessed June 8, 2026]
- [376] Anchore Syft. CLI tool and library for generating a Software Bill of Materials from container images and filesystems. Github [Online]. Available: <https://github.com/anchore/syft> [Accessed June 8, 2026].
- [377] Aqua Trivy. The All-in-One Security Scanner, Aqua Security Software [Online]. Available: <https://trivy.dev/> [Accessed June 8, 2026].
- [378] S. Papastergiou, H. Mouratidis, and E.-M. Kalogeraki, "Cyber security incident handling, warning and response system for the european critical information infrastructures (cyberSANE)," in *Engineering Applications of Neural Networks (EANN 2019)*, J. Macintyre, L. Iliadis, I. Maglogiannis, and C. Jayne, Eds., *Communications in Computer and Information Science*, vol. 1000. Cham, Switzerland: Springer, 2019, pp. 476–487. [doi: 10.1007/978-3-030-20257-6\\_41](https://doi.org/10.1007/978-3-030-20257-6_41).
- [379] N. Polatidis and C. K. Georgiadis, "A multi-level collaborative filtering method that improves recommendations", *Expert Systems with Applications*, vol. 48, pp. 100–110, Apr. 2016, [doi: 10.1016/j.eswa.2015.11.023](https://doi.org/10.1016/j.eswa.2015.11.023).
- [380] Open-Source Intelligence (OSINT). OSINT framework, OSINT community. [Online]. Available: <https://osintframework.com/>. [Accessed June 8, 2026]
- [381] F.Schenkelberg, Effective Risk Mitigation Strategies, Accendo Reliability, 2026.[Online]. Available: <https://accendoreliability.com/4-effective-risk-mitigation-strategies/> [Accessed June 8, 2026]
- [382] MITIGATE EU H2020, Multidimensional, IntegraTed, rIsk assessment framework and dynamic, collaborative Risk ManaGement tools for critical information infrAstrucTurEs, CORDIS European Commission. [Online]. Available: <https://cordis.europa.eu/project/id/653212/reporting> [Accessed June 8, 2026]
- [383] CyberSANE EU H2020, Cyber Security Incident Handling, Warning and Response System for the European Critical Infrastructures. CORDIS European Commission. [Online]. Available: <https://cordis.europa.eu/project/id/833683> [Accessed June 8, 2026]
- [384] Fasoo Co., Ltd.FED 5 SP1. Common Criteria portal. [Online]. Available: [https://commoncriteriaportal.org/files/epfiles/FED%205%20SP1\\_ST\\_1.2\\_en.pdf](https://commoncriteriaportal.org/files/epfiles/FED%205%20SP1_ST_1.2_en.pdf) [Accessed June 8, 2026]

- [385] Protection Profile for Electronic Document Encryption. Common Criteria portal. . [Online]. Available: [https://www.commoncriteriaportal.org/nfs/ccpfiles/files/ppfiles/KECS-PP-0821a-2017\\_PP\\_EN.pdf](https://www.commoncriteriaportal.org/nfs/ccpfiles/files/ppfiles/KECS-PP-0821a-2017_PP_EN.pdf) [Accessed June 8, 2026]
- [386] Cryptographic Module for CSP Signing Operations with Backup - PP CMCSOB. SOG-IS Protection Profile portal. . [Online]. Available: [https://www.sogis.eu/uk/pp\\_pages/hsm/pp\\_hsm2.html](https://www.sogis.eu/uk/pp_pages/hsm/pp_hsm2.html) [Accessed June 8, 2026]
- [387] Federal Office for Information Security 'Guidelines for Developer Documentation according to Common Criteria Version 3.1.' [Online]. Available: [https://www.commoncriteriaportal.org/files/ccfiles/CommonCriteriaDevelopersGuide\\_1\\_0.pdf](https://www.commoncriteriaportal.org/files/ccfiles/CommonCriteriaDevelopersGuide_1_0.pdf) [Accessed June 8, 2026]
- [388] Network Device international Technical Community (ND iTC), Collaborative Protection Profile for Network Devices v3.0., Apr. 2023. [Online]. Available: [https://commoncriteriaportal.org/files/ppfiles/NDcPP\\_v3\\_0.pdf](https://commoncriteriaportal.org/files/ppfiles/NDcPP_v3_0.pdf) [Accessed June 8, 2026]
- [389] Common Criteria Administrator Guide, Cellcrypt Trusted Communications., 2022, [Online]. Available: <https://device.report/m/1ed78f05afdce29900c6257317e32b71c5322933ba6e2052bb0fe6376d898a23.pdf> [Accessed June 8, 2026]
- [390] IDNOMIC, Common Criteria Security Target., 2021. [Online]. Available: <https://cyber.gouv.fr/sites/default/files/2021/05/anssi-cible-2021-17en.pdf> [Accessed June 8, 2026]
- [391] Protection Profile for Application Software, v1.5, NIAP., 2021. [Online]. Available: [https://commoncriteria.github.io/pp/application/application-release.html#ext-comp-FPT\\_TUD\\_EXT](https://commoncriteria.github.io/pp/application/application-release.html#ext-comp-FPT_TUD_EXT) [Accessed June 8, 2026]
- [392] RUGGEDCOM ROS v4.2.2.F, Siemens., 2018. [Online]. Available: [https://cache.industry.siemens.com/dl/files/226/109760226/att\\_993693/v1/ROS-F\\_v4.2.2.F\\_Security-Target\\_Reference-Guide\\_EN.pdf](https://cache.industry.siemens.com/dl/files/226/109760226/att_993693/v1/ROS-F_v4.2.2.F_Security-Target_Reference-Guide_EN.pdf) [Accessed June 8, 2026]
- [393] Protection Profile for General Purpose Operating Systems., 2022. [Online]. Available: [https://www.commoncriteriaportal.org/files/ppfiles/PP\\_OS\\_V4.2.1.pdf](https://www.commoncriteriaportal.org/files/ppfiles/PP_OS_V4.2.1.pdf) [Accessed June 8, 2026]
- [394] Protection Profile Virtualization, v1.1, NIAP. [Online]. Available: [https://www.commoncriteriaportal.org/nfs/ccpfiles/files/ppfiles/PP\\_VIRTUALIZATION\\_BASE\\_V1.1.pdf](https://www.commoncriteriaportal.org/nfs/ccpfiles/files/ppfiles/PP_VIRTUALIZATION_BASE_V1.1.pdf) [Accessed June 8, 2026]
- [395] Mapping Between PP-Module for Authentication Servers, Version 1.0, 2023-01-25 and NIST SP 800-53 Revision 5, Jan. 2023. [Accessed June 8, 2026]
- [396] E. M. Kalogeraki and S. Papastergiou, **Security Functional Requirements (SFRs) Classification, ver. 1.0, Aug. 2024., CUSTODES HE project** [Online]. Available: <https://custodes-project.eu/wp-content/uploads/useruploads/CUSTODES-Security-Requirements-Classification-v1.pdf>
- [397] CUSTODES, A Certification approach for dynamic, agile and reUSable assessment fOr composite systems of ICT proDucts, servicEs, and processeS. CORDIS European Commission. [Online]. Available: <https://cordis.europa.eu/project/id/101120684> [Accessed June 8, 2026]
- [398] European Commission. "Shaping Europe's digital future. ICT supply chain security: EU adopts a toolbox to mitigate risks", European Commission. February 13, 2026. [Online]. Available: <https://digital-strategy.ec.europa.eu/en/news/ict-supply-chain-security-eu-adopts-toolbox-mitigate-risks> [Accessed June 8, 2026]

# Appendices

## Appendix A: Glossary

The following table presents definitions of terms utilised in this dissertation and their related sources deriving either from regulatory instruments or standards or best practices or prominent/acknowledged publications. The definition of some concepts may be characterised as “cybersecurity”, or “business” or “general”, or “conformity assessment”, or “quality assurance” definition (wherever required) to illustrate the corresponding perspectives.

Table 85. Glossary of definitions and terms utilized in the current dissertation.

| Term                                      | Definition                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Related sources                                   |
|-------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------|
| <b>Access control</b>                     | Means to ensure that physical and logical access to assets is authorized and restricted based on business and information security requirements.                                                                                                                                                                                                                                                                                                                                                                                                                                                                | <a href="#">ISO/IEC 27002: 2022</a> [66]          |
| <b>Accountability</b>                     | The state of being answerable (in response) for assigned actions and decisions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | <a href="#">ISO/IEC 27000: 2018</a> [53]          |
| <b>Accreditation</b>                      | An attestation by a national accreditation body that a conformity assessment body meets the requirements set by harmonised standards and, where applicable, any additional requirements including those set out in relevant sectoral schemes, to carry out a specific conformity assessment activity.                                                                                                                                                                                                                                                                                                           | <a href="#">Regulation (EC) No 765/2008</a> [160] |
|                                           | Third-party attestation related to a conformity assessment body, conveying formal demonstration of its competence impartiality and consistent operation in performing specific conformity assessment activities                                                                                                                                                                                                                                                                                                                                                                                                 | <a href="#">ISO/IEC 17000:2020</a> [57]           |
| <b>Accreditation Body</b>                 | Authoritative body that performs accreditation.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | <a href="#">ISO/IEC 17000:2020</a> [57]           |
| <b>Adversary</b>                          | Individual, group, organisation, or government that conducts or has the intent to conduct detrimental activities                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | <a href="#">NIST SP 800-30 Rev. 1</a> [125]       |
| <b>Advanced Persistent Threats (APTs)</b> | An adversary with sophisticated levels of expertise and significant resources deriving from multiple different attack vectors (e.g., cyber, physical, and deception) who generates opportunities to achieve its objectives which are typically to establish and extend its presence within the information technology infrastructure of organisations over a long period to infiltrate organisations, steal information, disrupt operations, or maintain hidden access. APTs are persistent, adaptive, and determined, continuously adjusting their tactics to evade defenses and achieve long-term objectives. | <a href="#">NIST SP 800-30 Rev. 1</a> [125]       |

|                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                     |
|-----------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| <b>Attack Simulation and Evidence Chains Generation (ASECG)</b> | A model that estimates credible vulnerability chains on ICT assets in relation to a confirmed security event.                                                                                                                                                                                                                                                                                                     | Defined in this dissertation (see Section 6.2.2.5)                                  |
| <b>Asset</b>                                                    | Anything (e.g. hardware, software, network, information) that has value (potential or actual value) to the organisation (the value can be tangible or intangible, financial or non-financial, and includes consideration of risks and liabilities). An asset extends beyond physical goods or hardware, and includes software, information, people, reputation or agreements. ( <i>cybersecurity definition</i> ) | <a href="#">ISO/IEC 20001-1:2018</a> , <a href="#">ISO/IEC 27002: 2022</a> [66]     |
|                                                                 | Entity that the owner of the Target of Evaluation resumably places value on. ( <i>conformity assessment / IT evaluation definition</i> )                                                                                                                                                                                                                                                                          | <a href="#">ISO/IEC 15408-1:2026</a> [44]                                           |
|                                                                 | Item, thing or entity that has potential or actual value to an organisation. ( <i>General definition</i> )                                                                                                                                                                                                                                                                                                        | <a href="#">ISO/IEC 55000:2024</a> , <a href="#">ISO/IEC 19770-1:2017</a>           |
|                                                                 | ICT asset<br>Software or hardware in the network and information systems used by entities of the type referred to in Annexes I and II to Directive (EU) 2022/2555 [12]                                                                                                                                                                                                                                            | <a href="#">Cybersecurity Act 2 (proposal)</a> [49]                                 |
| <b>Assurance</b>                                                | Grounds for confidence that a Target of Evaluation meets the Security Functional Requirements (SFRs).                                                                                                                                                                                                                                                                                                             | <a href="#">CC:2022 Part 1 R1</a> [58] or <a href="#">ISO/IEC 15408-1:2026</a> [44] |
|                                                                 | Basis for confidence that an ICT product/ICT service /ICT process meets the security requirements of a specific European cybersecurity certification scheme, indicates the level at which an ICT product/ICT service/ICT process has been evaluated but as such does not measure the security of the ICT product/ICT service/ICT process concerned.                                                               | <a href="#">Regulation (EU) 2019/881</a> [13]<br>(Cybersecurity Act)                |
| <b>Attacker</b>                                                 | Person deliberately exploiting vulnerabilities in technical and non-technical security controls in order to steal or compromise information systems and networks, or to compromise availability to legitimate users of information system and network resources                                                                                                                                                   | <a href="#">ISO/IEC 27032:2023</a> [137]                                            |
| <b>Attack path</b>                                              | Steps that a threat takes or may take to plan, prepare for, and execute an attack.                                                                                                                                                                                                                                                                                                                                | <a href="#">ANSI/API STD 780</a>                                                    |
| <b>Attack Path Exploitability Level (APEL)</b>                  | Qualitative value that measures the level of exploitation for a given attack path towards a specific confirmed event with a specific IoC.                                                                                                                                                                                                                                                                         | Defined in this dissertation                                                        |
| <b>Attack vector</b>                                            | Path or means by which an attacker can gain access to a computer or network server in order to deliver a malicious outcome                                                                                                                                                                                                                                                                                        | <a href="#">ISO/IEC 27032:2023</a> [137]                                            |

|                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                       |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| <b>Attestation</b>        | <p>Issue of a statement, based on a decision, that fulfilment of <i>specified requirements</i> has been demonstrated</p> <p>The resulting statement, referred to in this document as a “statement of conformity”, is intended to convey the assurance that the specified requirements have been fulfilled. Such an assurance does not, of itself, provide contractual or other legal guarantees. First-party attestation and third-party attestation are distinguished by the terms <i>declaration</i>, <i>certification</i> and <i>accreditation</i> but there is no corresponding term applicable to second-party attestation.</p> | <a href="#">ISO/IEC 17000:2020</a> [57]                                               |
| <b>Audit</b>              | Systematic and independent process for obtaining evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled. ( <i>General definition</i> )                                                                                                                                                                                                                                                                                                                                                                                                                                             | <a href="#">ISO/IEC 27000: 2018</a> [53],<br><a href="#">ISO/IEC 28000:2022</a> [138] |
|                           | <p>Process for obtaining relevant information about an object of conformity assessment and evaluating it objectively to determine the extent to which specified requirements are fulfilled. For accreditation purposes, the audit process is called “assessment.</p> <p>(<i>Conformity Assessment-related definition</i>)</p>                                                                                                                                                                                                                                                                                                        | <a href="#">ISO/IEC 17000:2020</a> [57]                                               |
|                           | systematic and independent process for obtaining evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                       |
| <b>Authentication</b>     | Provision of assurance that a claimed characteristic of an entity is correct                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | <a href="#">ISO/IEC 27000: 2018</a> [53]                                              |
| <b>Authenticity</b>       | Property that an entity is what it claims to be.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | <a href="#">ISO/IEC 27000: 2018</a> [53]                                              |
| <b>Availability</b>       | Property of being accessible and usable on demand by an authorized entity.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | <a href="#">ISO/IEC 27000: 2018</a> [53]                                              |
| <b>AVA_VAN level</b>      | An assurance vulnerability analysis level that indicates the degree of cybersecurity evaluation activities carried out to determine the level of resistance against potential exploitability of flaws or weaknesses in the target of evaluation in its operational environment as set out in the Common Criteria.                                                                                                                                                                                                                                                                                                                    | EUCC implementing Regulation <a href="#">(EU) 2024/482</a> [14]                       |
| <b>Black Swan event</b>   | A rare event that can cause tremendous impact.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Defined in this Dissertation                                                          |
| <b>Behaviour analysis</b> | The act of examining malware interactions within its operating environment including file systems, the registry (if on Windows), the network, as well as other processes and Operating System components.                                                                                                                                                                                                                                                                                                                                                                                                                            | CNSSI No. 1011                                                                        |
| <b>Bot</b>                | A program operating as an agent for a user or another program or simulates a human activity. The most ubiquitous                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | <a href="#">ISO/IEC 27032:2023</a> [137]                                              |

|                                          |                                                                                                                                                                                                                                                                                                                         |                                                                                                                                   |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
|                                          | bots on the Web are programs accessing websites and gather their content for search engine indexes (i.e., spiders or crawlers)                                                                                                                                                                                          |                                                                                                                                   |
| <b>Business Partner</b>                  | Those contractors, suppliers or service providers that an organization contracts with to assist the organisation in its function as an organisation in the supply chain.                                                                                                                                                | <a href="#">ISO 28001:2007</a> [70]                                                                                               |
| <b>Business Process Management (BPM)</b> | Deals with organising, automating, monitoring and controlling business processes in organisations.                                                                                                                                                                                                                      | Kalogeraki et al. [93]                                                                                                            |
| <b>Certification</b>                     | Third-party attestation related to an object of conformity assessment with the exception of accreditation.                                                                                                                                                                                                              | <a href="#">ISO/IEC 17000:2020</a> [57]                                                                                           |
| <b>Certification Body</b>                | Third-party conformity assessment body operating certification schemes                                                                                                                                                                                                                                                  | <a href="#">ISO/IEC 17065:2012</a> [204]                                                                                          |
| <b>Cobot</b>                             | Robots interacting with humans in a collaborative behaviour in a shared space or working safely adjacently, alongside with them.                                                                                                                                                                                        | Zafar, Langås, and Sanfilippo (2024) [32]                                                                                         |
| <b>Composite product</b>                 | An ICT product that is evaluated together with another underlying ICT product that has already received an EUCC certificate and on whose security functionality the composite ICT product depend                                                                                                                        | EUCC implementing Regulation <a href="#">(EU) 2024/482</a>                                                                        |
| <b>Confidentiality</b>                   | Property that information is not made available or disclosed to unauthorized individuals, entities, or processes.                                                                                                                                                                                                       | <a href="#">ISO/IEC 27000: 2018</a> [53]                                                                                          |
| <b>Conformity</b>                        | Fulfilment of a requirement.<br>≠ non conformity: non-fulfilment of a requirement.                                                                                                                                                                                                                                      | <a href="#">ISO/IEC 27000: 2018</a> [53],<br><a href="#">ISO/IEC 17000:2020</a> [57],<br><a href="#">ISO/IEC 28000:2022</a> [138] |
| <b>Conformity Assessment</b>             | The process for evaluating and demonstrating whether specified requirements relating to an ICT product, ICT service or ICT process have been fulfilled. Conformity assessment includes a set of activities, such as but not limited to testing, inspection, validation, verification, certification, and accreditation. | <a href="#">ISO/IEC 17000:2020</a> [57]                                                                                           |
|                                          | The process of evaluating whether specified requirements, rules or claims associated with an ICT product, ICT service have been fulfilled.                                                                                                                                                                              | <a href="#">Cybersecurity Act: Regulation (EU) 2019/881</a> [13], <a href="#">Regulation (EC) No 765/2008</a> [160]               |
|                                          | The process of verifying whether the essential cybersecurity requirements set out in EU Cyber Resilience Act, Annex I have been fulfilled;                                                                                                                                                                              | <a href="#">Cyber Resilience Act</a> [11]                                                                                         |

