**ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ**

**ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ**
**ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ**

**Μεταπτυχιακό Πρόγραμμα Σπουδών**
**MSc Ασφάλεια Ψηφιακών Συστημάτων**

**ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ**

# Διαχείριση Επικινδυνότητας στην Εφοδιαστική Αλυσίδα: Σύγκριση NIST SP 800-161r1 & ISO 27036

**Ελεονώρα Κοπανίδη**

**Επιβλέπων Καθηγητής:**
**Στέφανος Γκρίτζαλης,** Καθηγητής

**ΠΕΙΡΑΙΑΣ**

**06/2025**

**ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ**

# Διαχείριση Επικινδυνότητας στην Εφοδιαστική Αλυσίδα: Σύγκριση NIST SP 800-161r1 & ISO 27036

**Όνομα Επώνυμο**

**Α.Μ.:** mte2314

# ΠΕΡΙΛΗΨΗ

Η ασφάλεια της εφοδιαστικής αλυσίδας καθίσταται ολοένα και πιο κρίσιμη στη σύγχρονη ψηφιακή εποχή, καθώς οι οργανισμοί εξαρτώνται σε μεγάλο βαθμό από εξωτερικούς παρόχους τεχνολογίας και υπηρεσιών. Αντικείμενο της παρούσας εργασίας αποτελεί η αναλυτική μελέτη και συγκριτική αξιολόγηση δύο σημαντικών πλαισίων ασφάλειας που αφορούν την εφοδιαστική αλυσίδα: του **NIST SP 800-161 Revision 1** και του **ISO/IEC 27036**, με στόχο την ανάδειξη της καταλληλότητας, της πληρότητας και της πρακτικής εφαρμογής τους.

Αρχικά, παρουσιάζεται η έννοια της κυβερνοασφάλειας στην εφοδιαστική αλυσίδα, οι απειλές που αντιμετωπίζουν οι οργανισμοί και οι κανονιστικές απαιτήσεις που απορρέουν από την Οδηγία **NIS2**. Στη συνέχεια, γίνεται εις βάθος ανάλυση της δομής, των αρχών και των διαδικασιών που ορίζονται στα δύο πρότυπα. Η μεθοδολογία που ακολουθήθηκε βασίστηκε στη διαμόρφωση ενός **ποσοτικού πλαισίου αξιολόγησης** δέκα (10) κατηγοριών κριτηρίων με επιμέρους δείκτες.

Η συγκριτική αξιολόγηση έδειξε ότι το NIST SP 800-161r1 υπερτερεί σε όρους πρακτικής εφαρμογής και ενσωμάτωσης της διαχείρισης κινδύνων της εφοδιαστικής αλυσίδας (C-SCRM) στο σύνολο των λειτουργιών ενός οργανισμού. Από την άλλη μεριά, το ISO 27036 προσφέρει ένα περισσότερο κανονιστικό και διαδικαστικό πλαίσιο, εστιάζοντας στις απαιτήσεις που πρέπει να καθορίζονται και να εφαρμόζονται από τα εμπλεκόμενα μέρη. Η σύγκλιση των δύο προτύπων προτείνεται ως βέλτιστη προσέγγιση για την ενίσχυση της κυβερνοανθεκτικότητας της εφοδιαστικής αλυσίδας.

Η εργασία καταλήγει στη διατύπωση συμπερασμάτων που επιβεβαιώνουν τη σημασία της πολυεπίπεδης διαχείρισης κινδύνων, τη σύνδεση της συμμόρφωσης με επιχειρησιακούς στόχους και την ανάγκη για μελλοντική έρευνα πάνω σε μεθόδους αξιολόγησης και υποστηρικτικών εργαλείων για τη διαχείριση κινδύνων στην εφοδιαστική αλυσίδα.

**ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ**: Κυβερνοασφάλεια Εφοδιαστικής Αλυσίδας

**ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ**: NIST SP 800-161r1, ISO/IEC 27036-2, εφοδιαστική αλυσίδα, διαχείριση κινδύνων, NIS2

# ABSTRACT

Supply chain security is becoming increasingly critical in the modern digital era, as organizations heavily depend on external providers of technology and services. This study aims to deliver an in-depth analysis and comparative assessment of two significant security frameworks addressing supply chain protection: **NIST SP 800-161 Revision 1** and **ISO/IEC 27036**, with the objective of highlighting their suitability, comprehensiveness, and practical applicability.

The research begins with an overview of cybersecurity in the supply chain, the threats organizations face, and the regulatory requirements introduced by the **NIS2 Directive**. It then proceeds with a detailed analysis of the structure, principles, and procedures defined in both standards. The methodology adopted is based on the development of a **quantitative evaluation framework**, comprising ten (10) categories of assessment criteria with associated indicators.

The comparative evaluation revealed that NIST SP 800-161r1 demonstrates superiority in terms of practical implementation and the integration of Cyber Supply Chain Risk Management (C-SCRM) into an organization's operational processes. On the other hand, ISO 27036 provides a more prescriptive and procedural framework, focusing on the definition and enforcement of requirements by the parties involved. The convergence of both standards is proposed as an optimal approach to strengthening the cyber resilience of supply chains.

The study concludes with findings that underscore the importance of multi-layered risk management, the alignment of compliance with business objectives, and the need for future research into evaluation methods and supporting tools for managing supply chain risks.

**SUBJECT AREA**: Supply Chain Cyber Security

**KEYWORDS**: NIST SP 800-161r1, ISO/IEC 27036-2, supply chain, risk management, NIS2

# ΕΥΧΑΡΙΣΤΙΕΣ

Με την ολοκλήρωση της παρούσας διπλωματικής εργασίας, κλείνει ένα πολύ σημαντικό κεφάλαιο της ακαδημαϊκής μου πορείας στο Μεταπτυχιακό Πρόγραμμα «Ασφάλεια Ψηφιακών Συστημάτων» του Τμήματος Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιώς.

Κατά τη διάρκεια των ακαδημαϊκών χρόνων, είχα την ευκαιρία να αποκτήσω πολύτιμες γνώσεις, να διευρύνω τους ορίζοντές μου και να δοκιμάσω τις δυνατότητές μου αλλά και τον ίδιο μου τον εαυτό, μέσα από προκλήσεις που συνέβαλαν καθοριστικά στην προσωπική και επιστημονική μου εξέλιξη.

Θα ήθελα να εκφράσω ιδιαίτερες ευχαριστίες στον επιβλέποντα καθηγητή της διπλωματικής μου εργασίας Κ. Στέφανο Γκρίτζαλη, ο οποίος μέσω της καθοδήγησης και στήριξής του όχι μόνο κατά τις Μεταπτυχιακές μου σπουδές, αλλά και κατά τα χρόνια μου ως προπτυχιακή φοιτήτρια στο τμήμα Ψηφιακών Συστημάτων αποτέλεσε πρότυπο και μέντορας για εμένα, συμβάλλοντας καθοριστικά στην απόφασή μου να εμβαθύνω και να ασχοληθώ επαγγελματικά με τον τομέα της Κυβερνοασφάλειας.

Τέλος, θέλω να ευχαριστήσω την οικογένεια και το σύντροφό μου, οι οποίοι στάθηκαν δίπλα μου σε αυτό το ταξίδι και ήταν εκεί για να με ενθαρρύνουν να δίνω παραπάνω ενέργεια και δύναμη, όταν εγώ ένιωθα πως αυτά είχαν στερέψει.

# ΠΕΡΙΕΧΟΜΕΝΑ

# ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

# ΚΑΤΑΛΟΓΟΣ ΣΧΗΜΑΤΩΝ

# ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

# ΠΡΟΛΟΓΟΣ

Η ασφάλεια στην εφοδιαστική αλυσίδα αποτελεί σήμερα ένα από τα πιο σύνθετα και κρίσιμα ζητήματα στο πεδίο της κυβερνοασφάλειας. Η αυξανόμενη εξάρτηση από τρίτα μέρη, η πολυπλοκότητα των ψηφιακών υποδομών και η διαρκής μεταβολή του τοπίου των απειλών καθιστούν επιτακτική την ανάγκη για αποτελεσματική διαχείριση κινδύνων κυβερνοασφάλειας σε όλα τα επίπεδα της εφοδιαστικής διαδικασίας.

Με βάση την προηγούμενη έρευνα που πραγματοποίησα σε ακαδημαϊκό επίπεδο με τη διαχείριση κινδύνων στην κυβερνοχώρο, και συγκεκριμένα μέσα από την πτυχιακή μου εργασία, στην οποία μελέτησα πρότυπα όπως το ISO/IEC 27005, το NIST SP 800-30 και άλλες σχετικές μεθοδολογίες, θεώρησα ιδιαίτερα ενδιαφέρον να εμβαθύνω στο πεδίο της ασφάλειας στην εφοδιαστική αλυσίδα. Ως εκ τούτου, το ακαδημαϊκό ενδιαφέρον και η ανάγκη κατανόησης των πρακτικών και διαδικασιών που εφαρμόζονται στην πράξη αποτέλεσαν το κίνητρο για την επιλογή του θέματος της παρούσας διπλωματικής εργασίας.

Η εργασία αυτή εντάσσεται στο πλαίσιο του Μεταπτυχιακού Προγράμματος «Ασφάλεια Ψηφιακών Συστημάτων» του Πανεπιστημίου Πειραιώς και εστιάζει στη συγκριτική αξιολόγηση δύο σημαντικών προτύπων που αφορούν τη διαχείριση κινδύνων κυβερνοασφάλειας στην εφοδιαστική αλυσίδα: του NIST SP 800-161r1 και του ISO/IEC 27036. Στόχος είναι η ανάδειξη των ομοιοτήτων, των διαφορών και της πρακτικής αξίας που φέρει το καθένα για την ενίσχυση της ανθεκτικότητας των οργανισμών.

# 1. ΕΙΣΑΓΩΓΗ

## 1.1 Εφοδιαστική Αλυσίδα και Κυβερνοασφάλεια

Στον σημερινό ψηφιοποιημένο κόσμο, η εφοδιαστική αλυσίδα (supply chain) αποτελεί όχι μόνο θεμέλιο της παγκόσμιας παραγωγής και διανομής αγαθών και υπηρεσιών, αλλά και έναν κρίσιμο φορέα διασποράς κινδύνων στον Κυβερνοχώρο. Η εφοδιαστική αλυσίδα, με την ευρύτερη έννοια, περιλαμβάνει ένα πολυσύνθετο δίκτυο από οργανισμούς, ανθρώπους, τεχνολογίες, διαδικασίες και πόρους που εμπλέκονται στην παραγωγή, μεταφορά, αποθήκευση και παράδοση προϊόντων ή υπηρεσιών στον τελικό καταναλωτή [5]. Στο πλαίσιο της Κυβερνοασφάλειας, ο όρος επεκτείνεται για να συμπεριλάβει και τις ψηφιακές σχέσεις: προμηθευτές λογισμικού, παρόχους cloud υπηρεσιών, προμηθευτές υλικού, εξωτερικούς συνεργάτες υποστήριξης IT, καθώς και εταιρείες που προσφέρουν λύσεις τρίτων. [2]

*Εικόνα 1: Εφοδιαστική Αλυσίδα και Κυβερνοασφάλεια*

*Πηγή: https://www.srm-solutions.com/blog/supply-chains-are-the-single-greatest-risk-to-cyber-security/*

Οι σύγχρονες επιχειρήσεις εξαρτώνται όλο και περισσότερο από ψηφιακές υποδομές και λογισμικό που προέρχεται από τρίτους, γεγονός που αυξάνει σημαντικά την έκθεσή τους σε κινδύνους. Η απουσία πλήρους διαφάνειας και ελέγχου στις πρακτικές ασφάλειας των εξωτερικών παρόχων αυξάνει τις ευπάθειες των πληροφοριακών συστημάτων. [9] Συνεπώς, οι οργανισμοί δεν προστατεύουν πλέον μόνο τα δικά τους πληροφοριακά περιουσιακά στοιχεία, αλλά και εκείνα που επηρεάζονται έμμεσα από συνεργασίες και υπηρεσίες τρίτων. Τα βασικά στοιχεία που απαιτούν προστασία περιλαμβάνουν ευαίσθητα δεδομένα, πνευματική ιδιοκτησία, αρχεία διαμόρφωσης, διαπιστευτήρια πρόσβασης, συστήματα κρίσιμων υποδομών και λογισμικό που ενσωματώνεται σε καθημερινές λειτουργίες των Οργανισμών. [9] [2]

Μία ορθή και επιτυχής **διαχείριση κινδύνων στην εφοδιαστική αλυσίδα** απαιτεί ολιστική προσέγγιση. Οι οργανισμοί πρέπει να αξιολογούν τους κινδύνους των προμηθευτών **(Vendor Risk Assessment)**, να εφαρμόζουν μηχανισμούς συνεχούς παρακολούθησης, να υιοθετούν αρχιτεκτονικές μηδενικής εμπιστοσύνης **(Zero Trust Architectures)** και να ενσωματώνουν αρχές ασφάλειας κατά τον σχεδιασμό **(Security by Design)** σε όλα τα στάδια. [5] Παρ' όλα αυτά, ακόμη και οργανισμοί με ώριμες

πολιτικές ασφάλειας έχουν υποστεί σοβαρές επιθέσεις λόγω κενών ασφαλείας στην εφοδιαστική τους αλυσίδας.

## 1.2 Απειλές και περιστατικά

Τρία χαρακτηριστικά παραδείγματα Κυβερνοεπιθέσεων αποδεικνύουν την κρισιμότητα του θέματος.

Η περίπτωση της **SolarWinds** το 2020 θεωρείται μία από τις πλέον καταστροφικές και τεχνικά προηγμένες Κυβερνοεπιθέσεις μέσω της εφοδιαστικής αλυσίδας. Οι επιτιθέμενοι - μια ομάδα που αποδίδεται στην APT29 (γνωστή και ως "Cozy Bear"), με δεσμούς με τη ρωσική Υπηρεσία Εξωτερικών Πληροφοριών (SVR) - κατάφεραν να διεισδύσουν στην αλυσίδα ανάπτυξης λογισμικού της εταιρείας SolarWinds, η οποία αναπτύσσει λογισμικό διαχείρισης υποδομών πληροφορικής.

Συγκεκριμένα, απέκτησαν πρόσβαση στο περιβάλλον ανάπτυξης του λογισμικού Orion Platform, που αποτελεί βασικό προϊόν της SolarWinds για τη διαχείριση δικτύων, διακομιστών και υποδομών. Εκεί, εισαγάγανε έναν κακόβουλο κώδικα τύπου backdoor, ο οποίος έλαβε την ονομασία **SUNBURST** (ή Solorigate). Ο κακόβουλος αυτός κώδικας ενσωματώθηκε σε επίσημες εκδόσεις του Orion και διανεμήθηκε μέσω των κανονικών μηχανισμών ενημέρωσης της SolarWinds, ανάμεσα στον Μάρτιο και τον Ιούνιο του 2020. [15]

Το αποτέλεσμα ήταν η **ακούσια εγκατάσταση του κακόβουλου κώδικα σε πάνω από 18.000 οργανισμούς** σε όλο τον κόσμο. Το SUNBURST έδινε τη δυνατότητα στους επιτιθέμενους να αποκτήσουν απομακρυσμένη πρόσβαση στα συστήματα των θυμάτων, να παρακάμπτουν μηχανισμούς ελέγχου, να κλέβουν ευαίσθητες πληροφορίες και να εξαπλώνονται εσωτερικά στα δίκτυα των οργανισμών, χρησιμοποιώντας τεχνικές υποκλοπής πιστοποιητικών και παραποίησης tokens. [7]

Μεταξύ των θυμάτων περιλαμβάνονταν πληθώρα ομοσπονδιακών υπηρεσιών των ΗΠΑ, όπως το Υπουργείο Εμπορίου, το Υπουργείο Εξωτερικών, το Υπουργείο Οικονομικών, η Εθνική Υπηρεσία Πυρηνικής Ασφάλειας και το Υπουργείο Εσωτερικής Ασφάλειας (DHS), καθώς και πολλές ιδιωτικές εταιρείες υψηλής τεχνολογίας, όπως η Microsoft, η Cisco και η FireEye, η τελευταία εκ των οποίων διαπίστωσε τελικά την παραβίαση.

Η επίθεση **γνωστοποιήθηκε τον Δεκέμβριο του 2020** και εκτιμάται ότι παρέμεινε αθόρυβα ενεργή για τουλάχιστον 9 μήνες. Οι ειδικοί εκτιμούν πως ο στόχος των επιτιθέμενων ήταν η στοχευμένη κατασκοπεία, η εξαγωγή πληροφοριών υψηλής αξίας και η υπονόμευση κρίσιμων υποδομών.

Το περιστατικό έδειξε για πρώτη φορά πως όλοι οι συνδεδεμένοι οργανισμοί εκτίθενται όταν ένας κρίκος της αλυσίδας διακυβεύεται. Η εμπιστοσύνη σε “νόμιμες” ψηφιακές πηγές, όπως οι επίσημες ενημερώσεις λογισμικού, μπορεί να καταρρεύσει εάν δεν συνοδεύεται από τεχνικές διασφάλισης, όπως η ακεραιότητα του κώδικα, οι επικυρωμένες ενημερώσεις και οι πολιτικές συνεχούς παρακολούθησης. [25] [9]

Μία ακόμα γνωστή Κυβερνοεπίθεση που εκδηλώθηκε τον Ιούνιο του 2017, με παγκόσμιο αντίκτυπο και συνολικές ζημίες που υπερέβησαν τα 10 δισεκατομμύρια δολάρια, είναι η **NotPety** [26]. Παρότι φαινομενικά επρόκειτο για ένα περιστατικό που είχε ως αποκλειστικό στόχο την Ουκρανία, οι επιπτώσεις του εξελίχθηκαν σε παγκόσμια κρίση ασφάλειας πληροφοριών, αναδεικνύοντας τον υψηλό κίνδυνο ενσωμάτωσης κακόβουλου λογισμικού σε κρίσιμες εφαρμογές της εφοδιαστικής αλυσίδας λογισμικού.

Η επίθεση ξεκίνησε με τη μόλυνση της ουκρανικής λογιστικής εφαρμογής M.E.Doc, η οποία χρησιμοποιούνταν από χιλιάδες εταιρείες για την υποβολή φορολογικών εγγράφων στην τοπική εφορία. Οι Κυβερνοεγκληματίες εισέβαλαν στο περιβάλλον ανάπτυξης της M.E.Doc και ενσωμάτωσαν τον κακόβουλο κώδικα του NotPetya σε επίσημη ενημέρωση της εφαρμογής. Η ενημέρωση διανεμήθηκε μέσω των νόμιμων καναλιών ενημέρωσης στους τελικούς χρήστες, ακριβώς όπως και στην περίπτωση της SolarWinds [9]

Το NotPetya **εμφανίστηκε αρχικά ως ransomware**, απαιτώντας λύτρα σε Bitcoin για την ανάκτηση των αρχείων. Ωστόσο, η αρχιτεκτονική του κακόβουλου λογισμικού ήταν σχεδιασμένη ώστε να καταστρέφει μόνιμα τα δεδομένα, κάτι που υποδηλώνει ότι ο πραγματικός στόχος της επίθεσης ήταν η πρόκληση επιχειρησιακής παράλυσης και όχι το οικονομικό όφελος. Χρησιμοποιώντας τα εργαλεία EternalBlue και Mimikatz, το NotPetya εξαπλωνόταν ταχύτατα εντός των δικτύων, αποκτώντας αυξημένα δικαιώματα και προκαλώντας μαζική κρυπτογράφηση των αρχείων των συστημάτων [22]

Η επίθεση επηρέασε τεράστιες πολυεθνικές επιχειρήσεις. Η **A.P. Moller-Maersk**, κολοσσός στη ναυτιλία και στα logistics, υπέστη πλήρη διακοπή λειτουργιών σε πάνω από 600 λιμάνια παγκοσμίως, ενώ η φαρμακευτική εταιρεία **Merck** και η υπηρεσία ταχυμεταφορών **FedEx** ανέφεραν απώλειες εκατοντάδων εκατομμυρίων δολαρίων λόγω διακοπής παραγωγής, καταστροφής δεδομένων και ανάγκης πλήρους επαναφοράς των συστημάτων τους από το μηδέν. Ακόμα και το ακτινολογικό σύστημα στο πυρηνικό εργοστάσιο του Τσέρνομπιλ επηρεάστηκε, αναγκάζοντας τους τεχνικούς να επαναφέρουν χειροκίνητα τις μετρήσεις ραδιενέργειας.

Η επίθεση NotPetya απέδειξε ότι ακόμα και ένα περιορισμένης χρήσης λογισμικό, όταν χρησιμοποιείται από κρίσιμους φορείς της εφοδιαστικής αλυσίδας, μπορεί να λειτουργήσει ως όχημα παγκόσμιας Κυβερνοεπίθεσης. Το περιστατικό έφερε στο προσκήνιο την ανάγκη για αυστηρή αξιολόγηση τρίτων προμηθευτών, επαλήθευση πηγών ενημερώσεων, καθώς και τη χρήση τεχνικών όπως **application whitelisting, segmentation και multi-factor authentication** για τον περιορισμό των επιπτώσεων μιας τέτοιας διαρροής.

Η NotPetya εντάσσεται πλέον στο παγκόσμιο λεξικό Κυβερνοασφάλειας ως χαρακτηριστικό παράδειγμα **"weaponized supply chain compromise"**, και χρησιμοποιείται ευρέως ως case study για την αναβάθμιση στρατηγικών ανθεκτικότητας έναντι ψηφιακών απειλών στην αλυσίδα εφοδιασμού.

Το 2025, η **Marks & Spencer (M&S)**, ένας από τους μεγαλύτερους βρετανικούς ομίλους λιανικής, αποτέλεσε στόχο Κυβερνοεπίθεσης στην αλυσίδα εφοδιασμού. Η επίθεση φέρεται να προήλθε από την διαβόητη ομάδα Κυβερνοεγκληματιών "Scattered Spider", γνωστή για προηγούμενες επιθέσεις σε πολυεθνικούς κολοσσούς όπως η MGM Resorts και η Caesars Entertainment. Η ιδιαίτερη σοβαρότητα του περιστατικού έγκειται στο γεγονός ότι οι εισβολείς **δεν στόχευσαν απευθείας την ίδια την M&S**, αλλά φέρεται να **εκμεταλλεύτηκαν ευπάθειες σε τρίτο τεχνολογικό πάροχο**, πιθανώς την Tata Consultancy Services (TCS), η οποία προσφέρει υπηρεσίες πληροφορικής στην M&S. [23]

Η μεθοδολογία της επίθεσης ήταν πολυσύνθετη και αξιοποίησε κυρίως τεχνικές κοινωνικής μηχανικής. Συγκεκριμένα, φέρεται να έγινε χρήση **SIM swapping**, με στόχο την παράκαμψη μηχανισμών ελέγχου ταυτότητας πολλαπλών παραγόντων (multi-factor authentication). Μέσω παραπλάνησης εργαζομένων με αυξημένα δικαιώματα

και απόκτησης αυτών, η ομάδα κατάφερε να αποκτήσει πρόσβαση σε κρίσιμα πληροφοριακά συστήματα της εταιρείας. Ως αποτέλεσμα, η M&S αναγκάστηκε να διακόψει ή να περιορίσει την προσφορά υπηρεσιών της, όπως οι ηλεκτρονικές παραγγελίες, οι ανέπαφες πληρωμές, και η υπηρεσία "Click and Collect" στα φυσικά καταστήματα. [24]

Οι συνέπειες της επίθεσης δεν περιορίστηκαν στον Κυβερνοχώρο. Προκάλεσαν **φυσικές λειτουργικές και οικονομικές επιπτώσεις** στον πραγματικό κόσμο, με τους καταναλωτές να αναφέρουν σημαντικά προβλήματα στις αγορές τους, ελλείψεις σε προϊόντα και καθυστερήσεις στις παραδόσεις. Η εταιρεία εκτιμά ότι οι άμεσες απώλειες σε λειτουργικά κέρδη ενδέχεται να ξεπεράσουν τις 300 εκατομμύρια λίρες, ενώ η χρηματιστηριακή της αξία μειώθηκε κατά 750 εκατομμύρια λίρες τις ημέρες που ακολούθησαν. [24]

Το περιστατικό επιβεβαίωσε μία τάση που εντείνεται: **οι επιθέσεις δεν χρειάζεται να στοχεύουν ευθέως τον "κύριο" οργανισμό για να είναι καταστροφικές**. Οι οργανισμοί εξαρτώνται πλέον από ένα περίπλοκο δίκτυο τρίτων παρόχων - από παρόχους υποδομής cloud και λογισμικού SaaS μέχρι παρόχους logistics και data analytics. Κάθε ένας από αυτούς αποτελεί δυνητικό "κρίκο" αδυναμίας στην αλυσίδα εφοδιασμού.

Η επίθεση στην M&S αναδεικνύει τη σημασία του Zero Trust μοντέλου ασφάλειας, της συστηματικής αξιολόγησης τρίτων παρόχων και της συνεχούς παρακολούθησης (continuous monitoring) όχι μόνο των εσωτερικών, αλλά και των εξωτερικών στοιχείων του ψηφιακού περιβάλλοντος. Επίσης, υπογραμμίζει τη σημασία ύπαρξης σχεδίων ανάκαμψης από περιστατικά (incident response plans) που να περιλαμβάνουν εξαρτώμενες υπηρεσίες και συνεργάτες.

Η περίπτωση αυτή, όπως και οι επιθέσεις στις SolarWinds (2020) και NotPetya (2017), καταδεικνύει τη στρατηγική στροφή των Κυβερνοεπιθέσεων προς τα τρίτα μέρη της αλυσίδας εφοδιασμού και την ανάγκη αντιμετώπισης της Κυβερνοασφάλειας ως οριζόντιου επιχειρησιακού κινδύνου και όχι μόνο ως τεχνικό ζήτημα. [9]

## 1.3 Γιατί η Εφοδιαστική Αλυσίδα αποτελεί στόχο;

Η Εφοδιαστική Αλυσίδα αποτελεί ένα από τα πλέον πιο ελκυστικά μέσα για Κυβερνοεπιθέσεις, λόγω της πολυπλοκότητας, της διασύνδεσης και της εξάρτησης από τρίτους παρόχους. Οι επιτιθέμενοι εκμεταλλεύονται τα κενά ασφαλείας της αλυσίδας για να αποκτήσουν πρόσβαση σε κρίσιμα συστήματα και δεδομένα.

Οι κύριοι λόγοι που καθιστούν την εφοδιαστική αλυσίδα ελκυστικό στόχο περιλαμβάνουν:

- Πολυπλοκότητα και έλλειψη διαφάνειας

  Οι σύγχρονες εφοδιαστικές αλυσίδες αποτελούνται από πολλαπλά επίπεδα προμηθευτών, υπεργολάβων και παρόχων υπηρεσιών, καθιστώντας δύσκολη την πλήρη εποπτεία και διαχείριση των κινδύνων. Η έλλειψη διαφάνειας και η περιορισμένη ορατότητα στις πρακτικές κυβερνοασφάλειας των συνεργατών αυξάνουν την πιθανότητα επιτυχημένων επιθέσεων. [8]

- Κενά ασφαλείας σε τρίτα μέρη

Οι επιτιθέμενοι συχνά στοχεύουν σε συνεργάτες, οι οποίοι μπορεί να μην διαθέτουν επαρκείς μηχανισμούς ασφαλείας. Μέσω αυτών, μπορούν να διεισδύσουν σε μεγαλύτερους οργανισμούς, εκμεταλλευόμενοι την εμπιστοσύνη που υπάρχει μεταξύ των μελών της αλυσίδας. [10]

- Γενικευμένη επίδραση

  Μια επιτυχημένη επίθεση σε έναν κρίκο της εφοδιαστικής αλυσίδας μπορεί να έχει εκτεταμένες συνέπειες, επηρεάζοντας πολλαπλούς οργανισμούς ταυτόχρονα. Η επίθεση στη SolarWinds (2020) που αναλύθηκε στην παράγραφο 1.2 αποτελεί ένα τέτοιο παράδειγμα γενικευμένης επίδρασης μέσω της αλυσίδας. [7]

- Δυσκολία εντοπισμού και αντιμετώπισης

  Η πολυπλοκότητα και η διασύνδεση των συστημάτων καθιστούν δύσκολη την έγκαιρη ανίχνευση και αντιμετώπιση των επιθέσεων. Οι επιτιθέμενοι μπορούν να παραμείνουν μη ανιχνεύσιμοι για μεγάλα χρονικά διαστήματα, αυξάνοντας τη ζημιά που προκαλούν. [8]

- Πρόσβαση σε ευαίσθητα δεδομένα

  Η εφοδιαστική αλυσίδα διαχειρίζεται μεγάλο όγκο ευαίσθητων δεδομένων, όπως πληροφορίες πελατών, οικονομικά στοιχεία και εμπορικά μυστικά. Η απόκτηση αυτών των δεδομένων αποτελεί κύριο στόχο για τους Κυβερνοεγκληματίες, είτε για οικονομικό όφελος είτε για βιομηχανική κατασκοπεία. [21]

Ολοκληρώνοντας, καθίσταται σαφές ότι η ασφάλεια της εφοδιαστικής αλυσίδας αποτελεί έναν κρίσιμο στρατηγικό πυλώνα για την προστασία των οργανισμών από σύγχρονες και εξελισσόμενες Κυβερνοαπειλές. Η κατανόηση των κινδύνων, η ενίσχυση της διαφάνειας και η συνεργασία με ασφαλείς και αξιόπιστους εταίρους είναι απαραίτητες προϋποθέσεις για τη θωράκιση της επιχειρησιακής συνέχειας και της εμπιστοσύνης σε ένα παγκοσμιοποιημένο περιβάλλον.