|                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                           |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
|                                   | <p>Demonstration that specified requirements are fulfilled</p> <p>The process of conformity assessment may have a negative outcome, i.e. demonstrating that the specified requirements are not fulfilled.</p> <p>Conformity assessment includes activities such as but not limited to testing, inspection, validation, certification,, and accreditation</p> <p>Conformity assessment is a series of functions. Activities contributing to any of these functions can be described as conformity assessment activities.</p> <p><i>(non-compliance definition)</i></p> | <a href="#">ISO/IEC 17000:2020</a> [57]                                                                                                   |
| <b>Conformity Assessment Body</b> | A Body that performs conformity assessment activities including calibration, testing, certification and inspection                                                                                                                                                                                                                                                                                                                                                                                                                                                    | <a href="#">Regulation (EC) No 765/2008</a> [160]                                                                                         |
|                                   | Body that performs conformity assessment activities, excluding accreditation.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | <a href="#">ISO/IEC 17000:2020</a> [57]                                                                                                   |
| <b>Consequences</b>               | Outcome of an event affecting objectives                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | <a href="#">ISO/IEC 27000: 2018</a> [53]                                                                                                  |
| <b>Contract</b>                   | Binding agreement                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | <a href="#">ISO 9000:2015</a>                                                                                                             |
| <b>Control</b>                    | <p>Risk Control</p> <p>Measure that is modifying risk. Controls include any process, policy, device, practice, or other actions which modify It is possible that controls not always exert the intended or assumed modifying effect.</p>                                                                                                                                                                                                                                                                                                                              | <a href="#">ISO/IEC 27000: 2018</a> [53],<br><a href="#">ISO 31073: 2022</a> , <a href="#">ISO 31000: 2018</a> [188]                      |
|                                   | <p>Security Control</p> <p>The safeguards or countermeasures prescribed for an information system or an organisation to protect the confidentiality, integrity, and availability of the system and its information.</p>                                                                                                                                                                                                                                                                                                                                               | <a href="#">NIST SP 800-53 Rev. 5</a>                                                                                                     |
|                                   | <p>A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.</p>                                                                                                                                                                                                                                                                                                                              | <a href="#">NIST SP 1800-15B</a> , <a href="#">NIST SP 1800-21B</a> , <a href="#">NIST SP 1800-27B</a> , <a href="#">NIST SP 1800-27C</a> |
| <b>Control objective</b>          | Statement describing what is to be achieved as a result of implementing controls.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | <a href="#">ISO/IEC 27000: 2018</a> [53]                                                                                                  |
| <b>Confidentiality</b>            | Property that information is not made available or disclosed to unauthorized individuals, entities, or processes.                                                                                                                                                                                                                                                                                                                                                                                                                                                     | <a href="#">ISO/IEC 27000: 2018</a> [53]                                                                                                  |



|                                                    |                                                                                                                                                                                                                                                                                  |                                                                  |
|----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------|
| <b>Conformity Assessment Body</b>                  | A Body that performs conformity assessment activities including calibration, testing, certification and inspection                                                                                                                                                               | <a href="#">Regulation (EC) No 765/2008</a> [160]                |
| <b>Countermeasures</b>                             | Actions taken to lower the likelihood of a security threat scenario succeeding in its objectives, or to reduce the likely consequences of a security threat scenario                                                                                                             | <a href="#">ISO28001: 2007</a> [70]                              |
| <b>Critical Information Infrastructures (CIIs)</b> | Critical Information Infrastructures (CIIs) are considered ICT infrastructures on which the smooth functioning of the internal market depends.                                                                                                                                   | <a href="#">NIS 2 Directive; Regulation (EU) 2022/2555</a> [12]  |
| <b>Critical service</b>                            | A critical service is a service that is essential for the maintenance of critical societal or economic activities.                                                                                                                                                               | <a href="#">NIS 2 Directive; Regulation (EU) 2022/2555</a> [12]  |
| <b>Customer</b>                                    | Person or organization that could or does receive a product or a service that is intended for or required by this person or organization.<br><br>e.g., consumer, client, end-user, retailer, receiver of product or service from an internal process, beneficiary and purchaser. | <a href="#">ISO9000:2015</a>                                     |
| <b>Cyber-hygiene</b>                               | Simple, routine measures to be implemented and carried out regularly by citizens, organisations and businesses to minimise their exposure to risks from cyber threats.                                                                                                           | <a href="#">NIS 2 Directive; Regulation (EU) 2022/2555</a> [12]  |
| <b>Cybersecurity</b>                               | The activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats.                                                                                                                                     | <a href="#">Cybersecurity Act; Regulation (EU) 2019/881</a> [13] |
|                                                    | Safeguarding of people, society, organisations and nations from cyber risks.                                                                                                                                                                                                     | <a href="#">ISO/IEC 27032:2023</a> [137]                         |
| <b>Cyberattack</b>                                 | (Successful or unsuccessful unauthorized) attempt to destroy, alter, disable, gain access to an asset (or any attempt to expose, steal, or make unauthorized use of an asset.                                                                                                    | <a href="#">ISO/IEC 27000: 2018</a> [53]                         |
|                                                    | An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.      | <a href="#">NIST SP 800-30 Rev. 1</a> [125]                      |
| <b>Cybersecurity standard</b>                      | A level of quality or attainment used as a measure (i.e., metric, baseline, rule, condition, requirement), norm, or model in comparative evaluations of products, systems, services, or processes.                                                                               | <a href="#">ISO/IEC 17000:2020</a> [57]                          |
| <b>Data</b>                                        | Facts about an object.                                                                                                                                                                                                                                                           | <a href="#">ISO 9000:2015</a>                                    |



|                                                    |                                                                                                                                                                                                                                                                                                                                                                                 |                                                                            |
|----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------|
| <b>Effectiveness</b>                               | Extent to which planned activities are realized and planned results achieved                                                                                                                                                                                                                                                                                                    | <a href="#">ISO/IEC 27000: 2018</a> [53],<br><a href="#">ISO 9000:2015</a> |
| <b>Event</b>                                       | Occurrence or change of a particular set of circumstances. An event can be one or more occurrences, and can have several causes.<br><br>An event can consist of something not happening. An event can sometimes be referred to as an “incident” or “accident”.                                                                                                                  | <a href="#">ISO 31000:2018</a> [188]                                       |
|                                                    | Information security event<br><br>Identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls or a previously unknown situation that can be security relevant.                                                                                                                               | <a href="#">ISO/IEC 27000: 2018</a> [53]                                   |
|                                                    | Occurrence indicating a possible breach of information security or failure of controls                                                                                                                                                                                                                                                                                          | <a href="#">ISO/IEC 27035:2023</a> [153]                                   |
| <b>Evaluation</b>                                  | Combination of the selection and determination functions of conformity assessment activities                                                                                                                                                                                                                                                                                    | <a href="#">ISO/IEC 17065:2012</a> [204]                                   |
| <b>Darknet</b>                                     | Network of secret websites within the Internet that can only be accessed with specific software.                                                                                                                                                                                                                                                                                | <a href="#">ISO/IEC 27032:2023</a> [137]                                   |
| <b>DevSecOps</b>                                   | DevSecOps is an extension of DevOps that integrates security practices, culture and automation throughout the software development lifecycle (SDLC). It embeds security controls, testing, and monitoring into continuous integration and continuous delivery (CI/CD) pipelines ensuring shared responsibility for security across development, operations, and security teams. | <a href="#">NIST SP 800-204C</a> [40]                                      |
|                                                    | Building, package, and deploy software systems in a secure and reliable way, covering the full software life cycle.                                                                                                                                                                                                                                                             | <a href="#">ISO/IEC/IEEE 32675:2022</a> [41]                               |
| <b>Entity</b>                                      | A natural or legal person created and recognised as such under the national law of its place of establishment, which may, acting under its own name, exercise rights and be subject to obligations.                                                                                                                                                                             | <a href="#">NIS 2 Directive; Regulation (EU) 2022/2555</a> [12]            |
| <b>European Cybersecurity Certification Scheme</b> | A comprehensive set of rules, technical requirements, standards and procedures that are established at Union level and that apply to the certification or conformity assessment of specific ICT products, ICT services or ICT processes.                                                                                                                                        | <a href="#">Cybersecurity Act; Regulation (EU) 2019/881</a> [13]           |

|                                                       |                                                                                                                                                                                                                                   |                                                                              |
|-------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|
| <b>EUCC certificate</b>                               | A cybersecurity certificate issued under the EUCC for ICT products, or for protection profiles that can be used exclusively in the ICT process of certification of ICT products.                                                  | EUCC implementing Regulation <a href="#">(EU) 2024/482</a> [14]              |
| <b>Hacking</b>                                        | Intentionally accessing a computer system without the authorization of the user or the owner.                                                                                                                                     | <a href="#">ISO/IEC 27032:2023</a> [137]                                     |
| <b>Information and Communication Technology (ICT)</b> | It encompasses all categories of ubiquitous technology used for the gathering, storing, transmitting, retrieving, display, representation, organization, management, security, processing or interchange of data and information. | <a href="#">NIST IR 8074 Vol. 2</a> [65],<br><a href="#">CNSSI 4009-2015</a> |
| <b>ICT product/service/process/supply chain</b>       | ICT product      An element or a group of elements of a network or information system;                                                                                                                                            | <a href="#">Cybersecurity Act; Regulation (EU) 2019/881</a> [13]             |
|                                                       | ICT service      A service consisting fully or mainly in the transmission, storing, retrieving or processing of information by means of network and information systems.                                                          |                                                                              |
|                                                       | ICT process      A set of activities performed to design, develop, deliver or maintain an ICT product or ICT service.                                                                                                             |                                                                              |
|                                                       | ICT supply chain      A group of ICT services, ICT products and ICT processes that encompass activities and actors involved at all stages upstream of a product being made available or a service being delivered on the market.  | <a href="#">Proposal of Cyber Resilience Act 2</a> [49]                      |
| <b>Impact</b>                                         | The effect on organisational operations, assets, individuals, other entities of a loss of confidentiality, integrity, or availability of information or a system.                                                                 | <a href="#">NIST SP 800-53 Rev. 5</a> [368]                                  |
| <b>Impact value</b>                                   | The assessed worst-case potential impact that could result from a compromise of the confidentiality, integrity, or availability of information expressed as a value of low, moderate, or high.                                    | <a href="#">NIST SP 800-53 Rev. 5</a> [368]                                  |
| <b>Indicator</b>                                      | Measure that provides an estimate or evaluation.                                                                                                                                                                                  | <a href="#">ISO/IEC 27000: 2018</a> [53]                                     |
| <b>Incident</b>                                       | An event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems.                    | <a href="#">NIS 2 Directive; Regulation (EU) 2022/2555</a> [12]              |
|                                                       | Security incident      Any act or circumstance that produces a consequence. ( <i>Supply chain security definition</i> )                                                                                                           | <a href="#">ISO28001: 2007</a> [70]                                          |

|                                |                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                     |                                                                 |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|
|                                | Information security incident                                                                                                                                                                                   | Identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls or a previously unknown situation that can be security relevant                                                                                                                      | <a href="#">ISO/IEC 27000: 2018</a> [53]                        |
|                                |                                                                                                                                                                                                                 | Related and identified information security event that can harm an organisation's assets or compromise its operations                                                                                                                                                                                                               | <a href="#">ISO/IEC 27035:2023</a> [153]                        |
|                                | Security, computer cybersecurity, cyberspace incident                                                                                                                                                           | An occurrence that actually or potentially jeopardises the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies | NIST Glossary of Terms                                          |
| Incident handling / management | Incident handling                                                                                                                                                                                               | Any actions and procedures aiming to prevent, detect, analyse, and contain or to respond to and recover from an incident                                                                                                                                                                                                            | <a href="#">NIS 2 Directive; Regulation (EU) 2022/2555</a> [12] |
|                                |                                                                                                                                                                                                                 | Actions of detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents                                                                                                                                                                                                           | <a href="#">ISO/IEC 27035:2023</a> [153]                        |
|                                |                                                                                                                                                                                                                 | The remediation or mitigation of violations of security policies and recommended practices.                                                                                                                                                                                                                                         | <a href="#">NIST SP 800-61 r3, PL 113-283 (FISMA)</a>           |
|                                | Information security Incident management                                                                                                                                                                        | Set of processes for detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents.                                                                                                                                                                                                | <a href="#">ISO/IEC 27000: 2018</a> [53]                        |
|                                |                                                                                                                                                                                                                 | Collaborative activities to handle information security incidents in a consistent and effective way.                                                                                                                                                                                                                                | <a href="#">ISO/IEC 27035:2023</a> [153]                        |
| Incident response              | The remediation or mitigation of violations of security policies and recommended practices.                                                                                                                     |                                                                                                                                                                                                                                                                                                                                     | <a href="#">NIST SP 800-61 r3, PL 113-283 (FISMA)</a>           |
|                                | Actions taken to mitigate or resolve an information security incident including those taken to protect and restore the normal operational conditions of an information system and the information stored in it. |                                                                                                                                                                                                                                                                                                                                     | <a href="#">ISO/IEC 27035:2023</a> [153]                        |

|                                                      |                                                                                                                                                                                                                                                         |                                                                 |
|------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|
| <b>Incident response plan</b>                        | The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber attacks against an organization's information system(s).                                                      | <a href="#">NIST SP 800-34 Rev. 1</a>                           |
| <b>Indicators of compromise (IoCs)</b>               | They are the digital evidence (artefacts) of potential cyberattacks on a system or network.                                                                                                                                                             | Defined in this dissertation                                    |
| <b>Information</b>                                   | Meaningful data.                                                                                                                                                                                                                                        | <a href="#">ISO 9000:2015</a>                                   |
|                                                      | Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.                                                                | <a href="#">FIPS 199</a> ,<br><a href="#">NIST SP 800-39</a>    |
| <b>Information security</b>                          | Preservation of Confidentiality, Integrity, and Availability (CIA) of information involving also the ensurance of other properties such as authenticity, accountability, non-repudiation, and reliability.                                              | <a href="#">ISO/IEC 27000: 2018</a> [53]                        |
| <b>Information security continuity</b>               | Processes and procedures for ensuring continued information security operations                                                                                                                                                                         | <a href="#">ISO/IEC 27000: 2018</a> [53]                        |
| <b>Impact analysis</b>                               | The analysis conducted by an organizational official to determine the extent to which changes to the information system have affected the security state of the system.                                                                                 | <a href="#">[NIST SP 800-37 Rev.2, 2018]</a>                    |
| <b>Information Security Management System (ISMS)</b> | Set of interrelated or interacting elements (can be applications, services, information technology assets, or other information-handling components) of an organisation to establish policies and objectives and processes to achieve those objectives. | <a href="#">ISO/IEC 27001: 2022</a> [55]                        |
| <b>Information security system</b>                   | Set of applications, services, information technology assets, or other information-handling components                                                                                                                                                  | <a href="#">ISO/IEC 27000: 2018</a> [53]                        |
| <b>Infrastructure</b>                                | Organization system of facilities, equipment and services needed to achive objectives.                                                                                                                                                                  | <a href="#">ISO 22300: 2025</a> [67]                            |
|                                                      | Critical Information Infrastructure (CII)      Critical Information Infrastructures (CIIs) are considered ICT infrastructures on which the smooth functioning of the internal market depends.                                                           | <a href="#">NIS 2 Directive; Regulation (EU) 2022/2555</a> [12] |
|                                                      | ICT infrastructure      Organization system of facilities, equipment and ICT services required for the operation of an entity (e.g. enterprise,                                                                                                         | Current Doctoral Thesis                                         |

|                                     |                                                                                                                                                                                                                                                                                                                                                                         |                                               |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------|
|                                     | organization, government) that processes, stores, retrieves, represents or exchanges data and information.                                                                                                                                                                                                                                                              |                                               |
| <b>Innovation</b>                   | New or changed object realising or redistributing value                                                                                                                                                                                                                                                                                                                 | <a href="#">ISO 9000:2015</a>                 |
| <b>Inspection</b>                   | Determination of conformity to specified requirements.<br>( <i>Quality Assurance -related and/or general definition</i> )                                                                                                                                                                                                                                               | <a href="#">ISO 9000:2015</a>                 |
|                                     | Examination of an object of conformity assessment and determination of its conformity with detailed requirements or, on the basis of professional judgement, with general requirements. Examination may include direct or indirect observations, which can encompass measurements or the output of instruments.<br>( <i>Conformity Assessment- related definition</i> ) | <a href="#">ISO/IEC 17000:2020</a> [57]       |
| <b>Integrity</b>                    | Property of accuracy and completeness                                                                                                                                                                                                                                                                                                                                   | <a href="#">ISO/IEC 27000: 2018</a> [53]      |
| <b>Internet of Everything (IoE)</b> | The networked connection of people, process, data, and things.                                                                                                                                                                                                                                                                                                          | Cisco (2013) [32]                             |
| <b>Linked Open Data</b>             | Published data on the Web connecting to each other with concrete statements recommending a Web of Data.                                                                                                                                                                                                                                                                 | <a href="#">T. B. Lee, 2000</a>               |
| <b>Likelihood</b>                   | Chance of something happening<br>(Defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period).                                                                                                                    | <a href="#">ISO 31000: 2018</a> [188]         |
| <b>Likelihood of occurrence</b>     | A weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability or a set of vulnerabilities. Determining the likelihood of threat events causing adverse impacts.                                                                                                                                | <a href="#">NIST SP 800-30 Rev. 1</a> , [125] |
| <b>Malware/ malicious software</b>  | Software designed with malicious intent containing features or capabilities that can potentially cause harm directly or indirectly to the user and/or the user's computer system (e.g., viruses, worms and trojans).                                                                                                                                                    | <a href="#">ISO/IEC 27032:2023</a> [137]      |
| <b>Managed security services</b>    | Outsourced cybersecurity activities (i.e., monitoring, detection, prevention, or response to cyber threats) a provider performs on behalf of a customer on an ongoing basis.                                                                                                                                                                                            | <a href="#">Regulation (EU) 2025/37</a> [47]  |
| <b>Management</b>                   | Coordinated activities to direct and control an organization.                                                                                                                                                                                                                                                                                                           | <a href="#">ISO 9000:2015</a>                 |