## 1.4 Η εξέλιξη των κυβερνοαπειλών στην εφοδιαστική αλυσίδα σε ποσοστά

Οι Κυβερνοαπειλές στην εφοδιαστική αλυσίδα παρουσιάζουν ανησυχητική και συνεχώς αυξανόμενη τάση τα τελευταία χρόνια, γεγονός που υπογραμμίζει την ανάγκη για αυστηρότερη εποπτεία και ενίσχυση των μέτρων ασφάλειας. Σύμφωνα με την έκθεση του ENISA για το Threat Landscape 2024, ο αριθμός των περιστατικών που αφορούν επιθέσεις στην εφοδιαστική αλυσίδα αυξήθηκε κατά 24% σε σχέση με το 2023, με το 14% αυτών να σχετίζονται άμεσα με παραβιάσεις μέσω προμηθευτών και τρίτων μερών. [11]

Η πολυπλοκότητα και το πλήθος των επιπέδων που απαρτίζουν τις σύγχρονες εφοδιαστικές αλυσίδες δυσχεραίνουν την ορατότητα και τον έλεγχο των κινδύνων, αφού συνεργάζονται πολλαπλοί προμηθευτές, υπεργολάβοι και πάροχοι υπηρεσιών. [6] Η έλλειψη διαφάνειας σχετικά με τις πρακτικές Κυβερνοασφάλειας των συνεργαζόμενων φορέων αυξάνει σημαντικά τις πιθανότητες επιτυχημένων επιθέσεων, με αποτέλεσμα να στοχοποιούνται συχνά οι αδύναμοι κρίκοι της αλυσίδας. Όπως επισημαίνει η Ευρωπαϊκή Επιτροπή, το 66% των επιθέσεων εστιάζει στον κώδικα και στα προϊόντα των προμηθευτών, προκαλώντας εκτεταμένες επιπτώσεις στους τελικούς χρήστες. [12]

Επιπλέον, οι Κυβερνοεγκληματίες εκμεταλλεύονται τη χρήση κακόβουλου λογισμικού σε ποσοστό 62% των περιστατικών και στοχεύουν κυρίως στην κλοπή ευαίσθητων

δεδομένων, όπως προσωπικών πληροφοριών και πνευματικής ιδιοκτησίας. [12]Αυτό επιβεβαιώνεται και από τα ευρήματα του Arcadian-IoT, όπου αναφέρεται πως το 66% των προμηθευτών δεν γνωρίζουν επακριβώς πώς έχουν παραβιαστεί τα συστήματά τους ή δεν αναφέρουν τα περιστατικά, αυξάνοντας τον κίνδυνο συνέχισης και επέκτασης των επιθέσεων. [6]

Ταυτόχρονα, η διάρκεια των διακοπών λειτουργίας που προκαλούνται από επιθέσεις στην αλυσίδα εφοδιασμού αυξάνεται σταθερά. Το 2024, η μέση διάρκεια διακοπής λειτουργίας λόγω τέτοιων επιθέσεων έφτασε τις 17 ώρες, έναντι 12 ωρών το 2023, επιφέροντας σημαντικές οικονομικές απώλειες και επιπτώσεις στην επιχειρησιακή συνέχεια. [28]

Παράλληλα, η έκθεση του InfoSecurity Europe υπογραμμίζει ότι οι επιθέσεις στην εφοδιαστική αλυσίδα προβλέπεται να γίνουν η κυρίαρχη μορφή κυβερνοεπιθέσεων μέσα στα επόμενα χρόνια, λόγω της ολοένα μεγαλύτερης εξάρτησης των οργανισμών από τρίτους προμηθευτές και της αυξανόμενης πολυπλοκότητας των πληροφοριακών συστημάτων. [16]

Η ανάγκη για ενίσχυση της Κυβερνοασφάλειας στην εφοδιαστική αλυσίδα δεν είναι πλέον θεωρητική, αλλά επιτακτική. Τα δεδομένα αποδεικνύουν ότι οι οργανισμοί που δεν εφαρμόζουν αυστηρά μέτρα ελέγχου, διαφάνειας και συνεργασίας με τους προμηθευτές τους, εκτίθενται σε σοβαρούς κινδύνους, οι οποίοι μπορούν να πλήξουν όχι μόνο την τεχνολογική τους υποδομή αλλά και την αξιοπιστία και τη φήμη τους στην αγορά. [11] [6]

## 1.5 Η ασφάλεια στην Εφοδιαστική Αλυσίδα υπό της προϋποθέσεις της NIS2


*Εικόνα 2: Οδηγία NIS2*

*Πηγή: https://www.enisa.europa.eu/*

Η οδηγία NIS2 (Network Information Systems Directive 2) εκδόθηκε στις 28 Νοεμβρίου 2022 (οδηγία (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 14ης Δεκεμβρίου 2022). Η NIS2, όπως και η προηγούμενη έκδοση της NIS, εστιάζουν στη διαχείριση κινδύνων για τους οργανισμούς. Η ΕΕ δηλώνει ότι η NIS είναι η πρώτη νομοθεσία σε επίπεδο ΕΕ για την ασφάλεια στον Κυβερνοχώρο με στόχο την επίτευξη ενός υψηλού κοινού επιπέδου Κυβερνοασφάλειας σε όλα τα κράτη μέλη.

Η NIS2 θα αλλάξει ιδιαίτερα τον τρόπο με τον οποίο οι οργανισμοί προσεγγίζουν και διαχειρίζονται την ασφάλεια της εφοδιαστικής αλυσίδας, ως μέρος μιας ολιστικής προσέγγισης της ασφάλειας στον Κυβερνοχώρο σε όλα τα κράτη μέλη της ΕΕ (και όχι μόνο). Με την εξασφάλιση κάθε τμήματος της αλυσίδας εφοδιασμού, η οδηγία θα προωθήσει ένα ισχυρό, ενιαίο μέτωπο Κυβερνοασφάλειας σε ολόκληρη την ΕΕ.

Οι υποχρεώσεις συμμόρφωσης τεκμηριώνονται στο Παράρτημα του εκτελεστικού κανονισμού της Ευρωπαϊκής Επιτροπής, που θεσπίστηκε στα πλαίσια της Οδηγίας, και αφορούν τόσο τις εσωτερικές διαδικασίες αξιολόγησης κινδύνων όσο και τη διαχείριση τρίτων μερών (third-party risk management) που εμπλέκονται στην παροχή υπηρεσιών ή προμηθειών ICT. [14]

### 1.5.1. Ενσωμάτωση της Εκτίμησης Κινδύνου στην Εφοδιαστική Αλυσίδα

Η αξιολόγηση κινδύνου αποτελεί τη βάση για τον καθορισμό κατάλληλων μέτρων προστασίας. Σύμφωνα με το άρθρο 21(2) της Οδηγίας, κάθε οντότητα υποχρεούται να:

- εντοπίζει και να αξιολογεί τις απειλές και τις ευπάθειες που επηρεάζουν τα δίκτυα και συστήματα πληροφορικής,
- λαμβάνει υπόψη την εξάρτηση από εξωτερικούς φορείς όπως προμηθευτές και παρόχους ICT υπηρεσιών,
- προσαρμόζει την πολιτική και τις συμβατικές απαιτήσεις προς τρίτους με βάση τα αποτελέσματα των εκτιμήσεων αυτών.

Αυτό συνδέεται άρρηκτα με το σημείο 5.1.4 του Παραρτήματος ΙΙ, το οποίο προβλέπει ότι τα αποτελέσματα της εκτίμησης κινδύνου (σύμφωνα με το σημείο 2.1) πρέπει να αντικατοπτρίζονται στις συμβάσεις με προμηθευτές.

Η οδηγία εισάγει τρεις μηχανισμούς για την ενίσχυση της ασφάλειας της εφοδιαστικής αλυσίδας:

- Coordinated Risk Assessment: Βασισμένη στο άρθρο 22 της οδηγίας, η διαδικασία αυτή πραγματοποιείται από την Ομάδα Συνεργασίας (Cooperation Group), σε συνεργασία με τον ENISA και την Ευρωπαϊκή Επιτροπή. Αφορά τον εντοπισμό κρίσιμων εξαρτήσεων, ευπαθειών και σημείων αποτυχίας σε συγκεκριμένες εφοδιαστικές αλυσίδες. Τα κριτήρια αξιολόγησης περιλαμβάνουν τόσο τεχνικούς όσο και μη τεχνικούς παράγοντες, όπως η εξάρτηση από προμηθευτές, η διαθεσιμότητα εναλλακτικών, και η ενδεχόμενη επιρροή τρίτων (Recitals 90, 91). Η μη συμμόρφωση με τα αποτελέσματα αυτής της αξιολόγησης μπορεί να θεωρηθεί παράβαση των υποχρεώσεων, ακόμη κι αν έχουν τηρηθεί οι λοιπές απαιτήσεις του άρθρου 21 (NIS2, Άρθρο 21 §3). [14]
- National Risk Assessment: Αν και δεν κατονομάζεται ρητά στην οδηγία παρέχεται στα κράτη μέλη η δυνατότητα να επεκτείνουν το πεδίο εφαρμογής σε οντότητες που δεν περιλαμβάνονται αρχικά. Αυτό ισχύει για φορείς με κρίσιμη σημασία για την εθνική ή περιφερειακή ασφάλεια, παρόχους μοναδικών υπηρεσιών ή οργανισμούς των οποίων η διακοπή λειτουργίας μπορεί να επηρεάσει σοβαρά τη δημόσια ασφάλεια ή τη διασυνοριακή λειτουργικότητα. Αυτό σημαίνει ότι ακόμη και φορείς που δεν υπάγονται τυπικά στις διατάξεις της NIS2 μπορεί τελικά να κληθούν να συμμορφωθούν πλήρως, εάν πληρούν ορισμένα εθνικά κριτήρια κινδύνου. [14]
- Internal Risk Assessment: Οι βασικές και σημαντικές οντότητες που υπάγονται στην οδηγία υποχρεούνται να αξιολογούν εσωτερικά τους κινδύνους που απορρέουν από τους προμηθευτές και παρόχους υπηρεσιών τους. Πρέπει να εξετάζουν τις ευπάθειες και τις διαδικασίες ασφαλούς ανάπτυξης που εφαρμόζουν οι συνεργάτες τους (Άρθρο 21 §2δ). Αυτό ενδέχεται να αποδειχθεί πρόκληση για οργανισμούς με περιορισμένους πόρους, καθώς απαιτεί τεχνική επάρκεια, εργαλεία, και πρόσβαση σε δεδομένα συμμόρφωσης τρίτων. [14]

### 1.5.2. Πολιτική Ασφάλειας Εφοδιαστικής Αλυσίδας (Supply Chain Security Policy)

Η Οδηγία προβλέπει, στο σημείο 5.1.1, την υποχρέωση κάθε υπόχρεης οντότητας να καθιερώσει και να εφαρμόζει πολιτική ασφάλειας εφοδιαστικής αλυσίδας. Η πολιτική αυτή καλείται να ρυθμίζει:

- τη σχέση με τους άμεσους προμηθευτές και παρόχους υπηρεσιών,
- τον προσδιορισμό και τη γνωστοποίηση του ρόλου του οργανισμού μέσα στην εφοδιαστική αλυσίδα.

Η πολιτική αυτή πρέπει να αναπτύσσεται με βάση τα αποτελέσματα της εκτίμησης κινδύνου (π.χ. καταγραφή πόρων, εξαρτήσεων και απειλών), και να προσαρμόζεται στις εκάστοτε συνθήκες του τομέα και των παρεχόμενων υπηρεσιών.

### 1.5.3. Κριτήρια Επιλογής Προμηθευτών και Συμβατικοί Όροι

Στο σημείο 5.1.2, ορίζεται ότι οι οντότητες οφείλουν να υιοθετούν κριτήρια επιλογής προμηθευτών και παρόχων υπηρεσιών, τα οποία περιλαμβάνουν:

- την αξιολόγηση των πρακτικών Κυβερνοασφάλειας των τρίτων μερών,
- την ανθεκτικότητα και αξιοπιστία των ICT προϊόντων και υπηρεσιών,
- την ικανότητα περιορισμού εξάρτησης από συγκεκριμένους προμηθευτές.

Στη συνέχεια, στο σημείο 5.1.4, καθορίζονται οι συμβατικές υποχρεώσεις που οφείλουν να ενσωματώνονται, όπως:

- απαιτήσεις Κυβερνοασφάλειας και ενημέρωσης για περιστατικά,
- έλεγχος υπεργολαβιών,
- διαχείριση τρωτοτήτων (vulnerability Handling),
- υποχρεώσεις κατά την αποχώρηση (data retrieval/disposal).

Τα παραπάνω εντάσσονται σε μια προσέγγιση risk-based procurement, όπου η ανάλυση κινδύνου καθοδηγεί τη σύναψη και το περιεχόμενο των συμβάσεων.

### 1.5.4. Συνεχής Παρακολούθηση και Αναθεώρηση

Όπως αναφέρεται στα σημεία 5.1.6 και 5.1.7, οι οργανισμοί πρέπει να εφαρμόζουν μηχανισμούς συνεχούς παρακολούθησης των συνεργατών και να επανεξετάζουν την πολιτική τους σε περιπτώσεις:

- αλλαγών στις πρακτικές ασφάλειας των προμηθευτών,
- σημαντικών επιχειρησιακών αλλαγών ή συμβάντων,
- αναθεωρήσεων υπηρεσιακού επιπέδου (SLAs).

Η παρακολούθηση πρέπει να συνοδεύεται από τεκμηριωμένες αναλύσεις και έγκαιρη λήψη μέτρων, με έμφαση στην αποτροπή κλιμάκωσης κινδύνων που προέρχονται από την εφοδιαστική αλυσίδα.

### 1.5.5. Κατάλογος Προμηθευτών και Ιχνηλασιμότητα

Σύμφωνα με το σημείο 5.2, απαιτείται η συστηματική καταγραφή όλων των άμεσων προμηθευτών και παρόχων υπηρεσιών, μαζί με:

- πληροφορίες επικοινωνίας,

- κατάλογο παρεχόμενων ICT προϊόντων, υπηρεσιών και διαδικασιών.

Η απαίτηση αυτή ενισχύει την ιχνηλασιμότητα (traceability) και την ικανότητα άμεσης αντίδρασης σε περίπτωση παραβίασης ή συμβάντος.

Συμπερασματικά, η Οδηγία NIS2 διαμορφώνει ένα συνεκτικό πλαίσιο για την ενσωμάτωση της εκτίμησης κινδύνου στις σχέσεις με τρίτους, ενισχύοντας τους Οργανισμούς, ώστε να υιοθετούν στρατηγικές ασφάλειας της εφοδιαστικής αλυσίδας. Η σύνδεση ανάμεσα σε πολιτικές, διαδικασίες προμηθειών και συνεχής παρακολούθηση του επιπέδου Κυβερνοασφάλειας των τρίτων, αποσκοπεί στη θωράκιση των κρίσιμων συστημάτων Πληροφορικής έναντι αυξανόμενων κινδύνων στον Κυβερνοχώρο. [36] [11]

# 2. Πρότυπα για την ασφάλεια της Εφοδιαστικής Αλυσίδας

## 2.1 Η ανάγκη διαχείρισης κινδύνων και συμμόρφωσης με διεθνή πρότυπα

Στο προηγούμενο κεφάλαιο παρουσιάστηκε η πολυπλοκότητα και η κρισιμότητα της εφοδιαστικής αλυσίδας στο σύγχρονο ψηφιακό περιβάλλον, καθώς και οι Κυβερνοαπειλές που τη στοχεύουν. Η εξέλιξη των επιθέσεων αποδεικνύει ότι δεν αρκεί πλέον η αποσπασματική διαχείριση κινδύνων. Αντιθέτως, απαιτείται **συστηματική συμμόρφωση με δομημένα πρότυπα και πλαίσια**, ώστε οι οργανισμοί να μπορούν να εντοπίζουν, να αξιολογούν και να αντιμετωπίζουν τους κινδύνους με συνέπεια, επανάληψη και αποδοτικότητα.

Η εφοδιαστική αλυσίδα περιλαμβάνει ένα εκτεταμένο δίκτυο προμηθευτών, υπεργολάβων, παρόχων τεχνολογίας και εξωτερικών συνεργατών. Η πολυεπίπεδη διασύνδεση αυτών των οντοτήτων εντείνει την αβεβαιότητα και δυσκολεύει την εκτίμηση του συνολικού κινδύνου Κυβερνοασφάλειας. [1] Παράλληλα, ο δυναμισμός της αγοράς και η συνεχής εξάρτηση από τρίτους αυξάνουν την πιθανότητα εισαγωγής απειλών, σκόπιμα ή ακούσια, στα εσωτερικά συστήματα των οργανισμών. [19]

Η αναγνώριση αυτών των προκλήσεων έχει οδηγήσει διεθνείς φορείς σε προτάσεις για την υιοθέτηση τυποποιημένων μεθοδολογιών διαχείρισης κινδύνων. Η εφαρμογή συγκεκριμένων πλαισίων, είτε προαιρετικών είτε υποχρεωτικών (π.χ. NIS2, ISO/IEC, NIST), προσφέρει ένα συνεκτικό και ελέγξιμο σύστημα ασφάλειας που επιτρέπει στους οργανισμούς να αποδεικνύουν συμμόρφωση και να χτίζουν την ανθεκτικότητα.

Σημαντικό είναι και το ζήτημα της νομοθετικής πίεσης. Η Οδηγία NIS2 (Directive (EU) 2022/2555), όπως αναφέρθηκε ήδη, υποχρεώνει πλέον οντότητες να ενσωματώνουν την ασφάλεια της εφοδιαστικής αλυσίδας στις πολιτικές τους, προωθώντας την ανάγκη για συγκεκριμένα μέτρα, αξιολογήσεις τρίτων, και τη διασφάλιση μέσω συμβατικών όρων.

Η υιοθέτηση προτύπων δεν είναι απλώς τεχνική απαίτηση αλλά **στρατηγικό μέσο μείωσης κινδύνου**. Μέσα από αυτό, επιτυγχάνεται:

- **Αντιμετώπιση ασυνέπειας** στις διαδικασίες και στις απαιτήσεις ασφαλείας.
- **Σαφήνεια** στην αξιολόγηση των τρίτων μερών και των παρεχόμενων προϊόντων ή υπηρεσιών.
- **Τεκμηρίωση** συμμόρφωσης προς τις ρυθμιστικές απαιτήσεις και τις εσωτερικές πολιτικές.

Ως εκ τούτου, η μελέτη των διεθνών προτύπων, τα οποία παρουσιάζονται στα επόμενα κεφάλαια, κρίνεται θεμελιώδης για την κατανόηση του τρόπου με τον οποίο η τυποποίηση συνδράμει στην ενίσχυση της ασφάλειας της εφοδιαστικής αλυσίδας.

## 2.2 Εισαγωγή στα πρότυπα και βασικοί ορισμοί

Η διαχείριση της ασφάλειας στην εφοδιαστική αλυσίδα απαιτεί την εφαρμογή διεθνών προτύπων που καθορίζουν συστηματικές προσεγγίσεις για την αναγνώριση, την αξιολόγηση και τη μείωση των κινδύνων που προκύπτουν από τους προμηθευτές και συνεργάτες. Δύο από τα πιο σημαντικά και ευρέως υιοθετημένα πρότυπα στον τομέα αυτό είναι το **ISO/IEC 27036** και το **NIST Special Publication 800-161 Revision 1**.

ISO/IEC 27036 είναι μια σειρά προτύπων που εστιάζει στην ασφάλεια των πληροφοριών σε σχέση με τις σχέσεις προμηθευτή-πελάτη (ή αγοραστή). Συγκεκριμένα, το πρότυπο αυτό παρέχει οδηγίες για τη διαχείριση κινδύνων που σχετίζονται με την προμήθεια προϊόντων και υπηρεσιών πληροφορικής, καλύπτοντας όλο το φάσμα της αλυσίδας εφοδιασμού. [30] ]Βασικός στόχος είναι η ενίσχυση της εμπιστοσύνης μεταξύ οργανισμών και προμηθευτών μέσω συστηματικών διαδικασιών ασφάλειας και ελέγχων.

Από την άλλη πλευρά, το NIST SP 800-161r1 αποτελεί ένα αναλυτικό πλαίσιο διαχείρισης κινδύνων εφοδιαστικής αλυσίδας με έμφαση σε κυβερνητικές και ιδιωτικές οντότητες που διαχειρίζονται κρίσιμες υποδομές. Το πρότυπο αυτό προσφέρει πρακτικές κατευθυντήριες οδηγίες για τον εντοπισμό, την αξιολόγηση και τη διαχείριση των απειλών που αφορούν την προμήθεια προϊόντων και υπηρεσιών τεχνολογίας, με στόχο την βελτίωση της ανθεκτικότητας και της ασφάλειας σε όλη την εφοδιαστική αλυσίδα. [29]

Παρακάτω, παρατίθενται οι βασικοί ορισμοί όπως περιγράφονται στα ανωτέρω πρότυπα, με στόχο τη θεμελίωση ενός ενιαίου θεωρητικού πλαισίου αναφοράς που θα υποστηρίξει την ανάλυση και σύγκριση τους στα επόμενα κεφάλαια.

**Ορισμοί από ISO/IEC 27036-1:2021** [30]

- **Προμηθευτής (Supplier):** οργανισμός ή άτομο που συνάπτει μία *συμφωνία* με τον *αγοραστή* για την προμήθεια ενός προϊόντος ή υπηρεσίας.
    - Σημείωση 1: Άλλοι συνήθεις όροι που χρησιμοποιούνται για τον προμηθευτή είναι: εργολάβος, παραγωγός, πωλητής ή προμηθευτής (vendor).
    - Σημείωση 2: Ο αγοραστής και ο προμηθευτής μπορούν να ανήκουν στον ίδιο οργανισμό.
    - Σημείωση 3: Οι τύποι προμηθευτών περιλαμβάνουν οργανισμούς που επιτρέπουν διαπραγμάτευση συμφωνιών με τον αγοραστή, καθώς και εκείνους που δεν την επιτρέπουν, π.χ. συμφωνίες άδειας τελικού χρήστη, όρους χρήσης ή κοινοποιήσεις πνευματικής ιδιοκτησίας/άδειες ανοιχτού κώδικα.
- **Αγοραστής (Acquirer):** Οποιοσδήποτε λαμβάνει προϊόντα ή υπηρεσίες από τρίτο μέρος.
    - Σημείωση 1: Η παροχή μπορεί ή και όχι να περιλαμβάνει νομισματικά κονδύλια.
- **Συμφωνία (Agreement):** Αμοιβαία αναγνώριση όρων και προϋποθέσεων υπό τους οποίους διεξάγεται μια σχέση συνεργασίας.
- **Εφοδιαστική Αλυσίδα (Supply Chain):** Σύνολο οργανισμών που συνδέονται μέσω συνόλου πόρων και διαδικασιών, όπου κάθε οργανισμός λειτουργεί είτε ως αγοραστής, προμηθευτής, είτε και τα δύο, προκειμένου να σχηματίσουν διαδοχικές σχέσεις προμηθευτή που εγκαθίστανται με την τοποθέτηση εντολών αγοράς, συμφωνιών ή άλλων επίσημων συμφωνιών προμήθειας.
    - Σημείωση 1: Η εφοδιαστική αλυσίδα μπορεί να περιλαμβάνει πωλητές, εργοστάσια παραγωγής, παρόχους μεταφορών και logistics, κέντρα διανομής, χονδρεμπόρους, και άλλους οργανισμούς που συμμετέχουν στην παραγωγή, επεξεργασία, σχεδίαση και ανάπτυξη, καθώς και στη διαχείριση και παροχή των προϊόντων ή υπηρεσιών.

- Σημείωση 2: Η ορατότητα της εφοδιαστικής αλυσίδας είναι σχετική με τη θέση του αγοραστή.

- **Σχέση Προμηθευτή (Supplier Relationship):** Συμφωνία ή συμφωνίες μεταξύ των αγοραστών και των προμηθευτών για τη διεξαγωγή επιχειρηματικής δραστηριότητας, την παροχή προϊόντων ή υπηρεσιών και την επίτευξη επιχειρηματικού οφέλους.

**Ορισμοί από NIST SP 800-161 Revision 1** [29]

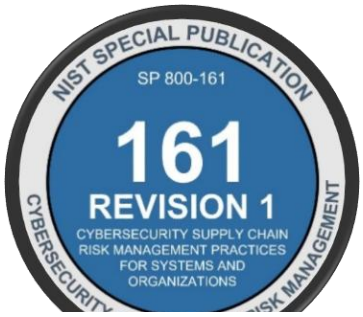
- **Εφοδιαστική αλυσίδα (supply chain):** Το διασυνδεδεμένο σύνολο πόρων και διαδικασιών μεταξύ και εντός πολλαπλών επιπέδων ενός οργανισμού ή επιχείρησης, όπου κάθε επίπεδο λειτουργεί ως αγοραστής (acquirer). Η αλυσίδα ξεκινά από την προμήθεια προϊόντων και υπηρεσιών και εκτείνεται σε όλο τον κύκλο ζωής τους.
- **Κίνδυνοι Κυβερνοασφάλειας στην Εφοδιαστική Αλυσίδα (Cybersecurity Risks throughout the Supply Chain):** Πιθανές βλάβες ή παραβιάσεις που μπορεί να προκύψουν από προμηθευτές, τις δικές τους εφοδιαστικές αλυσίδες, τα προϊόντα ή τις υπηρεσίες τους. Οι Κυβερνοκίνδυνοι προκύπτουν από απειλές που εκμεταλλεύονται τρωτά σημεία εντός των προϊόντων και υπηρεσιών που διακινούνται κατά μήκος της αλυσίδας ή από αδυναμίες στο ίδιο το δίκτυο της αλυσίδας.
- **Διαχείριση Κινδύνων Κυβερνοασφάλειας στην Εφοδιαστική Αλυσίδα (Cybersecurity Supply Chain Risk Management - C-SCRM):** Η διαχείριση των κινδύνων Κυβερνοασφάλειας που σχετίζονται με προϊόντα και υπηρεσίες ICT και OT καθ' όλο τον κύκλο ζωής τους. Η C-SCRM αποτελεί το σημείο σύγκλισης της παραδοσιακής διαχείρισης κινδύνων της εφοδιαστικής αλυσίδας (SCRM) με την ασφάλεια πληροφοριών και περιλαμβάνει ενέργειες για την αναγνώριση, αξιολόγηση και μετριασμό των κινδύνων. Εφαρμόζεται τόσο σε περιβάλλοντα πληροφορικής (IT) όσο και λειτουργικής τεχνολογίας (OT), καθώς και στο διαδίκτυο των πραγμάτων (IoT).

Η κατανόηση αυτών των βασικών εννοιών είναι κρίσιμη για την αποτίμηση και σύγκριση των υφιστάμενων διεθνών προτύπων που σχετίζονται με την Κυβερνοασφάλεια στην εφοδιαστική αλυσίδα. Στην επόμενη ενότητα, παρουσιάζεται αναλυτικά η προσέγγιση του NIST SP 800-161r1, όπως αυτή εκφράζεται μέσω των βασικών αρχών, πλαισίων και ελέγχων που προτείνει για την αποτελεσματική υλοποίηση C-SCRM σε οργανισμούς.

# 3. NIST SP 800-161 REVISION 1

## 3.1 Εισαγωγή στο Nist SP 800-161r1

Ο National Institute of Standards and Technology (NIST) ανέπτυξε το Special Publication (SP) 800-161r1, με τίτλο «**Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations**». Το πλαίσιο αυτό παρέχει κατευθυντήριες γραμμές για τη διαχείριση και τον μετριασμό των κινδύνων Κυβερνοασφάλειας στην εφοδιαστική αλυσίδα **(C-SCRM)**. Το πρότυπο δημοσιεύτηκε τον Μάιο του 2022 και ευθυγραμμίζεται με νομοθεσίες και ρυθμίσεις Κυβερνοασφάλειας των ΗΠΑ, όπως ο FISMA και το Executive Order 14028 on Improving the Nation's Cybersecurity.




*Εικόνα 3: NIST SP 800-161 Revision 1*

*Πηγή: https://www.linkedin.com/*

Το NIST SP 800-161r1 προσφέρει έναν συστηματικό τρόπο ενσωμάτωσης του C-SCRM στη διαχείριση κινδύνων Κυβερνοασφάλειας ενός οργανισμού.

Περιλαμβάνει μια προσέγγιση 4 φάσεων διαχείρισης κινδύνου, καθώς πρώτα καθορίζονται οι κίνδυνοι, έπειτα αξιολογούνται, ακολουθεί η υλοποίηση κατάλληλων μέτρων για τον μετριασμό τους και τέλος χρειάζεται η παρακολούθηση της ορθής λειτουργίας της διαδικασίας.

Επιπλέον, το πλαίσιο ενσωματώνει μέτρα ασφαλείας από το **NIST SP 800-53 Rev. 5**, καλύπτοντας τομείς όπως:

- Αξιολόγηση προμηθευτών (Supplier Risk Assessment)
- Πολιτικές ασφαλούς προμηθειών (Secure acquisition policies)
- Αντίδραση σε περιστατικά Κυβερνοασφάλειας (Incident Response)
- Έλεγχος πρόσβασης και παρακολούθηση εφοδιαστικής αλυσίδας (Access control & supply chain monitoring)

Μέσω της εφαρμογής του NIST SP 800 - 161 r1, οι Οργανισμοί θα επιτύχουν μεγαλύτερη διαφάνεια και ανθεκτικότητα στην αλυσίδα εφοδιασμού, μειώνοντας έτσι την πιθανότητα έκθεσής τους σε σχετικές Κυβερνοεπιθέσεις και τους κινδύνους που προκαλούνται από τους συνεργάτες τους. Τέλος, θα είναι σε θέση να εναρμονιστούν με διεθνείς και εθνικές ρυθμιστικές απαιτήσεις.

Αν και το πρότυπο σχεδιάστηκε κυρίως για ομοσπονδιακές υπηρεσίες των ΗΠΑ, μπορεί να χρησιμοποιηθεί από ιδιωτικές εταιρείες, παρόχους υπηρεσιών, και διεθνείς οργανισμούς που θέλουν να προστατεύσουν τις ICT και OT εφοδιαστικές αλυσίδες τους. [29]

## 3.2 Δομή Προτύπου

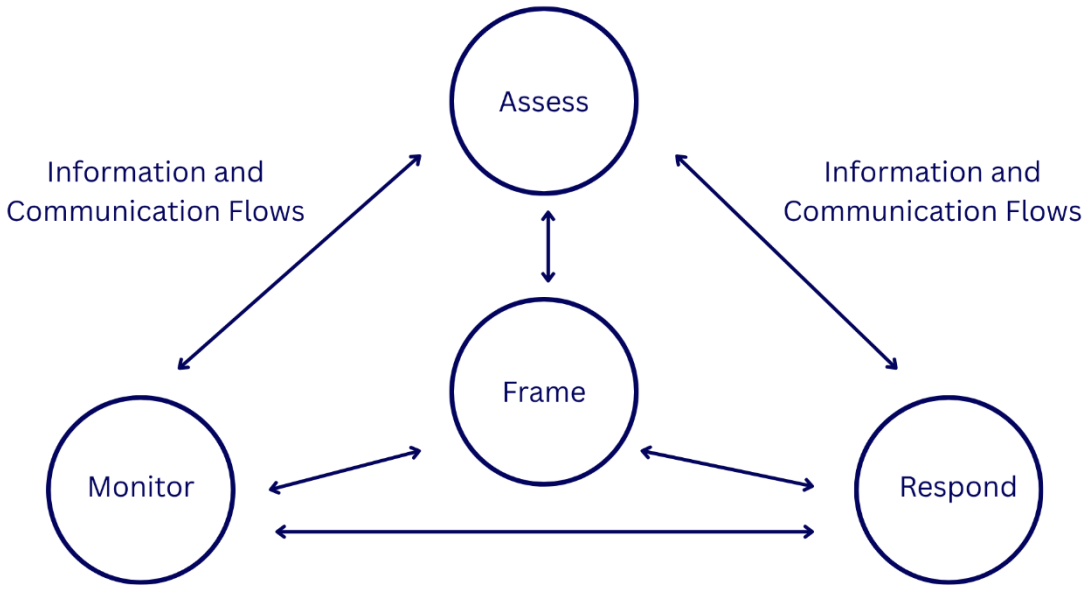
Το NIST SP 800-161r1, παρέχει μια συστηματική προσέγγιση στη C-SCRM. Το κύριο μέρος του προτύπου, αποτελείται από τρείς ενότητες, όπου κάθε μία προσφέρει αναλυτικές οδηγίες για την αναγνώριση, την αξιολόγηση και τον μετριασμό των κινδύνων Κυβερνοασφάλειας που αφορούν την εφοδιαστική αλυσίδα των συστημάτων ICT και OT.

Στην πρώτη ενότητα του προτύπου, εισάγονται οι έννοιες της C-SCRM, ενώ παράλληλα εκφράζεται η ανάγκη ύπαρξης της αφού οι απειλές που αντιμετωπίζουν οι Οργανισμοί, ολοένα και αυξάνονται. Επιπλέον, καθορίζονται οι βασικές αρχές διαχείρισης κινδύνων, καθώς και η σημασία ενσωμάτωσης της C-SCRM στην ολική στρατηγική των Οργανισμών για την Κυβερνοασφάλεια.

Η δεύτερη ενότητα αποτελεί τον βασικό κορμό του προτύπου, καθώς περιγράφεται αναλυτικά η ενσωμάτωση της C-SCRM στη διαχείριση κινδύνων.

Η προσέγγιση αυτή περιλαμβάνει 4 φάσεις

1. **Frame Risk**: Καθορισμός του πλαισίου και των πιθανών απειλών της εφοδιαστικής αλυσίδας.
2. **Assess Risk**: Αξιολόγηση ευπαθειών και πιθανών επιθέσεων.
3. **Respond to Risk**: Εφαρμογή μέτρων μετριασμού των κινδύνων.
4. **Monitor Risk**: Συνεχής παρακολούθηση και διατήρηση.




*Σχήμα 1: Nist SP 800 161r1 - Διαδικασία Διαχείρισης Κινδύνου*

Για τη σωστή και αποτελεσματική υλοποίηση της προσέγγισης, παρέχονται μεθοδολογίες και αναλυτικές οδηγίες για κυβερνητικούς φορείς, ιδιωτικές επιχειρήσεις και τεχνολογικούς παρόχους.

Στην εν λόγω ενότητα, παρουσιάζονται επίσης τα τρία επίπεδα ενσωμάτωσης της C-SCRM στον Οργανισμό:

- Επιχειρησιακό επίπεδο (Enterprise level)
- Επίπεδο επιχειρησιακών διαδικασιών (Mission and Business Process level)
- Λειτουργικό επίπεδο (Operational level)

Στην τρίτη ενότητα περιγράφονται τα προτεινόμενα μέτρα ασφάλειας συνοδευόμενα από την πρακτική εφαρμογής τους. Τα μέτρα ασφαλείας χωρίζονται σε συγκεκριμένες

κατηγορίες, όπως η αξιολόγηση κινδύνων προμηθευτών, η ασφαλής ανάπτυξη λογισμικού, η παρακολούθηση της ακεραιότητας των συστημάτων και οι συμβατικές απαιτήσεις ασφάλειας. Επιπλέον, προσφέρεται μια μεθοδολογία επιλογής και προσαρμογής των μέτρων, βοηθώντας τους οργανισμούς να ευθυγραμμίσουν τις πολιτικές ασφάλειάς τους με τις επιχειρησιακές τους ανάγκες.

Πέραν του βασικού περιεχόμενο, το NIST SP 800-161r1 περιλαμβάνει παραρτήματα που παρέχουν προτεινόμενα εργαλεία, πρότυπα εγγράφων και πρόσθετες παραπομπές για την εφαρμογή της C-SCRM.

- **Annex A: C-SCRM Security Controls**: Περιγράφει τα βασικά μέτρα ασφαλείας που πρέπει να εφαρμόζουν οι οργανισμοί.
- **Annex B: Control Summary**: Καταγράφονται τα συστήματα ελέγχου ασφαλείας σε σχέση με τις λειτουργίες διαχείρισης κινδύνων.
- **Annex C: Risk Exposure Framework**: Παρουσιάζονται παραδείγματα σεναρίων κινδύνου και μοντέλα λήψης αποφάσεων.
- **Annex D: C-SCRM Templates**: Περιλαμβάνει πρότυπα εγγράφων για τη στρατηγική C-SCRM, την αξιολόγηση κινδύνων και την εφαρμογή πολιτικών ασφαλείας.
- **Annex E: Federal Acquisition Supply Chain Security Act (FASCSA) Compliance**: Εξηγούνται οι απαιτήσεις κυβερνητικών προμηθειών των ΗΠΑ.
- **Annex F: Software Supply Chain Security Guidelines**: Αναφέρεται στην ασφάλεια του λογισμικού στην εφοδιαστική αλυσίδα, σε απάντηση στο Executive Order 14028.
- **Annex G: C-SCRM Activities in the Risk Management Process**: Περιγράφει πώς η C-SCRM ενσωματώνεται στο Risk Management Framework (RMF) του NIST.
- **Annex H: Glossary**: Περιλαμβάνει έναν λεξικογραφικό οδηγό βασικών όρων που χρησιμοποιούνται στο πρότυπο.
- **Annex I: Acronyms**: Παρέχεται ένας πίνακας τεχνικών συντομογραφιών και ρυθμιστικών όρων.
- **Annex J: Resources**: Παραθέτει σχετικά πρότυπα NIST, βιομηχανικά πρότυπα και κανονισμούς που σχετίζονται με την ασφάλεια της εφοδιαστικής αλυσίδας.

Η συνολική δομή του προτύπου εξασφαλίζει ότι λειτουργεί τόσο ως θεωρητικό πλαίσιο όσο και ως πρακτικός οδηγός. Παρέχει στους Οργανισμούς τη δυνατότητα να υιοθετήσουν και να προσαρμόσουν πρακτικές ασφαλείας στην εφοδιαστική αλυσίδα με βάση τις δικές τους ανάγκες και το επίπεδο κινδύνου. [29]

## 3.3 Πλαίσιο Διαχείρισης Κινδύνων στο NIST SP 800-161r1

### 3.3.1 Ενσωμάτωση του C-SCRM στη διαχείριση κινδύνων σε επιχειρησιακό επίπεδο

Η 2η ενότητα του προτύπου με τίτλο **“Integration of C-S into Enterprise-Wide Risk Management”** περιγράφει τη διαδικασία ενσωμάτωσης της C-SCRM στη διαχείριση

κινδύνων σε επιχειρησιακό επίπεδο, όπως περιγράφεται στο **NIST SP 800-39**. Η διαδικασία αυτή περιλαμβάνει τέσσερα συνεχή και επαναληπτικά βήματα, τα οποία ενισχύουν την αποτελεσματική διαχείριση των κινδύνων που σχετίζονται με την εφοδιαστική αλυσίδα.

Τα βήματα που ακολουθούνται είναι:

1. **Καθορισμός του Πλαισίου Κινδύνων (Frame Risk):** Το πρώτο βήμα της διαδικασίας, αφορά τον καθορισμό του πλαισίου, στο οποίο θα πρέπει να καθορίζεται το πλαίσιο στο οποίο θα πραγματοποιηθεί η διαχείριση κινδύνων. Αρχικά, οι Οργανισμοί πρέπει να κατανοήσουν το επίπεδο Κυβερνοασφάλειας, τη λειτουργία και δομή των πληροφοριακών τους υποδομών που υπάγονται αλλά και επηρεάζουν την εφοδιαστική αλυσίδα. Μετά από αυτή την ανάλυση θα είναι δυνατή η αναγνώριση των κινδύνων και ευπαθειών στην εφοδιαστική αλυσίδα.
2. **Αξιολόγηση Κινδύνων (Assess Risk)**: Μετά τον καθορισμό του πλαισίου κινδύνων, οι Οργανισμοί θα πρέπει να αξιολογήσουν και ταξινομήσουν τους κινδύνους, αναγνωρίζοντας τους προμηθευτές υψηλής επικινδυνότητας. Η ταξινόμηση των κινδύνων ανάλογα το επίπεδο κρισιμότητας των αγαθών του Οργανισμού, θα ορίσει ποιοι κίνδυνοι θα πρέπει να μετριαστούν άμεσα και ποιοι είναι εντός των αποδεκτών ορίων του Οργανισμού.
3. **Αντίδραση στον Κίνδυνο (Respond to Risk)**: Ακολουθεί η διαδικασία αντιμετώπισης των κίνδυνων, όπου οι Οργανισμοί θα πρέπει να εφαρμόσουν αντίμετρα με σκοπό τον μετριασμό του επιπέδου του κίνδυνου.
4. **Παρακολούθηση του Κινδύνου (Monitor Risk)**: Η διαχείριση κινδύνων είναι μια συνεχής διαδικασία, και οι οργανισμοί πρέπει να παρακολουθούν διαρκώς αλλαγές στο περιβάλλον της εφοδιαστικής τους αλυσίδας. Αυτό περιλαμβάνει την ανίχνευση νέων απειλών, την αξιολόγηση της αποτελεσματικότητας των μέτρων ασφαλείας και την αναπροσαρμογή στρατηγικών διαχείρισης κινδύνων. Η ύπαρξη μηχανισμών ανατροφοδότησης (feedback loop) επιτρέπει στους οργανισμούς να βελτιώνουν διαρκώς τις πρακτικές τους, έχοντας γνώμονα τα αποτελέσματα από προηγούμενα περιστατικά ασφαλείας.

Η διαχείριση κινδύνων Κυβερνοασφάλειας στην εφοδιαστική αλυσίδα είναι μια σύνθετη και απαιτητική διαδικασία που απαιτεί την ύπαρξη μίας Κουλτούρας εντός του Οργανισμού που να την ευνοεί. Παρόλα αυτά, μία C-SCRM για να καθίσταται αποτελεσματική δεν αρκεί μόνο τη συνεισφορά του οργανισμού, αλλά και τη συνεργασία των προμηθευτών και τρίτων μερών. Συμπερασματικά, υπάρχει η ανάγκη για μια δομημένη και συνεχή προσέγγιση, που περιλαμβάνει τον καθορισμό κρίσιμων επιχειρησιακών λειτουργιών, την αξιολόγηση κινδύνων προμηθευτών, την εφαρμογή μέτρων μετριασμού των κινδύνων και τη συνεχή παρακολούθηση και ενημέρωση για επερχόμενες απειλές.

Δεδομένου ότι οι κίνδυνοι της εφοδιαστικής αλυσίδας διαφέρουν ανάλογα με τον κλάδο, οι οργανισμοί πρέπει να προσαρμόζουν τη C-SCRM στις επιχειρησιακές τους ανάγκες. Επιπλέον, ένα καλά οργανωμένο πλαίσιο διαχείρισης κινδύνων εφοδιαστικής αλυσίδας δεν αποσκοπεί στην εξάλειψη αυτών, αλλά στη διαχείρισή τους, εξασφαλίζοντας ότι οι Οργανισμοί μπορούν να προσαρμόζονται σε νέες απειλές, να ανταποκρίνονται σε εσωτερικές αλλαγές και να ευθυγραμμίζονται με την εξελισσόμενη παγκόσμια εφοδιαστική αλυσίδα ICT.

#### 3.3.1.1 Πολυεπίπεδη διαχείριση κινδύνων

Η Πολυεπίπεδη Διαχείριση Κινδύνων σε Επιχειρησιακό Επίπεδο διασφαλίζει ότι η Διαχείριση Κινδύνων Κυβερνοασφάλειας στην Εφοδιαστική Αλυσίδα (C-SCRM) εφαρμόζεται με συνέπεια σε όλο τον οργανισμό, προωθώντας παράλληλα τη συνεχή βελτίωση και την αποτελεσματική επικοινωνία μεταξύ των ενδιαφερομένων μερών. Αυτό το μοντέλο διαχωρίζει τις δραστηριότητες της C-SCRM σε επίπεδα με ιεραρχική ταξινόμηση, επιτρέποντας την εφαρμογή στρατηγικών διαχείρισης κινδύνου ανάλογα με τη δομή και τις επιχειρησιακές ανάγκες του οργανισμού.

Η δομή χωρίζεται σε τρία ιεραρχικά επίπεδα καθορίζοντας διαφορετικούς ρόλους και αρμοδιότητες σε κάθε ένα από αυτά, διασφαλίζοντας ότι οι ενέργειες διαχείρισης κινδύνου είναι ευθυγραμμισμένες και προσαρμόζονται σε όλα τα στρώματα του οργανισμού.

1. **Επίπεδο 1: Επιχειρησιακό Επίπεδο (Enterprise Level):** Στο επίπεδο 1 της πυραμίδας, η διοίκηση καθορίζει τη συνολική στρατηγική C-SCRM, το πλαίσιο διακυβέρνησης και το σχέδιο εφαρμογής. Στο σημείο αυτό η διοίκηση πρέπει να αναπτύξει μια συνεκτική στρατηγική C-SCRM που να εναρμονίζεται με τους επιχειρηματικούς της στόχους και να ενσωματώνεται στη γενική διαχείριση κινδύνων (Enterprise Risk Management - ERM). Σημαντική είναι η καθιέρωση κατάλληλων δομών διακυβέρνησης και του λειτουργικού μοντέλου, που θα διασφαλίζουν σαφή κατανομή ρόλων και ευθυνών, καθώς και η διαμόρφωση πολιτικών που θέτουν το αποδεκτό επίπεδο κινδύνου (risk appetite). Παράλληλα, πρέπει να θεσπιστούν υψηλού επιπέδου πολιτικές, στόχοι και βασικοί δείκτες απόδοσης (KPIs), ώστε να αξιολογείται η αποτελεσματικότητα της C-SCRM. Οι αποφάσεις που λαμβάνονται στο επιχειρησιακό επίπεδο αφορούν τη στρατηγική συνεργασίας με προμηθευτές, την υιοθέτηση τεχνολογικών εργαλείων ασφαλείας και την ενίσχυση της ανθεκτικότητας της εφοδιαστικής αλυσίδας. Επιπλέον, η διαμόρφωση ενός C-SCRM Program Management Office (PMO) εξασφαλίζει τον συντονισμό και τη συνεχή επίβλεψη των σχετικών διαδικασιών.

   Οι βασικοί ενδιαφερόμενοι περιλαμβάνουν πρωτίστως την ανώτατη ηγεσία (Executive Leadership) της επιχείρησης, συμπεριλαμβανομένων του CEO, CIO, COO, CFO, CISO, CTO, CAO, CPO, CRO και άλλων στελεχών με καθοριστικό ρόλο στη διαχείριση κινδύνων και στη στρατηγική ασφάλειας.

1. **Επίπεδο 2: Επίπεδο Επιχειρησιακών Διαδικασιών (Mission and Business Process Level):** Το μεσαίο επίπεδο επικεντρώνεται στην ανάπτυξη στρατηγικών, πολιτικών και διαδικασιών που προσαρμόζονται στις ανάγκες της C-SCRM κάθε επιχειρησιακής διαδικασίας. Οι αρμόδιες ομάδες διαμορφώνουν κατευθυντήριες γραμμές και περιορισμούς, οι οποίοι διασφαλίζουν ότι τα νέα έργα πληροφορικής και οι σχετικές προμήθειες υλοποιούνται με τα ελάχιστα κενά ασφαλείας από την έναρξη του έργου.

   Σε αυτό το επίπεδο, αξιολογούνται ευπάθειες και αδυναμίες που προκύπτουν από τεχνικούς, ανθρώπινους ή οργανωτικούς παράγοντες, οι οποίοι ενδέχεται να εκθέσουν τον Οργανισμό σε Κυβερνοεπιθέσεις. Παράλληλα, καθορίζεται ένα σχέδιο C-SCRM, το οποίο ενσωματώνεται στο γενικότερο πλαίσιο διαχείρισης κινδύνων του Οργανισμού. Αυτό σημαίνει ότι προσδιορίζονται επίπεδα ανοχής κινδύνου (risk tolerances) προσαρμοσμένα στις εκάστοτε ανάγκες κάθε επιχειρησιακής διαδικασίας.

Η διαχείριση κινδύνων πραγματοποιείται σε συνεχή βάση, ενώ οι αρμόδιες ομάδες συνεργάζονται στενά με το C-SCRM Program Management Office (PMO) κυρίως, αλλά όχι μόνο, μέσω ανταλλαγής πληροφοριών. Επιπλέον, το επίπεδο επιχειρησιακών διαδικασιών λειτουργεί ως συνδετικός κρίκος μεταξύ του 1ου και 3ου επιπέδου διασφαλίζοντας ότι οι αποφάσεις και οι στρατηγικές που καθορίζονται από τη διοίκηση εφαρμόζονται και αξιολογούνται σε πρακτικό επίπεδο. Η διαδικασία αυτή περιλαμβάνει τη συνεχή αναφορά προς το ανώτατο επίπεδο και την ανάλυση δεδομένων από το λειτουργικό επίπεδο της πυραμίδας, διασφαλίζοντας έτσι την αποτελεσματικότητα της C-SCRM σε ολόκληρη την επιχείρηση.

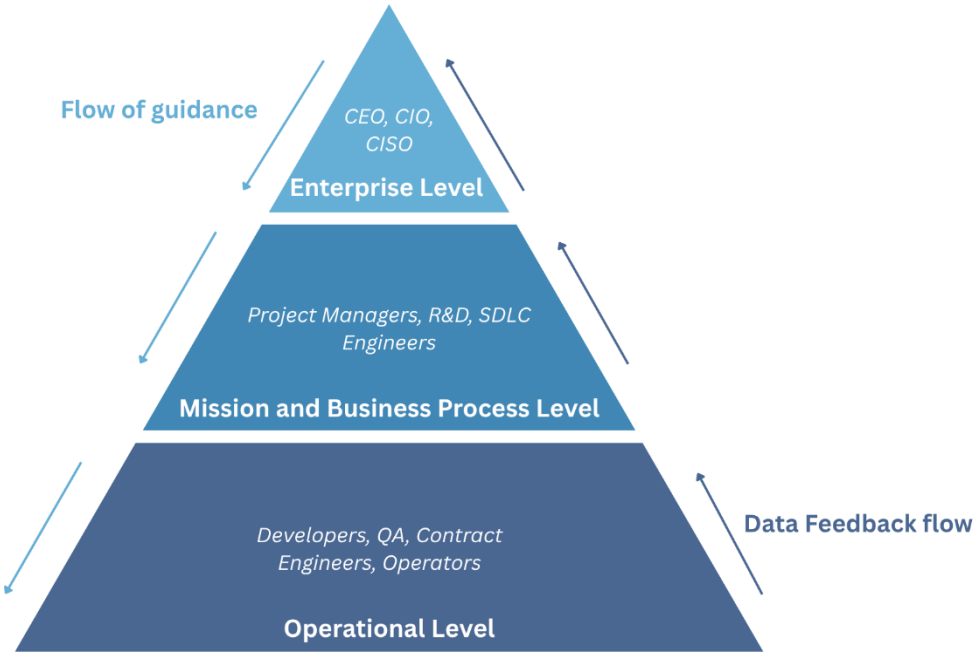
Οι βασικοί εμπλεκόμενοι σε αυτό το επίπεδο περιλαμβάνουν τη Διοίκηση Επιχειρησιακών Διαδικασιών (Business Management), η οποία αποτελείται από Program Managers (PMs), Project Managers, μέλη Integrated Project Teams (IPTs), ειδικούς Έρευνας και Ανάπτυξης (R&D), μηχανικούς επιφορτισμένους με την εποπτεία του Software Development Life Cycle (SDLC), καθώς και στελέχη υπεύθυνα για τη διαχείριση προμηθειών, την κοστολόγηση, την αξιοπιστία, την ασφάλεια, την ποιότητα και άλλους τομείς που σχετίζονται με το C-SCRM PMO.

2. **Επίπεδο 3: Λειτουργικό Επίπεδο (Operational Level):** Στο τρίτο και τελευταίο επίπεδο, πραγματοποιείται η πρακτική υλοποίηση του C-SCRM στις τεχνολογικές και λειτουργικές διαδικασίες ενός οργανισμού. Σε αυτό το σημείο, εξειδικευμένες ομάδες εργάζονται για την ανάπτυξη C-SCRM σχεδίων (C-SCRM plans) και την εφαρμογή των σχετικών πολιτικών και απαιτήσεων που έχουν καθοριστεί από τα ανώτερα επίπεδα (Enterprise Level & Mission and Business Process Level).

   Οι δραστηριότητες σε αυτό το επίπεδο περιλαμβάνουν την προσαρμογή των C-SCRM στρατηγικών και πολιτικών στο πλαίσιο συγκεκριμένων συστημάτων και την ενσωμάτωσή τους σε ολόκληρο τον κύκλο ζωής ανάπτυξης λογισμικού. Οι υπεύθυνοι του Λειτουργικού επιπέδου δεσμεύονται να πράττουν εντός των καθορισμένων περιορισμών και απαιτήσεων που τίθενται από τα ανώτερα στρώματα, ενώ παράλληλα διασφαλίζουν ότι οι πολιτικές εφαρμόζονται αποτελεσματικά σε κάθε στάδιο του τεχνολογικού και επιχειρησιακού περιβάλλοντος.

   Επιπλέον, το κατώτερο στρώμα κατέχει κρίσιμο ρόλο στην αναφορά δεδομένων και αναλύσεων C-SCRM προς το 2ο. Η συνεχής ροή πληροφοριών προς το 2ο επίπεδο διασφαλίζει ότι η στρατηγική διαχείρισης κινδύνων βασίζεται σε ρεαλιστικά δεδομένα από το πεδίο εφαρμογής και μπορεί να προσαρμόζεται στις νέες προκλήσεις και απειλές του κυβερνοχώρου.

   Το εν λόγω επίπεδο, αφορά κυρίως ειδικούς όπως αρχιτέκτονες συστημάτων, προγραμματιστές, ιδιοκτήτες συστημάτων, ειδικούς διασφάλισης ποιότητας (QA/QC), προσωπικό δοκιμών, υπεύθυνους συμβάσεων, μηχανικούς ελέγχου και χειριστές συστημάτων ελέγχου. [29]




*Σχήμα 2: Ιεραρχικά επίπεδα εφαρμογής της διαχείρισης κυβερνοκινδύνων στην αλυσίδα εφοδιασμού (C-SCRM)*

### 3.3.1.2 CSCRM PMO

Το Γραφείο Διαχείρισης Έργου για την Ασφάλεια της Εφοδιαστικής Αλυσίδας του Κυβερνοχώρου (C-SCRM PMO) που αναφέρθηκε παραπάνω, αποτελεί ένα κεντρικό όργανο που διευκολύνει τη διαχείριση των κινδύνων της εφοδιαστικής αλυσίδας σε επίπεδο επιχείρησης και επιχειρησιακών διαδικασιών.

Ο σκοπός αυτός, μπορεί να ικανοποιηθεί με τον ορισμό διάφορων μοντέλων λειτουργίας (π.χ. κεντρικοποιημένο, αποκεντρωμένο, υβριδικό). Παρόλα αυτά, το πιο αποδοτικά θεωρείται το κεντρικό C-SCRM PMO, όπου συγκεντρώνονται και ανατίθενται αρμοδιότητες για συγκεκριμένες δραστηριότητες C-SCRM, λειτουργώντας ως πάροχος υπηρεσιών για τις επιχειρησιακές διαδικασίες. Το C-SCRM PMO παρέχει υπηρεσίες όπως συμβουλευτική υποστήριξη, αξιολόγηση κινδύνων προμηθευτών και προϊόντων, διαχείριση μητρώου κινδύνων, συντονισμό πληροφοριών, εκπαίδευση, και αναφορές προς τα εκτελεστικά στελέχη.

Το PMO αποτελείται από εξειδικευμένους επαγγελματίες, οι οποίοι καθοδηγούν τη στρατηγική και την υλοποίηση της C-SCRM. Αναφέρεται ή περιλαμβάνει ανώτατα διοικητικά στελέχη και αντιπροσωπεύει διαφορετικούς τομείς, όπως την ασφάλεια πληροφοριών, τις προμήθειες, τη διαχείριση κινδύνων, τις νομικές υπηρεσίες και το ανθρώπινο δυναμικό.

Στο επιχειρησιακό επίπεδο, το PMO μπορεί να υποστηρίζει τη χάραξη στρατηγικής και πολιτικής C-SCRM, τον ορισμό του επιπέδου ανοχής κινδύνου, καθώς και την επικοινωνία και επεξήγηση των κινδύνων στα διοικητικά στελέχη. Στο επίπεδο επιχειρησιακών διαδικασιών, αναπτύσσονται πρότυπα στρατηγικής, διαδικασίες και οδηγίες, συμβάλλοντας στη δημιουργία και προσαρμογή σχεδίων C-SCRM. Παράλληλα, το PMO διενεργεί αξιολογήσεις κινδύνου προμηθευτών και παρόχων υπηρεσιών, υποστηρίζοντας την προστασία της εφοδιαστικής αλυσίδας από Κυβερνοαπειλές.

Τέλος, το PMO επηρεάζει και το Λειτουργικό επίπεδο, παρέχοντας καθοδήγηση σε ομάδες που διαχειρίζονται τεχνικά έργα, συμβάλλοντας στην επιλογή και προσαρμογή των κατάλληλων μέτρων ελέγχου C-SCRM.

Η ολική διαχείριση μέσω ενός C-SCRM PMO προσφέρει σημαντικά οφέλη, καθώς το συγκεκριμένο μοντέλο είναι ιδιαίτερα βοηθητικό για μεγάλους και πολύπλοκους οργανισμούς που απαιτούν εναρμονισμένες και ενοποιημένες πρακτικές C-SCRM σε ένα ευρύ φάσμα λειτουργιών και επιχειρησιακών διαδικασιών. Ωστόσο, κάθε επιχείρηση θα πρέπει να επιλέξει το κατάλληλο μοντέλο σύμφωνα με τους διαθέσιμους πόρους και το επιχειρηματικό της περιβάλλον. [29]

### 3.3.2 Παράγοντες υψηλής κρισιμότητας για την επιτυχία της C-SCRM

Η εφαρμογή της C-SCRM περιλαμβάνει πολλαπλούς παράγοντες υψηλής κρισιμότητας που διασφαλίζουν την ανθεκτικότητα του Οργανισμού απέναντι σε κινδύνους της εφοδιαστικής αλυσίδας.

1. **Εφαρμογή της C-SCRM κατά την απόκτηση ενός αγαθού / υπηρεσίας:** Η αποτελεσματική ενσωμάτωση της C-SCRM ξεκινά με τον προσδιορισμό των επιχειρησιακών αναγκών και εκτείνεται μέχρι την ανάπτυξη απαιτήσεων, την επιλογή προμηθευτών, την ανάθεση συμβάσεων και την συνεχή παρακολούθηση της απόδοσης της υπηρεσίας. Αυτή η ολιστική προσέγγιση εξασφαλίζει ότι οι απαιτήσεις Κυβερνοασφάλειας ενσωματώνονται στρατηγικά στον σχεδιασμό, την εκτέλεση και την επίβλεψη των διαδικασιών που σχετίζονται με τις προμήθειες.

   Οι οργανισμοί οφείλουν να λαμβάνουν την C-SCRM ως θεμελιώδες στοιχείο του σχεδιασμού προμηθειών, ξεκινώντας με την αξιολόγηση της κρισιμότητας προϊόντων και υπηρεσιών και τον καθορισμό αποδεκτών επιπέδων κινδύνου. Παράλληλα, οι οργανισμοί οφείλουν να εφαρμόζουν ειδικούς μηχανισμούς για τις προμήθειες, όπως καταλόγους εγκεκριμένων προϊόντων και προμηθευτών, λίστες απαγορευμένων πηγών και τυποποιημένα ερωτηματολόγια αξιολόγησης προμηθευτών.