|                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                         |
|---------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
|                                             | Management includes establishing policies, objectives and processes to achieve these objectives. Sometimes may refer to people, as well.                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                         |
| <b>Management System</b>                    | Organisation's structure for managing its processes or activities that transform inputs of resources into a product or service, which meet the organisation's objectives.                                                                                                                                                                                                                                                                                                                                                                                                                                 | <a href="#">ISO/IEC 28001: 2007</a> [70]                                                                                |
|                                             | <p>Set of interrelated or interacting elements of an organization to establish policies and objectives and processes to achieve those objectives.</p> <p>A management system can address a single discipline or several disciplines. The system elements include the organization's structure, roles and responsibilities, planning and operation. The scope of a management system may include the whole of the organization, specific and identified functions of the organization, specific and identified sections of the organization, or one or more functions across a group of organizations.</p> | <a href="#">ISO/IEC 27000: 2018</a> [53],<br><a href="#">ISO/IEC 28000:2022</a> [138],<br><a href="#">ISO 9000:2015</a> |
| <b>Measurement</b>                          | Process to determine a value.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | <a href="#">ISO 9000:2015</a> , <a href="#">ISO/IEC 28000:2022</a> [138]                                                |
| <b>Mitigation</b>                           | Limitation of the negative consequences of a particular event.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | <a href="#">ETSI TS 102 165-1</a>                                                                                       |
| <b>Monitoring</b>                           | <p>Determining the status of a system, a process or an activity</p> <p>To determine the status, there can be a need to check, supervise or critically observe (plan-do-check-act).</p>                                                                                                                                                                                                                                                                                                                                                                                                                    | <a href="#">ISO/IEC 28000:2022</a> [138]                                                                                |
|                                             | Continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected (Risk Management – related definition)                                                                                                                                                                                                                                                                                                                                                                                                        | <a href="#">ISO 31073: 2022</a>                                                                                         |
| <b>Network and Information System (NIS)</b> | <p>It can be: (i) an electronic communications network as defined in Article 2, point (1), of Directive (EU) 2018/1972; (ii) any device or group of interconnected or related devices, one or more of which, pursuant to a programme, carry out automatic processing of digital data; or (iii) digital data stored, processed, retrieved or transmitted by elements covered under points.</p> <p><u>Note:</u> (i) and (ii) are considered for the purposes of their operation, use, protection and maintenance.</p>                                                                                       | <a href="#">NIS 2 Directive; Regulation (EU) 2022/2555</a> [12]                                                         |
| <b>Non-repudiation</b>                      | Ability to prove the occurrence of a claimed event or action and its originating entities.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | <a href="#">ISO/IEC 27000: 2018</a> [53]                                                                                |

|                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                                                    |
|-----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| <b>Objective</b>                        | Result to be achieved. An objective can be strategic, tactical, or operational. Objectives can relate to different disciplines (e.g., financial, health and safety, and environmental goals) and can apply at different levels (e.g. strategic, organization-wide, project, product and process). An objective can be expressed in other ways, e.g. as an intended outcome, a purpose, an operational criterion, as an information security objective or by the use of other words with similar meaning (e.g., aim, goal, or target).<br><i>(General definition)</i>                                     | <a href="#">ISO/IEC 27000: 2018</a> [53],<br><a href="#">ISO/IEC 28000:2022</a> [138],<br><a href="#">ISO 9000:2015</a>            |
|                                         | Security objective      Security objectives set by the organisation, consistent with the information security policy, to achieve specific results.                                                                                                                                                                                                                                                                                                                                                                                                                                                       | <a href="#">ISO/IEC 27000: 2018</a> [53],<br><a href="#">ISO/IEC 28000:2022</a> [138]                                              |
| <b>Ontology</b>                         | An explicit specification of a conceptualization                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Gruber, et al, [116]                                                                                                               |
| <b>Opportunity</b>                      | Combination of circumstances expected to be favourable to objectives.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | <a href="#">ISO 31073: 2022</a>                                                                                                    |
|                                         | An opportunity is a positive situation in which gain is likely and over which one has a fair level of control. An opportunity to one party may pose a threat to another. Taking or not taking an opportunity are both sources of risk.                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                                                    |
| <b>Organisation</b>                     | Person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives.                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | <a href="#">ISO/IEC 27000: 2018</a> [53],<br><a href="#">ISO/IEC 27032:2023</a> [137],<br><a href="#">ISO/IEC 28000:2022</a> [138] |
| <b>Organisation in the supply chain</b> | Any entity that: <ul style="list-style-type: none"> <li>• manufactures, handles, processes, loads, consolidates, unloads or receives goods upon placement of a purchase order that at some point cross an international or economy border;</li> <li>• transports goods by any mode in the international supply chain regardless of whether their particular segment of the supply chain crosses national (or economy) boundaries; or</li> <li>• provides, manages or conducts the generation, distribution or flow of shipping information used by customs agencies or in business practices.</li> </ul> | <a href="#">ISO 28001:2007</a> [70]                                                                                                |
| <b>OWL (Web Ontology Language)</b>      | An ontology language, initiated by W3C, for the Semantic Web with formally defined meaning. OWL ontologies series (latest is OWL 2.0) provide classes, properties, individuals, and data values and are stored as Semantic Web documents. OWL 2 ontologies can be used along with information written in RDF. OWL 2 ontologies themselves are primarily exchanged as RDF documents.                                                                                                                                                                                                                      | <a href="#">OWL 2, W3C</a> [130]                                                                                                   |
| <b>Package URL (PURL)</b>               | An attempt to standardise existing approaches to reliably identify and locate software packages. A PURL is a URL string used to identify and locate a software package in a mostly                                                                                                                                                                                                                                                                                                                                                                                                                       | <a href="#">Github Advisory</a> [271]                                                                                              |

|                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                             |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                   | universal and uniform way across programming languages, package managers, packaging conventions, tools, APIs and databases.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                             |
| <b>Performance</b>                | <p>Measurable result.</p> <p>Performance can relate either to:</p> <ul style="list-style-type: none"> <li>quantitative or qualitative findings</li> <li>the management of activities, processes, products (including services), systems or organization.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                | <a href="#">ISO/IEC 27000: 2018</a> [53],<br><a href="#">ISO 9000:2015</a>                                                                                                  |
| <b>Points of Compromise (PoC)</b> | They refer to the specific entry points, vulnerable ICT assets, or pathways an attacker uses to infiltrate a network.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Current dissertation                                                                                                                                                        |
| <b>Policy</b>                     | Intentions and direction of an organization, as formally expressed by its top management,                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | <a href="#">ISO/IEC 27000: 2018</a> [53],<br><a href="#">ISO/IEC 28000:2022</a> [138],<br><a href="#">ISO 9000:2015</a>                                                     |
| <b>Process</b>                    | A group of interrelated or interconnected or interacting activities capable of turning inputs into outputs to deliver a result. <i>(General definition)</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | <a href="#">ISO/IEC 27000: 2018</a> [53],<br><a href="#">ISO/IEC 27002: 2022</a> [66],<br><a href="#">ISO 28000:2022</a> [138],<br><a href="#">ISO/IEC 17065:2012</a> [204] |
|                                   | ICT process      A set of activities performed to design, develop, deliver or maintain an ICT product or ICT service.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | <a href="#">Cybersecurity Act: Regulation (EU) 2019/881</a> [13]                                                                                                            |
|                                   | Business process      A structured set of activities designed for achieving specified business outcomes. <i>(Business definition)</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Davenport [68]                                                                                                                                                              |
| <b>Product</b>                    | Output or outcome provided by an organisation to interested parties.<br><i>(General definition)</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | <a href="#">ISO 22301:2019</a>                                                                                                                                              |
|                                   | <p>Result of a process</p> <p>Four generic product categories are noted:</p> <ul style="list-style-type: none"> <li>services (e.g. transport)</li> <li>software (e.g. computer program, dictionary);</li> <li>hardware (e.g. engine, mechanical part);</li> <li>processed materials (e.g. lubricant).</li> </ul> <p>Many products comprise elements belonging to different generic product categories. Whether the product is then called service, software, hardware or processed material depends on the dominant element. Products include results of natural processes, such as growth of plants and formation of other natural resources.</p> | <a href="#">ISO/IEC 17065:2012</a> [204],<br><a href="#">ISO 9000:2015</a>                                                                                                  |



|                                |                                                                                                                                                                                                                                                                                                                                                           |                                                                                                               |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|
|                                | Anything that can be offered to a market for attention, acquisition, use, or consumption that might satisfy a want or need.<br><i>(Business definition)</i>                                                                                                                                                                                               | P. Kotler [25]                                                                                                |
|                                | ICT product      An element or a group of elements of a network or information system;                                                                                                                                                                                                                                                                    | <a href="#">Cybersecurity Act; Regulation (EU) 2019/881</a> [13]                                              |
|                                | Product with digital elements      A software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately.                                                                                                                                                              | <a href="#">Cyber Resilience Act</a> [11]                                                                     |
| <b>Protection Profile (PP)</b> | Implementation-independent statement of security needs for a Target of Evaluation type.                                                                                                                                                                                                                                                                   | <a href="#">CC:2022 Part 1 R1</a> [58] or <a href="#">ISO/IEC 15408-1:2026</a> [44]                           |
|                                | An ICT process that lays down the security requirements for a specific category of ICT products, addressing implementation-independent security needs, and that may be used to assess ICT products falling into that specific category for the purpose of their certification.                                                                            | <a href="#">EUCC implementing Regulation (EU) 2024/482</a>                                                    |
| <b>Provider/ Supplier</b>      | <i>Organisation</i> hat provides a product or a service, e.g., producer, distributor, retailer or vendor of a product or a service.<br><br>In a contractual situation, a provider is sometimes called “contractor”.                                                                                                                                       | <a href="#">ISO 9000:2015</a>                                                                                 |
| <b>Quality</b>                 | Degree to which a set of inherent characteristics of an object fulfils.                                                                                                                                                                                                                                                                                   | <a href="#">ISO 9000:2015</a>                                                                                 |
| <b>Reliability</b>             | Property of consistent intended behaviour and results.                                                                                                                                                                                                                                                                                                    | <a href="#">ISO/IEC 27000: 2018</a> [53],                                                                     |
| <b>Requirement</b>             | Need or expectation that is stated, generally implied or obligatory. A <i>specified requirement</i> is one that is stated, for example in documented information.<br><br>“ <i>Generally implied</i> ” means that it is custom or common practice for the organization and interested parties that the need or expectation under consideration is implied. | <a href="#">ISO/IEC 27000: 2018</a> [53], <a href="#">ISO 28000:2022</a> [138], <a href="#">ISO 9000:2015</a> |
|                                | Security Requirement      Requirement, which is part of a ToE security specification as defined in a specific Security Target, Protection profile, PP-Module, functional package, or assurance package.                                                                                                                                                   | <a href="#">CC:2022 Part 1 R1</a> [58] or <a href="#">ISO/IEC 15408-1:2026</a> [44]                           |
|                                | Security Functional Requirement      Security requirement, which contributes to fulfil the target of evaluation (TOE) security problem definition (SPD), as defined in a specific Security Target (ST), Protection                                                                                                                                        | <a href="#">CC:2022 Part 1 R1</a> [58] or <a href="#">ISO/IEC 15408-1:2026</a> [44]                           |

|                                             |                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                             | Profile (PP), PP-Module or functional package.                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|                                             | Extended Security Functional Requirement                                                                                                                                                                                                                                                                                                                                                    | A Security Functional Requirement (SFR) developed by authors of a Protection Profile (PP) or PP-module or Security Target according to the rules and preserving the form and syntax identified in Common Criteria (CC) Part 2 or ISO/IEC 15408-2 which is not enlisted in any part of these publications.<br><br><a href="#">CC:2022 Part 1 R1</a> [58] or <a href="#">ISO/IEC 15408-1:2026</a> [44]                                                                                                                                                                                            |
| <b>Remote data processing</b>               | Data processing at a distance for which the software is designed and developed by the manufacturer, or under the responsibility of the manufacturer, and the absence of which would prevent the product with digital elements from performing one of its functions;                                                                                                                         | <a href="#">Cyber Resilience Act</a> [11]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Resilience</b>                           | Adaptive capacity of an organization in a complex and changing environment.                                                                                                                                                                                                                                                                                                                 | <a href="#">ISO 31073: 2022</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Resource Description Framework (RDF)</b> | A standard model for data interchange on the Web. RDF has features that facilitate data merging even if the underlying schemas differ, and it specifically supports the evolution of schemas over time without requiring all the data consumers to be changed.                                                                                                                              | <a href="#">W3C RDF, 2026</a> [129]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Risk</b>                                 | Effect ( <i>deviation from the expected — positive or negative</i> ) of uncertainty ( <i>the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood</i> ) on objectives. Risk is usually expressed in terms of risk sources, potential events, their consequences and likelihood<br><br>(general definition) | <a href="#">ISO 31073: 2022</a> , <a href="#">ISO 31000: 2018</a> [188]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|                                             | Cybersecurity Risk                                                                                                                                                                                                                                                                                                                                                                          | The potential for loss or disruption caused by an incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of the incident.<br><br><a href="#">NIS 2 Directive; Regulation (EU) 2022/2555</a> [12], <a href="#">Cyber Resilience Act</a> [11]                                                                                                                                                                                                                                                                              |
|                                             | Information Security Risk                                                                                                                                                                                                                                                                                                                                                                   | Effect ( <i>deviation from the expected — positive or negative</i> ) of uncertainty ( <i>the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood</i> ) on information security objectives. The potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organization. Risk is usually expressed in<br><br><a href="#">ISO/IEC 27000: 2018</a> [53], <a href="#">ISO/IEC 27005: 2022</a> , <a href="#">ISO 28000:2022</a> [138] |

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                      |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
|                            | <p>terms of risk sources, potential events, their consequences and likelihood.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                      |
|                            | <p>Information system-related security risks arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals and other organizations or entities. (<i>cybersecurity definition</i>)</p>                                                                                                                                 | <p><a href="#">NIST SP 800-137 (2011)</a></p>                                                                                        |
|                            | <p>Overall process of risk identification, risk analysis, and risk evaluation (<i>General definition</i>)</p>                                                                                                                                                                                                                                                                                                                                                                                                                    | <p><a href="#">ISO 31073: 2022</a>, <a href="#">ISO/IEC 27000: 2018</a> [53]</p>                                                     |
| <b>Risk assessment</b>     | <p>The process of identifying risks to organisational operations (including mission, functions, image, reputation), organizational assets, individuals, and other organizations or entities, resulting from an information system operation. It aims to comprehend the nature and determine the level of the identified risks. It is part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. (<i>Cybersecurity definition</i>)</p> | <p><a href="#">NIST SP 1800-21B</a>, <a href="#">NIST SP 800-137</a> (CNSSI 4009), <a href="#">NIST SP 800-160 Vol. 2 Rev. 1</a></p> |
| <b>Risk identification</b> | <p>Process of finding, recognising and describing risks. It identifies risk sources, events, their causes and their potential consequences. It can involve historical data, theoretical analysis, informed and expert opinions, and stakeholders' needs.</p>                                                                                                                                                                                                                                                                     | <p><a href="#">ISO 31073: 2022</a>, <a href="#">ISO/IEC 27000: 2018</a> [53]</p>                                                     |
| <b>Risk analysis</b>       | <p>The process to comprehend the nature of risk and determine the level of risk. It provides the basis for risk evaluation and decisions about risk treatment. Risk analysis includes risk estimation.</p>                                                                                                                                                                                                                                                                                                                       | <p><a href="#">ISO/IEC 27000: 2018</a> [53], <a href="#">ISO 31073: 2022</a></p>                                                     |
| <b>Risk control</b>        | <p>Measure that maintains and/or modifies risk.</p> <p>Risk controls include, but are not limited to, any process, policy, device, practice, or other conditions and/or actions which maintain and/or modify risk. Risk controls do not always exert the intended or assumed modifying effect.</p>                                                                                                                                                                                                                               | <p><a href="#">ISO 31073: 2022</a></p>                                                                                               |
| <b>Risk evaluation</b>     | <p>The process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable. Risk evaluation assists in the decision about risk treatment.</p>                                                                                                                                                                                                                                                                                                     | <p><a href="#">ISO/IEC 27000: 2018</a> [53], <a href="#">ISO 31073: 2022</a></p>                                                     |

|                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                       |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| <b>Risk level</b>              | magnitude of a risk or combination of risks, expressed in terms of the combination of consequences and their likelihood                                                                                                                                                                                                                                                                                                                                                                                                                    | <a href="#">ISO 31073: 2022</a> , <a href="#">ISO/IEC 27000: 2018</a> [53]            |
| <b>Risk management</b>         | Coordinated activities to direct and control an organisation or other entity with regard to risk. ( <i>General definition</i> )                                                                                                                                                                                                                                                                                                                                                                                                            | <a href="#">ISO/IEC 27000: 2018</a> [53],<br><a href="#">ISO 31000: 2018</a> [188]    |
|                                | Process of making management decisions based on an analysis of possible threats, their consequences, and their probability or likelihood of success. ( <i>Supply chain definition</i> )                                                                                                                                                                                                                                                                                                                                                    | <a href="#">ISO28001: 2007</a> [70]                                                   |
| <b>Risk management process</b> | Systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk. ( <i>Cybersecurity definition</i> )                                                                                                                                                                                                                                                                     | <a href="#">ISO/IEC 27000: 2018</a> [53],<br><a href="#">ISO/IEC 27005: 2022</a> [56] |
|                                | A process which is normally initiated for the purposes of optimising the organisation's resource allocation necessary to operate in a particular environment.                                                                                                                                                                                                                                                                                                                                                                              | <a href="#">ISO28001: 2007</a> [70]                                                   |
| <b>Risk treatment</b>          | <p>A set of processes to modify risk:</p> <ul style="list-style-type: none"> <li>• avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk</li> <li>• taking or increasing risk in order to pursue an opportunity</li> <li>• removing the risk source</li> <li>• changing the likelihood</li> <li>• changing the consequences</li> <li>• sharing the risk with another party or parties (including contracts and risk financing)</li> <li>• retaining the risk by informed choice.</li> </ul> | <a href="#">ISO/IEC 27000: 2018</a> [53],<br><a href="#">ISO 31073: 2022</a>          |
| <b>SCADA system</b>            | Generic name for a computerized system that is capable of gathering and processing data and applying operational controls over long distances. Typical uses include power transmission and distribution and pipeline systems. SCADA was designed for the unique communication challenges (e.g., delays, data integrity) posed by the various media that must be used, such as phone lines, microwave, and satellite. Usually shared rather than dedicated                                                                                  | <a href="#">NIST SP 800-82r3</a> [228]                                                |
| <b>Scenario</b>                | A sequential, narrative account of a hypothetical incident that provides the catalyst for the exercise and is intended to introduce situations that will inspire responses and thus allow demonstration of the exercise objectives.                                                                                                                                                                                                                                                                                                        | <a href="#">NIST SP 800-84</a>                                                        |
|                                | <p>Security threat scenario</p> <p>Means by which a potential security incident might occur.</p> <p>Moreover, a cyber threat scenario is assumed to be a use case in which a cyber threat can</p>                                                                                                                                                                                                                                                                                                                                          | <a href="#">ISO 28001:2007</a> [70]                                                   |