   Κατά τη φάση απόκτησης, είναι απαραίτητο να διεξάγεται έρευνα αγοράς με βάση την Κυβερνοασφάλεια, με στόχο την αξιολόγηση του προφίλ κινδύνου υποψήφιων προμηθευτών. Αυτό περιλαμβάνει την ανάλυση εξαρτήσεων της εφοδιαστικής αλυσίδας, γεωπολιτικών παραμέτρων, της ακεραιότητας του λογισμικού και του ιστορικού συμμόρφωσης ή περιστατικών παραβίασης. Τα άτομα που είναι αρμόδια για την προμήθεια, συμπεριλαμβανομένων των συμβασιούχων υπαλλήλων, τεχνικών ειδικών και υπευθύνων Κυβερνοασφάλειας, πρέπει να αξιολογούν τις προσφορές των διαφόρων προμηθευτών με βάση κριτήρια C-SCRM, αποφεύγοντας στρατηγικές επιλογής όπως η “χαμηλότερη τεχνικά αποδεκτή τιμή ” (LPTA), ιδιαίτερα για προϊόντα και υπηρεσίες ICT ή OT.

   Μετά την ανάθεση της σύμβασης, απαιτείται συνεχής παρακολούθηση για να διασφαλιστεί η συνεχής συμμόρφωση των προμηθευτών με τις απαιτήσεις C-SCRM του Οργανισμού. Αυτό περιλαμβάνει την επιβολή των απαιτήσεων και στους υπεργολάβους, τον έλεγχο συμμόρφωσης μέσω επιθεωρήσεων ή εξωτερικών αξιολογήσεων, καθώς και μηχανισμούς αναφοράς για περιστατικά ασφαλείας ή αλλαγές στο προφίλ κινδύνου του προμηθευτή. Οι συμβάσεις πρέπει να προβλέπουν διαδικασίες επαναξιολόγησης, διορθωτικών ενεργειών και δυνατότητα λύσης της σύμβασης σε περίπτωση μη αποδεκτού επιπέδου κινδύνου. Παράλληλα, ο οργανισμός οφείλει να διατηρεί δυναμικό κατάλογο των

σχέσεων με προμηθευτές, κατηγοριοποιημένο βάσει κρισιμότητας, ώστε να υποστηρίζεται η στοχευμένη εφαρμογή στρατηγικών C-SCRM.

Η επιτυχής εφαρμογή της C-SCRM εντός του πλαισίου των προμηθειών προϋποθέτει επίσης την ύπαρξη υποστήριξης από τη διοίκηση που αυτό συνεπάγεται την προσφορά των απαραίτητων πόρων. Η Διοίκηση πρέπει να δεσμευτεί ως προς την εξασφάλιση οικονομικών πόρων, κατάλληλη εκπαίδευση του προσωπικού και σαφή καθορισμό ρόλων και αρμοδιοτήτων σε όλα τα εμπλεκόμενα τμήματα. Επιπλέον, οι οργανισμοί πρέπει να αναπτύξουν επίσημη Στρατηγική και Σχέδιο Εφαρμογής της C-SCRM, τα οποία να εστιάζουν στην αντιστοίχιση των υφιστάμενων πρακτικών με τους επιθυμητούς στόχους ασφαλείας και τον εντοπισμό ευπαθειών.

Τέλος, μέσω της ενσωμάτωσης της C-SCRM στις πολιτικές, διαδικασίες και την κουλτούρα των προμηθευτών, οι οργανισμοί επιτυγχάνουν ενισχυμένη ορατότητα, έλεγχο και ανθεκτικότητα στην εφοδιαστική τους αλυσίδα. Η στρατηγική αυτή προσέγγιση ενισχύει όχι μόνο τη διαχείριση κινδύνων για επιμέρους προμήθειες αλλά και την συνολική ωριμότητα του επιπέδου Κυβερνοασφάλειας στον Οργανισμό, διασφαλίζοντας τη συμμόρφωση με το σχετικό κανονιστικό πλαίσιο.

2. **Κοινοποίηση Πληροφοριών:** Για την αναγνώριση, αξιολόγηση, παρακολούθηση και αντιμετώπιση των κινδύνων στην εφοδιαστική αλυσίδα, οι Οργανισμοί οφείλουν να ενσωματώσουν δομημένες διαδικασίες και δραστηριότητες κοινοποίησης πληροφοριών. Αυτό δύναται να περιλαμβάνει τη δημιουργία συμφωνιών ανταλλαγής πληροφοριών με ομότιμες επιχειρήσεις, εμπορικούς εταίρους και προμηθευτές. Μέσω της ανταλλαγής Πληροφοριών σχετικών με τους Κινδύνους στην Εφοδιαστική Αλυσίδα (Supply Chain Risk Information - SCRI), οι Οργανισμοί μπορούν να αξιοποιήσουν τη συλλογική γνώση, εμπειρία και ικανότητες της C-SCRM, αποκτώντας πιο ολοκληρωμένη εικόνα των απειλών που την αφορούν. Η ανταλλαγή πληροφοριών, είναι απαραίτητο να γίνεται μέσω επίσημων δομών, όπως τα Κέντρα Ανάλυσης και Ανταλλαγής Πληροφοριών (Information Sharing and Analysis Centers – ISACs), ώστε να αποφεύγονται νομικοί ή κανονιστικοί κίνδυνοι που ενδέχεται να προκύψουν από ανεπίσημες ή μη διαχειριζόμενες ανταλλαγές.

   Η διαδικασία κοινοποίησης πληροφοριών επιτρέπει στους Οργανισμούς να έχουν πρόσβαση σε κρίσιμες πληροφορίες, απαραίτητες για την κατανόηση και την αντιμετώπιση των κινδύνων Κυβερνοασφάλειας καθ' όλο το μήκος της εφοδιαστικής αλυσίδας. Παράλληλα, επιτρέπει την ανταλλαγή σχετικών πληροφοριών με άλλους εμπλεκόμενους φορείς, οι οποίοι είτε ενδέχεται να ωφεληθούν είτε απαιτείται να είναι ενήμεροι για αυτούς τους κινδύνους.

3. **Εκπαίδευση και ευαισθητοποίηση:** Η επιτυχής εφαρμογή της C-SCRM σε έναν οργανισμό απαιτεί τη συλλογική συμμετοχή όλων των εργαζομένων από διαφορετικά επίπεδα και τμήματα. Εργαζόμενοι από τμήματα όπως της Κυβερνοασφάλειας, των προμηθειών, της πληροφορικής, των νομικών, του ανθρωπίνου Δυναμικού, αλλά και η διαχείριση έργων και προγραμμάτων συνεισφέρουν στην αποτελεσματική αναγνώριση, μετριασμό και διαχείριση των κινδύνων στην εφοδιαστική αλυσίδα.

   Προκειμένου να υποστηριχθούν και να συντονιστούν οι παραπάνω ρόλοι, οι Οργανισμοί οφείλουν να δημιουργήσουν μια κουλτούρα Κυβερνοασφάλειας

που περιλαμβάνει οργανικά και τη C-SCRM. Αυτό επιτυγχάνεται μέσω της υλοποίησης γενικών και εξειδικευμένων προγραμμάτων εκπαίδευσης βάσει ρόλου, ώστε όλα τα άτομα να κατανοούν τις ευθύνες και το ρόλο τους στη συνολική ασφάλεια του οργανισμού. Οι εκπαιδεύσεις αυτές θα πρέπει να βασίζονται σε ελάχιστες απαιτήσεις κατάρτισης που ορίζονται σε επιχειρησιακό επίπεδο και να εξειδικεύονται στο επίπεδο επιχειρησιακών διαδικασιών και στο λειτουργικό επίπεδο, λαμβάνοντας υπόψη το επιχειρησιακό πλαίσιο και τον κίνδυνο ανά περίπτωση. Ιδιαίτερη σημασία πρέπει να δίνεται στην εκπαίδευση ατόμων με αυξημένες αρμοδιότητες στη C-SCRM, ώστε να κατανοούν πλήρως το εύρος ευθυνών τους, τις διαδικασίες που διαχειρίζονται, και τα βήματα απόκρισης σε περιστατικά που σχετίζονται με την εφοδιαστική αλυσίδα. Οι οργανισμοί θα πρέπει να αναπτύσσουν εκπαίδευση βάσει ρόλου, είτε ως νέο πρόγραμμα είτε ενσωματώνοντας περιεχόμενο σχετικό με τη C-SCRM σε ήδη υπάρχοντα προγράμματα εκπαίδευσης.

Επιπλέον, συνιστάται οι οργανισμοί να αξιοποιούν το NIST National Initiative for Cybersecurity Education (NICE) Framework, το οποίο παρέχει ένα κοινό λεξιλόγιο Κυβερνοασφάλειας που πρέπει να χρησιμοποιείται εσωτερικά σε έναν Οργανισμό. Το πλαίσιο NICE καθορίζει κατηγορίες, εξειδικεύσεις, ρόλους, γνώσεις, δεξιότητες και ικανότητες (Knowledge, Skills, Abilities – KSAs), καθώς και συγκεκριμένα καθήκοντα, υποστηρίζοντας έτσι την προσαρμοσμένη εκπαίδευση και την αποτελεσματική επικοινωνία εντός του οργανισμού γύρω από τα ζητήματα ασφάλειας.

4. **Βασικές πρακτικές C-SCRM:** Οι βασικές πρακτικές της C-SCRM βασίζονται σε πρότυπα πρακτικών από διαφορετικούς κλάδους και ενσωματώνουν ένα δυναμικά εξελισσόμενο σύνολο από δυνατότητες. Στόχος τους είναι να αναδείξουν ένα κρίσιμο υποσύνολο από πρακτικές, τις οποίες οι οργανισμοί πρέπει να θέσουν ως προτεραιότητα για την επίτευξη ενός βασικού επιπέδου ωριμότητας (base-level maturity), πριν προχωρήσουν στην ανάπτυξη πιο προηγμένων δυνατοτήτων C-SCRM. Η εφαρμογή αυτών των πρακτικών θα πρέπει να προσαρμόζεται στο συγκεκριμένο επιχειρησιακό περιβάλλον, λαμβάνοντας υπόψη τους διαθέσιμους πόρους, το προφίλ κινδύνου και τις ιδιαιτερότητες του οργανισμού.

   Οι C-SCRM Key Practices περιλαμβάνουν τις εξής ενέργειες:

   - Τη δια-επιχειρησιακή ενσωμάτωση (enterprise-wide integration) των αρχών της C-SCRM σε όλες τις λειτουργίες και δομές του οργανισμού.
   - Την καθιέρωση επίσημου προγράμματος C-SCRM (formal program) με καθορισμένους ρόλους, πολιτικές και διαδικασίες.
   - Την αναγνώριση και διαχείριση κρίσιμων προϊόντων, υπηρεσιών και προμηθευτών (critical products, services, and suppliers).
   - Την εις βάθος κατανόηση της δομής της εφοδιαστικής αλυσίδας (understanding the supply chain) του οργανισμού.
   - Τη στενή συνεργασία με κρίσιμους προμηθευτές (collaboration with critical suppliers), προάγοντας τη διαφάνεια και τη συνυπευθυνότητα.
   - Την ένταξη των προμηθευτών σε δραστηριότητες ανθεκτικότητας και βελτίωσης (resilience and improvement activities).

- Την συνεχή αξιολόγηση και παρακολούθηση (continuous assessment and monitoring) καθ' όλη τη διάρκεια της σχέσης με τους προμηθευτές.
- Τον πλήρη κύκλο ζωής στον σχεδιασμό (full life cycle planning) που καλύπτει από την αρχική μέχρι και το τέλος μιας προμήθειας.

Η στοχευμένη εφαρμογή αυτών των βασικών πρακτικών ενισχύει ουσιαστικά την ανθεκτικότητα, την ωριμότητα και την ασφάλεια του οργανισμού απέναντι σε σύνθετες και μεταβαλλόμενες απειλές που προκύπτουν από την εφοδιαστική αλυσίδα.

5. **Θεμελιώδεις πρακτικές:** Η εφαρμογή θεμελιωδών πρακτικών C-SCRM αποτελεί βασική προϋπόθεση για την επιτυχημένη και αποδοτική συνεργασία των οργανισμών με ενοποιητές συστημάτων system integrators) και λοιπούς κρίσιμους προμηθευτές. Οι προμηθευτές ενδέχεται να βρίσκονται σε διαφορετικά επίπεδα ωριμότητας αναφορικά με την υιοθέτηση πρότυπων πρακτικών, επομένως είναι απαραίτητη η σταδιακή εφαρμογή θεμελιακών δράσεων, οι οποίες ενισχύουν τις δυνατότητες ενός οργανισμού να αναπτύξει και να υλοποιήσει πιο προηγμένες πολιτικές C-SCRM.
   - Σύσταση Γραφείου Διαχείρισης Προγράμματος για την Ασφάλεια της Εφοδιαστικής Αλυσίδας (C-SCRM PMO) για τον συντονισμό όλων των ενεργειών C-SCRM στον οργανισμό.
   - Υποστήριξη από την ανώτατη διοίκηση (executive leadership) για ενίσχυση πόρων, πολιτικής και στρατηγικής C-SCRM.
   - Εφαρμογή ιεραρχίας και διαδικασίας διαχείρισης κινδύνων σύμφωνα με NIST SP 800-39 και SP 800-30 Rev.1.
   - Ενσωμάτωση των απαιτήσεων C-SCRM στις πολιτικές διακυβέρνησης του οργανισμού.
   - Ανάλυση κρισιμότητας προμηθευτών, προϊόντων και υπηρεσιών για στοχευμένη προστασία.
   - Ευαισθητοποίηση και εκπαίδευση προσωπικού με εκπαίδευση βάσει ρόλου (role-based training) για θέματα C-SCRM.
   - Ενσωμάτωση C-SCRM σε προμήθειες και πολιτικές απόκτησης Τεχνολογιών Πληροφορικής, π.χ. FITARA (Federal Information Technology Acquisition Reform Act).
   - Καθιέρωση διαδικασίας εκτίμησης επιπέδου κρισιμότητας βάσει FIPS 199.
   - Αξιολόγηση προμηθευτών με εκτίμηση κινδύνου που περιλαμβάνει ανάλυση κρισιμότητας, απειλών και ευπαθειών.
   - Εφαρμογή προγράμματος διασφάλισης ποιότητας και ελέγχου (QA/QC – Quality Assurance / Quality Control) για προϊόντα και υπηρεσίες.
   - Καθορισμός ρόλων και ευθυνών μεταξύ εφοδιαστικής αλυσίδας, Κυβερνοασφάλειας, πληροφορικής, νομικής, ανθρώπινου δυναμικού κ.ά.
   - Δέσμευση πόρων και ύπαρξη ελεγχόμενου προσωπικού με αρμοδιότητες στη C-SCRM.
   - Εφαρμογή μέτρων ασφάλειας βάσει του NIST SP 800-53 Rev. 5.

- Εσωτερικοί έλεγχοι συμμόρφωσης με βάση τις πολιτικές ασφάλειας.
- Πολιτική διαχείρισης προμηθευτών με αγορές μόνο από κατασκευαστές πρωτότυπου εξοπλισμού (OEMs – Original Equipment Manufacturers) ή εξουσιοδοτημένους διανομείς.
- Πρόγραμμα διαχείρισης περιστατικών ασφάλειας (Incident Management Program) με ανάλυση βασικής αιτίας (root cause analysis).
- Μηχανισμοί επιβεβαίωσης ευπαθειών, με αναφορές και διαδικασία αποκατάστασης.
- Διακυβέρνηση για ενσωματωμένο λογισμικό μέσω SBOMs (Software Bill of Materials) και αξιολόγηση κρισιμότητας, απειλών και εκμεταλλευσιμότητας.

6. **Πρακτικές διατήρησης:** Οι Πρακτικές διατήρησης αποτελούν το επόμενο βήμα για τους οργανισμούς που έχουν ήδη εγκαθιδρύσει και εφαρμόσει τις θεμελιώδεις πρακτικές της C-SCRM. Ενώ οι θεμελιώδεις πρακτικές επικεντρώνονται στη δημιουργία βασικών δομών και πολιτικών, οι πρακτικές διατήρησης αποσκοπούν στη διατήρηση, ενίσχυση και επέκταση της αποτελεσματικότητας της C-SCRM. Βασίζονται στη συνεργασία ανάμεσα σε διάφορους τομείς, στη συνεχή παρακολούθηση, στρατηγική διαχείρισης κινδύνου και την επικοινωνία μεταξύ φορέων, εντός και εκτός του οργανισμού.

   Οι οργανισμοί οφείλουν να προσεγγίσουν τις ακόλουθες πρακτικές:

   - **Συνεργασία με Threat-Informed Security Program:** Ενσωμάτωση πρακτικών και μηχανισμών που βασίζονται σε πραγματικές πληροφορίες απειλών, ενισχύοντας τη στρατηγική λήψης αποφάσεων.
   - **Μηχανισμοί αξιοπιστίας (Confidence-Building Mechanisms):** Εφαρμογή εργαλείων αξιολόγησης, όπως third-party assessments, on-site inspections και διεθνείς πιστοποιήσεις (π.χ. ISO/IEC 27001), για την αξιολόγηση της ασφάλειας κρίσιμων προμηθευτών.
   - **Διαρκής παρακολούθηση & επαναξιολόγηση προμηθευτών:** Καθιέρωση επίσημων διαδικασιών και χρονικών πλαισίων για τον συνεχή επανέλεγχο προϊόντων, υπηρεσιών και σχέσεων προμηθευτών, ώστε να ανιχνεύονται αλλαγές στο risk profile.
   - **Καθορισμός ανοχής κινδύνου και ορίων:** Χρήση του οργανωτικού C-SCRM προφίλ κινδύνου για τον ορισμό αποδεκτών επιπέδων κινδύνου και τη λήψη αποκεντρωμένων αποφάσεων σε ευθυγράμμιση με στρατηγικούς στόχους.
   - **Δομημένη ανταλλαγή πληροφοριών (Information Sharing):** Συμμετοχή σε ISACs, συνεργασία με τη FASC και άλλους κρατικούς φορείς για τη συλλογική ενίσχυση της ανθεκτικότητας και της ετοιμότητας έναντι απειλών στην εφοδιαστική αλυσίδα.
   - **Ενσωμάτωση C-SCRM σε ανώτατο επίπεδο διαχείρισης κινδύνου:** Ανάδειξη κρίσιμων κινδύνων του C-SCRM στο ανώτατο επίπεδο διαχείρισης κινδύνου του οργανισμού (π.χ. enterprise risk committee).

- **Ενίσχυση της εκπαίδευσης με C-SCRM θεματολογία:** Προσαρμογή των εκπαιδευτικών προγραμμάτων ανά ρόλο με C-SCRM θεματολογία για τμήματα όπως IT, procurement, legal, HR, engineering κ.λπ.
- **Οριζόντια ενσωμάτωση C-SCRM στον κύκλο ζωής προϊόντων/συστημάτων:** Εφαρμογή επαναληπτικών, τεκμηριωμένων διαδικασιών που περιλαμβάνουν πρακτικές απόκτησης.
- **Ενσωμάτωση απαιτήσεων C-SCRM σε συμβάσεις:** Σαφής ένταξη C-SCRM όρων και υποχρεώσεων στη «γλώσσα» συμβολαίων με προμηθευτές.
- **Συμμετοχή κρίσιμων προμηθευτών σε σχέδια αντιμετώπισης κρίσεων:** Συμπερίληψη βασικών προμηθευτών σε διαδικασίες επιχειρησιακής συνέχειας, ανάκαμψης και προσομοίωσης απόκρισης σε περιστατικά.
- **Συνεργασία με εξωτερικούς παρόχους για βελτίωση των κυβερνοπρακτικών τους:** Πρωτοβουλίες για την ενίσχυση των ικανοτήτων Κυβερνοασφάλειας των τρίτων μερών που συμμετέχουν στην εφοδιαστική αλυσίδα.
- **Καθορισμός και παρακολούθηση δεικτών απόδοσης:** Ανάπτυξη δεικτών απόδοσης (KPIs) που επιτρέπουν στη διοίκηση να λαμβάνει τεκμηριωμένες αποφάσεις και να αξιολογεί την αποτελεσματικότητα των πολιτικών C-SCRM.

7. **Πρακτικές ενίσχυσης:** Οι Πρακτικές ενίσχυσης αποτελούν το τρίτο και πλέον εξελιγμένο επίπεδο ωρίμανσης στην C-SCRM. Εφαρμόζονται από οργανισμούς που έχουν ήδη υιοθετήσει τις προηγούμενες πρακτικές που αναφέρθηκαν και στοχεύουν στη μετάβαση από μια αντιδραστική (reactive) προσέγγιση σε μια προβλεπτική (predictive) στρατηγική διαχείρισης κινδύνου.

   Οι πρακτικές αυτές προωθούν την αυτοματοποίηση, τη χρήση ποσοτικών μοντέλων ανάλυσης κινδύνου και την αξιοποίηση δεικτών καθοδήγησης (leading indicators) για τη λήψη στρατηγικών αποφάσεων πριν την εκδήλωση των απειλών.

   - **Αυτοματοποίηση διαδικασιών C-SCRM**: Εφαρμογή αυτοματοποιημένων μηχανισμών όπου είναι εφικτό, για ενίσχυση της συνέπειας, αποδοτικότητας και της βέλτιστης αξιοποίησης των κρίσιμων πόρων.
   - **Ποσοτική ανάλυση κινδύνου με μοντέλα βασισμένα σε πιθανότητες**: Υιοθέτηση ποσοτικών μεθόδων ανάλυσης κινδύνου, όπως Bayesian ανάλυση, για ελαχιστοποίηση της αβεβαιότητας, βελτιστοποίηση της κατανομής πόρων και μέτρηση αποτελεσματικότητας απόκρισης (ROI of response actions).
   - **Μετάβαση από reactive σε predictive στρατηγική**: Χρήση οδηγών C-SCRM δεικτών για την ανάπτυξη στρατηγικών που προσαρμόζονται προληπτικά σε αλλαγές του προφίλ κινδύνου, πριν την εμφάνιση επιπτώσεων.
   - **Συμμετοχή σε κοινότητες πρακτικής (Community of Practice):** Ίδρυση ή συμμετοχή σε Centers of Excellence ή παρόμοιες κοινότητες

ανταλλαγής βέλτιστων πρακτικών για συνεχή βελτίωση και καινοτομία στις διαδικασίες C-SCRM.

Η εφαρμογή των πρακτικών αυτών ενισχύει τη στρατηγική ικανότητα των οργανισμών να διαχειρίζονται Κυβερνοκινδύνους σε όλο τον κύκλο ζωής των συστημάτων, προϊόντων και υπηρεσιών, παρέχοντας ευελιξία, προσαρμοστικότητα και ανθεκτικότητα στις δυναμικές συνθήκες της εφοδιαστικής αλυσίδας.

8. **Αξιολόγηση Ικανοτήτων και Μετρήσεις Απόδοσης**: Η μέτρηση της αποτελεσματικότητας και της ωριμότητας της C-SCRM αποτελεί κρίσιμο παράγοντα για την παρακολούθηση, βελτιστοποίηση και στρατηγική διαχείριση των κινδύνων Κυβερνοασφάλειας στην εφοδιαστική αλυσίδα. Οι οργανισμοί καλούνται να εφαρμόσουν μεθόδους αξιολόγησης που να επιτρέπουν ποσοτική και ποιοτική αποτύπωση της προόδου, της συμμόρφωσης, της αποδοτικότητας και της επίδρασης των μέτρων C-SCRM στο συνολικό επιχειρησιακό επίπεδο κινδύνου.

   Η αξιολόγηση μπορεί να περιλαμβάνει, τη χρήση δομημένων πλαισίων αξιολόγησης (π.χ. NIST Cybersecurity Framework – CSF) για τη μέτρηση της προόδου και της ωριμότητας, την παρακολούθηση της προόδου υλοποίησης C-SCRM πρωτοβουλιών σε σχέση με τους επιχειρησιακούς στόχους, τη μέτρηση της αποτελεσματικότητας των πρακτικών ως προς τη μείωση της έκθεσης σε κινδύνους και την ενίσχυση των αποτελεσμάτων ασφαλείας.

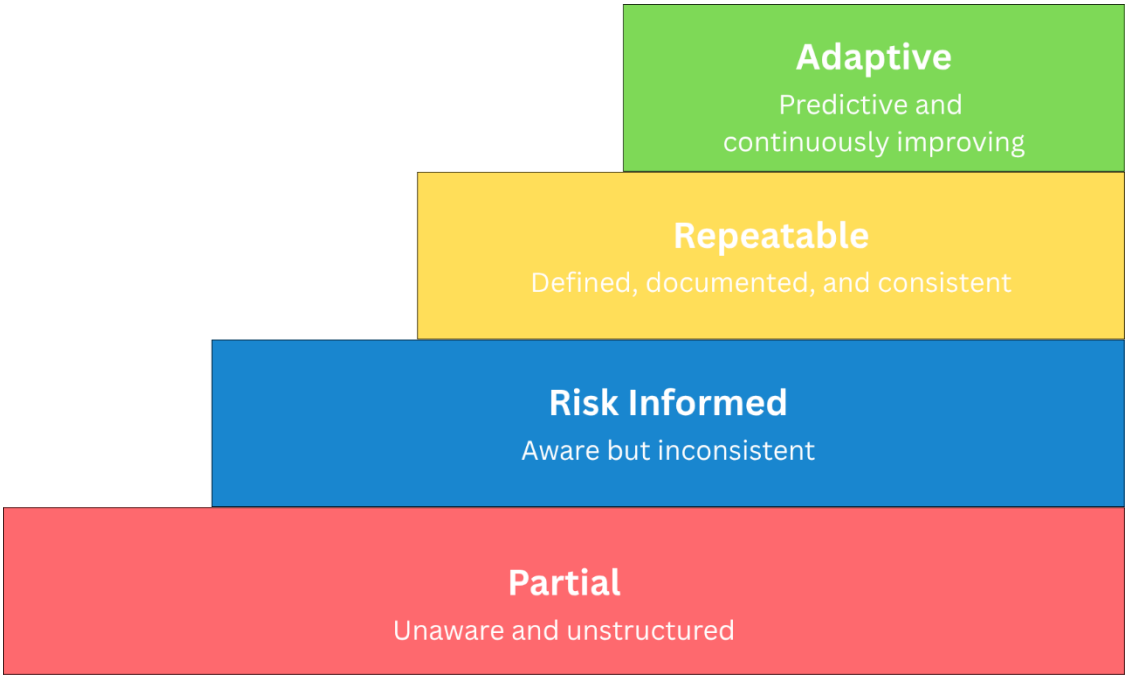
   Οι πρακτικές αυτές βασίζονται στη συλλογή και ανάλυση δεδομένων, στην υλοποίησή τους στο οργανωτικό πλαίσιο και στη συστηματική αναφορά, ώστε να καθίσταται δυνατή η λήψη τεκμηριωμένων αποφάσεων για τη συμμόρφωση και την αποφυγή οικονομικών ζημιών από περιστατικά Κυβερνοασφάλειας.

   Η εφαρμογή στρωματοποίησης του NIST CSF **(NIST CSF Implementation Tiers)** προσφέρει ένα κλιμακωτό μοντέλο αξιολόγησης της C-SCRM ωριμότητας, καθορίζοντας 4 επίπεδα:

   - **Επίπεδο 1 – Μερικό (Partial)**: Έλλειψη κατανόησης των κινδύνων και απουσία δομημένων διαδικασιών ή συνεργασιών.
   - **Επίπεδο 2 – Γνώση Κινδύνων (Risk Informed)**: Βασική αναγνώριση των κινδύνων αλλά χωρίς συστηματική ανταλλαγή πληροφοριών.
   - **Επίπεδο 3 – Επαναληπτικό (Repeatable)**: Πλήρως τεκμηριωμένες και επαναλαμβανόμενες διαδικασίες, με επίσημη διαχείριση και συνεργασία με εξωτερικούς εταίρους.
   - **Επίπεδο 4 – Προσαρμοστικό (Adaptive)**: Στρατηγική που χρησιμοποιεί δεδομένα σε πραγματικό χρόνο, ενεργή ανταλλαγή πληροφοριών και συνεχής βελτίωση μέσω θεσμοθετημένης γνώσης, που προσφέρει τη δυνατότητα πρόβλεψης.

   Η συστηματική παρακολούθηση και αξιολόγηση των ικανοτήτων και της απόδοσης ενός προγράμματος C-SCRM αποτελεί αναπόσπαστο στοιχείο της επιχειρησιακής ανθεκτικότητας και στρατηγικής διαχείρισης κινδύνων. Η εφαρμογή μετρήσιμων δεικτών επιτρέπει στους οργανισμούς να διασφαλίζουν τη συμμόρφωση με πρότυπα και κανονισμούς, να βελτιστοποιούν την κατανομή πόρων, και να τεκμηριώνουν την αποτελεσματικότητα των μέτρων που υλοποιούν. Επιπλέον, η διαχείριση της απόδοσης ενισχύει τη λογοδοσία των εμπλεκόμενων

φορέων (stakeholders), ενώ συμβάλλει στη μείωση κόστους μέσω της πρόληψης περιστατικών ασφαλείας. Τέλος, λειτουργεί ως μοχλός για τη συνεχή ωρίμανση και στρατηγικό επαναπροσδιορισμό των C-SCRM διαδικασιών, καθιστώντας τον οργανισμό πιο ευέλικτο και προσαρμοστικό σε ένα συνεχώς μεταβαλλόμενο περιβάλλον απειλών. [29]




*Σχήμα 3: NIST CSF - επίπεδα ωριμότητα C-SCRM*

9. **Ανάπτυξη και Μέτρηση Δεικτών Απόδοσης:** Η μέτρηση της απόδοσης στο πλαίσιο του C-SCRM αποτελεί μία απαραίτητη διαδικασία για τη βελτίωση της λογοδοσίας, της αποτελεσματικότητας και της λήψης στρατηγικών αποφάσεων.