|                                   |                                                                                                                                                                                                                                                                                                                         |                                                                                                                                           |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
|                                   | compromise an ICT asset by exploiting vulnerabilities and weaknesses.                                                                                                                                                                                                                                                   |                                                                                                                                           |
| <b>Security</b>                   | Resistance to intentional acts designed to cause harm or damage to or by the supply chain.                                                                                                                                                                                                                              | <a href="#">ISO28001: 2007</a> [70]                                                                                                       |
| <b>Security control</b>           | The safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information.                                                                                                                                | <a href="#">NIST SP 800-53 Rev. 5</a> [368]                                                                                               |
|                                   | A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.                                                                                       | <a href="#">NIST SP 1800-15B</a> , <a href="#">NIST SP 1800-21B</a> , <a href="#">NIST SP 1800-27B</a> , <a href="#">NIST SP 1800-27C</a> |
| <b>Security declaration</b>       | Documented commitment by a business partner, which specifies security measures implemented by that business partner, including, at a minimum, how goods and physical instruments of international trade are safeguarded, associated information is protected and security measures are demonstrated and verified.       | <a href="#">ISO28001: 2007</a> [70]                                                                                                       |
| <b>Security management</b>        | A system of coordinated policies, processes and practices through which an organisation manages its security objectives.                                                                                                                                                                                                | <a href="#">ISO 28000:2022</a> [138]                                                                                                      |
| <b>Security management policy</b> | Overall intentions and direction of an organization, related to the security and the framework for the control of security-related processes and activities that are derived from and consistent with the organization's policy and regulatory requirements.                                                            | <a href="#">ISO 28000:2022</a> [138]                                                                                                      |
| <b>Security policy</b>            | Rules, directives and practices that govern how assets, are managed, protected and distributed within an organization and its ICT systems.                                                                                                                                                                              | <a href="#">ISO/IEC 27000: 2018</a> [53]                                                                                                  |
| <b>Security requirement</b>       | A requirement levied on a system or an organisation which is derived from applicable laws, Executive Orders, directives, regulations, policies, standards, procedures, or mission/business needs to ensure that confidentiality, integrity, and availability of information is being processed, stored, or transmitted. | <a href="#">NIST Glossary</a> [34]<br>(NIST 800-171, NIST 800-53, CNSSI 4009-2015, FIPS 200)                                              |
|                                   | Requirement which is part of a Target of Evaluation security specification, as defined in a Protection Profile.                                                                                                                                                                                                         | <a href="#">CC:2022 Part 1 R1</a> [58] or <a href="#">ISO/IEC 15408-1:2026</a> [44]                                                       |
| <b>Security threat scenario</b>   | Means by which a potential security incident might occur.                                                                                                                                                                                                                                                               | <a href="#">ISO 28001:2007</a> [70]                                                                                                       |

|                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                  |
|----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------|
| <b>Service</b>                               | <p>Output of an organisation with at least one activity necessarily performed between the organisation and the customer.</p> <p>The dominant elements of a service are generally intangible. Service often involves activities at the interface with the customer to establish customer requirements as well as upon delivery of the service and can involve a continuing relationship such as banks, accountancies or public organizations, e.g. schools or hospitals.</p> | <a href="#">ISO 9000:2015</a>                                    |
|                                              | <p>Critical service</p> <p>A critical service is a service that is essential for the maintenance of critical societal or economic activities.</p>                                                                                                                                                                                                                                                                                                                           | <a href="#">NIS 2 Directive; Regulation (EU) 2022/2555</a> [12]  |
|                                              | <p>ICT service</p> <p>A service consisting fully or mainly in the transmission, storing, retrieving or processing of information by means of network and information systems.</p>                                                                                                                                                                                                                                                                                           | <a href="#">Cybersecurity Act; Regulation (EU) 2019/881</a> [13] |
|                                              | <p>Supply chain service (SCS)</p> <p>A network of the supply chain operators and their supporting units that function for the transaction of resources, to develop services, transfer the underlying resources into supporting and core services and deliver the services to the end-customer/user.</p>                                                                                                                                                                     | Baltacioglu et al., 2007 [91]                                    |
| <b>Service Level Agreement (SLA)</b>         | <p>Documented agreement between the organisation and the customer that identifies services and their agreed performance. In addition, a Service Level Agreement (SLA) can also be established between the organisation and an external/internal supplier, or a customer acting as a supplier.</p> <p>An SLA can be included in a contract or another type of documented agreement.</p>                                                                                      | <a href="#">ISO 20000-1:2018</a> [375]                           |
| <b>Software Package Data Exchange (SPDX)</b> | <p>An open, international standard (ISO/IEC 5962) created by the Linux Foundation. It provides a standardised format to communicate a Software Bill of Materials (SBOM), including component details, licenses, copyrights, and security references across the software supply chain.</p>                                                                                                                                                                                   | <a href="#">FOSS</a> ,<br><a href="#">ISO/IEC 5962</a>           |
| <b>Stakeholder</b>                           | <p>Person or organisation that can affect, be affected by, or perceive itself to be affected by a decision or activity</p> <p>Customers, owners, people in an organization providers, bankers, regulators, unions, partners or society that can include competitors or opposing pressure groups.</p>                                                                                                                                                                        | <a href="#">ISO9000:2015</a>                                     |
| <b>Standard</b>                              | <p>A standard as defined in point (1) of Article 2 of Regulation (EU) No 1025/2012</p>                                                                                                                                                                                                                                                                                                                                                                                      | <a href="#">Regulation (EU) No 1025/2012</a> [182]               |

|                                   |                                                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                            |                                                                                                        |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|
|                                   | Security implementation standard                                                                                                                                                                                                                                                                           | Document specifying authorized ways for realizing security                                                                                                                                                 | <a href="#">ISO/IEC 27000: 2018</a> [53]                                                               |
| <b>Strategy</b>                   | Plan to achieve a long-term or overall                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                            | <a href="#">ISO 9000:2015</a>                                                                          |
| <b>Supply Chain</b>               | Linked set of resources and processes that upon placement of a purchase order begins with the sourcing of raw material and extends through the manufacturing, processing, handling and delivery of goods and related services to the purchaser. <i>(Supply chain security definition)</i>                  |                                                                                                                                                                                                            | <a href="#">ISO 28001:2007</a> [70]                                                                    |
|                                   | System of interconnected networks that facilitate the sourcing, transformation and delivery of goods and services between producers, manufacturers, distributors and end user. <i>(Business definition related to security and resilience)</i>                                                             |                                                                                                                                                                                                            | <a href="#">ISO 22300:2025</a>                                                                         |
|                                   | ICT supply chain                                                                                                                                                                                                                                                                                           | A group of ICT services, ICT products and ICT processes that encompass activities and actors involved at all stages upstream of a product being made available or a service being delivered on the market. | <a href="#">Proposal of Cyber Resilience Act 2</a> [49]                                                |
|                                   | International supply chain                                                                                                                                                                                                                                                                                 | Supply chain that at some point crosses an international or economic border.                                                                                                                               | <a href="#">ISO28001: 2007</a> [70]                                                                    |
|                                   | Global supply chain                                                                                                                                                                                                                                                                                        | A complex network of various organizations diffused across multiple tiers and distant locations.                                                                                                           | Choi and Hong (2002) [73]                                                                              |
| <b>Supply Chain Continuity</b>    | The expected outcome of proper performance, which can be achieved by taking measures to ensure the supply chain resilience and vigilance.                                                                                                                                                                  |                                                                                                                                                                                                            | Blos et al., 2015 [83]                                                                                 |
| <b>Supply chain integrity</b>     | Indication of the conformance of the supply chain to good practices and specifications associated with its operations.                                                                                                                                                                                     |                                                                                                                                                                                                            | ENISA (2015) [77]                                                                                      |
| <b>Supply Chain Management</b>    | The systemic, strategic coordination of the traditional business functions and their tactics across these functions within a particular organisation and across processes within the supply chain, aiming to improve the long-term performance of the individual entities and the supply chain as a whole. |                                                                                                                                                                                                            | (Mentzer et al. 2001; Power, 2005; Burgess et al., 2006; Papastergiou Papastergiou et al., 2020) [378] |
| <b>Supply Chain Service (SCS)</b> | A network of the supply chain operators and their supporting units that function for the transaction of resources, to develop services, transfer the underlying resources into supporting and core services and deliver the services to the end-customer/user.                                             |                                                                                                                                                                                                            | Baltacioglu et al., 2007 [91]                                                                          |

|                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                              |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>System</b>                     | Set of interrelated or interacting elements                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <a href="#">ISO 9000:2015</a>                                                                                                                                                |
| <b>Target of Evaluation (ToE)</b> | A set of software, firmware and/or hardware, or a combination of these, possibly accompanied by guidance, which is the subject of an evaluation.                                                                                                                                                                                                                                                                                                                                              | <a href="#">CC:2022 Part 1 R1</a> [58] or <a href="#">ISO/IEC 15408-1:2026</a> [44]                                                                                          |
|                                   | An ICT product or part thereof, or a protection profile as part of an ICT process, which is subjected to cybersecurity evaluation to receive EUCC certification.                                                                                                                                                                                                                                                                                                                              | <a href="#">EUCC implementing Regulation (EU) 2024/482</a>                                                                                                                   |
| <b>Testing</b>                    | Determination of one or more characteristics of an object of conformity assessment according to a procedure.                                                                                                                                                                                                                                                                                                                                                                                  | <a href="#">ISO/IEC 17000:2020</a> [57]                                                                                                                                      |
| <b>Threat (Cyber)</b>             | Any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons.                                                                                                                                                                                                                                                                                                            | <a href="#">Cybersecurity Act: Regulation (EU) 2019/881</a> [13], <a href="#">NIS 2 Directive: Regulation (EU) 2022/2555</a> [12], <a href="#">Cyber Resilience Act</a> [11] |
|                                   | Potential cause of an unwanted incident, which can result in harm to a system or organisation.                                                                                                                                                                                                                                                                                                                                                                                                | <a href="#">ISO/IEC 27000: 2018</a> [53], <a href="#">ISO/IEC 27032:2023</a> [137]                                                                                           |
|                                   | Any circumstance or event with the potential to adversely impact organisational operations (including mission, functions, image, or reputation), organisational assets, or individuals through an information system via unauthorised access, destruction, disclosure, modification of information, and/or denial of service. In addition, it is the potential for a threat-source to successfully exploit a particular information system vulnerability. ( <i>Cybersecurity definition</i> ) | <a href="#">FIPS 200</a>                                                                                                                                                     |
| <b>Threat Assessment</b>          | Process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat.                                                                                                                                                                                                                                                                                                                                                           | <a href="#">NIST SP 800-30 Rev. 1</a> [125]                                                                                                                                  |
| <b>Threat Level</b>               | Cyber threat occurrence estimation to an ICT asset.                                                                                                                                                                                                                                                                                                                                                                                                                                           | E.M. Kalogeraki, S. Papastergiou, M. Mouraitidis, and N. Polemi (2018) [1] based on works of [371],[372].                                                                    |
| <b>Traceability</b>               | Ability to trace the history, application or location of an object. When considering a product or a service, traceability can relate to: — the origin of materials and parts; — the processing history; — the distribution and location of the product or service after delivery                                                                                                                                                                                                              | <a href="#">ISO 9000:2015</a>                                                                                                                                                |



|               |                                                                                                                                                                                                                                                                                                     |                                                                                                                   |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| User          | Person or process using the system in order to gain access to some system resident or system accessible service                                                                                                                                                                                     | <a href="#">ETSI TS 102 165-1</a>                                                                                 |
| Validation    | Confirmation, through the provision of objective evidence that the requirements for a specific intended use or application have been fulfilled                                                                                                                                                      | <a href="#">ISO 9000:2015</a> , 17000                                                                             |
|               | Confirmation of plausibility for a specific intended use or application through the provision of objective evidence that specified requirements have been fulfilled<br><br>Validation can be applied to claims to confirm the information declared with the claim regarding an intended future use. | <a href="#">ISO/IEC 17000:2020</a> [57]                                                                           |
| Verification  | Confirmation, through the provision of objective evidence,, that specified requirements have been fulfilled                                                                                                                                                                                         | <a href="#">ISO/IEC 17000:2020</a> [57],<br><a href="#">ISO 9000:2015</a> ,                                       |
| Vulnerability | Weakness of an asset or control that <u>can</u> be exploited by one or more threats. so that an event with a negative consequence occurs.                                                                                                                                                           | <a href="#">ISO/IEC 27000: 2018</a> [53],<br><a href="#">ISO/IEC 27005: 2022</a>                                  |
|               | Weakness, susceptibility or flaw of ICT products or ICT services that can be exploited by a cyber threat.                                                                                                                                                                                           | <a href="#">NIS 2 Directive; Regulation (EU) 2022/2555</a> [12]                                                   |
|               | Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.                                                                                                                                        | <a href="#">NIST SP 800-37 Rev. 2</a> ,<br><a href="#">NIST SP 800-53A Rev.5</a> ,<br><a href="#">NISTIR 7622</a> |
|               | A behaviour or set of conditions present in a system, product, component, or service (functional) that violates an implicit or explicit security policy. A vulnerability can be thought of as a weakness or exposure that allows a security impact or consequence.                                  | <a href="#">ISO/IEC 29147: 2018</a>                                                                               |
|               | Intrinsic properties of something resulting in susceptibility to a risk source that can lead to an event with a consequence.                                                                                                                                                                        | <a href="#">ISO 31073: 2022</a>                                                                                   |
|               | Exploitable vulnerability<br>Weakness in the ToE that can be used to violate the Security Functional Requirements (SFRs) in the operational environment for the ToE.                                                                                                                                | <a href="#">ISO/IEC 15408-1:2026</a> [44]                                                                         |
|               | A vulnerability that has the potential to be effectively used by an adversary under practical operational conditions                                                                                                                                                                                | <a href="#">Cyber Resilience Act</a> [11]                                                                         |
|               | Confirmed vulnerability<br>Detailed reports exist, or functional reproduction is possible (functional exploits may provide this). Source code is available to independently verify the assertions of the research, or the author or vendor of the                                                   | <a href="#">FIRST CVSS 3.1</a> [139]                                                                              |

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                       |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
|                                 | affected code has confirmed the presence of the vulnerability.                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                       |
|                                 | <p>Potential/unknown vulnerability</p> <p>Potential vulnerabilities are suspected, but not confirmed weaknesses. Unknown vulnerabilities are reports of impacts that indicate a vulnerability is present, but that the cause of the vulnerability is unknown or they may differ on the cause or impacts of the vulnerability. Reporters are uncertain of the true nature of the vulnerability, and there is little confidence in the validity of the reports.</p> | <p><a href="#">ISO/IEC 15408-1:2026</a> [44],<br/> <a href="#">FIRST CVSS 3.1</a></p> |
| <b>Vulnerability Assessment</b> | Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.                                                                                                                                                                    | <a href="#">NIST SP 800-30 Rev. 1</a> [125]                                           |
| <b>Vulnerability severity</b>   | The severity of a vulnerability is an assessment of the relative importance of mitigating/remediating the vulnerability. The severity can be determined by the extent of the potential adverse impact if such a vulnerability is exploited by a threat source. Thus, the severity of vulnerabilities, in general, is context-dependent.                                                                                                                           | <a href="#">NIST SP 800-30 Rev. 1</a> [125]                                           |
| <b>Zero-day attack</b>          | An attack that exploits a previously unknown hardware, firmware, or software vulnerability.                                                                                                                                                                                                                                                                                                                                                                       | <p><a href="#">CNSSI 4009-2015</a><br/> <a href="#">NISTIR 8011 Vol. 3</a></p>        |

## Appendix B: Acronyms and Abbreviations

The following table enlists and defines all acronyms and abbreviations appearing in the current dissertation.