   Όπως αποτυπώνεται στο Σχήμα 4, η ανάπτυξη δεικτών απόδοσης βασίζεται σε έναν κυκλικό και δυναμικό μηχανισμό αξιολόγησης, ο οποίος ξεκινά με την ταυτοποίηση των ενδιαφερομένων μερών (π.χ. CISO, CIO, CEO) και συνεχίζεται με τον καθορισμό στόχων και αντικειμενικών σκοπών που συμφωνούν με τις προτεραιότητες στρατηγικής του οργανισμού.

   Ακολουθεί η ανασκόπηση πολιτικών, οδηγιών και διαδικασιών, ώστε να εντοπιστούν τα επιθυμητά πρότυπα και ελεγκτικοί μηχανισμοί. Στο στάδιο της επισκόπησης της υλοποίησης, συλλέγονται δεδομένα από αξιολογήσεις προμηθευτών, POA&Ms, και άλλες πηγές. Η αξιολόγηση του επιπέδου υλοποίησης συνδέει τα διαθέσιμα μέτρα με τα πρότυπα και τις πολιτικές C-SCRM, ώστε να αποτυπωθεί η πρόοδος. Επιπλέον, εξετάζεται η αποδοτικότητα και αποτελεσματικότητα του προγράμματος C-SCRM σε σχέση με τις στρατηγικές επιδιώξεις και πραγματοποιείται ανάλυση του αντίκτυπου στη λειτουργία και την αποστολή του οργανισμού (π.χ. εξοικονόμηση κόστους, μείωση κινδύνων).


*Σχήμα 4: Διαδικασία ανάπτυξης C-SCRM δεικτών απόδοσης*

Η διαδικασία αυτή είναι επαναλαμβανόμενη και επιτρέπει την επανεξέταση και προσαρμογή των στόχων, διασφαλίζοντας ότι οι δείκτες μένουν ενημερωμένοι και σύμφωνοι με την εξελισσόμενη επιχειρησιακή πραγματικότητα. Επομένως, η μέτρηση της απόδοσης αποτελεί θεμέλιο λίθο για μια ώριμη και διαρκώς εξελισσόμενη C-SCRM.

10. **Πόροι και Χρηματοδότηση:** Η επιτυχής διαχείριση κινδύνων στην εφοδιαστική αλυσίδα προϋποθέτει τη διάθεση επαρκών και επαναλαμβανόμενων οικονομικών και ανθρώπινων πόρων. Η ενσωμάτωση αναγκών χρηματοδότησης στον στρατηγικό σχεδιασμό και στις διαδικασίες προϋπολογισμού ενός οργανισμού αποτελεί καθοριστικό παράγοντα για την ίδρυση, υποστήριξη και ωρίμανση ενός ολοκληρωμένου C-SCRM πλαισίου. Η εξασφάλιση πόρων όχι μόνο αντικατοπτρίζει τη δέσμευση της διοίκησης για την Κυβερνοασφάλεια της εφοδιαστικής αλυσίδας, αλλά συμβάλλει και στη λογοδοσία και στην επίτευξη μετρήσιμων αποτελεσμάτων μέσω της σύνδεσης των κονδυλίων με συγκεκριμένες επιδόσεις.

    Η κατανομή των πόρων θα πρέπει να γίνεται με στρατηγικό σχεδιασμό βάσει στόχων, ώστε να διασφαλίζεται η βέλτιστη χρήση περιορισμένων πόρων. Ο οργανισμός οφείλει να αξιολογεί ποιες ανάγκες μπορούν να καλυφθούν με υφιστάμενους πόρους, ποιες απαιτούν επανεπένδυση ή ανακατανομή, και ποιες δικαιολογούν νέες χρηματοδοτικές αιτήσεις, ενδεχομένως μέσω τεκμηριωμένων επενδυτικών προτάσεων. Οι πόροι διακρίνονται σε **συνεχείς ανάγκες** (π.χ. εκπαίδευση, λειτουργικά έξοδα) και **ειδικές επενδύσεις** (π.χ. ανάπτυξη νέου συστήματος ή πρόσληψη ειδικών). Η ύπαρξη ενός **μακροπρόθεσμου προϋπολογισμού για τη C-SCRM**, σε συντονισμό με τους υπεύθυνους αποστολής, διαδικασιών και χρηματοδότησης, ενισχύει τον ορθολογικό προγραμματισμό και διευκολύνει τη μέτρηση αποδοτικότητας των επενδύσεων.

Επιπλέον, η αξιοποίηση κοινών υπηρεσιών και μηχανισμών κατανομής κόστους μεταξύ διαφορετικών λειτουργικών μονάδων μπορεί να ενισχύσει την αποδοτικότητα, ιδιαίτερα όταν υπάρχει τεχνολογική υποδομή που υποστηρίζει αυτοματοποίηση και συγκεντρωτική παροχή υπηρεσιών. Η ορατότητα του προϋπολογισμού και η τεκμηρίωση της σχέσης του με τις αποδόσεις του προγράμματος ενισχύει τη διαφάνεια, την υπευθυνότητα και επιτρέπει στην ηγεσία να προσαρμόσει στόχους, χρονοδιαγράμματα και προσδοκίες. [29]

## 3.4 Παράρτημα Α: Αντίμετρα

Το Παράρτημα Α του προτύπου εστιάζει στην παρουσίαση και εξειδίκευση των μέτρων ασφαλείας για την C-SCRM, με στόχο την αποτελεσματική προστασία της εφοδιαστικής αλυσίδας έναντι Κυβερνοαπειλών. Βασιζόμενο στη δομή και τη φιλοσοφία του NIST SP 800-53, Rev. 5, το παράρτημα προσαρμόζει, επεκτείνει και εξειδικεύει αντίμετρα (controls) σχετικά με τη διαχείριση κινδύνου στην εφοδιαστική αλυσίδα ψηφιακών προϊόντων και υπηρεσιών (ICT/OT).

Η προσέγγιση ακολουθεί ένα **μοντέλο κάλυψης (overlay model)**, επιλέγοντας από το γενικό πλαίσιο του SP 800-53 εκείνα τα controls που έχουν άμεση συνάφεια με το C-SCRM και παρέχοντας πρόσθετη καθοδήγηση ή νέους ελέγχους όπου κρίνεται απαραίτητο. Τα μέτρα οργανώνονται σε 20 θεματικές οικογένειες και καλύπτουν τις ανάγκες και των τριών επιπέδων διαχείρισης κινδύνου, επιχειρησιακό, επιχειρησιακών διαδικασιών και λειτουργικό. Η κάθε οικογένεια περιέχει ένα πλήθος βασικών αντιμέτρων (base controls) που η υλοποίησή τους είναι απαραίτητη αλλά και ένα σύνολο προαιρετικών αντιμέτρων (enhancements) τα οποία συμπληρώνουν τα βασικά.

Για παράδειγμα, το αντίμετρο με κωδικό και τίτλο **AC-3 – Access Enforcement** (Επιβολή Ελέγχου Πρόσβασης) ανήκει στην οικογένεια Access Control που είναι η 1η οικογένεια αντιμέτρων που υπάρχει στο annex A. Το αντίμετρο, απαιτεί την εφαρμογή φυσικών και λογικών μηχανισμών ελέγχου πρόσβασης, με ρητές συνέπειες για παραβιάσεις και υποχρεωτική εφαρμογή από προμηθευτές (flow-down). Το **AC-3(8)** αποτελεί προαιρετική επέκταση του βασικού αντιμέτρου και απαιτεί την άμεση ανάκληση δικαιωμάτων πρόσβασης όταν δεν χρειάζονται ή παραβιάζονται, καθώς και επιστροφή credentials (π.χ. κάρτες, tokens). Το **AC-3(9)** (επίσης προαιρετική επέκταση) απαιτεί ελεγχόμενη κοινοποίηση πληροφοριών του supply chain σε τρίτους για την αποφυγή διαρροών. Όλα ισχύουν για τα επίπεδα 2 και 3.

Συνολικά τα βασικά αντίμετρα που υπάρχουν μέσα στο πρότυπο είναι **182**, ενώ υπάρχουν και **110** προαιρετικά αντίμετρα. [29]

| ID | Family | Base Controls | Enhancements | Scope |
|---|---|---|---|---|
| AC | Access control | 13 | 10 | Περιορισμός της πρόσβασης σε συστήματα, λειτουργίες και πληροφορίες μόνο σε εξουσιοδοτημένους χρήστες, συσκευές και διεργασίες, εξασφαλίζοντας ότι η πρόσβαση είναι κατάλληλη, περιορισμένη και ελεγχόμενη στην εφοδιαστική αλυσίδα. |
| AT | Awareness and training | 4 | 7 | Διασφάλιση ότι το προσωπικό γνωρίζει τους κινδύνους που απειλούν την εφοδιαστική αλυσίδα και έχει εκπαιδευτεί κατάλληλα, συμπεριλαμβανομένης της ενημέρωσης για κινδύνους και πρακτικές που σχετίζονται με τη C-SCRM. |
| AU | Audit and Accountability | 9 | 5 | Καταγραφή και προστασία των αρχείων καταγραφής δραστηριοτήτων με σκοπό την ανίχνευση, ανάλυση και απόδοση ευθύνης, υποστηρίζοντας την αναγνώριση και διερεύνηση περιστατικών που σχετίζονται με την εφοδιαστική αλυσίδα. |
| CA | Assessment, Authorization, and Monitoring | 5 | 2 | Περιοδική αξιολόγηση, έγκριση και συνεχής παρακολούθηση των συστημάτων για να διασφαλίζεται η αποτελεσματικότητα των μέτρων ασφαλείας. |
| CM | Configuration Management | 14 | 27 | Καθορισμός και διατήρηση ασφαλών βασικών ρυθμίσεων και καταλόγους περιουσιακών στοιχείων, διασφαλίζοντας τον έλεγχο αλλαγών καθ' όλη τη διάρκεια ζωής των συστημάτων. |
| CP | Contingency Planning | 8 | 8 | Διασφάλιση ύπαρξης σχεδίων για την αδιάκοπη λειτουργία, αντίδραση σε καταστροφές και ανάκαμψη, ώστε να διατηρείται η διαθεσιμότητα κρίσιμων πληροφοριακών πόρων. |
| IA | Identification and Authentication | 7 | 3 | Αναγνώριση και επιβεβαίωση ταυτότητας χρηστών, διεργασιών και συσκευών πριν την απόκτηση πρόσβασης σε συστήματα. |
| IR | Incident Response | 6 | 6 | Καθορισμός ικανότητας για ανίχνευση, αντιμετώπιση, αποκατάσταση και αναφορά περιστατικών ασφαλείας που επηρεάζουν την αλυσίδα εφοδιασμού. |
| MA | Maintenance | 7 | 6 | Εξασφάλιση ελέγχου των διαδικασιών συντήρησης, που συχνά περιλαμβάνουν τρίτους και αποτελούν κρίσιμο μέρος της εφοδιαστικής αλυσίδας. |
| MP | Media Protection | 4 | | Προστασία μέσων αποθήκευσης (φυσικά και ψηφιακά), περιορισμός πρόσβασης και ορθή καταστροφή ή καθαρισμό πριν από την επαναχρησιμοποίηση ή απόρριψη. |
| PE | Physical and Environmental protection | 9 | 4 | Περιορισμός φυσικής πρόσβασης και προστασία συστημάτων και υποδομών από φυσικές και περιβαλλοντικές απειλές, σημαντικό και στο πλαίσιο του logistics. |
| PL | Planning | 7 | 1 | Τεκμηρίωση και τακτική ενημέρωση σχεδίων ασφάλειας για την περιγραφή των ελέγχων και της συμπεριφοράς των χρηστών σε πληροφοριακά συστήματα. |
| PM | Program Management | 30 | | Υποστήριξη ασφάλειας σε επίπεδο επιχείρησης, παρέχοντας το πλαίσιο διαχείρισης για δραστηριότητες C-SCRM σε όλο τον οργανισμό. |
| PS | Personnel Security | 4 | | Άτομα με κρίσιμους ρόλους πρέπει να είναι αξιόπιστα και η σωστές πρακτικές πρόσβασης κατά τη διάρκεια και μετά αλλαγών προσωπικού. |

| | | | | |
|---|---|---|---|---|
| PT | Personally identifiable information processing and Transparency | 1 | | Διαχείριση διαφάνειας και επεξεργασίας προσωπικών δεδομένων (PII), συμπεριλαμβανομένων των πρακτικών απορρήτου από τους προμηθευτές. |
| RA | Risk Assessment | 7 | 2 | Περιοδική αξιολόγηση κινδύνων για λειτουργίες, περιουσιακά στοιχεία και άτομα που σχετίζονται με τη λειτουργία των πληροφοριακών συστημάτων. |
| SA | System and Services Acquisition | 14 | 10 | Διασφάλιση ότι η ασφάλεια ενσωματώνεται στον κύκλο ζωής των συστημάτων και υπηρεσιών και ότι οι προμηθευτές εφαρμόζουν επαρκή μέτρα ασφάλειας. |
| SC | System and Communications Protection | 12 | 10 | Έλεγχος και σωστή μετάδοση πληροφοριών, ορθός σχεδιασμός αρχιτεκτονικής συστημάτων ώστε να εξασφαλίζεται η ασφάλεια των επικοινωνιών. |
| SI | System and information Integrity | 8 | 4 | Ανίχνευση και διόρθωση ελαττωμάτων στα συστήματα, προστασία από κακόβουλο λογισμικό και απόκριση σε προειδοποιήσεις ασφαλείας. |
| SR | Supply Chain Risk management | 13 | 5 | Εφαρμογή ελέγχων για τον εντοπισμό, την αξιολόγηση και τη μείωση των κινδύνων που προκύπτουν από την εξάρτηση σε τρίτους προμηθευτές, υπηρεσίες και προϊόντα ICT/OT. |

*Πίνακας 1: Nist SP 800 161r1 Security Controls*

Η εφαρμογή των μέτρων αυτών μπορεί να πραγματοποιηθεί τόσο για τον ίδιο το Οργανισμό όσο και σε εξωτερικούς συνεργάτες, όπως προμηθευτές, κατασκευαστές, system integrators και παρόχους υπηρεσιών.

Παράλληλα, δίνεται έμφαση στη σωστή επιλογή, προσαρμογή και τεκμηρίωση των C-SCRM controls, προκειμένου να εξασφαλίζεται μια αποτελεσματική, ευέλικτη και προσαρμοσμένη στις ανάγκες της επιχείρησης διαχείριση κινδύνου στην εφοδιαστική αλυσίδα.

Το Παράρτημα αναδεικνύει τη σημασία της στοχευμένης επιλογής μέτρων ασφαλείας, της σύνδεσής τους με το πλαίσιο προμηθειών και συμβάσεων, καθώς και της συνεχούς αξιολόγησης και παρακολούθησης της υλοποίησής τους, συμβάλλοντας στη συνολική ενίσχυση της ανθεκτικότητας του οργανισμού. Λειτουργεί ως τεχνικό συμπλήρωμα της στρατηγικής που αναπτύχθηκε στα προηγούμενα κεφάλαια της παρούσας εργασίας. Επιπλέον αποτελεί το τεχνικό εργαλείο εφαρμογής των αρχών της C-SCRM, παρέχοντας ένα οργανωμένο πλαίσιο ελέγχων και κατευθυντήριων οδηγιών.

Μέσα από τη σωστή επιλογή, προσαρμογή και εφαρμογή των C-SCRM αντιμέτρων, οι οργανισμοί μπορούν να υλοποιήσουν στην πράξη τις στρατηγικές και τους παράγοντες υψηλής κρισιμότητας που αναλύθηκαν. [29]

## 3.5 Σύνοψη

Το NIST SP 800-161r1 αποτελεί ένα από τα πληρέστερα και πιο σύγχρονα πρότυπα για την ανάπτυξη και εφαρμογή ενός ολοκληρωμένου πλαισίου Διαχείρισης Κινδύνου Εφοδιαστικής Αλυσίδας Κυβερνοασφάλειας.

Με τη δομημένη προσέγγιση πολλαπλών επιπέδων, παρέχει στους οργανισμούς μια πολύ καλά δομημένη μεθοδολογία ανάπτυξης C-SCRM για να αντιμετωπίζουν με συνέπεια και αποτελεσματικότητα τις αυξανόμενες Κυβερνοαπειλές που διαπερνούν την εφοδιαστική τους αλυσίδα.

Η ενσωμάτωση του C-SCRM σε κάθε στάδιο του κύκλου ζωής ενός προϊόντος ή υπηρεσίας ενδυναμώνει την ανθεκτικότητα, μειώνει την έκθεση σε κινδύνους και ενισχύει την εμπιστοσύνη προς τους προμηθευτές και συνεργάτες.

Καθώς το τοπίο των Κυβερνοαπειλών εξελίσσεται δυναμικά, η συνεχής προσαρμογή και η ωρίμανση των C-SCRM δυνατοτήτων καθίστανται κρίσιμη όχι μόνο για την προστασία των επιχειρησιακών στόχων, αλλά και για τη διαφύλαξη της εθνικής ασφάλειας. Το πρότυπο θέτει το θεμέλιο για μια προοδευτική και προληπτική κουλτούρα Κυβερνοασφάλειας που αποτελεί πλέον επιτακτική ανάγκη στη σύγχρονη ψηφιακή εποχή. [29]

# 4. ISO 27036

## 4.1 Εισαγωγή στο ISO 27036


*Εικόνα 4:ISO 27036*

Το ISO 27036 είναι ένα διεθνές πρότυπο που ανήκει στην οικογένεια προτύπων ISO/IEC 27000. Η εν λόγω σειρά προτύπων παρέχει κατευθυντήριες οδηγίες για τη δημιουργία, υλοποίηση, παρακολούθηση και βελτίωση ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ISMS). Το ISO 27036 εστιάζει στις σχέσεις των οργανισμών με προμηθευτές (suppliers), παρέχοντας οδηγίες για την αποτελεσματική διαχείριση των κινδύνων που σχετίζονται με την ανταλλαγή προϊόντων, υπηρεσιών ή άλλων πόρων μεταξύ ενός οργανισμού και των συνεργατών του. [30]

### 4.1.1 Σκοπός

Στόχος του προτύπου είναι η παροχή κατευθυντήριων οδηγιών στους οργανισμούς, με σκοπό τον εντοπισμό, την αξιολόγηση και διαχείριση της επικινδυνότητας που σχετίζεται με την ανταλλαγή προϊόντων και υπηρεσιών με τρίτα μέρη.

Οι σχέσεις αγοραστή (acquirer) – προμηθευτή (supplier) που ορίζονται στο ISO 27036 δύναται να αποτελούν, η αγορά προϊόντων (**Supplier relationship for products**), η παροχή υπηρεσιών (**Supplier relationship for services**), η εφοδιαστική αλυσίδα στις Τεχνολογίες Πληροφοριών και Επικοινωνιών (**ICT Supply Chain**), η παροχή υπολογιστικών υπηρεσιών μέσω του Νέφους (**Cloud Computing**).

Προκειμένου να επιτευχθούν οι παραπάνω σχέσεις μεταξύ ενός οργανισμού και ενός προμηθευτή, απαιτείται η παροχή πρόσβασης στα συστήματα και τις πληροφορίες του πρώτου από τον δεύτερο, και όχι μόνο. Αυτό καθιστά προφανές πως προκύπτουν πολλοί κίνδυνοι ασφάλειας πληροφοριών, οι οποίοι είναι απαραίτητο να είναι διαχειρίσιμοι, μέσω ενός σχετικού πλαισίου. [30]

### 4.1.2 Πεδίο εφαρμογής

Το ISO 27036 εφαρμόζεται σε οργανισμούς κάθε μεγέθους και κλάδου που συνεργάζονται με εξωτερικούς φορείς και επιθυμούν ή είναι υποχρεωμένοι, ανάλογα με το είδους τους, να εφαρμόσουν ένα πλαίσιο διαχείρισης κινδύνων που σχετίζονται με αυτές τις συνεργασίες.

Το πρότυπο επισημαίνει ότι η ασφάλεια πληροφοριών δεν αφορά μόνο την τεχνολογία αλλά και τη διαχείριση των διαδικασιών και των σχέσεων με τους ανθρώπους. Ιδιαίτερα εστιάζει:

- Στη συμβολή του **ανθρώπινου παράγοντα** στην ασφάλεια.
- Στη σημασία της ύπαρξης **σαφήνειας** και **διαφάνειας** στις σχέσεις και συμφωνίες με τους προμηθευτές.

- Στην ανάγκη **διαρκούς αξιολόγησης και παρακολούθησης** των σχέσεων με τους προμηθευτές.

## 4.2 Δομή Προτύπου

Σε μία σχέση οι προμηθευτές μπορεί να έχουν άμεση ή έμμεση πρόσβαση σε πληροφορίες και συστήματα ενός οργανισμού ή να παρέχουν προϊόντα όπως λογισμικό, υλικό και υπηρεσίες που συνδέονται με την επεξεργασία πληροφοριών.

Για τη διαχείριση αυτών των κινδύνων το ISO/IEC 27036 προσφέρει συγκεκριμένες κατευθυντήριες γραμμές που βασίζονται στα πρότυπα ISO/IEC 27001 και ISO/IEC 27002, ενσωματώνοντας παράλληλα πρακτικές για την προστασία της ασφάλειας πληροφοριών σε όλα τα στάδια της σχέσης/ συνεργασίας.

Το πρότυπο χωρίζεται σε τέσσερα μέρη, όπως απεικονίζεται στην αρχιτεκτονική του:

1. Μέρος 1: Γενική δομή και έννοιες (Part 1: Overview and Concepts)
   Το πρώτο μέρος του προτύπου περιλαμβάνει τη γενική παρουσίαση της ασφάλειας πληροφοριών στις σχέσεις με προμηθευτές. Παρουσιάζει:
   - **Βασικές έννοιες** που σχετίζονται με την ασφάλεια πληροφοριών στην εφοδιαστική αλυσίδα αλλά κι άλλες που θα αναφέρονται συχνά και στα επόμενα μέρη του προτύπου.
   - **Μία γενική εικόνα** της σημασίας ενός πλαισίου διαχείρισης κινδύνων αλλά και των ίδιων των κινδύνων.

   Το 1ο Μέρος λειτουργεί ως θεμέλιο για την κατανόηση του σκοπού και του αντικειμένου του προτύπου με σκοπό την εισαγωγή στα επόμενα μέρη.

2. Μέρος 2: Απαιτήσεις (Part 2: Requirements)
   Το δεύτερο μέρος εστιάζει στην καθιέρωση συγκεκριμένων απαιτήσεων που πρέπει να ικανοποιούνται για την ασφάλεια πληροφοριών στις σχέσεις με προμηθευτές. Καλύπτει:
   - Τον καθορισμό υψηλών απαιτήσεων για αγοραστές και προμηθευτές **κατά την καθιέρωση της στρατηγικής δομής πριν ξεκινήσει η σχέση.**
   - Τον καθορισμό απαιτήσεων για αγοραστές και προμηθευτές, **μετά την έναρξη της σχέσης και για όσο αυτή διαρκεί.**

3. Μέρος 3: Κατευθυντήριες γραμμές για τη διαχείριση κινδύνων στην αλυσίδα εφοδιασμού της τεχνολογίας πληροφοριών (ICT) (Part 3: Guidelines for Information and Communication Technology (ICT) Supply Chain Security)
   Το τρίτο μέρος επικεντρώνεται στις σχέσεις προμηθευτών που σχετίζονται με την τεχνολογία πληροφοριών και επικοινωνιών (ICT). Παρουσιάζει:
   - Τις **απειλές και προκλήσεις ασφάλειας** που σχετίζονται με την προμήθεια τεχνολογικών υπηρεσιών.
   - Βασικές **πρακτικές ασφάλειας** για την παροχή ICT υπηρεσιών.
   - Τον **κύκλο ζωής** της παροχής υπηρεσιών ICT.

4. Μέρος 4: Οδηγίες για την ασφάλεια στις υπηρεσίες cloud (Part 4: Guidelines for Security of Cloud Services)
   Το τέταρτο και τελευταίο μέρος, εξειδικεύεται στην ασφάλεια της παροχής υπηρεσιών cloud. Παρουσιάζει:

- **Προκλήσεις και απειλές** που προκύπτουν από τη διάθεση υπηρεσιών Cloud.
- Προτεινόμενα μέτρα ασφάλειας πληροφοριών **κατά την απόκτηση μιας υπηρεσίας Cloud.**
- Προτεινόμενα μέτρα ασφάλειας πληροφοριών για του **παρόχους υπηρεσιών Cloud.** [30]


*Εικόνα 5: ISO 27036 μέρη*

## 4.3 Μέρος 1: Γενική δομή και έννοιες (Part 1: Overview and Concepts)

Το πρώτο μέρος του προτύπου ISO/IEC 27036, με τίτλο "Γενική Δομή και Έννοιες" (ISO/IEC 27036-1), αποτελεί το θεμέλιο για την κατανόηση και την εφαρμογή των αρχών ασφάλειας πληροφοριών στις σχέσεις με προμηθευτές. Το πρώτο μέρος λειτουργεί ως εισαγωγή στα επόμενα και θέτει τις βάσεις για τη συστηματική διαχείριση των κινδύνων που προκύπτουν από τη συνεργασία με τρίτους.

Το **ISO/IEC 27036-1-2021** καθορίζει τις βασικές έννοιες, την ορολογία και τις θεμελιώδεις αρχές που διέπουν τη διαχείριση σχέσεων προμηθευτών. Έχει σχεδιαστεί για να παρέχει μια ολιστική κατανόηση της σημαντικότητας της ασφάλειας πληροφοριών στο πλαίσιο των σχέσεων με προμηθευτές και εστιάζει στη σημασία της εμπιστοσύνης μεταξύ των εμπλεκόμενων μερών, προωθώντας τη διαφάνεια και τη συνεργασία. Βασικός στόχος είναι η κατανόηση της ανάγκης διασφάλισης των πληροφοριών που μοιράζονται οι οργανισμοί με τους προμηθευτές τους και η συνεχής προστασία τους καθ' όλη τη διάρκεια της συνεργασίας.

Ως εισαγωγή, το μέρος 1 περιγράφει την προσέγγιση που πρέπει να ακολουθείται για την αναγνώριση και την αντιμετώπιση των κινδύνων. Αυτό περιλαμβάνει τη δημιουργία ενός πλαισίου για την αναγνώριση των απειλών που σχετίζονται με την αλληλεπίδραση με προμηθευτές. Για την καλύτερη κατανόηση, αναφέρονται παραδείγματα κινδύνων που προκύπτουν από την παροχή μίας υπηρεσίας ή προϊόντος και δύνανται να υπονομεύσουν την εμπιστοσύνη στις επιχειρηματικές δραστηριότητες και να επεκταθούν σε ολόκληρο τον κύκλο ζωής της σχέσης με τον προμηθευτή, από τον αρχικό σχεδιασμό έως και τη λήξη της συνεργασίας. Ένα βασικό πρόβλημα εντοπίζεται στην έλλειψη συντονισμένης διακυβέρνησης (coordination of governance) και στον ασαφή καθορισμό ρόλων και ευθυνών για την ασφάλεια των πληροφοριών. Ιδιαίτερα σε μεγάλους οργανισμούς, οι σχέσεις με προμηθευτές δημιουργούνται από διαφορετικές

εσωτερικές μονάδες μέσω ανομοιογενών διαδικασιών, χωρίς ενιαία παρακολούθηση ή έλεγχο, γεγονός που καθιστά δύσκολη την αξιολόγηση και αντιμετώπιση των κινδύνων. Οι κίνδυνοι εντείνονται όταν οι προμηθευτές έχουν πρόσβαση σε πληροφορίες ή συστήματα του αγοραστή, χωρίς να έχουν προηγηθεί σαφείς συμφωνίες σχετικά με τα απαιτούμενα μέτρα ασφάλειας ή την κατανομή ευθυνών. Επιπλέον, η κακή επικοινωνία, οι πολιτισμικές ή νομικές διαφορές και η υπερβολική εξάρτηση από τους μηχανισμούς ελέγχου του τρίτου μέρους ενδέχεται να προκαλέσουν κενά και συγκρούσεις στα εφαρμοζόμενα μέτρα ασφάλειας. Οι συνέπειες μπορεί να περιλαμβάνουν μη εξουσιοδοτημένη πρόσβαση σε δεδομένα, μη συμμόρφωση με το κανονιστικό πλαίσιο , διακοπή λειτουργίας και να προκαλέσει αρνητικό αντίκτυπο στη φήμη του οργανισμού. Ως εκ τούτου, η αποτελεσματική διαχείριση των σχέσεων με προμηθευτές απαιτεί θεσμοθετημένες συμφωνίες, ευθυγράμμιση των απαιτήσεων ασφάλειας πληροφοριών και συνεχή εκτίμηση των κινδύνων, ώστε να διασφαλίζεται η προστασία των κρίσιμων πληροφοριακών πόρων. Επιπλέον, τίθεται το θεωρητικό υπόβαθρο για την εφαρμογή συγκεκριμένων πολιτικών και διαδικασιών που εξασφαλίζουν την προστασία των πληροφοριών.

Μεταξύ των σημαντικών αρχών που εισάγει το ISO/IEC 27036-1 είναι η ανάγκη προσαρμογής των πολιτικών ασφάλειας πληροφοριών ανάλογα με το είδος της συνεργασίας. Στο πρότυπο σημειώνεται ότι η διαχείριση κινδύνων πρέπει να είναι μια δυναμική διαδικασία, καθώς οι προκλήσεις και οι απειλές μπορεί να εξελίσσονται κατά τη διάρκεια της συνεργασίας. Παράλληλα, επισημαίνεται ότι η διασφάλιση της συμμόρφωσης με κανονισμούς προστασίας δεδομένων αποτελεί θεμελιώδη προϋπόθεση για κάθε επιχειρηματική σχέση. [30]

## 4.4 Μέρος 2: Απαιτήσεις (Part 2: Requirements)

Το 2ο μέρος της σειράς ISO/IEC 27036 περιγράφει τις απαιτήσεις διαχείρισης σχέσεων με προμηθευτές από τη μεριά της ασφάλειας πληροφοριών. Αποτελεί τον πυρήνα της σειράς, παρέχοντας λεπτομερείς οδηγίες για το πώς οι οργανισμοί μπορούν να δημιουργούν, να συντηρούν και να λήγουν συνεργασίες με τρίτους φορείς με τρόπο που δεν επιφέρει επιπτώσεις και δεν αναπτύσσει κινδύνους παραβίασης της ασφάλειας πληροφοριών. Η προσέγγιση που ακολουθεί βασίζεται στη διαχείριση του κύκλου ζωής της σχέσης με τον προμηθευτή, από την αρχική επιλογή αυτού έως την τελική διακοπή της σχέσης, με κάθε στάδιο να περιλαμβάνει συγκεκριμένες διαδικασίες και απαιτήσεις.

Το πρότυπο καθορίζει τις διαδικασίες που πρέπει να ακολουθήσουν οι οργανισμοί για να εξασφαλίσουν την προστασία πληροφοριών και δεδομένων που ανταλλάσσονται κατά τη διάρκεια των σχέσεων με τους προμηθευτές.

Αρχικά, ορίζονται οι βασικές και υψηλού επιπέδου απαιτήσεις ασφάλειας πληροφοριών που υλοποιούνται στη διαχείριση σχέσεων **με πολλούς προμηθευτές**, κατά την καθιέρωση της στρατηγικής δομής **πριν ξεκινήσει η σχέση** και χωρίζεται σε τέσσερις βασικούς άξονες:

1. Διαδικασίες σύναψης συμφωνίας (Agreement Processes)
   Σκοπός είναι για κάθε ενδιαφερόμενο μέρος να καθιερωθεί μία στρατηγική για τη σχέση αγοραστή – προμηθευτή. Από τη μεριά του ο αγοραστής, πρέπει να ορίσει μια στρατηγική, όπου θα βασίζεται στο επιτρεπτό όριο κινδύνου ασφάλειας πληροφοριών του ίδιου (acquirer's risk tolerance) και να καθοριστεί μία

βασική γραμμή αναφοράς ασφάλειας πληροφοριών (information security baseline) που θα χρησιμοποιηθεί στο σχεδιασμό, στη προετοιμασία, στη διαχείριση και τερματισμό της απόκτησης ενός προϊόντος ή υπηρεσίας. Αντίστοιχα ο προμηθευτής, πρέπει να ορίσει μια στρατηγική, όπου θα βασίζεται στο επιτρεπτό όριο κινδύνου ασφάλειας πληροφοριών του ίδιου (supplier's risk tolerance) και να ορίσει επίσης μία βασική γραμμή αναφοράς ασφάλειας πληροφοριών (information security baseline) που θα χρησιμοποιηθεί στο σχεδιασμό, στη προετοιμασία, στη διαχείριση και λήξη της προμήθειας ενός προϊόντος ή υπηρεσίας.

Οι απαιτήσεις από τη μεριά του αγοραστή κατά την περίοδο απόκτησης μιας υπηρεσίας ή ενός προϊόντος, επιγραμματικά περιλαμβάνουν τον ορισμό, την υλοποίηση, τη διατήρηση και τη βελτίωση μιας στρατηγικής που θα περιέχει μεταξύ άλλων,

- ένα **πλαίσιο ασφάλειας πληροφοριών** για την αξιολόγηση των κινδύνων που προκύπτουν με την αγορά ενός προϊόντος ή υπηρεσίας,
- ένα πλαίσιο για τον **ορισμό των απαιτήσεων κατά τη φάση του σχεδιασμού** (planning process),
- ένα πλαίσιο που θα περιγράφει τα κριτήρια επιλογής του προμηθευτή,
- τις **υψηλού επιπέδου απαιτήσεις** που θα χρειαστούν σε διάφορες φάσεις (έναρξη, υλοποίηση, τερματισμός) της συνεργασίας, π.χ. στη περίπτωση που η προμήθεια του προϊόντος/ υπηρεσίας μεταφερθεί σε διαφορετικό προμηθευτή,
- ορισμός **υπεύθυνου προσώπου** για τη διαχείριση της ασφάλειας πληροφοριών στη σχέση με τους προμηθευτές και
- **ανανέωση της στρατηγικής** μία φορά τη χρόνο ή και νωρίτερα αν χρειάζεται.

Οι απαιτήσεις από τη μεριά του προμηθευτή κατά τη φάση προμήθειας μιας υπηρεσίας ή ενός προϊόντος είναι ακριβώς οι ίδιες με αυτές του αγοραστή με τη διαφορά ότι αναφέρονται στην προμήθεια και όχι την απόκτηση μιας υπηρεσίας ή ενός προϊόντος.

2. Οργανωτικές διαδικασίες έναρξης έργων (Organizational Project-Enabling Processes)

Σκοπός είναι η διαμόρφωση του περιβάλλοντος, των δυνατοτήτων και των υποδομών που είναι απαραίτητες για την αποτελεσματική διαχείριση και εκτέλεση έργων και προγραμμάτων. Οι εν λόγω διαδικασίες ευθυγραμμίζουν τα έργα με τους στρατηγικούς στόχους, διασφαλίζοντας τη συνέπεια, την αποδοτικότητα και τη συμμόρφωση με τις βέλτιστες πρακτικές. Το πρότυπο ορίζει τις παρακάτω απαιτήσεις για τα δύο μέρη:

- Καθορισμός **διεργασίας για τον ορισμό μοντέλου του κύκλου ζωής** της σχέσης αγοραστή - προμηθευτή. Για την καθιέρωση της εν λόγω διεργασίας χρειάζεται ο ορισμός, η διατήρηση και επιβεβαίωση της διαθεσιμότητας των πολιτικών, διεργασιών, διαδικασιών και μοντέλων κύκλου ζωής.
- Ορισμός **διεργασίας διαχείρισης των υποδομών του Οργανισμού** στο πλαίσιο ασφάλειας πληροφοριών. Για τον σκοπό αυτό το 27036-2

περιγράφει τις σχετικές απαιτήσεις που είναι κοινές για όλα τα μέρη, όπως ο ορισμός φυσικών και λογικών δυνατοτήτων ασφάλειας υποδομών, και τον ορισμό και διατήρηση διακανονισμού έκτακτης ανάγκης για τη συνέχιση της απόκτησης ή προσφοράς ενός αγαθού/ υπηρεσίας σε περίπτωση περιστατικού ασφαλείας.

- Δημιουργία **διαδικασίας ελέγχου ασφάλειας πληροφοριών και όλης της επιχειρηματικής αποστολής** για κάθε έργο που εμπλέκονται ο αγοραστής και ο προμηθευτής ξεχωριστά. Απαραίτητη είναι η αναγνώριση και κατηγοριοποίηση των προμηθευτών και αγοραστών με βάση την ευαισθησία των δεδομένων που έχουν πρόσβαση ο καθένας, όπως και η δημιουργία και διατήρηση πλάνου λήξης (termination plan) έργου. Σ 'αυτό το σημείο από τη μεριά του αγοραστή μόνο υπάρχει μία ακόμα απαίτηση, η οποία έχει να κάνει με την τεκμηριωμένη αξιολόγηση του προμηθευτή για κάθε έργο ξεχωριστά.
- Διασφάλιση ότι το **ανθρώπινο δυναμικό** που εμπλέκεται δεν έχει ποινικό μητρώο, είναι κατάλληλα εκπαιδευμένο, γνωρίζει τις πολιτικές και διαδικασίες, αξιολογείται τακτικά και σε περίπτωση φυγής κάποιου υπευθύνου ατόμου θα υπάρχει άλλο άτομο άμεσα αντικαταστάσιμο.
- Διασφάλιση της **ποιότητας των προϊόντων και υπηρεσιών** που θα φτάσουν στους καταναλωτές, αλλά και η δυνατότητα επαναχρησιμοποίησης γνώσεων στη διαδικασία.

3. Διαδικασίες Τεχνικής Διαχείρισης (Technical Management Processes)

Σκοπός των διαδικασιών αυτών είναι η διασφάλιση ότι οι απαιτήσεις ασφάλειας ενσωματώνονται στην προμήθεια, ανάπτυξη και διαχείριση έργων που σχετίζονται με προμηθευτές. Αυτό επιτυγχάνεται μέσω μιας δομημένης προσέγγισης στη διαχείριση κινδύνων, τον σχεδιασμό έργων, τη μέτρηση, τη διαμόρφωση και τη λήψη αποφάσεων, ώστε να αντιμετωπίζονται όλες οι πτυχές της ασφάλειας πληροφοριών καθ' όλη τη διάρκεια του κύκλου ζωής της εφοδιαστικής αλυσίδας. Επιπλέον, σημειώνεται η ανάγκη για τους Οργανισμούς να καθιερώσουν σαφείς μεθοδολογίες για τη μείωση των κινδύνων ασφαλείας πληροφοριών που προκύπτουν από τις σχέσεις με προμηθευτές. Οι απαιτήσεις που περιγράφονται, ισχύουν τόσο για τους αγοραστές όσο και για τους προμηθευτές, διασφαλίζοντας ότι τα μέτρα ασφαλείας εφαρμόζονται και από τις δύο πλευρές:

- Ορισμός **διαδικασίας Σχεδιασμού Έργου**, όπου διασφαλίζεται ότι η ασφάλεια πληροφοριών ενσωματώνεται στον σχεδιασμό των έργων. Οι αγοραστές και οι προμηθευτές πρέπει να λαμβάνουν υπόψη τις επιπτώσεις των απαιτήσεων ασφαλείας στο κόστος, τα χρονοδιαγράμματα και τις αρμοδιότητες του έργου. Επιπλέον, είναι κρίσιμη η προστασία ευαίσθητων εσωτερικών δεδομένων, όπως πνευματική ιδιοκτησία, προσωπικά δεδομένα και οικονομικά αρχεία.
- Ορισμός **διαδικασίας αξιολόγησης και ελέγχου του έργου** ώστε να διασφαλιστεί η συμμόρφωση με τις προκαθορισμένες απαιτήσεις ασφαλείας και λειτουργικότητας. Εγγυάται ότι τα έργα ευθυγραμμίζονται με τους προϋπολογισμούς, τις τεχνικές απαιτήσεις και τα χρονοδιαγράμματα, ενώ παράλληλα παρακολουθεί συνεχώς τους κινδύνους ασφαλείας.
- Ορισμός **διαδικασίας διαχείρισης αποφάσεων**, έτσι ώστε οι οργανισμοί να επιλέξουν την πιο συμφέρουσα πορεία δράσης όταν υπάρχουν

εναλλακτικές επιλογές. Εξασφαλίζει ότι οι ανησυχίες για την ασφάλεια λαμβάνονται υπόψη σε όλες τις βασικές αποφάσεις που επηρεάζουν τις σχέσεις με τους προμηθευτές.

- Δημιουργία **πλαισίου διαχείρισης κινδύνων** που θα στοχεύει στον εντοπισμό, την αξιολόγηση και την αντιμετώπιση των κινδύνων που προκύπτουν από την προμήθεια και τη συνεργασία με προμηθευτές. Το πλαίσιο αυτό πρέπει να επανεξετάζεται περιοδικά ώστε να αντικατοπτρίζει αλλαγές στις επιχειρηματικές, νομικές, κανονιστικές και συμβατικές απαιτήσεις. Οι απαιτήσεις που περιγράφονται σχετικά με την εν λόγω διεργασία είναι:
  - η αξιολόγηση προμηθευτών και αγοραστών με βάση το ιστορικό συναλλαγών και τη συμμόρφωση με τις συμβατικές υποχρεώσεις,
  - ο καθορισμός απαιτήσεων ασφαλείας στις συμβάσεις και τις συμφωνίες και
  - η εφαρμογή πλαισίων κατηγοριοποίησης κινδύνων για την ανάλυση πιθανών ευπαθειών στις σχέσεις με προμηθευτές.

- Ορισμός **διαδικασίας διαχείρισης διαμόρφωσης** όπου διασφαλίζεται η ακεραιότητα και ο έλεγχος των διαμορφώσεων που σχετίζονται με τους προμηθευτές καθ' όλη τη διάρκεια του έργου. Οι οργανισμοί ενθαρρύνονται να ενσωματώσουν μηχανισμούς διαχείρισης αλλαγών και ελέγχου.

- Θέσπιση **μέτρων προστασίας απορρήτου, ακρίβειας και πληρότητας** για τη διαχείριση δεδομένων προμηθευτών. Τα πλαίσια ISMS που βασίζονται στο ISO/IEC 27001 μπορούν να ενισχύσουν την ασφάλεια σε αυτόν τον τομέα.

- Ανάπτυξη **πλαισίου μέτρησης για τη συλλογή, ανάλυση και αναφορά σχετικών δεικτών**. Οι αγοραστές και οι προμηθευτές πρέπει να συμφωνήσουν σχετικά με το τι θα μετρηθεί, πώς θα αναφερθεί και ποιες διορθωτικές ενέργειες απαιτούνται εάν δεν επιτευχθούν τα όρια ασφαλείας.

- Ορισμός **διαδικασίας διασφάλισης ποιότητας** που βεβαιώνει ότι το υπάρχον πλαίσιο διαχείρισης ποιότητας του οργανισμού εφαρμόζεται σε έργα που σχετίζονται με προμηθευτές. Αν και δεν επιβάλλονται συγκεκριμένοι στόχοι ασφαλείας, αυτή η διαδικασία διασφαλίζει ότι οι απαιτήσεις ασφαλείας λαμβάνονται υπόψη στους συνολικούς ελέγχους ποιότητας του έργου.

4. Τεχνικές Διαδικασίες (Technical Processes)

Στόχος είναι η καθιέρωση μιας συστηματικής προσέγγισης για την αξιολόγηση των κινδύνων και των απαιτήσεων ασφαλείας στα πρώιμα στάδια του κύκλου ζωής του έργου. Αυτό περιλαμβάνει τον καθορισμό μέτρων ασφαλείας στην ανάλυση επιχειρηματικών απαιτήσεων και στην τεχνική αρχιτεκτονική των προϊόντων και υπηρεσιών που αφορούν τους προμηθευτές.

- Ορισμός **Διαδικασίας Επιχειρησιακής Ανάλυσης** όποτ διασφαλίζεται ότι οι παράγοντες ασφάλειας των πληροφοριών ενσωματώνονται στην επιχειρησιακή ανάλυση όταν συνεργάζονται με προμηθευτές. Αυτό είναι

απαραίτητο για την ευθυγράμμιση των μέτρων ασφαλείας με τους επιχειρηματικούς στόχους και την αποφυγή τυχόν ευπαθειών στις συνεργασίες με προμηθευτές.

- Ο **αγοραστής** πρέπει να διασφαλίσει ότι οι ανησυχίες ασφαλείας πληροφοριών ενσωματώνονται στην επιχειρηματική ανάλυση για την επίτευξη ισορροπίας μεταξύ επιχειρησιακών στόχων και απαιτήσεων ασφάλειας πληροφοριών.
- Ο **προμηθευτής**, πρέπει να λαμβάνει υπόψη του και να αντιμετωπίζει τις ανησυχίες ασφαλείας κατά την ευθυγράμμιση των υπηρεσιών ή προϊόντων του με τις επιχειρηματικές ανάγκες του αγοραστή.

- Ορισμός **διαδικασίας Ορισμού Αρχιτεκτονικής**, που στοχεύει στη διαμόρφωση ενός τεχνικού πλαισίου που εξασφαλίζει τη διαρκή προστασία των προϊόντων ή υπηρεσιών στις σχέσεις με προμηθευτές. Η δημιουργία μιας ασφαλούς και συνεπούς αρχιτεκτονικής βάσης είναι απαραίτητη για τη διατήρηση της ασφάλειας των πληροφοριών σε όλο τον κύκλο ζωής του προϊόντος ή της υπηρεσίας.
  - Ο **αγοραστής**, είναι υπεύθυνος για τον καθορισμό, την εφαρμογή, τη διατήρηση και τη βελτίωση των απαιτήσεων ασφαλείας για προϊόντα ή υπηρεσίες που σχετίζονται με προμηθευτές.
  - Ο **προμηθευτής**, πρέπει να διασφαλίσει ότι οι απαιτήσεις ασφαλείας που καθορίζονται από τον αγοραστή εφαρμόζονται με συνέπεια σε όλα τα προϊόντα και τις υπηρεσίες.

Στη συνέχεια του προτύπου, ορίζονται οι βασικές και υψηλού επιπέδου απαιτήσεις ασφάλειας πληροφοριών που υλοποιούνται στη διαχείριση σχέσεων **με έναν προμηθευτή, κατά την καθιέρωση αλλά και διατήρηση της σχέσης** και χωρίζεται σε πέντε βασικούς άξονες:

1. Διαδικασία σχεδιασμού των σχέσεων με τους προμηθευτές (Supplier relationship planning process)
   Στόχος είναι να διασφαλιστεί η ορθή διαχείριση της ασφάλειας πληροφοριών στη σχέση με τον προμηθευτή. Συγκεκριμένα, περιλαμβάνονται:
   - **Δημιουργία εγγράφου** που θα αφορά την τεκμηρίωση της απόφασης σχετικά με την προμήθεια ενός προϊόντος ή υπηρεσίας, από τη διοίκηση.
   - Η **διαχείριση των σχετικών ζητημάτων** που συνδέονται με την ασφάλεια πληροφοριών κατά τη διάρκεια της σχέσης με τον προμηθευτή.

   Βασικά στοιχεία που πρέπει να ληφθούν υπόψη κατά την εκτέλεση της διαδικασίας αποτελούν:
   - η στρατηγική σχέσης με τον προμηθευτή,
   - τα κίνητρα και οι προσδοκίες της διοίκησης από την προμήθεια του προϊόντος ή της υπηρεσίας,
   - το προβλεπόμενο πεδίο εφαρμογής του προϊόντος ή της υπηρεσίας,
   - τα συμπεράσματα από συναφή αναφορές, όπως αξιολογήσεις κινδύνου, εκτιμήσεις επιπτώσεων στην ιδιωτικότητα και δοκιμές διείσδυσης και
   - η υφιστάμενη τεκμηρίωση διαχείρισης σχέσεων με προμηθευτές.

   Οι βασικές δραστηριότητες που εκτελούνται στη διαδικασία σχεδιασμού της σχέσης με τον προμηθευτή περιλαμβάνουν:

- την ταυτοποίηση και αξιολόγηση των κινδύνων ασφάλειας πληροφοριών που σχετίζονται με την προμήθεια,
- την ανάθεση ρόλων και ευθυνών για τη διαχείριση της ασφάλειας πληροφοριών στη σχέση με τον προμηθευτή,
- την ανάλυση της νομικής και κανονιστικής συμμόρφωσης που επηρεάζει τη σχέση με τον προμηθευτή,
- τον καθορισμό ενός σχεδίου διαχείρισης σχέσης με τον προμηθευτή που να συνάδει με τη στρατηγική της επιχείρησης και
- την δημιουργία ελάχιστων απαιτήσεων ασφάλειας πληροφοριών που πρέπει να τηρούνται καθ' όλη τη διάρκεια της σχέσης.

Τα αποτελέσματα της εν λόγω διαδικασίας θα είναι:

- μια **αξιολόγηση κινδύνου ασφάλειας πληροφοριών** και ένα σχέδιο αντιμετώπισης κινδύνων,
- η **τεκμηριωμένη απόφαση** της διοίκησης σχετικά με την αποδοχή ή απόρριψη της προμήθειας, βασισμένη στην αξιολόγηση κινδύνου, και
- το **σχέδιο διαχείρισης σχέσης** με τον προμηθευτή.

Η διαδικασία αυτή διασφαλίζει ότι οι οργανισμοί λαμβάνουν τεκμηριωμένες αποφάσεις σχετικά με την προμήθεια προϊόντων ή υπηρεσιών, ενσωματώνοντας πρακτικές ασφαλείας πληροφοριών στη σχέση με τους προμηθευτές.

2. Διαδικασία επιλογής προμηθευτών (Supplier Selection process)

Σκοπός της διαδικασίας, είναι να διασφαλίσει ότι ο προμηθευτής θα παρέχει κατάλληλα μέτρα ασφαλείας πληροφοριών για το προϊόν ή την υπηρεσία που θα προσφέρει. Ο αγοραστής οφείλει να καθορίσει απαιτήσεις ασφαλείας πληροφοριών στα έγγραφα διαγωνισμού, ενώ πρέπει να αξιολογήσει το επίπεδο του κινδύνου ασφάλειας πληροφοριών του προμηθευτή πριν τον επιλέξει.

Ο **αγοραστής** έχει την ευθύνη να καθορίσει τα **κριτήρια επιλογής** των προμηθευτών, ώστε να διασφαλιστεί ότι οι υποψήφιοι προμηθευτές πληρούν τις απαιτήσεις ασφάλειας πληροφοριών. Στο πλαίσιο αυτό, πρέπει να εξεταστούν τόσο νομικά και κανονιστικά ζητήματα, όσο και η συμμόρφωση με διεθνή πρότυπα όπως το ISO/IEC 27001. Παράλληλα, πρέπει να πραγματοποιηθεί **εκτίμηση κινδύνων**, η οποία θα καθορίσει το αποδεκτό όριο του κινδύνου και τα αποτελέσματα της θα ενσωματωθούν σε ένα σχέδιο διαχείρισης κινδύνων.

Μία από τις πιο σημαντικές ενέργειες του **αγοραστή** είναι η προετοιμασία των **εγγράφων διαγωνισμού** (Request For Proposal – RFP, Invitation To Tender – ITT). Η ύπαρξη συμφωνιών εμπιστευτικότητας είναι κρίσιμη ώστε να διασφαλιστεί η προστασία των δεδομένων κατά τη διάρκεια της διαδικασίας επιλογής. Τα έγγραφα του διαγωνισμού πρέπει να περιέχουν σαφείς τεχνικές προδιαγραφές, απαιτήσεις ασφαλείας πληροφοριών, δείκτες απόδοσης και πιθανά πρόστιμα σε περίπτωση μη συμμόρφωσης.

Μετά τη λήψη των προσφορών των προμηθευτών, ο **αγοραστής** πρέπει να αξιολογήσει την κάθε μία προσφορά με βάση τα κριτήρια που έχει καθορίσει. Η διαδικασία αυτή περιλαμβάνει την επαλήθευση της συμμόρφωσης των προμηθευτών με τις απαιτήσεις ασφαλείας πληροφοριών, προκειμένου να διασφαλιστεί ότι ο προμηθευτής που θα επιλεγεί είναι κατάλληλος για τη συνεργασία.

Ο **προμηθευτής**, από την πλευρά του, οφείλει να αναλύσει τις απαιτήσεις που του έχουν τεθεί και να κρίνει αν μπορεί να συμμορφωθεί με αυτές. Εάν αποφασίσει να συμμετάσχει στο διαγωνισμό, πρέπει να προετοιμάσει ένα **σχέδιο αντιμετώπισης κινδύνων** και να υπογράψει τις απαραίτητες **συμφωνίες εμπιστευτικότητας**, διασφαλίζοντας ότι τα δεδομένα του αγοραστή δεν θα εκτεθούν σε μη εξουσιοδοτημένα τρίτα μέρη.
Πρέπει επίσης να διαχειριστεί τυχόν υπεργολάβους που θα συμμετέχουν για την παροχή της υπηρεσίας ή του προϊόντος. Αυτό σημαίνει ότι πρέπει να ενημερώσει τον αγοραστή για τη **χρήση υπεργολάβων** αν αυτή υπάρχει, και να διασφαλίσει ότι οι υπεργολάβοι συμμορφώνονται με τις ίδιες απαιτήσεις ασφαλείας πληροφοριών. Επίσης, οφείλει να υποβάλει μία πλήρη και διαφανή **προσφορά**, περιγράφοντας τα μέτρα ασφαλείας που προτίθεται να εφαρμόσει.

Σημαντικό κομμάτι της διαδικασίας είναι η **αξιολόγηση των κινδύνων** από την πλευρά του προμηθευτή. Εφόσον εντοπιστούν κίνδυνοι που καθιστούν δύσκολη ή αδύνατη τη συμμόρφωση με τις απαιτήσεις του αγοραστή, ο προμηθευτής μπορεί να αποφασίσει να μην συμμετάσχει στο διαγωνισμό. Η απόφαση αυτή βασίζεται στη σύγκριση μεταξύ των απαιτήσεων ασφαλείας πληροφοριών και των δυνατοτήτων του προμηθευτή να συμμορφωθεί με αυτές.

Στο τέλος της διαδικασίας, ο **αγοραστής και** ο **προμηθευτής** πρέπει να παράγουν συγκεκριμένα παραδοτέα. Ο αγοραστής δημιουργεί τα κριτήρια επιλογής προμηθευτών, τις συμφωνίες εμπιστευτικότητας, το έγγραφο διαγωνισμού και τα αποτελέσματα της αξιολόγησης των απαντήσεων των προμηθευτών. Ο προμηθευτής, από την πλευρά του, παράγει μία αξιολόγηση κινδύνου, μία απάντηση στο διαγωνισμό και, εφόσον απαιτείται, υπογράφει τη συμφωνία εμπιστευτικότητας.

Η διαδικασία αυτή συμβάλλει στη διασφάλιση της **διαφάνειας**, και την εξασφάλιση ότι η συνεργασία των μερών δεν θέτει σε κίνδυνο την ασφάλεια πληροφοριών του Οργανισμού.

3. Διαδικασία έναρξης σχέσης (Supplier relationship agreement process)

Στόχος της διαδικασίας έναρξης της σχέσης μεταξύ αγοραστή -προμηθευτή είναι η εφαρμογή των απαιτήσεων ασφάλειας πληροφοριών, ώστε να διασφαλιστεί η προστασία των δεδομένων, των πληροφοριακών συστημάτων και των επιχειρηματικών λειτουργιών που επηρεάζονται από τη συνεργασία. Περιλαμβάνει τον καθορισμό ρόλων και ευθυνών, την εφαρμογή μέτρων ασφάλειας και τη διαχείριση κινδύνων που σχετίζονται με την προμήθεια υπηρεσιών ή προϊόντων.

Για τη διαδικασία σύναψης συμφωνίας απαιτείται η ύπαρξη:

- **Στρατηγικής σχέσης** προμηθευτή τόσο από την πλευρά του αγοραστή όσο και από τον προμηθευτή,
- το **έγγραφο διαγωνισμού**, το οποίο περιέχει τις απαιτήσεις ασφαλείας,
- η **προσφορά** του προμηθευτή, που περιγράφει πώς θα συμμορφωθεί και με ποιες απαιτήσεις ασφαλείας.

Η διαδικασία περιέχει τις παρακάτω απαιτήσεις:

- **Καθορισμός της συμφωνίας**, όπου ο αγοραστής και ο προμηθευτής διαμορφώνουν μια συμφωνία που περιλαμβάνει τις απαιτήσεις ασφάλειας και τους δείκτες απόδοσης.
- **Ορισμός ρόλων και οι ευθύνες** κάθε πλευράς που αφορούν στη διαχείριση ασφάλειας πληροφοριών.
- Δημιουργία **σχεδίου ασφαλούς μετάβασης**, σε περίπτωση που η υπηρεσία μεταφέρεται από άλλον προμηθευτή. Το σχέδιο περιλαμβάνει μηχανισμούς διασφάλισης της ακεραιότητας, εμπιστευτικότητας και διαθεσιμότητας των δεδομένων.
- Καθορισμός **διαδικασίας διαχείρισης αλλαγών** (Information security change management procedure) που διασφαλίζει ότι οι τροποποιήσεις στη συνεργασία δεν θα επηρεάζουν αρνητικά την ασφάλεια.
- Ορισμός **διαδικασίας αναγνώρισης, αναφοράς και αντιμετώπισης περιστατικών ασφάλειας.**
- Ο αγοραστής πρέπει να παρακολουθεί τη συμμόρφωση του προμηθευτή με τις απαιτήσεις ασφαλείας, αλλά και ο προμηθευτής να τηρεί τα συμφωνηθέντα μέτρα ασφαλείας και να αναφέρει τυχόν αποκλίσεις.
- **Προστασία της πνευματικής ιδιοκτησίας και δεδομένων**, όπου καθορίζονται το είδος των δεδομένων και των πληροφοριακών συστημάτων που χρησιμοποιούνται κατά τη διάρκεια της συνεργασίας.

Σε περίπτωση λήξης της συνεργασίας, απαιτείται σχέδιο τερματισμού, το οποίο περιλαμβάνει:

- Την **καταστροφή των δεδομένων** που χρησιμοποιήθηκαν κατά τη διάρκεια της συνεργασίας.
- **Μηχανισμούς διασφάλισης** ότι η μεταφορά των δεδομένων γίνεται με ασφάλεια.
- **Δεσμεύσεις για τη μη αποκάλυψη ευαίσθητων πληροφοριών** μετά τη λήξη της συνεργασίας.
- **Έλεγχο της συμμόρφωσης** με τις απαιτήσεις ασφάλειας και παροχή αποδείξεων καταστροφής δεδομένων, όπου απαιτείται.

Με την ολοκλήρωση της εν λόγω διαδικασίας, θα πρέπει να υπάρχουν:

- **υπογεγραμμένη συμφωνία σχέσης**, η οποία θα αποθηκεύεται με τρόπο που εξασφαλίζει την ακεραιότητα και την εμπιστευτικότητα
- οριστικές **διαδικασίες διαχείρισης περιστατικών και αλλαγών**
- τεκμηριωμένο **σχέδιο τερματισμού της συνεργασίας**,
- καθορισμένος **τρόπος ασφαλούς ανταλλαγής πληροφοριών**
- συμφωνημένες **διαδικασίες συμμόρφωσης και διορθωτικών ενεργειών**.