Table 86. Acronyms and Abbreviations.

| Acronym/Abbreviation | Description                                            |
|----------------------|--------------------------------------------------------|
| ADF                  | Activity Decision Flow                                 |
| AI                   | Artificial Intelligence                                |
| AI Act               | Artificial Intelligence Act                            |
| AIS                  | Automatic Identification System                        |
| APT                  | Advanced Persistent Threat                             |
| AR                   | Availability Requirement                               |
| ASECG                | Attack Simulation and Evidence Chains Generation       |
| ATT&CK               | Adversarial Tactics, Techniques, and Common Knowledge  |
| APEL                 | Attack Path Exploitability Level                       |
| API                  | Application Programming Interface                      |
| BIMCO                | Baltic and International Maritime Council              |
| BPM                  | Business Process Management                            |
| BPMN                 | Business Process Modelling Language                    |
| CA                   | Conformity Assessment                                  |
| CAB                  | Conformity Assessment Body                             |
| CADA                 | Cloud and AI Development Act                           |
| CAPEC                | Common Attack Pattern Enumerations and Classifications |
| CC                   | Common Criteria                                        |
| CCRA                 | Common Criteria Recognition Agreement                  |

|                     |                                                                   |
|---------------------|-------------------------------------------------------------------|
| <b>CDC</b>          | Corporate Domain Controller                                       |
| <b>CE</b>           | Conformité Européene (European Conformity) marking                |
| <b>CEM (CC/CEM)</b> | Common Methodology for Information Technology Security Evaluation |
| <b>CER</b>          | Critical Entities Resilience (CER Directive (EU) 2022/2557)       |
| <b>CERT</b>         | Computer Emergency Response Team                                  |
| <b>CI</b>           | Critical Infrastructure                                           |
| <b>CIA triad</b>    | Confidentiality, Integrity, and Availability                      |
| <b>CI/CD</b>        | Continuous Integration/Continuous Delivery (or Deployment)        |
| <b>CII</b>          | Critical Information Infrastructure                               |
| <b>CIL</b>          | Cumulative Impact Level                                           |
| <b>CISO</b>         | Chief Information Security Officer                                |
| <b>CLI</b>          | Command Line Interface                                            |
| <b>COOP</b>         | Continuity Of Operations                                          |
| <b>CPE</b>          | Common Platform Enumeration                                       |
| <b>CPS</b>          | Cyber Physical System                                             |
| <b>CR</b>           | Confidentiality Requirement                                       |
| <b>CRA</b>          | Cyber Resilience Act (Regulation (EU) 2024/2847)                  |
| <b>CRL</b>          | Cumulative Risk Level                                             |
| <b>CSA</b>          | Cybersecurity Act (Regulation (EU) 2019/881)                      |
| <b>C-SCRM</b>       | Cyber Supply Chain Risk Management                                |
| <b>CSIRT</b>        | Computer Security Incident Response Team                          |
| <b>CSRS</b>         | Computer Security Resource Center                                 |
| <b>CTL</b>          | Cybersecurity Threat Landscape                                    |

|                   |                                                                         |
|-------------------|-------------------------------------------------------------------------|
| <b>CToE</b>       | Composite Target of Evaluation                                          |
| <b>CVE</b>        | Common Vulnerabilities and Exposures                                    |
| <b>CVL</b>        | Cumulative Vulnerability Level                                          |
| <b>CVSS</b>       | Common Vulnerability Scoring System                                     |
| <b>CWE</b>        | Common Weakness Enumeration                                             |
| <b>CWSS</b>       | Common Weakness Scoring System                                          |
| <b>CWRAF</b>      | Common Weakness Risk Analysis Framework                                 |
| <b>CYSM</b>       | CYber/Physical Security Management system                               |
| <b>DCS</b>        | Distributed Control Systems                                             |
| <b>DG CONNECT</b> | Directorate-General for Communications Networks, Content and Technology |
| <b>DevOps</b>     | Development and Operations                                              |
| <b>DevSecOps</b>  | Development, Security, Operations                                       |
| <b>DHS</b>        | Department of Homeland Security                                         |
| <b>DIG</b>        | Description Logic Implementation Group                                  |
| <b>DL</b>         | Description Logic                                                       |
| <b>DRL</b>        | Deep Reinforcement learning                                             |
| <b>DNS</b>        | Domain Name System                                                      |
| <b>DNV</b>        | Det Norske Veritas                                                      |
| <b>DORA</b>       | Digital Operational Resilience Act (Regulation (EU) 2022/2554)          |
| <b>DDoS</b>       | Distributed Denial-of-Service attack                                    |
| <b>DoS</b>        | Denial-of-service attack                                                |
| <b>DSM</b>        | Digital Single Market                                                   |
| <b>DSR</b>        | Design Science Research                                                 |

|              |                                                                      |
|--------------|----------------------------------------------------------------------|
| <b>DSRM</b>  | Design Science Research Management                                   |
| <b>ECDIS</b> | Electronic Chart Display and Information System                      |
| <b>ECRL</b>  | Entry's Chain Risk Level                                             |
| <b>ECSF</b>  | European Cybersecurity Skills Framework                              |
| <b>ECIL</b>  | Entry's Chain Impact Level                                           |
| <b>ECVL</b>  | Entry's Chain Vulnerability Level                                    |
| <b>EDI</b>   | Electronic Data Interchange                                          |
| <b>EL</b>    | Exploitability Level                                                 |
| <b>ELC</b>   | Exploitation Level Chain                                             |
| <b>EMSA</b>  | European Maritime Safety Agency                                      |
| <b>EMS</b>   | Energy Management System                                             |
| <b>ENISA</b> | European Network and Information Security Agency                     |
| <b>EPC</b>   | Event-driven Process Chains                                          |
| <b>EPSS</b>  | Exploitability Prediction Scoring System                             |
| <b>ERP</b>   | Enterprise Resource Planning                                         |
| <b>ETA</b>   | Event Tree Analysis                                                  |
| <b>ETSI</b>  | European Telecommunications Standards Institute                      |
| <b>EU</b>    | European                                                             |
| <b>EUCC</b>  | European Common Criteria-based cybersecurity certification scheme    |
| <b>EUCS</b>  | European Union Cybersecurity Certification Scheme for Cloud Services |
| <b>eUICC</b> | Embedded Universal Integrated Circuit Card                           |
| <b>EUVD</b>  | European Union Vulnerability Database                                |
| <b>eIDAS</b> | European Digital Identity                                            |

|                     |                                                                    |
|---------------------|--------------------------------------------------------------------|
| <b>EUMSS</b>        | European Cybersecurity certification for Managed Security Services |
| <b>XaaS</b>         | Everything-as-a-Service                                            |
| <b>Extended SFR</b> | Extended Security Functional Requirement                           |
| <b>FDI</b>          | Foreign Direct Investment                                          |
| <b>FIRST</b>        | Forum of Incident Response and Security Teams                      |
| <b>FTA</b>          | Fault Tree Analysis                                                |
| <b>GDPR</b>         | General Data Protection Regulation                                 |
| <b>GNN</b>          | Graph Neural Network                                               |
| <b>GNSS</b>         | Global Navigation Satellite System                                 |
| <b>HCI</b>          | Human-Computer Interaction                                         |
| <b>HIDS</b>         | Host-based Intrusion Detection System                              |
| <b>HMI</b>          | Human Machine Interface                                            |
| <b>HMM</b>          | Hidden Markov Model                                                |
| <b>I4</b>           | Industrie 4.0                                                      |
| <b>IACS</b>         | International Association of Classification Societies              |
| <b>IAPH</b>         | International Association of Ports and Harbors                     |
| <b>ICIL</b>         | Individual Chain Impact Level                                      |
| <b>ICS</b>          | Industrial Control System                                          |
| <b>ICT</b>          | Information and Communications Technology                          |
| <b>ICVL</b>         | Individual Chain Vulnerability Level                               |
| <b>IDS</b>          | Intrusion Detection Systems                                        |
| <b>IEC</b>          | International Electrotechnical Commission                          |
| <b>IEEE</b>         | Institute of Electrical and Electronics Engineers                  |

|                   |                                                     |
|-------------------|-----------------------------------------------------|
| <b>IIoT</b>       | Industrial Internet of things                       |
| <b>IL</b>         | Impact Level                                        |
| <b>IoC</b>        | Indicators of Compromise                            |
| <b>IoE</b>        | Internet of Everything                              |
| <b>IoT</b>        | Internet of things                                  |
| <b>IM</b>         | Incident Manager                                    |
| <b>IMO</b>        | International Maritime Organisation                 |
| <b>I3P</b>        | Institute for Information Infrastructure Protection |
| <b>IP address</b> | Internal Protocol address                           |
| <b>IPRL</b>       | Individual Propagated Risk Level                    |
| <b>IR</b>         | Integrity Requirement                               |
| <b>ISM</b>        | International Safety Management                     |
| <b>ISMS</b>       | Information Security Management System              |
| <b>ISO</b>        | International Organization for Standardization      |
| <b>ISPS</b>       | International Ship and Port Facility Security Code  |
| <b>IT</b>         | Information Technology                              |
| <b>iTC</b>        | International Technical Community (iTC)             |
| <b>IVL</b>        | Individual Vulnerability Level                      |
| <b>JRC</b>        | Joint Research Centre                               |
| <b>KM</b>         | Knowledge Management                                |
| <b>KPI</b>        | Key Performance Indicator                           |
| <b>KRM</b>        | Knowledge Risk Management                           |
| <b>LEA</b>        | Law Enforcement Agency                              |



|               |                                               |
|---------------|-----------------------------------------------|
| <b>LNG</b>    | Liquefied Natural Gas                         |
| <b>LOTS</b>   | Living Off Trusted Sites                      |
| <b>M2M</b>    | Machine-to-Machine                            |
| <b>MISP</b>   | Malware Information Sharing Platform          |
| <b>ML</b>     | Machine Learning                              |
| <b>MLoSC</b>  | Maritime and Logistics Supply Chain           |
| <b>MTU</b>    | Master Terminal Unit                          |
| <b>MoD</b>    | Ministry of Defence (UK)                      |
| <b>MAC</b>    | Modified Attack Complexity                    |
| <b>MA</b>     | Modified Availability                         |
| <b>MAV</b>    | Modified Attack Vector                        |
| <b>MC</b>     | Modified Confidentiality                      |
| <b>MESS</b>   | Modified Exploitability Sub Score             |
| <b>ME</b>     | Microenterprise                               |
| <b>MI</b>     | Modified Integrity                            |
| <b>MISS</b>   | Modified Impact Sub-Score                     |
| <b>MPR</b>    | Modified Privileges Required                  |
| <b>MRN</b>    | Master Reference Number                       |
| <b>MSA</b>    | Multi-Stage Network Attacks                   |
| <b>MUI</b>    | Modified User Interaction                     |
| <b>MulVAL</b> | Multihost, multistage, Vulnerability Analysis |
| <b>NetSPA</b> | Network Security Planning Architecture        |
| <b>NIDS</b>   | Network-based Intrusion Detection System      |

|                      |                                                                    |
|----------------------|--------------------------------------------------------------------|
| <b>NIS Directive</b> | Network and Information System Directive                           |
| <b>NIST</b>          | National Institute of Standards and Technology                     |
| <b>NVD</b>           | National Vulnerability Database (NIST)                             |
| <b>OCTAVE</b>        | Operationally Critical Threat, Asset, and Vulnerability Evaluation |
| <b>OES</b>           | Operator of Essential Service                                      |
| <b>OIS</b>           | Operator of Important Service                                      |
| <b>ORT</b>           | Open Risk Taxonomy                                                 |
| <b>OSP</b>           | Organisational Security Policy                                     |
| <b>OT</b>            | Operation Technology                                               |
| <b>OSINT</b>         | Open-Source Intelligence                                           |
| <b>OSV</b>           | Open Source Vulnerabilities                                        |
| <b>OTT</b>           | Open Threat Taxonomy                                               |
| <b>OWASP</b>         | Open Web Application Security Project                              |
| <b>OWL</b>           | Web Ontology Language                                              |
| <b>PAS</b>           | Publicly Available Specification                                   |
| <b>PASTA</b>         | Process for Attack Simulation and Threat Analysis                  |
| <b>PCS</b>           | Port Community System                                              |
| <b>PDE</b>           | Product with Digital Elements                                      |
| <b>PSS</b>           | Product-Service System                                             |
| <b>PFSO</b>          | Port Facility Security Officer                                     |
| <b>PLD</b>           | Product Liability Directive                                        |
| <b>PMIS</b>          | Port Management Information System                                 |
| <b>PoC</b>           | Points of Compromise                                               |

|              |                                                  |
|--------------|--------------------------------------------------|
| <b>PP</b>    | Protection Profile                               |
| <b>PKI</b>   | Public Key Infrastructure                        |
| <b>PRL</b>   | Propagated Risk Level                            |
| <b>PURL</b>  | Package URL                                      |
| <b>PVL</b>   | Propagated Vulnerability Level                   |
| <b>QCI</b>   | Quantum Communication Infrastructure             |
| <b>RA</b>    | Risk Assessment                                  |
| <b>RED</b>   | Radio Equipment Directive (Directive 2014/53/EU) |
| <b>RDF</b>   | Resource Description Framework                   |
| <b>RFID</b>  | Radio Frequency Identification                   |
| <b>RL</b>    | Reinforcement learning                           |
| <b>ROSE</b>  | Reference Ontology for Security Engineering      |
| <b>SAE</b>   | Society of Automotive Engineers                  |
| <b>SAT</b>   | Satellite                                        |
| <b>SBOM</b>  | Software Bill of Material                        |
| <b>SBPM</b>  | Semantic Business Process Management             |
| <b>SCADA</b> | Supervisory Control and Data Acquisition         |
| <b>SCS</b>   | Supply Chain Service                             |
| <b>SCM</b>   | Supply Chain Management                          |
| <b>SCRM</b>  | Supply Chain Risk Management                     |
| <b>SD</b>    | Security Declaration                             |
| <b>SDLC</b>  | Software Development Life Cycle                  |
| <b>SDO</b>   | Standards Development Organisation               |

|               |                                                        |
|---------------|--------------------------------------------------------|
| <b>SFR</b>    | Security Functional Requirement                        |
| <b>SIS</b>    | Ship Information System                                |
| <b>SLA</b>    | Service Level Agreement                                |
| <b>SME</b>    | Small and Medium Sized Enterprise                      |
| <b>SOC</b>    | Security Operations Centre                             |
| <b>SOG-IS</b> | Senior Officials Group – Information Systems Security  |
| <b>SOLAS</b>  | Safety of Life At Sea Convention                       |
| <b>SSM-CR</b> | Situated Scoring Methodology for Cyber Resiliency      |
| <b>SP</b>     | Special Publication                                    |
| <b>SPARQL</b> | SPARQL Protocol and RDF Query Language                 |
| <b>SPDX</b>   | Software Package Data Exchange                         |
| <b>STIX</b>   | Structured Threat Information Expression               |
| <b>TAXII</b>  | Trusted Automated Exchange of Intelligence Information |
| <b>TL</b>     | Threat Level                                           |
| <b>TLD</b>    | Top-level Domain                                       |
| <b>ToE</b>    | Target of Evaluation                                   |
| <b>TOS</b>    | Terminal Operating System                              |
| <b>TR</b>     | Technical Report                                       |
| <b>TS</b>     | Technical Specifications                               |
| <b>TTPs</b>   | Tactics, Techniques, and Procedures                    |
| <b>TVA</b>    | Topological Analysis of Network Attack Vulnerability   |
| <b>TVRA</b>   | Threat, Vulnerability, Risk Analysis                   |
| <b>UAV</b>    | Unmanned Aerial Vehicles                               |

|               |                                                     |
|---------------|-----------------------------------------------------|
| <b>UML</b>    | Unified Modelling Language                          |
| <b>UN</b>     | United Nations                                      |
| <b>UNCTAD</b> | United Nations Conference on Trade and Development  |
| <b>URI</b>    | Uniform Resource Identifier                         |
| <b>URL</b>    | Uniform Resource Locator                            |
| <b>UST</b>    | Unified Service Theory                              |
| <b>VERIS</b>  | Vocabulary for Event Recording and Incident Sharing |
| <b>VHF</b>    | Very High Frequency                                 |
| <b>VLMM</b>   | Variable Length Markov Model                        |
| <b>VOMM</b>   | Variable Order Markov Model                         |
| <b>VTMS</b>   | Vessel Traffic Management Service                   |
| <b>VTs</b>    | Vessel Traffic Service                              |
| <b>W3C</b>    | World Wide Web Consortium                           |
| <b>WASC</b>   | Web Application Security Consortium                 |
| <b>XAI</b>    | Explainable Artificial Intelligence                 |

## Appendix C: Documents and Forms

### SECURITY DECLARATION AND STATEMENT OF APPLICATION (SDA)

The current Security Declaration and statement of Application (hereafter referred to as “SDA”) is made effective as of the following date \_\_\_\_\_ by and between the following business partners of the ICT product and/or ICT supply chain service (ICT SCS) considered as the Target of Evaluation (hereafter referred to as “TOE”):

ICT stakeholder (hereafter referred to as “Secured Party” A)

Business Partner A (hereafter referred to as “Secured Party” B)

Business Partner B (hereafter referred to as “Secured Party” C)

.....

#### - PART A -

The Secured Parties of this document **agree/declare/reached consensus upon** the following:

- the selected TOE (providing a short description) .....
- the designated ICT provider (hereafter referred to as “ICT-provider”);
- the purpose of the assessment (Risk Assessment or Conformity Assessment);
- the conditions subject to the recognition of certificate (indicating the certification scheme that will be followed);
- the conditions of the consistent application of the criteria and methods between evaluation and certification scheme;
- the assurance level (hereafter referred to as “AL”) of certificate of the applied security certification scheme that will be adopted including existing limitations (if any);
- the designated assessor (in case of a Conformity Assessment performance);
- the assigned security requirements, security objectives, security target and security problem;
- on the specified risk level(s);
- rest content included in the current document

In addition, all Secured Parties **declare their commitment** upon:

- developing/ assessing the ICT Protection Profile (hereafter referred to as “ICT-PP”) [in case a SCS is included in the evaluation, it shall be referred];
- mapping the TOE assets with vulnerabilities and implemented controls, to identify security gaps;
- undertaking appropriate controls wherever required to reach the previously defined security level;
- they have provided all the appropriate documentation of their organisation that justifies all the above (included hereafter in the “Annex”)

- PART B -

Additional conventions and privacy considerations.

.....  
.....

Herewith, all the Secured Parties confirm that they have read and understood the entire SDA, acknowledge it as fully binding upon them. The undersigned, herewith, take the responsibility of informing the persons concerned accordingly.

IN WITNESS WHEREOF, the parties are bound by the SDA as follows:

\_\_\_\_\_

\_\_\_\_\_ *Secured Party A (Organization name/Name of representative)*

-----  
Date

-----  
Signature

## Appendix D: Assessment scales

### D1. CyberICT Probability Scale

This is the generic probability 5-level scale to calculate values in both quantitative and qualitative formats for the CyberICT approach.

Table 87. CyberICT generic assessment scale.

| Quantitative Value     | Average Numeric Value | Worst Case Numeric Value | Qualitative Value |
|------------------------|-----------------------|--------------------------|-------------------|
| 0.00 – 0.19 (0%-19%)   | 0.10 (10%)            | 0.19 (19%)               | Very Low (VL)     |
| 0.20 – 0.39 (20%-39%)  | 0.30 (30%)            | 0.39 (39%)               | Low (L)           |
| 0.40 – 0.59 (40%-59%)  | 0.50 (50%)            | 0.59 (59%)               | Moderate (M)      |
| 0.60 – 0.79 (60%-79%)  | 0.70 (70%)            | 0.79 (79%)               | High (H)          |
| 0.80 – 1.00 (80%-100%) | 0.90 (90%)            | 0.100 (100%)             | Very High (VH)    |

### D2. NIS 2 Directive Essential and Important services

The table below presents the criticality of services, characterised either as “essential” or “important” by NIS 2 Directive.

Table 88. CyberICT SCS criticality scale.

| ICT stakeholder                             | Industry sectors of essential and important services<br>(NIS 2 Directive [12])                                                                                                                                                                                                                             |
|---------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Operator of Important Services (OIS)</b> | 1. Postal and courier services, 2. Waste Management, 3. Manufacture, production, and distribution of chemicals, 4. Food production, processing, and distribution, 5. Manufacturing, 6. Digital Providers.                                                                                                  |
| <b>Operator of Essential Services (OES)</b> | 1. Energy (electricity, oil, gas), 2. Transport (air, rail, water, road), 3. Banking, 4. Financial market infrastructures, 5. Health (including hospitals and private clinics), 6. Drinking water supply and distribution, 7. Waste Water, 8. Digital infrastructure, 9. Public Administration, 10. Space. |

### D3. Threat scale of ICT assets

The threat scale to estimate the cyber threat occurrence to a given ICT asset is presented in the following, based on the works of [1],[371]–[372].



Table 89. Threat Scale.

| Threat Level<br>(Qualitative value) | Threat level<br>(Quantitative value range)<br>% | Resources                                                                                                                            |                                                                                                                   |                                                                                                                   |
|-------------------------------------|-------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
|                                     |                                                 | Historical data of past incidents                                                                                                    | Human experience, expertise, intuition and knowledge                                                              | Web sources and open repositories                                                                                 |
| Very High (VH)                      | 0.80 – 1.00<br>(80%-100%)                       | This threat was realised <b>more than once (&gt;1) in the last year</b> (12 month period).                                           | Threat expectation of occurrence within the assets of the ICT stakeholder/business partner: <b>VH</b> (80%-100%)  | Threat expectation of occurrence within the assets of the ICT stakeholder/business partner: <b>VH</b> (80%-100%)  |
| High (H)                            | 0.60 – 0.79<br>(60%-79%)                        | This threat was realised <b>once (=1) in the last 1 year</b> (12 month period).                                                      | Threat expectation of occurrence within the assets of the ICT stakeholder/business partner: <b>H</b> (60%-79%)    | Threat expectation of occurrence within the assets of the ICT stakeholder/business partner: <b>H</b> (60%-79%)    |
| Moderate (M)                        | 0.40 – 0.59<br>(40%-59%)                        | <b>More than one (&gt;1)</b> incident of this threat was realised <b>in the last 2 years</b> .                                       | Threat expectation of occurrence within the assets of the ICT stakeholder/business partner: <b>M</b> (40%-59%)    | Threat expectation of occurrence within the assets of the ICT stakeholder/business partner: <b>M</b> (40%-59%)    |
| Low (L)                             | 0.20 – 0.39<br>(20%-39%)                        | <b>At most one (<math>\leq 1</math>)</b> incident of this threat was realised <b>in the last 2 years</b> .                           | Threat expectation of occurrence within the assets of the ICT stakeholder/business partner: <b>L</b> (20%-39%)    | Threat expectation of occurrence within the assets of the ICT stakeholder/business partner: <b>L</b> (20%-39%)    |
| Very Low (VL)                       | 0.01 – 0.19<br>(0%-19%)                         | <b>At most one (<math>\leq 1</math>)</b> incident of this threat was realised in the <b>last 3 years</b> or no incident was realised | Threat expectation of occurrence within the assets of the ICT stakeholder/business partner: <b>VL</b> (up to 20%) | Threat expectation of occurrence within the assets of the ICT stakeholder/business partner: <b>VL</b> (up to 20%) |

#### D4. Exploitability and impact related metrics

The following tables follow the Modified exploitability related metrics of CVSS 3.1 specification [139].

Table 90. CVSS 3.1 Modified Attack Vector (MAV defining how a vulnerability can be technically reached).

| Value        | Description                                                                                                                                                                                                                                                                                                            | Score |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| Physical (P) | The attack requires the attacker to physically touch or manipulate the vulnerable component. The interaction can be brief or persistent and examples include cold boot attacks, tampering with physical ports, or removing hardware components (e.g., firewire attacks).                                               | 0.20  |
| Local (L)    | The vulnerable component is not bound to the network stack, and the attacker requires local access to the system. This access is achieved either via a local shell, terminal sessions, physical console, or by tricking a local, authenticated user into running malicious code (e.g., a privilege escalation attack). | 0.55  |
| Adjacent (A) | The attacker must have logical access to the victim's local network. This includes access via local network protocols (e.g., ARP spoofing, Ethernet, Wi-Fi or Bluetooth attacks) or via logically bound trusted networks (e.g., local VPNs, MPLS, or shared physical broadcast domains).                               | 0.62  |
| Network (N)  | The vulnerable component is bound to the network stack, and the attack can be executed remotely across a network (e.g., over the internet). The attacker does not need local access or logical proximity, and exploits do not require prior access to the vulnerable system.                                           | 0.85  |

Table 91. CVSS 3.1 Modified Attack Complexity (MAC).

| Value    | Description                                                                                                                                                                         | Score |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| High (H) | Specialised conditions exist, such as a race condition with a narrow window, or a requirement for social engineering methods that would be readily noticed by knowledgeable people. | 0.44  |
| Low (L)  | There are no special conditions for exploiting the vulnerability, such as when the system is available to large numbers of users, or the vulnerable configuration is ubiquitous.    | 0.77  |

Table 92. CVSS 3.1 Modified Privileges Required (MPR).

| Value    | Description                                                                                                                                                                  | Score                                                  |
|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------|
| High (H) | The attacker requires privileges that provide significant (e.g., administrative) control over the vulnerable component allowing access to component-wide settings and files. | 0.27<br>(or 0.5 if Scope / Modified Scope is Changed)  |
| Low (L)  | The attacker requires privileges that provide basic user capabilities that could normally affect only settings and files owned by a user.                                    | 0.62<br>(or 0.68 if Scope / Modified Scope is Changed) |
| None (N) | There is no requirement for the attacker to authenticate to launch the attack.                                                                                               | 0.85                                                   |

Table 93. CVSS 3.1 Modified User Interaction (MUI).

| Metric Value | Description                                                                                                                  | Score |
|--------------|------------------------------------------------------------------------------------------------------------------------------|-------|
| None (N)     | There is no requirement for the attacker to authenticate to launch the attack.                                               | 0.85  |
| Required (L) | Successful exploitation of this vulnerability requires a user to take some action before the vulnerability can be exploited. | 0.62  |

Table 94. CVSS 3.1 Environmental group metrics.

| Metric Name                                                                                  | Qualitative value | Score |
|----------------------------------------------------------------------------------------------|-------------------|-------|
| Modified Confidentiality (MC)/<br>Modified Integrity (MI) /<br>Modified Availability (MA)    | None              | 0     |
|                                                                                              | Low               | 0.22  |
|                                                                                              | High              | 0.56  |
| Confidentiality Requirement (CR)/ Integrity Requirement (IR) / Availability Requirement (AR) | Not defined       | 1     |
|                                                                                              | Low               | 0.5   |
|                                                                                              | Medium            | 1     |
|                                                                                              | High              | 1.5   |

Table 95. CVSS 3.1 MISS sub-score and Scope metric.

| Modified Scope | MISS formula                                                                              |
|----------------|-------------------------------------------------------------------------------------------|
| Changed        | $7.52 \times (\text{MISS} - 0.029) - 3.25 \times (\text{MISS} \times 0.9731 - 0.02)^{13}$ |
| Unchanged      | $6.42 \times \text{MISS}$                                                                 |

## D5. Attacker's Profile

The attacker's profile is identified considering the attacker's capability and location, as presented in the following tables. The quantitative values follow normalised ordinal operational scales. The proposed scales represent relative exploitability utilities intended for attack graph propagation analysis (rather than absolute attacker's measurement). The ranking of the attacker's capability in Table 96 is identified considering the attacker's capability and attacker's intention metrics defined in NIST SP 800-30 [125].

Table 96. The ranking of Attacker's capability.

| Assessment Scale of Attacker's Capability |                          |               |                                                                                                                                                                                   |
|-------------------------------------------|--------------------------|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Qualitative Values                        | Semi-Quantitative Values |               | Description                                                                                                                                                                       |
| <b>Very High (VH)</b>                     | 0.85-1<br>(85%–100%)     | 0.93<br>(93%) | The adversary has a very sophisticated level of expertise, is well resourced, and can generate opportunities to support multiple successful, continuous, and coordinated attacks. |
| <b>High (H)</b>                           | 0.65-0.85<br>(65%–84%)   | 0.75<br>(75%) | The adversary has a sophisticated level of expertise, with significant resources and opportunities to support multiple successful coordinated attacks.                            |
| <b>Moderate (M)</b>                       | 0.35-0.64<br>(35%–64%)   | 0.50<br>(50%) | The adversary has moderate resources, expertise, and opportunities to support multiple successful attacks.                                                                        |
| <b>Low (L)</b>                            | 0.15-0.34<br>(15%–34%)   | 0.25<br>(25%) | The adversary has limited resources, expertise, and opportunities to support a successful attack.                                                                                 |
| <b>Very Low (VL)</b>                      | 0-0.14<br>(0%–14%)       | 0.07<br>(7%)  | The adversary has very limited resources, expertise, and opportunities to support a successful attack.                                                                            |

Table 97. The ranking of Attacker's location showing from where an attacker currently operates.

| Metric Value | Score      |
|--------------|------------|
| Physical (P) | 0.20 (20%) |
| Local (L)    | 0.40 (40%) |
| Adjacent (A) | 0.70 (70%) |
| Network (N)  | 1 (100%)   |

Table 98. Mapping Attacker's location with CVSS 3.1 Attack Vector metric.

| Attacker Location | MAV: Physical | MAV: Local  | MAV: Adjacent | MAV: Network |
|-------------------|---------------|-------------|---------------|--------------|
| <b>Physical</b>   | Can exploit   | Can exploit | Can exploit   | Can exploit  |
| <b>Local</b>      | Blocked       | Can exploit | Can exploit   | Can exploit  |
| <b>Adjacent</b>   | Blocked       | Blocked     | Can exploit   | Can exploit  |
| <b>Network</b>    | Blocked       | Blocked     | Blocked       | Can exploit  |

## D6. Results of the Evidence Chain Generation real-life scenario.

The following table illustrates all asset interdependency chains and vulnerability chains derived from the Port Authority scenario, described in Section 6.4.3.2.

Table 99. Depiction of all vulnerability chains of all cyberdependent assets combinations of the Port Authority scenario, presented in Section 6.4.3.2.

| Entry Point                    | Target Point                    | Asset Interdependency Chains                                                                      | Vulnerability Chains                              |
|--------------------------------|---------------------------------|---------------------------------------------------------------------------------------------------|---------------------------------------------------|
| A <sub>1</sub> ,V <sub>1</sub> | A <sub>3</sub> ,V <sub>6</sub>  | A <sub>1</sub> ,V <sub>1</sub> → A <sub>5</sub> ,V <sub>12</sub> → A <sub>3</sub> ,V <sub>6</sub> | V <sub>1</sub> → V <sub>12</sub> → V <sub>6</sub> |
|                                | A <sub>3</sub> ,V <sub>6</sub>  | A <sub>1</sub> ,V <sub>1</sub> → A <sub>5</sub> ,V <sub>13</sub> → A <sub>3</sub> ,V <sub>8</sub> | V <sub>1</sub> → V <sub>13</sub> → V <sub>6</sub> |
|                                | A <sub>3</sub> ,V <sub>7</sub>  | A <sub>1</sub> ,V <sub>1</sub> → A <sub>5</sub> ,V <sub>12</sub> → A <sub>3</sub> ,V <sub>7</sub> | V <sub>1</sub> → V <sub>12</sub> → V <sub>7</sub> |
|                                | A <sub>3</sub> ,V <sub>7</sub>  | A <sub>1</sub> ,V <sub>1</sub> → A <sub>5</sub> ,V <sub>13</sub> → A <sub>3</sub> ,V <sub>7</sub> | V <sub>1</sub> → V <sub>13</sub> → V <sub>7</sub> |
|                                | A <sub>3</sub> ,V <sub>8</sub>  | A <sub>1</sub> ,V <sub>1</sub> → A <sub>5</sub> ,V <sub>12</sub> → A <sub>3</sub> ,V <sub>8</sub> | V <sub>1</sub> → V <sub>12</sub> → V <sub>8</sub> |
|                                | A <sub>3</sub> ,V <sub>8</sub>  | A <sub>1</sub> ,V <sub>1</sub> → A <sub>5</sub> ,V <sub>13</sub> → A <sub>3</sub> ,V <sub>8</sub> | V <sub>1</sub> → V <sub>13</sub> → V <sub>8</sub> |
|                                | A <sub>5</sub> ,V <sub>12</sub> | A <sub>1</sub> ,V <sub>1</sub> → A <sub>5</sub> ,V <sub>12</sub>                                  | V <sub>1</sub> → V <sub>12</sub>                  |
|                                | A <sub>5</sub> ,V <sub>13</sub> | A <sub>1</sub> ,V <sub>1</sub> → A <sub>5</sub> ,V <sub>13</sub>                                  | V <sub>1</sub> → V <sub>13</sub>                  |
|                                | A <sub>3</sub> ,V <sub>6</sub>  | A <sub>1</sub> ,V <sub>1</sub> → A <sub>2</sub> ,V <sub>4</sub> → A <sub>3</sub> ,V <sub>6</sub>  | V <sub>1</sub> → V <sub>4</sub> → V <sub>6</sub>  |
|                                | A <sub>3</sub> ,V <sub>7</sub>  | A <sub>1</sub> ,V <sub>1</sub> → A <sub>2</sub> ,V <sub>4</sub> → A <sub>3</sub> ,V <sub>7</sub>  | V <sub>1</sub> → V <sub>4</sub> → V <sub>7</sub>  |
|                                | A <sub>3</sub> ,V <sub>8</sub>  | A <sub>1</sub> ,V <sub>1</sub> → A <sub>2</sub> ,V <sub>4</sub> → A <sub>3</sub> ,V <sub>8</sub>  | V <sub>1</sub> → V <sub>4</sub> → V <sub>8</sub>  |
|                                | A <sub>3</sub> ,V <sub>6</sub>  | A <sub>1</sub> ,V <sub>1</sub> → A <sub>2</sub> ,V <sub>5</sub> → A <sub>3</sub> ,V <sub>6</sub>  | V <sub>1</sub> → V <sub>5</sub> → V <sub>6</sub>  |
|                                | A <sub>3</sub> ,V <sub>8</sub>  | A <sub>1</sub> ,V <sub>1</sub> → A <sub>2</sub> ,V <sub>5</sub> → A <sub>3</sub> ,V <sub>8</sub>  | V <sub>1</sub> → V <sub>5</sub> → V <sub>8</sub>  |
|                                | A <sub>2</sub> ,V <sub>4</sub>  | A <sub>1</sub> ,V <sub>1</sub> → A <sub>2</sub> ,V <sub>4</sub>                                   | V <sub>1</sub> → V <sub>4</sub>                   |
|                                | A <sub>2</sub> ,V <sub>5</sub>  | A <sub>1</sub> ,V <sub>1</sub> → A <sub>2</sub> ,V <sub>5</sub>                                   | V <sub>1</sub> → V <sub>5</sub>                   |
|                                | A <sub>3</sub> ,V <sub>7</sub>  | A <sub>1</sub> ,V <sub>1</sub> → A <sub>2</sub> ,V <sub>5</sub> → A <sub>3</sub> ,V <sub>7</sub>  | V <sub>1</sub> → V <sub>5</sub> → V <sub>7</sub>  |
| A <sub>1</sub> ,V <sub>2</sub> | A <sub>3</sub> ,V <sub>6</sub>  | A <sub>1</sub> ,V <sub>2</sub> → A <sub>5</sub> ,V <sub>12</sub> → A <sub>3</sub> ,V <sub>6</sub> | V <sub>2</sub> → V <sub>12</sub> → V <sub>6</sub> |
|                                | A <sub>3</sub> ,V <sub>6</sub>  | A <sub>1</sub> ,V <sub>2</sub> → A <sub>5</sub> ,V <sub>13</sub> → A <sub>3</sub> ,V <sub>8</sub> | V <sub>2</sub> → V <sub>13</sub> → V <sub>6</sub> |
|                                | A <sub>3</sub> ,V <sub>7</sub>  | A <sub>1</sub> ,V <sub>2</sub> → A <sub>5</sub> ,V <sub>12</sub> → A <sub>3</sub> ,V <sub>7</sub> | V <sub>2</sub> → V <sub>12</sub> → V <sub>7</sub> |
|                                | A <sub>3</sub> ,V <sub>7</sub>  | A <sub>1</sub> ,V <sub>2</sub> → A <sub>5</sub> ,V <sub>13</sub> → A <sub>3</sub> ,V <sub>7</sub> | V <sub>2</sub> → V <sub>13</sub> → V <sub>7</sub> |
|                                | A <sub>3</sub> ,V <sub>8</sub>  | A <sub>1</sub> ,V <sub>2</sub> → A <sub>5</sub> ,V <sub>12</sub> → A <sub>3</sub> ,V <sub>8</sub> | V <sub>2</sub> → V <sub>12</sub> → V <sub>8</sub> |
|                                | A <sub>3</sub> ,V <sub>8</sub>  | A <sub>1</sub> ,V <sub>2</sub> → A <sub>5</sub> ,V <sub>13</sub> → A <sub>3</sub> ,V <sub>8</sub> | V <sub>2</sub> → V <sub>13</sub> → V <sub>8</sub> |
|                                | A <sub>5</sub> ,V <sub>12</sub> | A <sub>1</sub> ,V <sub>2</sub> → A <sub>5</sub> ,V <sub>12</sub>                                  | V <sub>2</sub> → V <sub>12</sub>                  |
|                                | A <sub>5</sub> ,V <sub>13</sub> | A <sub>1</sub> ,V <sub>2</sub> → A <sub>5</sub> ,V <sub>13</sub>                                  | V <sub>2</sub> → V <sub>13</sub>                  |
|                                | A <sub>3</sub> ,V <sub>6</sub>  | A <sub>1</sub> ,V <sub>2</sub> → A <sub>2</sub> ,V <sub>4</sub> → A <sub>3</sub> ,V <sub>6</sub>  | V <sub>2</sub> → V <sub>4</sub> → V <sub>6</sub>  |
|                                | A <sub>3</sub> ,V <sub>7</sub>  | A <sub>1</sub> ,V <sub>2</sub> → A <sub>2</sub> ,V <sub>4</sub> → A <sub>3</sub> ,V <sub>7</sub>  | V <sub>2</sub> → V <sub>4</sub> → V <sub>7</sub>  |
|                                | A <sub>3</sub> ,V <sub>8</sub>  | A <sub>1</sub> ,V <sub>2</sub> → A <sub>2</sub> ,V <sub>4</sub> → A <sub>3</sub> ,V <sub>8</sub>  | V <sub>2</sub> → V <sub>4</sub> → V <sub>8</sub>  |
|                                | A <sub>3</sub> ,V <sub>6</sub>  | A <sub>1</sub> ,V <sub>2</sub> → A <sub>2</sub> ,V <sub>5</sub> → A <sub>3</sub> ,V <sub>6</sub>  | V <sub>2</sub> → V <sub>5</sub> → V <sub>6</sub>  |
|                                | A <sub>3</sub> ,V <sub>7</sub>  | A <sub>1</sub> ,V <sub>2</sub> → A <sub>2</sub> ,V <sub>5</sub> → A <sub>3</sub> ,V <sub>7</sub>  | V <sub>2</sub> → V <sub>5</sub> → V <sub>7</sub>  |
|                                | A <sub>3</sub> ,V <sub>8</sub>  | A <sub>1</sub> ,V <sub>2</sub> → A <sub>2</sub> ,V <sub>5</sub> → A <sub>3</sub> ,V <sub>8</sub>  | V <sub>2</sub> → V <sub>5</sub> → V <sub>8</sub>  |
|                                | A <sub>2</sub> ,V <sub>4</sub>  | A <sub>1</sub> ,V <sub>2</sub> → A <sub>2</sub> ,V <sub>4</sub>                                   | V <sub>2</sub> → V <sub>4</sub>                   |