4. Διαδικασία διαχείρισης των σχέσεων με τους προμηθευτές (Supplier relationship management process)

Η διαχείριση της σχέσης με τον προμηθευτή είναι απαραίτητη για τη διατήρηση της ασφάλειας των πληροφοριών καθ' όλη τη διάρκεια της συνεργασίας. Ο αγοραστής και ο προμηθευτής έχουν συγκεκριμένες ευθύνες για να εξασφαλίσουν τη συμμόρφωση με τις συμφωνημένες διαδικασίες ασφαλείας. Ο **αγοραστής** πρέπει να διασφαλίζει την ασφάλεια των πληροφοριών, ενώ παράλληλα

να διαχειρίζεται τη μετάβαση ενός προϊόντος ή μιας υπηρεσίας όταν υπάρχει αλλαγή προμηθευτή ή λειτουργικού ελέγχου, εκπαιδεύοντας το προσωπικό που επηρεάζεται, αντιμετωπίζοντας αλλαγές και περιστατικά που σχετίζονται με την ασφάλεια και παρακολουθώντας διαρκώς τη συμμόρφωση του προμηθευτή. Αντίστοιχα, ο **προμηθευτής** υποστηρίζει τον αγοραστή σε αυτές τις δραστηριότητες, βοηθώντας στη μετάβαση, εκπαιδεύοντας το προσωπικό, διαχειριζόμενος αλλαγές και περιστατικά ασφαλείας και συμμετέχοντας στη διαδικασία ελέγχου και επιβολής της συμμόρφωσης.

Για την εκτέλεση αυτών των δραστηριοτήτων, απαιτούνται τα **αποτελέσματα** που προκύπτουν από τη διαδικασία έναρξης της σχέσης, με ιδιαίτερη έμφαση στα δεδομένα παρακολούθησης της συμμόρφωσης και στα ιστορικά στοιχεία από τους ελέγχους που έχουν πραγματοποιηθεί. Ο αγοραστής πρέπει να καθορίσει ποιος θα είναι υπεύθυνος για την παρακολούθηση και την επιβολή της συμμόρφωσης του προμηθευτή, λαμβάνοντας υπόψη τα προηγούμενα αποτελέσματα. Ο προμηθευτής, από την πλευρά του, πρέπει να παρέχει πληροφορίες βασισμένες σε προηγούμενες διαδικασίες συμμόρφωσης που εφαρμόστηκαν σε άλλες συνεργασίες.

Για την επίτευξη των στόχων της διαχείρισης της σχέσης με τον προμηθευτή, απαιτούνται συγκεκριμένες ενέργειες από κάθε πλευρά:

- Ο αγοραστής οφείλει να διασφαλίσει ότι ο προμηθευτής έχει λάβει και κατανοήσει πλήρως τις απαιτήσεις ασφάλειας των πληροφοριών που ορίζονται στη συμφωνία.
- Η μετάβαση ενός προϊόντος ή μιας υπηρεσίας πρέπει να πραγματοποιείται σύμφωνα με το καθορισμένο σχέδιο μετάβασης, με άμεση επικοινωνία σε περίπτωση απρόβλεπτων καταστάσεων.
- Οποιαδήποτε αλλαγή ή περιστατικό σχετικό με την ασφάλεια των πληροφοριών πρέπει να διαχειρίζεται σύμφωνα με τις καθορισμένες διαδικασίες, ενώ το προσωπικό πρέπει να εκπαιδεύεται τακτικά ώστε να διατηρείται η συμμόρφωση με τις πολιτικές ασφαλείας.
- Ο αγοραστής πρέπει να παρακολουθεί γενικότερες αλλαγές που μπορεί να επηρεάσουν την προμηθευτική σχέση, όπως μεταβολές στη δομή της επιχείρησης, την οικονομική κατάσταση, την ιδιοκτησία, τη σύνθεση του προϊόντος, τις πιστοποιήσεις ασφαλείας ή τις νομικές και κανονιστικές απαιτήσεις.
- Ο προμηθευτής πρέπει να υποστηρίζει τον αγοραστή στη διαδικασία παρακολούθησης της συμμόρφωσης, παρέχοντας αναφορές σχετικά με κινδύνους ασφαλείας που έχουν εντοπιστεί, ενημερώνοντας για τα διορθωτικά μέτρα που έχουν ληφθεί και υποβάλλοντας περιοδικές εκθέσεις συμμόρφωσης.

Με την ολοκλήρωση της διαδικασίας εξασφαλίζεται η **διαφάνεια** και η **λογοδοσία** στη διαχείριση της σχέσης. Ο αγοραστής πρέπει να παράγει εκθέσεις εκτίμησης κινδύνου και ελέγχου συμμόρφωσης, καθώς και να κρατά αρχείο των στοιχείων που αφορούν αλλαγές στην ασφάλεια και περιστατικών. Αν απαιτείται, ο αγοραστής πρέπει επίσης να παρέχει εκθέσεις εκτέλεσης του σχεδίου μετάβασης και επικαιροποίησης της συμφωνίας. Ο προμηθευτής, από την πλευρά του, πρέπει να προστατεύει την ακεραιότητα, τη διαθεσιμότητα και την

εμπιστευτικότητα της ενημερωμένης συμφωνίας, διατηρώντας επίσης αρχείο των συμφωνημένων διορθωτικών μέτρων και της κατάστασής τους.

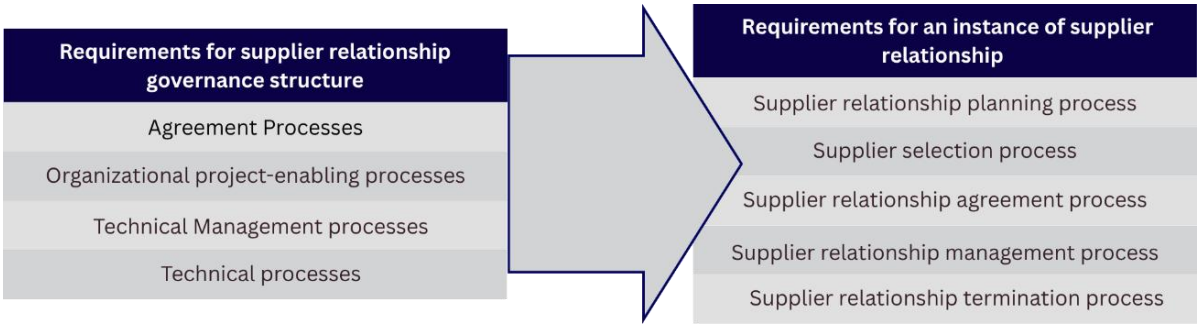
5. Διαδικασία τερματισμού της σχέσης με τον προμηθευτή (Supplier relationship termination process)
Κατά τη διαδικασία τερματισμού της σχέσης, τα δύο μέρη πρέπει να ακολουθήσουν το σχέδιο τερματισμού που έχει καθοριστεί και να διασφαλίσουν ότι δεν θα προκύψουν προβλήματα και κίνδυνοι ασφάλειας πληροφοριών.

Για την ομαλή εκτέλεση αυτής της διαδικασίας, πρέπει να ληφθούν υπόψη οι απαιτούμενες απαιτήσεις, όπως ορίζονται στο σχετικό πλαίσιο της συμφωνίας.

Οι δραστηριότητες που πρέπει να εκτελεστούν περιλαμβάνουν:

- Την **τεκμηρίωση τυχόν αιτιών που οφείλονται στην ασφάλεια πληροφοριών** και οδήγησαν στην απόφαση τερματισμού και την αξιολόγηση των σχετικών κινδύνων.
- Σε περίπτωση που προκύψει ανάγκη για άμεσο τερματισμό, ο αγοραστής μπορεί να ενεργοποιήσει το **σχέδιο επιχειρησιακής συνέχειας** (Business Continuity Plan - BCP), ειδικά αν η προμήθεια του προϊόντος ή της υπηρεσίας είναι κρίσιμη για τη λειτουργία του.
- **Απόφαση** για το αν η παροχή του αγαθού θα ακυρωθεί πλήρως ή αν θα μεταβιβαστεί σε άλλο προμηθευτή ή θα επιστραφεί στον αγοραστή.
- Ανάπτυξη **πλάνου επικοινωνίας** για την ενημέρωση του προσωπικού και τρίτων μερών που επηρεάζονται από τον τερματισμό της σχέσης.
- Ορισμός **υπεύθυνου** για τη διαχείριση της διαδικασίας σύμφωνα με το σχέδιο τερματισμού, καθώς και να διατηρηθεί ένα επικαιροποιημένο απόθεμα των περιουσιακών στοιχείων που χρησιμοποιούνται στην παροχή της υπηρεσίας ή του προϊόντος.
- **Συμφωνία** για το ποια περιουσιακά στοιχεία θα επιστραφούν στον αγοραστή ή σε νέο προμηθευτή, ποια θα παραμείνουν στον προμηθευτή και ποια θα καταστραφούν ή θα διατηρηθούν.
- Διασφάλιση ότι τα **λογικά και φυσικά δικαιώματα πρόσβασης** που είχαν παραχωρηθεί στον προμηθευτή για τη διαχείριση των εσωτερικών περιουσιακών στοιχείων του αγοραστή αφαιρούνται εγκαίρως.
- **Αμοιβαία συμφωνία** μεταξύ των δύο μερών σχετικά με την ολοκλήρωση του τερματισμού της παρεχόμενης υπηρεσίας ή προϊόντος.

Με το πέρας της διαδικασίας, ο αγοραστής πρέπει να έχει ένα σαφές πλάνο επικοινωνίας για τον τερματισμό, τον ορισμό υπευθύνου, μία ενημερωμένη καταγραφή των περιουσιακών στοιχείων που χρησιμοποιούνται στην προμήθεια και μία αναφορά εκτέλεσης του σχεδίου τερματισμού. Επιπλέον, εφόσον είναι απαραίτητο, μπορεί να περιλαμβάνεται μια αξιολόγηση κινδύνων και ένα σχέδιο διαχείρισης, αναφορές εκτέλεσης μεταβατικών σχεδίων, πιστοποιητικά καταστροφής περιουσιακών στοιχείων, καθώς και αναφορές απομάκρυνσης αφαίρεσης πρόσβασης. Σε περίπτωση συνεχιζόμενων απαιτήσεων εμπιστευτικότητας, πρέπει να διασφαλίζεται η ύπαρξη ολοκληρωμένων συμφωνιών εμπιστευτικότητας. Αντίστοιχα, ο προμηθευτής είναι υπεύθυνος για την εκπλήρωση των δικών του αντίστοιχων υποχρεώσεων και την παροχή των σχετικών αποτελεσμάτων που αποδεικνύουν τη συμμόρφωση με τη διαδικασία τερματισμού. [31]




*Σχήμα 5: ISO 27036-2 - Θεμελιώσεις απαιτήσεις ασφάλειας πληροφοριών*

## 4.5 Μέρος 3: Κατευθυντήριες γραμμές για τη διαχείριση κινδύνων στην αλυσίδα εφοδιασμού της τεχνολογίας πληροφοριών (ICT) (Part 3: Guidelines for Information and Communication Technology (ICT) Supply Chain Security)

Το **ISO/IEC 27036-3:2013** αποτελεί μέρος της σειράς ISO/IEC 27036 και εστιάζει στην ασφάλεια στην εφοδιαστική αλυσίδα των Τεχνολογιών Πληροφορικής και Επικοινωνιών (ICT supply chain), διασφαλίζοντας ότι οι κίνδυνοι που προκύπτουν από πολυσύνθετες εφοδιαστικές αλυσίδες αποτελούν μέρος ενός αποδοτικού πλαισίου διαχείρισης. Το 3ο μέρος του προτύπου, αφορά οργανισμούς που αποκτούν προϊόντα και υπηρεσίες ICT, επιτρέποντάς τους να μετριάσουν τους σχετικούς κινδύνους. Αναφέρεται τόσο σε οργανωτικούς όσο και σε τεχνικούς κινδύνους, (εισαγωγή κακόβουλου κώδικα, πλαστά προϊόντα Τεχνολογίας Πληροφοριών κλπ.), και προτείνει πρακτικές ασφάλειας στις διαδικασίες του κύκλου ζωής των συστημάτων και του λογισμικού (system and software lifecycle processes).

Το πρότυπο ευθυγραμμίζεται με το ISO/IEC 15288 και ISO/IEC 12207 για τις διαδικασίες κύκλου ζωής. Επιπλέον, καλύπτει τις απαιτήσεις του ISO/IEC 27002 που αφορά τα μέτρα ασφάλειας πληροφοριών που πρέπει να υλοποιούνται. Ωστόσο, δεν καλύπτει το κομμάτι της διαχείρισης επιχειρησιακής συνέχειας, η οποία εξετάζεται στο ISO/IEC 27031.

Οι διαδικασίες που περιλαμβάνονται στο 3ο μέρος του προτύπου αφορούν τη σχέση που θα καθιερωθεί, τα έργα και την υποστήριξή τους, τη διαχείριση διαμόρφωσης, καθώς και τεχνικές διαδικασίες. Τέλος, αξιοποιείται το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ISMS) του ISO/IEC 27001 για την ενσωμάτωση της ασφάλειας στην εφοδιαστική αλυσίδα. Τα μέτρα του ISO/IEC 27002 αντιστοιχίζονται στις διαδικασίες κύκλου ζωής ώστε να διασφαλιστεί η πλήρης ενσωμάτωση πρακτικών ασφάλειας στις σχέσεις προμηθευτών.

Οι διαδικασίες του κύκλου ζωής μία ICT εφοδιαστικής αλυσίδας περιλαμβάνουν:

1. Διαδικασία Συμφωνιών (Agreement Processes)
   Η διαδικασία συμφωνίας στην ασφάλεια αλυσίδας εφοδιασμού ΤΠΕ (ICT supply chain security), περιλαμβάνει δύο βασικές ενότητες:
   - τη διαδικασία απόκτησης (Acquisition Process) και
   - την διαδικασία προμήθειας (Supply Process),

   που περιγράφονται στο πρότυπο ISO/IEC 27002 και παρέχουν καθοδήγηση για τη διαχείριση των απαιτήσεων ασφάλειας πληροφοριών κατά τη διάρκεια της συμφωνίας.

   Για τη **διαδικασία απόκτησης**, ο αγοραστής πρέπει να:

- προετοιμάσει τη **διαδικασία απόκτησης**, καθορίζοντας στρατηγικές προμήθειας, απαιτήσεις για την ασφάλεια πληροφοριών και τις απαιτήσεις για τη διαχείριση των προμηθευτών στην αλυσίδα εφοδιασμού.
- **επικοινωνήσει την πρόθεση του** να αποκτήσει ένα προϊόν ή υπηρεσία και να επιλέξει τους κατάλληλους προμηθευτές με βάση το κατά πόσο πληρούν τις απαιτήσεις που έχει θέσει.

Ακολουθεί η διαδικασία διαπραγμάτευσης και συμφωνίας με τον προμηθευτή, όπου περιλαμβάνονται οι απαιτήσεις για την προστασία της ακεραιότητας των προϊόντων ΤΠΕ που αποκτώνται (integrity of ICT products). Είναι απαραίτητο όσο η συμφωνία είναι σε ισχύ να παρακολουθείται η εκτέλεση της, μέσω της αξιολόγησης των επιδόσεων των προμηθευτών και της διεξαγωγής ελέγχων (audits).

Για τη **διαδικασία προμήθειας,** ο προμηθευτής πρέπει να:

- ενσωματώσει δραστηριότητες που εξασφαλίζουν και αποδεικνύουν ότι διαχειρίζονται σωστά τους κινδύνους της αλυσίδας εφοδιασμού. Αυτές περιλαμβάνουν την **αναγνώριση ευκαιριών** (Identify opportunities), όπου ο προμηθευτής καθορίζει την ύπαρξη ενός αγοραστή που χρειάζεται το προϊόν ή την υπηρεσία.
- μελετήσει το **RFP** (Respond to a tender) αξιολογώντας τα αιτήματα και προετοιμάζοντας μια απάντηση που να ικανοποιεί τις απαιτήσεις ασφάλειας πληροφοριών.
- προσαρμόσει τις απαιτήσεις ασφάλειας για κάθε σχέση με τον αγοραστή. Στη διαδικασία αυτή περιλαμβάνεται και η **διαπραγμάτευση συμφωνίας** (Initiate an agreement) με τον αγοραστή, καθώς και η **εκτέλεση της συμφωνίας** σύμφωνα με τα σχέδια του προμηθευτή (Execute the agreement).
- εξασφαλίζει ότι η **παράδοση του προϊόντος ή παροχή υπηρεσίας** γίνεται σύμφωνα με τα συμφωνημένα κριτήρια και παρέχει την απαιτούμενη υποστήριξη στον αγοραστή.

Τέλος, η διαδικασία ολοκληρώνεται με τη **σύναψη της συμφωνίας** (Close the agreement), όπου ο προμηθευτής αποδέχεται την αμοιβή και διασφαλίζει ότι τα μέτρα ασφαλείας παραμένουν σε ισχύ ακόμη και μετά την ολοκλήρωση της διαδικασίας.

2. Διαδικασία οργάνωσης έργων (Organizational Project-Enabling Processes)

Η διαδικασία οργάνωσης έργων (Organizational Project-Enabling Processes) αποτελείται από διάφορες διαδικασίες και έχει ως στόχο τη δημιουργία του περιβάλλοντος, στο οποίο πραγματοποιούνται τα έργα. Εκτός αν αναφέρεται ρητά, οι διαδικασίες αυτές εφαρμόζονται και στα δύο μέρη.

Οι διαδικασίες που πρέπει να πραγματοποιηθούν περιλαμβάνουν:

- **Διαδικασία διαχείρισης μοντέλου του κύκλου ζωής** (Life Cycle Model Management Process) έχει ως σκοπό τον ορισμό, τη συντήρηση και την εξασφάλιση της διαθεσιμότητας πολιτικών, διαδικασιών κύκλου ζωής και μοντέλων για χρήση από τον Οργανισμό.
- **Διαδικασία διαχείρισης υποδομών** (Infrastructure Management Process) έχει ως σκοπό την παροχή της αναγκαίας υποδομής για την

υποστήριξη των μερών καθ' όλη τη διάρκεια του κύκλου ζωής των έργων. Αυτή η διαδικασία περιλαμβάνει την εξασφάλιση της διαφάνειας των διαδικασιών, του περιβάλλοντος και των συναφών πόρων που απαιτούνται για την κατασκευή ή λειτουργία των προϊόντων ή υπηρεσιών, την καθιέρωση διαδικασιών φυσικής ασφάλειας για τα υλικά και μέσα, και τη δημιουργία ασφαλούς κώδικα (code repository) με ελεγχόμενη και επιθεωρημένη πρόσβαση.

- **Διαδικασία διαχείρισης χαρτοφυλακίου έργων** (Project Portfolio Management Process) έχει ως σκοπό την έναρξη και τη διατήρηση των αναγκαίων έργων για την επίτευξη των στρατηγικών στόχων του Οργανισμού.
- **Διαδικασία διαχείρισης ανθρώπινων πόρων** (Human Resource Management Process) εξασφαλίζει ότι η οργάνωση διαθέτει τους απαραίτητους ανθρώπινους πόρους και διατηρεί τις δεξιότητές τους σύμφωνα με τις ανάγκες της επιχείρησης. Εκτός από την εφαρμογή των διαδικασιών ανθρώπινων πόρων στο ISO/IEC 15288 και των ελέγχων ασφάλειας ανθρώπινων πόρων στο ISO/IEC 27002, οι αγοραστές και οι προμηθευτές πρέπει να εκπαιδεύουν το προσωπικό τους. Αυτό περιλαμβάνει την ανάπτυξη προγραμμάτων ευαισθητοποίησης και εκπαίδευσης σε πρακτικές ασφαλούς προγραμματισμού και την εφαρμογή αξιολογήσεων του προσωπικού για τις γνώσεις τους πάνω σε σχετικά θέματα.
- **Διαδικασία διαχείρισης ποιότητας** (Quality Management Process) περιλαμβάνει την διαχείριση ευπαθειών και την ενσωμάτωση δοκιμών για αδυναμίες και ευπάθειες σε όλες τις φάσεις του κύκλου ζωής του συστήματος, από το σχεδιασμό και την αρχιτεκτονική μέχρι τις δοκιμές του λογισμικού και του υλικού πριν από την παράδοση και εγκατάσταση.

3. Διαδικασία έργων (Project Process)

Οι διαδικασίες έργων (Project Processes) αφορούν τον αυστηρό έλεγχο και την υποστήριξη της διαχείρισης έργων για τα συστήματα και τα έργα που αφορούν σε ICT (Information and Communication Technology) αλυσίδες εφοδιασμού. Οι διαδικασίες αυτές, εκτός αν αναφέρεται ρητά κάτι διαφορετικό, ισχύουν για όλα τα εμπλεκόμενα μέρη.

Οι διαδικασίες που πρέπει να πραγματοποιηθούν περιλαμβάνουν:

- **Διαδικασία σχεδιασμού έργου** (Project Planning Process) έχει ως στόχο την παραγωγή και κοινοποίηση μιας αποτελεσματικής εκτέλεσης του έργου. Στα έργα που αφορούν ICT προϊόντα και υπηρεσίες που δημιουργούνται και παραδίδονται μέσω γεωγραφικά κατανεμημένων αλυσίδων εφοδιασμού υπό τον έλεγχο πολλών οντοτήτων, οι αγοραστές και οι προμηθευτές πρέπει να ενσωματώσουν συγκεκριμένα ζητήματα ασφάλειας πληροφοριών κατά τον σχεδιασμό. Αυτά περιλαμβάνουν τη συνεκτίμηση των επιπτώσεων που μπορεί να έχει η ασφάλεια πληροφοριών στα χρονοδιαγράμματα και τους πόρους του έργου, καθώς και τις νομικές απαιτήσεις που σχετίζονται με την ICT αλυσίδα εφοδιασμού.
- **Διαδικασία αξιολόγησης και ελέγχου του έργου** (Project Assessment and Control Process) σκοπεύει στη μέτρηση της κατάστασης του έργου και στην καθοδήγηση της εκτέλεσης του σύμφωνα με τον σχεδιασμό, τους χρόνους και το προϋπολογισμό. Οι αγοραστές πρέπει να εκτελούν

περιοδικούς ελέγχους συμμόρφωσης των προϊόντων ή υπηρεσιών των προμηθευτών για να εξασφαλίσουν ότι παραμένουν συμβατοί με τις απαιτήσεις τους, καταγράφοντας τα αποτελέσματα αυτών των ελέγχων σε εκθέσεις συμμόρφωσης.

- **Διαδικασία διαχείρισης αποφάσεων** (Decision Management Process), έχει ως στόχο την επιλογή της καταλληλότερης επιλογής όταν υπάρχουν εναλλακτικές.
- **Διαδικασία διαχείρισης κινδύνων** (Risk Management Process) αποσκοπεί στην αναγνώριση, ανάλυση, αντιμετώπιση και παρακολούθηση των κινδύνων με συνεχή αξιολόγηση. Οι αγοραστές και οι προμηθευτές πρέπει να εφαρμόσουν συγκεκριμένες δραστηριότητες για να αντιμετωπίσουν τους κινδύνους ασφάλειας της ICT αλυσίδας εφοδιασμού, όπως η αναγνώριση απειλών και ευπαθειών που σχετίζονται με τα ICT προϊόντα και υπηρεσίες, η αποτύπωση αυτών των κινδύνων και η ανάπτυξη στρατηγικών για την διαχείριση των κινδύνων. Επιπλέον, είναι απαραίτητο να παρακολουθούν την ICT αλυσίδα για πιθανούς κινδύνους και να προσαρμόζουν τις στρατηγικές αξιολόγησης και αντιμετώπισης κινδύνων αναλόγως.
- **Διαδικασία διαχείρισης διαμόρφωσης** (Configuration Management Process) εστιάζει στη διατήρηση της ακεραιότητας όλων των αποτελεσμάτων ενός έργου ή διαδικασίας και στη διασφάλιση της διαθεσιμότητάς τους στους εμπλεκόμενους. Οι αγοραστές και οι προμηθευτές πρέπει να ελέγχουν την πρόσβαση και τις αλλαγές σε όλα τα υλικά και τα έγγραφα που σχετίζονται με τα ICT προϊόντα και υπηρεσίες, διασφαλίζοντας την ασφάλεια κατά τη διάρκεια όλων των σταδίων της ζωής τους, από τον σχεδιασμό μέχρι την απόσυρση τους.
- **Διαδικασία διαχείρισης πληροφοριών** (Information Management Process) έχει ως στόχο την παροχή σχετικών, έγκαιρων, πλήρων και, αν απαιτείται, εμπιστευτικών πληροφοριών στους καθορισμένους αποδέκτες κατά τη διάρκεια και μετά τον κύκλο ζωής της ICT αλυσίδας εφοδιασμού.
- **Διαδικασία μέτρησης** (Measurement Process) έχει ως στόχο τη συλλογή, ανάλυση και αναφορά δεδομένων που σχετίζονται με τα προϊόντα και τις διαδικασίες του οργανισμού για να υποστηρίξει τη διαχείριση των διαδικασιών και να αποδείξει την ποιότητα των προϊόντων.

4. Τεχνική Διαδικασία (Technical Process)

Η διαδικασία αυτή καλύπτει όλο τον κύκλο ζωής των προϊόντων και υπηρεσιών, από τον καθορισμό των απαιτήσεων έως τη μετατροπή τους σε υλοποιήσιμες λύσεις, τη χρήση και τη συντήρησή τους, μέχρι και την τελική απόρριψή τους. Μέρος της αποτελούν πολλές διαδικασίες, οι οποίες διασφαλίζουν ότι τα προϊόντα και οι υπηρεσίες ανταποκρίνονται στις απαιτήσεις των ενδιαφερόμενων μερών, διατηρώντας παράλληλα την ακεραιότητα και την ασφάλεια της αλυσίδας εφοδιασμού των ICT. Εκτός εάν αναφέρεται διαφορετικά, οι διαδικασίες αυτές εφαρμόζονται τόσο στους αγοραστές όσο και στους προμηθευτές.

- **Διαδικασία Καθορισμού Απαιτήσεων Ενδιαφερομένων μερών** (Stakeholder Requirements Definition Process) απαιτεί τον καθορισμό και την τεκμηρίωση απαιτήσεων ασφαλείας βάσει αξιολογήσεων κινδύνου, κανονιστικών απαιτήσεων και επιχειρησιακών προσδοκιών. Περι-

λαμβάνει την αναγνώριση απειλών για κρίσιμες λειτουργίες, τη διασφάλιση της ακεραιότητας δεδομένων και συστημάτων, καθώς και τη θέσπιση απαιτήσεων διαθεσιμότητας και εμπιστευτικότητας για τους προμηθευτές. Επιπλέον, επιβάλλει την ενσωμάτωση προσδοκιών ασφαλείας στη διαδικασία παράδοσης προϊόντων και υπηρεσιών, ενώ παράλληλα καθορίζει τις συνέπειες των παραβιάσεων ασφαλείας.