|               | $A_2, V_5$    | $A_1, V_2 \rightarrow A_2, V_5$                         | $V_2 \rightarrow V_5$                    |
|---------------|---------------|---------------------------------------------------------|------------------------------------------|
| $A_1, V_3$    | $A_3, V_7$    | $A_1, V_3 \rightarrow A_5, V_{12} \rightarrow A_3, V_7$ | $V_3 \rightarrow V_{12} \rightarrow V_7$ |
|               | $A_3, V_8$    | $A_1, V_3 \rightarrow A_5, V_{12} \rightarrow A_3, V_8$ | $V_3 \rightarrow V_{12} \rightarrow V_8$ |
|               | $A_3, V_6$    | $A_1, V_3 \rightarrow A_5, V_{12} \rightarrow A_3, V_6$ | $V_3 \rightarrow V_{12} \rightarrow V_6$ |
|               | $A_3, V_6$    | $A_1, V_3 \rightarrow A_5, V_{13} \rightarrow A_3, V_6$ | $V_3 \rightarrow V_{13} \rightarrow V_6$ |
|               | $A_3, V_7$    | $A_1, V_3 \rightarrow A_5, V_{13} \rightarrow A_3, V_7$ | $V_3 \rightarrow V_{13} \rightarrow V_7$ |
|               | $A_3, V_8$    | $A_1, V_3 \rightarrow A_5, V_{13} \rightarrow A_3, V_8$ | $V_3 \rightarrow V_{13} \rightarrow V_8$ |
|               | $A_3, V_6$    | $A_1, V_3 \rightarrow A_2, V_4 \rightarrow A_3, V_6$    | $V_3 \rightarrow V_4 \rightarrow V_6$    |
|               | $A_3, V_6$    | $A_1, V_3 \rightarrow A_2, V_5 \rightarrow A_3, V_6$    | $V_3 \rightarrow V_5 \rightarrow V_6$    |
|               | $A_3, V_7$    | $A_1, V_3 \rightarrow A_2, V_4 \rightarrow A_3, V_7$    | $V_3 \rightarrow V_4 \rightarrow V_7$    |
|               | $A_3, V_7$    | $A_1, V_3 \rightarrow A_2, V_5 \rightarrow A_3, V_7$    | $V_3 \rightarrow V_5 \rightarrow V_7$    |
|               | $A_3, V_8$    | $A_1, V_3 \rightarrow A_2, V_4 \rightarrow A_3, V_8$    | $V_3 \rightarrow V_4 \rightarrow V_8$    |
|               | $A_3, V_8$    | $A_1, V_3 \rightarrow A_2, V_4 \rightarrow A_3, V_8$    | $V_3 \rightarrow V_5 \rightarrow V_8$    |
|               | $A_2, V_4$    | $A_1, V_3 \rightarrow A_2, V_4$                         | $V_3 \rightarrow V_4$                    |
|               | $A_2, V_5$    | $A_1, V_3 \rightarrow A_2, V_5$                         | $V_3 \rightarrow V_5$                    |
|               | $A_5, V_{12}$ | $A_1, V_3 \rightarrow A_5, V_{12}$                      | $V_3 \rightarrow V_{12}$                 |
|               | $A_5, V_{13}$ | $A_1, V_3 \rightarrow A_5, V_{13}$                      | $V_3 \rightarrow V_{13}$                 |
| $A_2, V_4$    | $A_3, V_6$    | $A_2, V_4 \rightarrow A_3, V_6$                         | $V_4 \rightarrow V_6$                    |
|               | $A_3, V_7$    | $A_2, V_4 \rightarrow A_3, V_7$                         | $V_4 \rightarrow V_7$                    |
|               | $A_3, V_8$    | $A_2, V_4 \rightarrow A_3, V_8$                         | $V_4 \rightarrow V_8$                    |
| $A_2, V_5$    | $A_3, V_6$    | $A_2, V_5 \rightarrow A_3, V_6$                         | $V_5 \rightarrow V_6$                    |
|               | $A_3, V_7$    | $A_2, V_5 \rightarrow A_3, V_7$                         | $V_5 \rightarrow V_7$                    |
|               | $A_3, V_8$    | $A_2, V_5 \rightarrow A_3, V_8$                         | $V_5 \rightarrow V_8$                    |
| $A_4, V_9$    | $A_3, V_6$    | $A_4, V_9 \rightarrow A_2, V_4 \rightarrow A_3, V_6$    | $V_9 \rightarrow V_4 \rightarrow V_6$    |
|               | $A_3, V_6$    | $A_4, V_9 \rightarrow A_2, V_5 \rightarrow A_3, V_6$    | $V_9 \rightarrow V_5 \rightarrow V_6$    |
|               | $A_3, V_7$    | $A_4, V_9 \rightarrow A_2, V_4 \rightarrow A_3, V_7$    | $V_9 \rightarrow V_4 \rightarrow V_7$    |
|               | $A_3, V_7$    | $A_4, V_9 \rightarrow A_2, V_5 \rightarrow A_3, V_7$    | $V_9 \rightarrow V_5 \rightarrow V_7$    |
|               | $A_3, V_8$    | $A_4, V_9 \rightarrow A_2, V_4 \rightarrow A_3, V_8$    | $V_9 \rightarrow V_4 \rightarrow V_8$    |
|               | $A_3, V_8$    | $A_4, V_9 \rightarrow A_2, V_5 \rightarrow A_3, V_8$    | $V_9 \rightarrow V_5 \rightarrow V_8$    |
|               | $A_2, V_4$    | $A_4, V_9 \rightarrow A_2, V_4$                         | $V_9 \rightarrow V_4$                    |
|               | $A_2, V_5$    | $A_4, V_9 \rightarrow A_2, V_5$                         | $V_9 \rightarrow V_5$                    |
| $A_5, V_{12}$ | $A_3, V_6$    | $A_5, V_{12} \rightarrow A_3, V_6$                      | $V_{12} \rightarrow V_6$                 |

|               |            |                                                         |                                          |
|---------------|------------|---------------------------------------------------------|------------------------------------------|
|               | $A_3, V_7$ | $A_5, V_{12} \rightarrow A_3, V_7$                      | $V_{12} \rightarrow V_7$                 |
|               | $A_3, V_8$ | $A_5, V_{12} \rightarrow A_3, V_8$                      | $V_{12} \rightarrow V_8$                 |
| $A_5, V_{13}$ | $A_3, V_6$ | $A_5, V_{13} \rightarrow A_3, V_6$                      | $V_{13} \rightarrow V_6$                 |
|               | $A_3, V_7$ | $A_5, V_{13} \rightarrow A_3, V_7$                      | $V_{13} \rightarrow V_7$                 |
|               | $A_3, V_8$ | $A_5, V_{13} \rightarrow A_3, V_8$                      | $V_{13} \rightarrow V_8$                 |
| $A_4, V_{10}$ | $A_3, V_6$ | $A_4, V_{10} \rightarrow A_2, V_4 \rightarrow A_3, V_6$ | $V_{10} \rightarrow V_4 \rightarrow V_6$ |
|               | $A_3, V_6$ | $A_4, V_{10} \rightarrow A_2, V_5 \rightarrow A_3, V_6$ | $V_{10} \rightarrow V_5 \rightarrow V_6$ |
|               | $A_3, V_7$ | $A_4, V_{10} \rightarrow A_2, V_4 \rightarrow A_3, V_7$ | $V_{10} \rightarrow V_4 \rightarrow V_7$ |
|               | $A_3, V_7$ | $A_4, V_{10} \rightarrow A_2, V_5 \rightarrow A_3, V_7$ | $V_{10} \rightarrow V_5 \rightarrow V_7$ |
|               | $A_3, V_8$ | $A_4, V_{10} \rightarrow A_2, V_4 \rightarrow A_3, V_8$ | $V_{10} \rightarrow V_4 \rightarrow V_8$ |
|               | $A_3, V_8$ | $A_4, V_{10} \rightarrow A_2, V_5 \rightarrow A_3, V_8$ | $V_{10} \rightarrow V_5 \rightarrow V_8$ |
|               | $A_2, V_4$ | $A_4, V_{10} \rightarrow A_2, V_4$                      | $V_{10} \rightarrow V_4$                 |
|               | $A_2, V_5$ | $A_4, V_{10} \rightarrow A_2, V_5$                      | $V_{10} \rightarrow V_5$                 |
| $A_4, V_{11}$ | $A_3, V_6$ | $A_4, V_{11} \rightarrow A_2, V_4 \rightarrow A_3, V_6$ | $V_{11} \rightarrow V_4 \rightarrow V_6$ |
|               | $A_3, V_6$ | $A_4, V_{11} \rightarrow A_2, V_5 \rightarrow A_3, V_6$ | $V_{11} \rightarrow V_5 \rightarrow V_6$ |
|               | $A_3, V_7$ | $A_4, V_{11} \rightarrow A_2, V_4 \rightarrow A_3, V_7$ | $V_{11} \rightarrow V_4 \rightarrow V_7$ |
|               | $A_3, V_7$ | $A_4, V_{11} \rightarrow A_2, V_5 \rightarrow A_3, V_7$ | $V_{11} \rightarrow V_5 \rightarrow V_7$ |
|               | $A_3, V_8$ | $A_4, V_{11} \rightarrow A_2, V_4 \rightarrow A_3, V_8$ | $V_{11} \rightarrow V_4 \rightarrow V_8$ |
|               | $A_3, V_8$ | $A_4, V_{11} \rightarrow A_2, V_5 \rightarrow A_3, V_8$ | $V_{11} \rightarrow V_5 \rightarrow V_8$ |
|               | $A_2, V_4$ | $A_4, V_{11} \rightarrow A_2, V_4$                      | $V_{11} \rightarrow V_4$                 |
|               | $A_2, V_5$ | $A_4, V_{11} \rightarrow A_2, V_5$                      | $V_{11} \rightarrow V_5$                 |

The table below analyses the calculation of the Individual Vulnerability Level (IVL) for all vulnerability chains presented in Figure 48 for the Port Authority scenario, described in Section 6.4.3.2 following the approach, described in Section 6.2.2.5.

Table 100. The Individual Vulnerability Level (IVL) analysis for each vulnerability of each asset of interest, according to the Port Authority scenario, presented in Section 6.4.3.2.

| Vulnerability   | Asset          | IVL numeric values<br>( $IVL_v = 8.22 \cdot MAV \cdot MAC \cdot MPR \cdot MUI$ ) | IVL normalised values<br>$IVL_{vnorm} = \frac{MESS_v - MESS_{Min}}{MESS_{Min} - MESS_{Max}}$ | IVL qualitative values<br>(cf. Table 87) |
|-----------------|----------------|----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|------------------------------------------|
| V <sub>1</sub>  | A <sub>1</sub> | 3.8870                                                                           | 0.9992                                                                                       | VL <sub>V1</sub> = VH                    |
| V <sub>3</sub>  | A <sub>1</sub> | 3.8870                                                                           | 0.9992                                                                                       | VL <sub>V3</sub> = VH                    |
| V <sub>4</sub>  | A <sub>2</sub> | 3.8870                                                                           | 0.9992                                                                                       | VL <sub>V4</sub> = VH                    |
| V <sub>5</sub>  | A <sub>2</sub> | 2.8353                                                                           | 0.7126                                                                                       | VL <sub>V5</sub> = H                     |
| V <sub>6</sub>  | A <sub>3</sub> | 1.8346                                                                           | 0.4399                                                                                       | VL <sub>V6</sub> = M                     |
| V <sub>7</sub>  | A <sub>3</sub> | 3.8870                                                                           | 0.9992                                                                                       | VL <sub>V7</sub> = VH                    |
| V <sub>8</sub>  | A <sub>3</sub> | 1.8346                                                                           | 0.4399                                                                                       | VL <sub>V8</sub> = M                     |
| V <sub>9</sub>  | A <sub>4</sub> | 3.8870                                                                           | 0.9992                                                                                       | VL <sub>V9</sub> = VH                    |
| V <sub>10</sub> | A <sub>4</sub> | 3.8870                                                                           | 0.9992                                                                                       | VL <sub>V10</sub> = VH                   |
| V <sub>11</sub> | A <sub>4</sub> | 3.8870                                                                           | 0.9992                                                                                       | VL <sub>V11</sub> = VH                   |
| V <sub>12</sub> | A <sub>5</sub> | 2.8353                                                                           | 0.7126                                                                                       | VL <sub>V12</sub> = H                    |
| V <sub>13</sub> | A <sub>5</sub> | 2.8353                                                                           | 0.7126                                                                                       | VL <sub>V13</sub> = H                    |

Table 101. The Exploitability Level (EL) estimation analysis for each vulnerability of each asset of interest, according to the Port Authority scenario, presented in Section 6.4.3.2.

| Vulnerability   | Asset          | EL numeric values<br>(Attacker's Capability = Low,<br>Attacker's Location = Network)<br>$EL_{vi} = w_1 IVL_v + w_2 P_i$ | EL qualitative values<br>(cf. Table 87) |
|-----------------|----------------|-------------------------------------------------------------------------------------------------------------------------|-----------------------------------------|
| V <sub>1</sub>  | A <sub>1</sub> | 0.8870                                                                                                                  | EL <sub>V1</sub> = VH                   |
| V <sub>3</sub>  | A <sub>1</sub> | 0.8870                                                                                                                  | EL <sub>V3</sub> = VH                   |
| V <sub>4</sub>  | A <sub>2</sub> | 0.8870                                                                                                                  | EL <sub>V4</sub> = VH                   |
| V <sub>5</sub>  | A <sub>2</sub> | 0.6863                                                                                                                  | EL <sub>V5</sub> = H                    |
| V <sub>6</sub>  | A <sub>3</sub> | 0.4954                                                                                                                  | EL <sub>V6</sub> = M                    |
| V <sub>7</sub>  | A <sub>3</sub> | 0.8870                                                                                                                  | EL <sub>V7</sub> = VH                   |
| V <sub>8</sub>  | A <sub>3</sub> | 0.4954                                                                                                                  | EL <sub>V8</sub> = M                    |
| V <sub>9</sub>  | A <sub>4</sub> | 0.8870                                                                                                                  | EL <sub>V9</sub> = VH                   |
| V <sub>10</sub> | A <sub>4</sub> | 0.8870                                                                                                                  | EL <sub>V10</sub> = VH                  |
| V <sub>11</sub> | A <sub>4</sub> | 0.8870                                                                                                                  | EL <sub>V11</sub> = VH                  |
| V <sub>12</sub> | A <sub>5</sub> | 0.6863                                                                                                                  | EL <sub>V12</sub> = H                   |
| V <sub>13</sub> | A <sub>5</sub> | 0.6863                                                                                                                  | EL <sub>V13</sub> = H                   |



## D7. Assurance Details mappings

Table 102. Assurance details mapping of Common Criteria and EUCC [44] to set the CToE evaluation boundaries.

| CC Evaluation Assurance Level                      | CC Vulnerability Analysis Level                       | Attack Potential | EUCC Assurance Level |
|----------------------------------------------------|-------------------------------------------------------|------------------|----------------------|
| EAL1: Functionally Tested                          | AVA_VAN.1: Vulnerability survey                       | Basic            | Substantial          |
| EAL2: Structurally Tested                          | AVA_VAN.2: Vulnerability analysis                     | Basic            | Substantial          |
| EAL3: Methodically Tested and Checked              | AVA_VAN.2: Vulnerability analysis                     | Basic            | Substantial          |
| EAL4: Methodically Designed, Tested, and Reviewed  | AVA_VAN.3: Focused vulnerability analysis             | Enhanced Basic   | High                 |
| EAL5: Semi-formally Designed and Tested            | AVA_VAN.4: Methodical vulnerability analysis          | Moderate         | High                 |
| EAL6: Semi-formally Verified, Designed, and Tested | AVA_VAN.5: Advanced methodical vulnerability analysis | High             | High                 |
| EAL7: Formally Verified, Designed, and Tested      | AVA_VAN.5: Advanced methodical vulnerability analysis | High             | High                 |

## D8. Protection Profile classifications

The following table presents snapshots of the developed classification of Security Functional Requirements (SFRs) and extended SFRs, identified from multiple sources of the Common Criteria Portal [385]–[394], mapped with the security and privacy controls of NIST 800-30 [125]. The entire classification can be found in [396].

Table 103. Classification of Security Functional Requirements with security and privacy controls.

| SFR Family Identifier | SFR Family Name                   | Identifier | Name                                              | Extended SFR Description | SFR direct dependencies | SFR indirect dependencies | Extended SFRs Required dependencies | Control Identifier | Control (or Control Enhancement) Name                                               | Security Control Baseline - Low | Security Control Baseline - Moderate | Security Control Baseline - High |
|-----------------------|-----------------------------------|------------|---------------------------------------------------|--------------------------|-------------------------|---------------------------|-------------------------------------|--------------------|-------------------------------------------------------------------------------------|---------------------------------|--------------------------------------|----------------------------------|
| FAU_ARP               | Security audit automatic response | FAU_ARP.1  | Security Audit Automatic Response Security Alarms |                          | FAU_SAA.1               | FAU_GE N.1, FPT_ST M.1    |                                     | AU-5               | Response to Audit Logging Process Failures                                          | x                               | X                                    | X                                |
|                       |                                   |            |                                                   |                          |                         |                           |                                     | AU-5(1)            | Response to Audit Logging Process Failures   Storage Capacity Warning               |                                 |                                      | X                                |
|                       |                                   |            |                                                   |                          |                         |                           |                                     | AU-5(2)            | Response to Audit Logging Process Failures   Real-time Alerts                       |                                 |                                      | X                                |
|                       |                                   |            |                                                   |                          |                         |                           |                                     | AU-5(3)            | Response to Audit Logging Process Failures   Configurable Traffic Volume Thresholds |                                 |                                      |                                  |
|                       |                                   |            |                                                   |                          |                         |                           |                                     | AU-5(4)            | Response to Audit Logging Process Failures   Shutdown on Failure                    |                                 |                                      |                                  |
|                       |                                   |            |                                                   |                          |                         |                           |                                     | PE-6(2)            | Monitoring Physical Access   Automated Intrusion Recognition and Responses          |                                 |                                      |                                  |
|                       |                                   |            |                                                   |                          |                         |                           |                                     | SI-3               | Malicious Code Protection                                                           | x                               | X                                    | X                                |
|                       |                                   |            |                                                   |                          |                         |                           |                                     | SI-3(8)            | Malicious Code Protection   Detect Unauthorized Commands                            |                                 |                                      |                                  |
|                       |                                   |            |                                                   |                          |                         |                           |                                     | SI-4(5)            | System Monitoring   System-generated Alerts                                         |                                 | X                                    | X                                |
|                       |                                   |            |                                                   |                          |                         |                           |                                     | SI-4(7)            | System Monitoring   Automated Response to Suspicious Events                         |                                 |                                      |                                  |

|  |  |  |  |  |  |  |  |          |                                                                                                 |  |  |   |
|--|--|--|--|--|--|--|--|----------|-------------------------------------------------------------------------------------------------|--|--|---|
|  |  |  |  |  |  |  |  | SI-4(22) | System Monitoring   Unauthorized Network Services                                               |  |  | X |
|  |  |  |  |  |  |  |  | SI-7(2)  | Software, Firmware, and Information Integrity   Automated Notifications of Integrity Violations |  |  | X |
|  |  |  |  |  |  |  |  | SI-7(5)  | Software, Firmware, and Information Integrity   Automated Response to Integrity Violations      |  |  | X |

| SFR Family Identifier | SFR Family Name                | Identifier | Name                                                        | Extended Description | SFR | SFR direct dependencies | SFR indirect dependencies | Extended SFRs Required dependencies | Control Identifier | Control (or Control Enhancement) Name                      | Security Control Baseline - Low | Security Control Baseline - Moderate | Security Control Baseline - High |
|-----------------------|--------------------------------|------------|-------------------------------------------------------------|----------------------|-----|-------------------------|---------------------------|-------------------------------------|--------------------|------------------------------------------------------------|---------------------------------|--------------------------------------|----------------------------------|
| FAU_GEN               | Security audit data generation | FAU_GEN.1  | Security Audit Data Generation<br>Audit Data Generation     |                      |     | FPT_STM.1               |                           |                                     | AU-2               | Event Logging                                              | x                               | X                                    | X                                |
|                       |                                |            |                                                             |                      |     |                         |                           |                                     | AU-3               | Content of Audit Records                                   | x                               | X                                    | X                                |
|                       |                                |            |                                                             |                      |     |                         |                           |                                     | AU-3(1)            | Content of Audit Records   Additional Audit Information    |                                 | X                                    | X                                |
|                       |                                |            |                                                             |                      |     |                         |                           |                                     | AU-12              | Audit Record Generation                                    | x                               | X                                    | X                                |
|                       |                                | FAU_GEN.2  | Security Audit Data Generation<br>User Identity Association |                      |     | FAU_GEN.1, FIA_UID.1    |                           |                                     | AU-3               | Content of Audit Records                                   | x                               | X                                    | X                                |
| FAU_SAA               | Security audit analysis        | FAU_SAA.1  | Security Audit Analysis<br>Potential Violation Analysis     |                      |     | FAU_GEN.1               | FPT_STM.1                 |                                     | SI-4               | System Monitoring                                          | x                               | X                                    | X                                |
|                       |                                | FAU_SAA.2  | Security Audit Analysis<br>Profile-Based Anomaly Detection  |                      |     | FIA_UID.1               |                           |                                     | AC-2(12)           | Account Management   Account Monitoring for Atypical Usage |                                 |                                      | X                                |
|                       |                                |            |                                                             |                      |     |                         |                           |                                     | SI-4               | System Monitoring                                          | x                               | X                                    | X                                |
|                       |                                |            |                                                             |                      |     |                         |                           |                                     |                    |                                                            |                                 |                                      |                                  |

|         |                       |           |                                                         |  |           |  |         |                                                             |   |   |   |
|---------|-----------------------|-----------|---------------------------------------------------------|--|-----------|--|---------|-------------------------------------------------------------|---|---|---|
|         |                       | FAU_SAA.3 | Security Audit Analysis<br>Simple Attack Heuristics     |  |           |  | SI-3(7) | Malicious Code Protection  <br>Nonsignature-based Detection |   |   |   |
|         |                       |           |                                                         |  |           |  | SI-4    | System Monitoring                                           | x | X | X |
|         |                       | FAU_SAA.4 | Security Audit Analysis<br>Complex Attack<br>Heuristics |  |           |  | SI-3(7) | Malicious Code Protection  <br>Nonsignature-based Detection |   |   |   |
|         |                       |           |                                                         |  |           |  | SI-4    | System Monitoring                                           | x | X | X |
| FAU_SAR | Security Audit Review | FAU_SAR.1 | Security Audit Review<br>Audit Review                   |  | FAU_GEN.1 |  | AU-7    | Audit Record Reduction and<br>Report Generation             |   | X | X |

The following table presents the classification that interrelates the Security Objectives with the Security Functional Requirements (SFRs) and the extended SFRs [45],[384]-[394].

Table 104. Classification of Security objectives with Security Functional Requirements.

| Categor<br>ies                            | Types of<br>Security<br>Objectiv<br>es | Objective name                      | Objective Description                                                                                                                                                                                                                                                                                                                                                              | Mapping with Requirements                                                       |
|-------------------------------------------|----------------------------------------|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| Security<br>objectiv<br>es for<br>the ToE | Certificate<br>issuance                | OT.CERTIFICATES                     | The TSF must ensure that certificates, certificate revocation lists, and certificate status information are valid, and conformant to the applied framework.                                                                                                                                                                                                                        | FDP_CER_EXT.1, FDP_CER_EXT.2,<br>FDP_CER_EXT.3, FDP_CSI_EXT.1,<br>FDP_CRL_EXT.1 |
|                                           |                                        | OT.NON_REPUDI<br>ATION              | The ToE will prevent a subscriber from avoiding accountability for sending a message by providing evidence that the subscriber sent the message; and control communications from unknown source.                                                                                                                                                                                   | FCO_NRO_EXT.2, FCO_NRR_EXT.2                                                    |
|                                           |                                        | OT.CONFIGURATI<br>ON_MANAGEMEN<br>T | The ToE will conduct configuration management to assure identification of system connectivity (software, hardware, and firmware), and components (software, hardware, and firmware), auditing of configuration data, and controlling changes to configuration items.                                                                                                               | FMT_MOF.1, FMT_MTD.1                                                            |
|                                           | Known<br>State                         | OT.KNOWN_STAT<br>E                  | The ToE will provide sufficient measures to ensure it is operating in a known state. At minimum this includes management functionality to allow the security functionality to be configured and self-test functionality that allows it to assert its own integrity. It may also include auditing functionality that can be used to determine the operational behaviour of the ToE. | FAU_GEN.1, FMT_SMF.1, FAU_SEL.1,<br>FMT_SMF_EXT.1, FPT_TST_EXT.1                |

|  |                    |                              |                                                                                                                                                                                                                                                                                  |                                                                                                |
|--|--------------------|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|
|  | Key Escrow         | OT.KEY_ESCROW                | The ToE will provide a key escrow mechanism, allowing the retrieving of users private ciphering keys. This mechanism is based on the ciphering of users' private keys by the master key contained in the Hardware Security Module (HSM).                                         | FCS_COP.1, FCS_CKM_EXT.1, FCS_CKM_EXT.2, FPT_SKP_EXT.1                                         |
|  | Verifiable Updates | OT.VERIFIABLE_UPDATES        | The ToE will provide the capability to help ensure that any updates to the ToE can be verified by the administrator to be unaltered and (optionally) from a trusted source.                                                                                                      | FPT_TUD_EXT.1                                                                                  |
|  | System Monitoring  | OT.SYSTEM_MONITORING         | The ToE will provide the capability to generate audit data and send those data to an external IT entity. The ToE will record in audit records: date and time of action and the entity responsible for the action.                                                                | FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.3, FAU_SEL.1, FAU_STG.1, FCS_NTP_EXT.1, FPT_STM_EXT.1 |
|  |                    | OT.AUDIT_PROTECTION          | The ToE will protect audit records against unauthorised access, modification, or deletion to ensure accountability of user actions.                                                                                                                                              | FAU_STG.1                                                                                      |
|  |                    | OT.AUDIT_LOSS_RESPONSE       | The ToE will respond to possible loss of audit records when audit trail storage is full or nearly full by alerting administrators and inviting them to save audit files.                                                                                                         | FAU_STG.3                                                                                      |
|  |                    | OT.SELF_PROTECTION           | The TOE supports system resilience and security by enabling real-time diagnostics of its functionality, securely handling failure states to prevent exploitation, and enforcing residual data purging to protect sensitive information on decommissioned or refurbished devices. | FAU_GEN.1, FDP_RIP.1, FPT_FLS.1                                                                |
|  | ToE Authorised Use | OT.TOE_ADMINISTRATION        | The TOE enforces role-based access control to ensure that only authorized privileged users (e.g., administrators, operators, CA staff, and auditors) can access, configure, and manage system functions, including certificate management and audit logs.                        | FIA_UAU.2, FIA_UID.2, FMT_MOF.1, FMT_MTD.1, FMT_SMR.1, FMT_SMR.2, FTA_SSL.4                    |
|  |                    | OT.AUTHORIZED_ADMINISTRATION | All network devices are expected to provide services that allow the security functionality of the device to be managed.                                                                                                                                                          | FAU_STG.1, FAU_SAR.1, FAU_STG.1, FMT_CFG_EXT.1, FMT_SMF.1, FIA_ATD.1                           |
|  |                    | OT.MANAGE                    | The TSF shall provide all the functions and facilities necessary to manage ToE security mechanisms and shall restrict such management actions to authorised users.                                                                                                               | FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1, FTA_TAB.1, FTP_TRP.1                    |
|  |                    | OT.AUTHORIZED_USE            | The ToE shall provide mechanisms that prevent and detect its unauthorised use.                                                                                                                                                                                                   | FAU_GEN.1, FCS_CKM.3, FIA_UAU.6, FMT_SMF.1, FCS_STG_EXT.1                                      |

|  |                                      |                                          |                                                                                                                                                                                                                                                                                                                     |                                                                                                                                                          |
|--|--------------------------------------|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
|  |                                      | OT.AUTHENTICAT<br>ION                    | To address the issues associated with unauthorised disclosure of information in transit, a compliant ToE's authentication ability (e.g. IPsec) will allow the TSF to establish VPN connectivity with a remote VPN gateway or peer and ensure that any such connection attempt is both authenticated and authorised. | FIA_X509_EXT.2, FIA_X509_EXT.3,<br>FDP_IFC_EXT.1, FCS_IPSEC_EXT.1,<br>FIA_BMA_EXT.1, FCS_EAPTLS_EXT.1                                                    |
|  |                                      | OT.CRYPTOGRAP<br>HIC_FUNCTIONS           | To address the issues associated with unauthorised disclosure of information in transit, a compliant ToE will implement cryptographic capabilities. These capabilities are intended to maintain confidentiality and allow for detection and modification of data that is transmitted outside of the ToE.            | FCS_CKM.1, FCS_CKM.2, FCS_COP.1,<br>FTP_ITC.1, FPT_ITT.1, FTP_TRP.1,<br>FTP_ITC.1, FCS_CKM_EXT.1,<br>FTP_DIT_EXT.1, FCS_IPSEC_EXT.1,<br>FCS_EAPTLS_EXT.1 |
|  |                                      | OT.NONDISCLOSU<br>RE                     | The TOE mitigates information disclosure by protecting sensitive data at rest and in transit through secure erasure, protected storage, and controlled network communications.                                                                                                                                      | FDP_RIP.2, FCS_CKM_EXT.2,<br>FDP_VPN_EXT.1                                                                                                               |
|  |                                      | OT.USER_AUTHEN<br>TICATION               | The ToE shall provide a mechanism to assess authentication requests and respond with an authentication assertion based on data that is supplied in the request.                                                                                                                                                     | FTA_TSE.1, FIA_AFL.1,<br>FCS_FIA_X509_EXT.1                                                                                                              |
|  |                                      | OT.TRUSTED<br>_RELYING_PARTY             | The ToE shall provide mechanisms to authenticate itself to a federated relying party (RP) and authenticate a federated RP before providing an identity assertion.                                                                                                                                                   | FTP_ITC.1, FCS_EAPTLS_EXT.1                                                                                                                              |
|  |                                      | OT.SECURITY_ASS<br>OCIATION              | The ToE shall provide the information to the relying party to enable it to verify that the claimant has possession of an authentication key.                                                                                                                                                                        | FCO_NRO.1, FCO_NRR.1,<br>FCS_EAPTLS_EXT.1                                                                                                                |
|  | Access<br>Control                    | OT.DISCRETIONAR<br>Y_ACCESS              | The TSF shall control access of subjects and/or users to named resources based on identity of the object, subject or user. The TSF shall allow authorised users to specify for each access mode which users/subjects are allowed to access a specific named object in that access mode.                             | FDP_ACC.1, FDP_ACF.1                                                                                                                                     |
|  |                                      | OT.TOE_ACCESS                            | The ToE shall provide mechanisms that control a user's logical access to user data and to the TSF.                                                                                                                                                                                                                  | FDP_ACC.1, FDP_ACF.1, FIA_ATD.1,<br>FTA_MCS.1, FTA_TSE.1, FPT_TRC.1                                                                                      |
|  | Residual<br>Informatio<br>n Clearing | OT.RESIDUAL_INF<br>ORMATION_CLEA<br>RING | The ToE will ensure that any data contained in a protected resource is not available when the resource is reallocated.                                                                                                                                                                                              | FDP_RIP.1, FDP_RIP.2                                                                                                                                     |

|  |                 |                    |                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                          |
|--|-----------------|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | Secure Networks | OT.MEDIA_RECORDING | The ToE can capture and store metadata for the communications it facilitates in the form of call detail records and optionally store audio/video recordings of such communications. This data can be used to create a record of potential unauthorised or malicious activity that is occurring on the network in which the ToE is deployed. | FAU_GEN.1, FAU_STG.1, FCS_NTP_EXT.1, FPT_STM_EXT.1, FAU_VVR_EXT.1                                                                                                                        |
|  |                 | OT.SECURE_COMMS    | To address both passive (eavesdropping) and active (packet modification) network attack threats, conformant OSEs provide mechanisms to create trusted channels for CSP and sensitive data. Both CSP and sensitive data should not be exposed outside of the platform.                                                                       | FCS_RBG_EXT.1, FCS_CKM.1, FCS_CKM.2, FCS_COP.1, FDP_IFC_EXT.1, FIA_X509_EXT.1, FIA_X509_EXT.2, FTP_ITC_EXT.1                                                                             |
|  |                 | OT.SECURE_VVOIP    | The TOE securely manages VVoIP communications by providing authentication and encryption, enforcing routing policies to ensure legitimate traffic delivery and blocking unauthorized flows, and supporting secure software and firmware updates for endpoint protection.                                                                    | FDP_IFC.1, FDP_IFF.1, FIA_UAU.2, FTP_ITC.1, FCS_DTLSS_EXT.1, FCS_TLSS_EXT.1, FCS_TLSS_EXT.2, FIA_X509_EXT.1, FIA_X509_EXT.2, FIA_X509_EXT.3, FPT_STM_EXT.1, FPT_TUD_EXT.1, FCS_NTP_EXT.1 |
|  | Accountability  | OT.ACCOUNTABILITY  | The TOE supports system monitoring and incident response by generating and transmitting audit information that enables administrators to detect, diagnose, and respond to configuration issues and security compromises..                                                                                                                   | FAU_GEN.1, FTP_ITC_EXT.1                                                                                                                                                                 |
|  | Integrity       | OT.INTEGRITY       | The TOE preserves system integrity by ensuring the authenticity and integrity of software updates and by employing execution environment protections that increase the difficulty of system compromise.                                                                                                                                     | FPT_TUD_EXT.1, FPT_TUD_EXT.2, FCS_COP.1, FIA_X509_EXT.1, FPT_TST_EXT.1, FTP_ITC_EXT.1, FIA_AFL.1, FIA_UAU.5                                                                              |

The following table presents the classification that interrelates the Security Objectives with the STRIDE threat categories [260].

Table 105. Classification of STRIDE threat categories with security objectives.

| Objective                        | STRIDE Threat Categories                               |
|----------------------------------|--------------------------------------------------------|
| OT.CERTIFICATES                  | Spoofing, Information Disclosure                       |
| OT.CONFIGURATION_MANAGEMENT      | Tampering, Elevation of Privilege                      |
| OT.KNOWN_STATE                   | Tampering, Denial of Service                           |
| OT.KEY_ESCROW                    | Information Disclosure, Elevation of Privilege         |
| OT.VERIFIABLE_UPDATES            | Tampering, Elevation of Privilege                      |
| OT.SYSTEM_MONITORING             | Repudiation, Denial of Service, Elevation of Privilege |
| OT.AUDIT_PROTECTION              | Tampering, Repudiation                                 |
| OT.AUDIT_LOSS_RESPONSE           | Repudiation, Denial of Service                         |
| OT.SELF_PROTECTION               | Tampering, Denial of Service, Elevation of Privilege   |
| OT.TOE_ADMINISTRATION            | Spoofing, Elevation of Privilege                       |
| OT.AUTHORIZED_ADMINISTRATION     | Spoofing, Elevation of Privilege                       |
| OT.MANAGE                        | Elevation of Privilege, Tampering                      |
| OT.AUTHORIZED_USE                | Spoofing, Elevation of Privilege                       |
| OT.AUTHENTICATION                | Spoofing                                               |
| OT.CRYPTOGRAPHIC_FUNCTIONS       | Information Disclosure, Tampering                      |
| OT.NONDISCLOSURE                 | Information Disclosure                                 |
| OT.USER_AUTHENTICATION           | Spoofing                                               |
| OT.TRUSTED_RELIVING_PARTY        | Spoofing, Tampering                                    |
| OT.SECURITY_ASSOCIATION          | Spoofing, Information Disclosure, Tampering            |
| OT.DISCRETIONARY_ACCESS          | Elevation of Privilege, Information Disclosure         |
| OT.TOE_ACCESS                    | Spoofing, Elevation of Privilege                       |
| OT.RESIDUAL_INFORMATION_CLEARING | Information Disclosure                                 |
| OT.MEDIA_RECORDING               | Information Disclosure, Repudiation                    |
| OT.SECURE_COMMS                  | Spoofing, Information Disclosure, Tampering            |
| OT.SECURE_VVOIP                  | Spoofing, Information Disclosure, Denial of Service    |
| OT.ACCOUNTABILITY                | Repudiation                                            |
| OT.INTEGRITY                     | Tampering                                              |