- **Διαδικασία Ανάλυσης Απαιτήσεων** (Requirements Analysis Process), η οποία απαιτεί τον καθορισμό και την ενσωμάτωση των απαραίτητων μέτρων ασφαλείας στις τεχνικές απαιτήσεις και τις επιχειρησιακές διαδικασίες. Προκειμένου να αντιμετωπιστούν συγκεκριμένοι κίνδυνοι ασφαλείας στην αλυσίδα εφοδιασμού ICT, οι συμμετέχοντες στη διαδικασία θα πρέπει να διασφαλίζουν ότι κάθε στοιχείο χαρακτηρίζεται από διαφορετικό επίπεδο κρισιμότητας ανάλογα με τον σκοπό και τη χρήση του. Οι αξιολογήσεις κινδύνου και οι παράγοντες ασφαλείας θα πρέπει να ενσωματώνονται σε όλες τις διαχειριστικές, λειτουργικές και τεχνικές απαιτήσεις, καθώς και στις επιχειρησιακές διαδικασίες, ώστε να προστατεύονται τα στοιχεία, οι απαιτήσεις και οι πρακτικές από παραβιάσεις εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας. Επιπλέον, οι τεχνικές απαιτήσεις θα πρέπει να περιλαμβάνουν κριτήρια αμυντικού σχεδιασμού (defensive design criteria), διασφαλίζοντας ότι τα διαθέσιμα σχέδια και οι διαδικασίες διατηρούν την αποστολή και απόδοση του συστήματος, αλλά και την ασφάλεια των στοιχείων. Επίσης απαραίτητη, είναι η προστασία των απαιτήσεων και της σχετικής τεκμηρίωσης από πιθανή έκθεση ή μη εξουσιοδοτημένη πρόσβαση που μπορεί να οδηγήσει σε απώλεια της εμπιστευτικότητας, της ακεραιότητας ή της διαθεσιμότητας λόγω παραβίασης στην αλυσίδα εφοδιασμού ICT. Η συνεχής παρακολούθηση και η επαναξιολόγηση των τεχνικών απαιτήσεων είναι επίσης ζωτικής σημασίας, ώστε να προσαρμόζονται κατάλληλα μέσω εγκεκριμένων διαδικασιών διαχείρισης αλλαγών (change management procedures) και να διασφαλίζεται η προστασία των κρίσιμων στοιχείων και διαδικασιών καθ' όλη τη διάρκεια του κύκλου ζωής τους. Επιπλέον, είναι απαραίτητο να αναγνωρίζονται λειτουργικές έννοιες και σενάρια που σχετίζονται με πιθανές περιπτώσεις κακής χρήσης ή εκμετάλλευσης των συστημάτων.
- **Διαδικασία Αρχιτεκτονικού Σχεδιασμού** (Architectural Design Process) στο πλαίσιο της οποίας απαιτείται η ενσωμάτωση τεχνικών ασφαλείας στο σχεδιασμό των αρχιτεκτονικών λύσεων για τη μείωση των πιθανών κινδύνων. Ο αρχιτεκτονικός σχεδιασμός πρέπει να λαμβάνει υπόψη τόσο τα προβλεπόμενα όσο και τα μη προβλεπόμενα σενάρια χρήσης, επιλέγοντας και εφαρμόζοντας σχεδιαστικές λύσεις που ευθυγραμμίζονται με την ανοχή κινδύνου (risk tolerance) του αγοραστή. Είναι επίσης σημαντικό να περιοριστεί ο αριθμός, το μέγεθος και τα προνόμια των κρίσιμων στοιχείων, καθώς και να μειωθεί η πολυπλοκότητα του σχεδιασμού, της παραγωγής και της υλοποίησης, αφού η υπερβολική πολυπλοκότητα μπορεί να οδηγήσει σε προβλήματα εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας, αλυσιδωτές αποτυχίες και δυσκολίες στην ανάλυση των πηγών των σφαλμάτων και περιστατικών (root cause analysis). Ο σχεδιασμός θα πρέπει να περιλαμβάνει μηχανισμούς ασφαλείας και αντίμετρα, όπως είναι η κρυπτογράφηση, ο έλεγχο πρόσβασης,

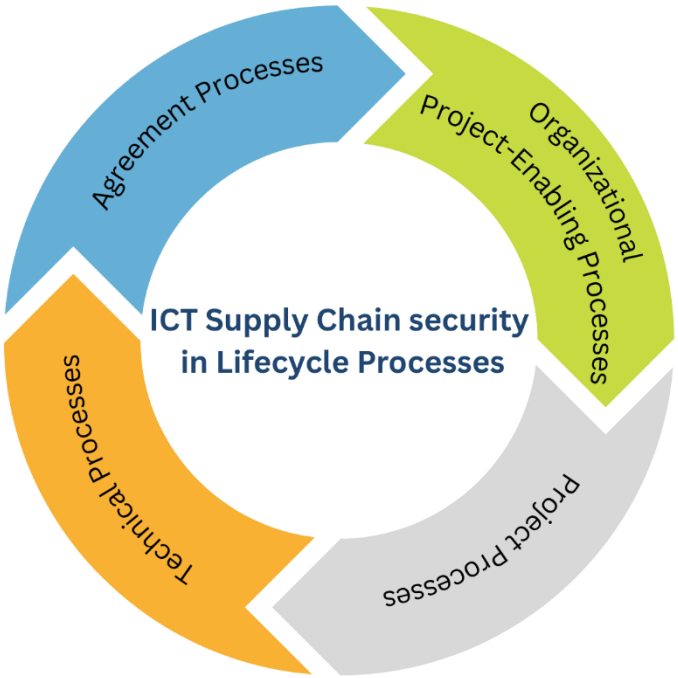
η διαχείριση ταυτότητας και εργαλεία ανίχνευσης κακόβουλου λογισμικού. Επιπλέον, η χρήση μηχανισμών ασφάλειας (εικονικές μηχανές, καραντίνα, sandboxing και μονόδρομες έξοδοι κ.α.) βοηθά στη μείωση της πιθανότητας διάδοσης κακόβουλων ενεργειών σε όλο το μήκος της αλυσίδας. Οι αρχιτεκτονικές λύσεις θα πρέπει να περιλαμβάνουν επίσης αντίμετρα και μηχανισμούς μετριασμού για την αντιμετώπιση των αδυναμιών και των ευπαθειών του συστήματος, ενσωματώνοντας τεχνικές προγραμματισμού και ρυθμίσεις διαμόρφωσης. Μια ακόμα βασική πτυχή του σχεδιασμού είναι η δυνατότητα αύξησης της απομόνωσης του συστήματος (system isolation), ακόμη και αν αυτό μειώνει τη λειτουργικότητά του, προκειμένου να αποτραπούν επιθέσεις μέχρι να διατεθεί μια νέα ενημέρωση (patch). Τα στοιχεία του συστήματος θα πρέπει να σχεδιάζονται ώστε να είναι ανθεκτικά σε καταστάσεις σφάλματος (υπερβολικές τάσεις - excessive voltages, αριθμητικά δεδομένα εκτός αποδεκτών ορίων -numbers out of range).

- **Διαδικασίας παράδοσης** (delivery process), πρέπει να σχεδιαστούν κατάλληλοι μηχανισμοί ώστε να αποτραπεί η έκθεση ή μη εξουσιοδοτημένη πρόσβαση στα στοιχεία κατά τη μεταφορά τους. Επιπλέον, πρέπει να προβλέπονται μηχανισμοί αυτόματης ανάκαμψης και πλεονάζοντα συστήματα, διασφαλίζοντας ότι δεν είναι ευάλωτα σε κοινές αποτυχίες (common mode failures). Ο σχεδιασμός πρέπει να βασίζεται σε τεχνικές διεπαφές και απαιτήσεις βασισμένες σε πρότυπα, ώστε να επιτρέπεται η τροποποίηση ή αντικατάσταση στοιχείων σε περίπτωση παραβίασης της αλυσίδας εφοδιασμού. Τέλος, πρέπει να περιλαμβάνονται μηχανισμοί επαλήθευσης που θα χρησιμοποιούνται κατά την υλοποίηση και λειτουργία του συστήματος.
- **Διαδικασία Υλοποίησης** (Implementation Process), όπου διασφαλίζει την ανάπτυξη ενός στοιχείου συστήματος σύμφωνα με τις απαιτήσεις ασφαλείας της αλυσίδας εφοδιασμού ICT. Οι προμηθευτές πρέπει να υλοποιούν τον αρχιτεκτονικό σχεδιασμό και να εντοπίζουν τυχόν αποκλίσεις, εφαρμόζοντας κατάλληλα μέτρα μετριασμού. Πρέπει να χρησιμοποιούνται ασφαλείς γλώσσες προγραμματισμού, να ενσωματώνονται πρότυπα διεπαφών και να εφαρμόζονται δοκιμές επαλήθευσης (fuzz testing, static & dynamic testing). Η πρόσβαση στα δεδομένα δοκιμών πρέπει να προστατεύεται, ενώ η διαθεσιμότητα κρίσιμων στοιχείων διασφαλίζεται μέσω διαφοροποίησης προμηθευτών. Επιπλέον, οι περιττές λειτουργίες πρέπει να αφαιρούνται για την αποφυγή μη εξουσιοδοτημένης πρόσβασης.
- **Διαδικασία Ενσωμάτωσης** (Integration Process), διασφαλίζει ότι το προϊόν ή η υπηρεσία δημιουργείται σύμφωνα με τον αρχιτεκτονικό σχεδιασμό, λαμβάνοντας υπόψη την ασφάλεια της αλυσίδας εφοδιασμού ICT και την τεκμηρίωση των υφιστάμενων συστημάτων.
- **Διαδικασία Επαλήθευσης** (Verification Process) επιβεβαιώνει ότι οι απαιτήσεις σχεδιασμού πληρούνται, εστιάζοντας στην ασφάλεια της αλυσίδας εφοδιασμού. Περιλαμβάνει έλεγχο κώδικα, ανάλυση ευπαθειών, έλεγχο κακόβουλου λογισμικού και χρήση εργαλείων συμμόρφωσης. Επιπλέον, αξιολογεί πιστοποιήσεις και βεβαιώσεις προμηθευτών για τη συμμόρφωση και την ακεραιότητα των προϊόντων.
- **Διαδικασία Μετάβασης** (Transition Process), όπου διασφαλίζει την ικανότητα παροχής ή παραλαβής προϊόντων και υπηρεσιών σύμφωνα

με τις απαιτήσεις των ενδιαφερομένων στο επιχειρησιακό περιβάλλον. Για τους αγοραστές , η διαδικασία περιλαμβάνει τη διαχείριση αποθεμάτων, την ενσωμάτωση προϊόντων στο σύστημα αποθήκευσης, τη διασφάλιση ελεγχόμενης παράδοσης από εξουσιοδοτημένο προσωπικό και την εφαρμογή μηχανισμών ανίχνευσης μη εξουσιοδοτημένης πρόσβασης. Επίσης, απαιτεί κρυπτογράφηση δεδομένων, έλεγχο ψηφιακών υπογραφών και προστασία από κακόβουλο λογισμικό. Οι προμηθευτές οφείλουν να διασφαλίσουν την προστασία του λογισμικού από κακόβουλες παρεμβάσεις, να εφαρμόσουν μηχανισμούς ελέγχου γνησιότητας, όπως ψηφιακές υπογραφές και ολογραφικές ετικέτες (hologram tags), και να προσφέρουν διαδικασίες ασφαλούς παράδοσης τόσο για διαδικτυακές όσο και για φυσικές μεταφορές. Τέλος, πρέπει να εφαρμόσουν μηχανισμούς προστασίας από παραβιάσεις, ώστε να εξασφαλίζεται η ακεραιότητα του προϊόντος κατά τη μεταφορά.

- **Διαδικασία Επικύρωσης** (Validation Process), όπου διασφαλίζει ότι τα προϊόντα και οι υπηρεσίες συμμορφώνονται με τις απαιτήσεις των ενδιαφερομένων και επιτελούν την προβλεπόμενη λειτουργία τους στο επιχειρησιακό περιβάλλον. Οι αγοραστές πρέπει να επαληθεύουν την αυθεντικότητα και ακεραιότητα των προϊόντων, μέσω ελέγχων που βασίζονται στις προδιαγραφές του προμηθευτή και στη μεταξύ τους συμφωνία. Περιλαμβάνονται δοκιμές όπως επιθεώρηση υλικού και λογισμικού, ανίχνευση κακόβουλου λογισμικού, ευπαθειών και έλεγχος πηγαίου κώδικα. Επιπλέον, χρησιμοποιούνται μη επεμβατικά εργαλεία επικύρωσης κατασκευαστή (OEM validation tools) και εκτελούνται δοκιμές ανθενκτικότητας, καθώς και παρακολούθηση αλλαγών μέσω απομακρυσμένης συντήρησης (remote maintenance tracking).
- **Διαδικασία Λειτουργίας** (Operation Process), όπου διασφαλίζει την παροχή προϊόντων και υπηρεσιών σύμφωνα με τις συμφωνημένες απαιτήσεις. Οι προμηθευτές οφείλουν να αποστέλλουν προϊόντα με ασφαλείς προεπιλεγμένες ρυθμίσεις (secured by default) σύμφωνα με τις ανάγκες των αγοραστών. Επιπλέον, οι αναβαθμίσεις και η συντήρηση πρέπει να περιλαμβάνουν δραστηριότητες ολοκλήρωσης συστήματος και προσαρμογής κώδικα, ενώ όλες οι λειτουργικές διαδικασίες πρέπει να συμμορφώνονται με απαιτήσεις και πρακτικές ασφάλειας πληροφοριών.
- **Διαδικασία Συντήρησης** (Maintenance Process), όπου στοχεύει στη διατήρηση της λειτουργικότητας των συστημάτων και των στοιχείων τους, διαχειριζόμενη ταυτόχρονα τους σχετικούς κινδύνους ασφαλείας. Για την επίτευξη αυτού, οι αγοραστές και οι προμηθευτές πρέπει να ενσωματώνουν στις συμβάσεις τους ρήτρες που μειώνουν τον κίνδυνο της αλυσίδας εφοδιασμού και να διατηρούν σχέσεις με κατασκευαστές OEM για την απόκτηση γνήσιων και αξιόπιστων ανταλλακτικών.
- **Διαδικασία Απόρριψης** (Disposal Process), όπου αφορά τη διαχείριση του τέλους ζωής των στοιχείων της αλυσίδας εφοδιασμού ICT, διασφαλίζοντας ότι η απόρριψη τους δεν δημιουργεί κινδύνους ασφάλειας, όπως η διαρροή δεδομένων ή η εισαγωγή πλαστών προϊόντων στην αγορά. Για την προστασία των δεδομένων, οι αγοραστές και οι προμηθευτές πρέπει να διατηρούν αλυσίδα φύλαξης των στοιχείων προς απόρριψη, αποτρέποντας μη εξουσιοδοτημένη πρόσβαση σε προσωπικές ή ευαίσθητες πληροφορίες.

Οι διαδικασίες αυτές πρέπει να ελέγχονται τακτικά, ώστε να διασφαλίζεται η συμμόρφωσή τους με τις πολιτικές ασφαλείας της αλυσίδας εφοδιασμού. [32]




*Σχήμα 6: Διαδικασίες κύκλου ζωής της ICT εφοδιαστικής αλυσίδας*

## 4.6 Μέρος 4: Οδηγίες για την ασφάλεια στις υπηρεσίες cloud (Part 4: Guidelines for Security of Cloud Services)

Το 4ο μέρος του ISO 27036, προορίζεται να χρησιμοποιείται σε συνδυασμό με τα υπόλοιπα μέρη και λειτουργεί ως επιπλέον οδηγός για την ασφάλεια πληροφοριών, με έμφαση στις υπηρεσίες νέφους (cloud services). Το πρότυπο αναφέρει διάφορα είδη κινδύνων στο νέφος, ανάλογα με το μοντέλο ανάπτυξης αυτού (δημόσιο, ιδιωτικό, υβριδικό). Η χρήση υπηρεσιών νέφους συνεπάγεται διάφορους κινδύνους για τους αγοραστές, οι οποίοι προκύπτουν από παράγοντες όπως η έλλειψη ελέγχου και διαφάνειας, οι άγνωστες διαδικασίες διαχείρισης δεδομένων και η πιθανή καθυστέρηση στην ανίχνευση περιστατικών ασφαλείας.

Οι κύριοι κίνδυνοι περιλαμβάνουν:

- **Έλλειψη ελέγχου τοποθεσίας και πρόσβασης στα δεδομένα**: Οι αγοραστές δεν γνωρίζουν πού αποθηκεύονται τα δεδομένα τους ή ποιος έχει πρόσβαση σε αυτά, δημιουργώντας κινδύνους για την ακεραιότητα, την ανιχνευσιμότητα και την ιδιωτικότητα.
- **Άγνωστες διαδικασίες μετάδοσης δεδομένων**: Η απουσία διαφάνειας στη μεταφορά δεδομένων μπορεί να επηρεάσει την εμπιστευτικότητα και την ακεραιότητά τους.
- **Διαχείριση πρόσβασης αυξημένων δικαιωμάτων**: Η ύπαρξη άγνωστων υπερδιαχειριστών ή διαχειριστών συστημάτων μπορεί να αυξήσει τον κίνδυνο μη εξουσιοδοτημένης πρόσβασης.
- **Απειλές κακόβουλου λογισμικού**: Οι ανεπαρκείς μηχανισμοί προστασίας στις υποδομές, τις πλατφόρμες ή τις εφαρμογές νέφους μπορούν να επιτρέψουν κακόβουλες επιθέσεις.

- **Έλλειψη αρχείων καταγραφής**: Η απουσία καταγραφής συμβάντων μειώνει την ικανότητα εντοπισμού και ανάλυσης περιστατικών ασφαλείας.
- **Δυσκολία ανάκτησης ή διαγραφής δεδομένων**: Οι αγοραστές μπορεί να μην έχουν τη δυνατότητα να ανακτήσουν δεδομένα κατά τη διάρκεια της υπηρεσίας ή να διασφαλίσουν τη διαγραφή τους μετά τη λήξη της σύμβασης.

Στο 4ο μέρος, περιγράφεται ο κύκλος ζωής απόκτησης υπηρεσιών νέφους. Ο εν λόγω κύκλος, περιλαμβάνει διαδικασίες που σχετίζονται με τη διαχείριση των σχέσεων μεταξύ του πελάτη (cloud service customer) και του παρόχου (cloud service provider) υπηρεσιών νέφους.

Οι διαδικασίες που περιγράφονται είναι οι:

- **Διαδικασία απόκτησης** (Acquisition Process): ο πελάτης πρέπει να δημιουργήσει μια σαφή στρατηγική σχέση με τον πάροχο, η οποία θα περιλαμβάνει την κατανόηση των μέτρων ασφαλείας, την αποτελεσματική επικοινωνία και τη σαφήνεια στις ευθύνες και τους ρόλους. Παράλληλα, πρέπει να εφαρμόσει αρχές για τον μετριασμό των κινδύνων και να επεκτείνει την πολιτική ασφάλειας ώστε να καλύπτει τις υπηρεσίες νέφους.
- **Διαδικασία παροχής** (Supply Process): ο πάροχος πρέπει να καθορίσει τις ευθύνες του, να παρέχει πληροφορίες για τα μέτρα ασφαλείας και να διασφαλίσει τη διαφάνεια μέσω δημοσιοποίησης σχετικών πιστοποιήσεων. Επιπλέον, πρέπει να προσδιορίσει μέτρα ανθεκτικότητας και αποκατάστασης καταστροφών, να ενημερώνει τους πελάτες για αλλαγές και να παρέχει διαβεβαιώσεις ασφαλείας. Ως εκ τούτου, ο πάροχος πρέπει να εξασφαλίζει την ασφαλή μεταφορά και αποθήκευση δεδομένων, να εφαρμόζει διαδικασίες διαχωρισμού δεδομένων πολλαπλών πελατών και να διαθέτει σαφή πολιτική καταστροφής δεδομένων μετά τη λήξη της σύμβασης.
- **Διαδικασίες οργανωτικής υποστήριξης έργων**: πρέπει να ακολουθούνται οι προδιαγραφές των ISO/IEC 27036-2 και ISO/IEC 27036-3. Κατά τη διαχείριση των έργων, εκτελούνται διάφορες διαδικασίες που περιλαμβάνουν αρχικά, το σχεδιασμό, την αξιολόγηση και λήψη αποφάσεων. Αν και η ασφάλεια νέφους είναι σημαντική, δεν παρέχεται επιπλέον καθοδήγηση πέρα από τα γενικά πρότυπα. Οι οργανισμοί πρέπει να διασφαλίσουν ότι λαμβάνουν υπόψη τις σχετικές αρχές κατά τον σχεδιασμό, την αξιολόγηση και τη λήψη αποφάσεων.

Επιπλέον, γίνεται λόγος για τη διαχείριση κινδύνων, όπου οι πελάτες πρέπει να καθορίσουν ποια δεδομένα θα διαχειρίζονται στο νέφος, καθώς και τους νομικούς και κανονιστικούς κινδύνους. Οι πάροχοι, πρέπει να διασφαλίσουν ότι πληρούν τις απαιτήσεις ασφαλείας που ορίζονται στη SLA και να διαχειρίζονται σωστά την επιστροφή ή την καταστροφή των δεδομένων κατά τη λήξη της υπηρεσίας. Επιπροσθέτως, πρέπει να αναλύουν οποιεσδήποτε αλλαγές στην υπηρεσία και να ενημερώνουν τους πελάτες τους, ώστε να αποφεύγονται κίνδυνοι λόγω ανεπαρκούς επικοινωνίας ή ξαφνικών αλλαγών. Εξίσου απαραίτητο, είναι να εξετάζουν αν τα δεδομένα ταυτοποίησης των χρηστών είναι και προσωπικά δεδομένα, ενώ οι πελάτες πρέπει να γνωρίζουν τις πολιτικές ασφαλείας του παρόχου σχετικά με την προστασία της ιδιωτικότητας.

Παρόλο που η σημασία της ασφάλειας υπηρεσιών νέφους αναγνωρίζεται, δεν υπάρχουν επιπλέον οδηγίες πέρα από τα γενικά ISO πρότυπα, κάτι που υποδεικνύει ότι οι οργανισμοί πρέπει να αναπτύξουν τις δικές τους μεθοδολογίες αξιολόγησης κινδύνου ασφάλειας πληροφοριών.

Κατά τις διαδικασίες που αφορούν το τεχνικό κομμάτι, περιγράφεται ο κύκλος ζωής των υπηρεσιών νέφους και πώς πρέπει να διαχειρίζονται οι απαιτήσεις ασφαλείας σε κάθε στάδιο. Για τον καθορισμό, την ανάλυση και τον σχεδιασμό απαιτήσεων, δεν παρέχεται πρόσθετη καθοδήγηση πέρα από τις γενικές αρχές των ISO/IEC 27036-2 και 27036-3, επομένως οι οργανισμοί πρέπει να ενσωματώνουν τις αρχές ασφαλείας από νωρίς στη διαδικασία.

Οι πελάτες πρέπει να εφαρμόζουν σταδιακά τις υπηρεσίες νέφους, ξεκινώντας από χαμηλού κινδύνου λειτουργίες, ενώ οι πάροχοι είναι υπεύθυνοι για την εφαρμογή και παρακολούθηση ελέγχων ασφαλείας. Οι αλλαγές στην υπηρεσία και τα περιστατικά ασφαλείας πρέπει να παρακολουθούνται προσεκτικά από όλους τους εμπλεκόμενους. Οι πάροχοι πρέπει να καταγράφουν τη διαδικασία διαγραφής δεδομένων και να παρέχουν πιστευτήρια στους πελάτες.

Στη συνέχεια, αναφέρονται τα μέτρα ασφάλειας που πρέπει να εφαρμόζουν οι πάροχοι υπηρεσιών cloud, λαμβάνοντας υπόψη το είδος της υπηρεσίας, το μοντέλο ανάπτυξης και τις απαιτήσεις των πελατών. Αρχικά, αναφέρεται ότι τα μέτρα που εφαρμόζονται για τη μείωση των κινδύνων και απειλών ποικίλλουν ανάλογα με το συνδυασμό δυνατοτήτων, κατηγορίας υπηρεσιών, μοντέλου ανάπτυξης και του προφίλ των πελατών. Οι πάροχοι cloud που στοχεύουν σε πελάτες με αυξημένες απαιτήσεις ασφάλειας πρέπει να ενσωματώνουν ισχυρότερα μέτρα προστασίας και να παρέχουν υψηλότερο επίπεδο διασφάλισης, λαμβάνοντας υπόψη το νομικό και βιομηχανικό πλαίσιο της αγοράς τους. Παρότι η συμμόρφωση με νομικές και κανονιστικές απαιτήσεις είναι ευθύνη του πελάτη, η ικανότητα του παρόχου να υποστηρίξει αυτή τη συμμόρφωση καθορίζει την επιτυχία του.

Η εφαρμογή ενός **Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ISMS)**, όπως ορίζεται από το πρότυπο ISO/IEC 27001, θεωρείται βασική προϋπόθεση για την ασφάλεια πληροφοριών ενός παρόχου cloud. Επιπλέον, ο πάροχος θα πρέπει να εφαρμόζει το κατάλληλο σύνολο μέτρων ασφαλείας τόσο σε οργανωτικό όσο και σε υπηρεσιακό επίπεδο, ενώ είναι σημαντικό να διαμορφώνει σαφείς πολιτικές που να επικοινωνούν τις πρακτικές του σχετικά με την ασφάλεια πληροφοριών στους πελάτες του. Το σετ αντιμέτρων που απαιτείται διαφοροποιείται ανάλογα με την υπηρεσία και το επιχειρηματικό πλαίσιο, ενώ η έλλειψη συγκεκριμένων μέτρων μπορεί να είναι μια συνειδητή επιχειρηματική επιλογή που μειώνει το επίπεδο ασφάλειας, αλλά αυξάνει την ευελιξία της υπηρεσίας.

Οι πάροχοι υπηρεσιών cloud μπορούν να ενισχύσουν την εμπιστοσύνη των πελατών τους επιδεικνύοντας τη συμμόρφωσή τους με διεθνή πρότυπα όπως το ISO/IEC 27001 και εφαρμόζοντας κατάλληλους ελέγχους ασφαλείας βάσει της φύσης των υπηρεσιών που προσφέρουν και των απαιτήσεων της αγοράς τους. Η επικοινωνία αυτής της συμμόρφωσης προς τους πελάτες μπορεί να γίνει μέσω δηλώσεων που τεκμηριώνουν τη συμμόρφωση της υπηρεσίας με συγκεκριμένα πρότυπα. Αν και η συμμόρφωση με τα διεθνή πρότυπα δεν εξαλείφει πλήρως τους κινδύνους, βοηθά στη μείωσή τους και αυξάνει την εμπιστοσύνη των πελατών.

Στο τέλος του 4ου μέρους του προτύπου υπάρχουν 2 παραρτήματα. Το παράρτημα Α παρέχει καθοδήγηση σχετικά με την εφαρμογή μέτρων ασφάλειας πληροφοριών στις

υπηρεσίες cloud, λαμβάνοντας υπόψη τόσο την οπτική του πελάτη όσο και του παρόχου υπηρεσιών cloud. Ο πελάτης εστιάζει στην προστασία των δικών του πληροφοριών, ανεξάρτητα από το αν χρησιμοποιεί υπηρεσία cloud ή όχι, ενώ ο πάροχος πρέπει να διασφαλίζει όχι μόνο τις δικές του πληροφορίες αλλά και εκείνες των πελατών, ενσωματώνοντας μέτρα ασφαλείας στη διαχείριση των υπηρεσιών του.

Ο Πίνακας Α.1 στο **annex A** παρέχει αντιστοιχίες μεταξύ των τύπων υπηρεσιών cloud (IaaS, PaaS, SaaS), των μοντέλων ανάπτυξης (public, private, hybrid cloud) και των σχετικών προτύπων ασφάλειας πληροφοριών.

Από την άλλη, το **annex B** παρατίθεται ένας πίνακας αντιστοίχισης των ISO/IEC 27036-4, ISO/IEC 27017 ο οποίος επισημαίνει τις περιοχές στις οποίες απαιτείται ευθυγράμμιση πρακτικών ασφάλειας μεταξύ του πελάτη και του παρόχου cloud υπηρεσιών, υποστηρίζοντας έτσι τη διαλειτουργικότητα και τη συμμόρφωση με καθιερωμένα πρότυπα ασφάλειας πληροφοριών.

Για την ασφάλεια στις σχέσεις με cloud παρόχους, το πρότυπο ISO/IEC 27036-4 παρέχει ένα πλαίσιο διαδικασιών. Η αντιστοίχισή του με το ISO/IEC 27017 επιτρέπει στον οργανισμό να αναγνωρίσει ποιοι έλεγχοι ασφαλείας είναι κρίσιμοι σε κάθε φάση του κύκλου ζωής της συνεργασίας με τον πάροχο cloud. [33]

## 4.7 Σύνοψη

Το πρότυπο ISO/IEC 27036 αποτελεί έναν ολοκληρωμένο οδηγό για την ασφαλή διαχείριση σχέσεων με προμηθευτές, εστιάζοντας στην προστασία της πληροφορίας σε όλα τα στάδια της συνεργασίας. Η ανάλυση των τεσσάρων μερών του προτύπου ανέδειξε τη σημασία της καθιέρωσης πολιτικών και διαδικασιών, της αξιολόγησης και διαχείρισης κινδύνων, της ενσωμάτωσης απαιτήσεων ασφάλειας σε συμβάσεις, και της συνεχούς παρακολούθησης της ασφάλειας σε όλο το μήκος της αλυσίδας εφοδιασμού. Το πρότυπο παρέχει ένα ισχυρό θεμέλιο για την ενίσχυση της ανθεκτικότητας των οργανισμών έναντι των κινδύνων που προκύπτουν από τη συνεργασία με τρίτους, λειτουργώντας συμπληρωματικά προς άλλα πρότυπα ασφάλειας πληροφοριών, όπως το ISO/IEC 27001. Η υιοθέτησή του συμβάλλει όχι μόνο στη μείωση των κινδύνων, αλλά και στην ενίσχυση της εμπιστοσύνης μεταξύ των προμηθευτών και αγοραστών/ πελατών.

# 5. Συγκριτική Αξιολόγηση

## 5.1 Σκοπός

Μέρος της παρούσας διπλωματικής διατριβής, αποτελεί η σύγκριση και εξαγωγή συμπερασμάτων των δύο προτύπων NIST SP 800 – 161r1 και ISO 27036 που αναλύθηκαν.

Η παρούσα συγκριτική αξιολόγηση εστιάζει στην ανάλυση των δύο προτύπων βάσει διαφόρων θεματικών κατηγοριών και κριτηρίων, όπως το πεδίο εφαρμογής, το επίπεδο ωριμότητας ο σκοπός και η κάλυψη των επιχειρησιακών αναγκών, η πληρότητα της μεθοδολογίας διαχείρισης κινδύνων και η ανάγκη επανάληψης της, η διαλειτουργικότητα με άλλα σχετικά πλαίσια, ευθυγράμμιση με διεθνής Κανονισμούς, η επάρκεια των προτεινόμενων μέτρων ασφάλειας, η απαιτητικότητα της πρακτικής εφαρμογής, η συνεισφορά της διοίκησης και η διάθεση πόρων, η υποστήριξη και συμβατότητα με εργαλεία διαχείρισης κινδύνων και, τέλος, το επίπεδο εμπιστοσύνης μεταξύ των εμπλεκόμενων μερών. Ο καθορισμός των τελικών κατηγοριών κριτηρίων βασίστηκε τόσο στο κείμενο των προτύπων ISO/IEC 27036-2:2021 και NIST SP 800-161r1 όσο και σε επιστημονικές πηγές.

Η κατανόηση των διαφορών και συγκλίσεων μεταξύ των δύο προτύπων είναι ιδιαίτερης σημασίας για οργανισμούς που καλούνται να επιλέξουν ή να συνδυάσουν πρακτικές, με στόχο την επίτευξη ισορροπίας μεταξύ συμμόρφωσης, ασφάλειας και λειτουργικής αποδοτικότητας.

## 5.2 Μεθοδολογία

Η συγκριτική αξιολόγηση των δύο προτύπων βασίστηκε σε μια προσέγγιση πολλαπλών κριτηρίων, η οποία στόχευε στην πλήρη αποτύπωση των βασικών χαρακτηριστικών των προτύπων όσον αφορά τη διαχείριση κινδύνων στην εφοδιαστική αλυσίδα κυβερνοασφάλειας. Για το σκοπό αυτό, δημιουργήθηκε ένας πίνακας που παρέχει μια ολιστική εικόνα της εφαρμοσιμότητας, πληρότητας και λειτουργικότητας κάθε προτύπου, τόσο σε θεωρητικό, όσο και σε πρακτικό επίπεδο.

### 5.2.1 Κατηγορίες κριτηρίων αξιολόγησης

Για τη δημιουργία του πίνακα συγκριτικής αξιολόγησης, επιλέχθηκαν **δέκα (10) κατηγορίες κριτηρίων**. Οι κατηγορίες αυτές είναι οι εξής:

1. **Πεδίο Εφαρμογής (Scope of Applicability):**
    - Κάλυψη διαφορετικών οργανωτικών μεγεθών: Εξετάζεται κατά πόσο το πρότυπο μπορεί να εφαρμοστεί τόσο σε μικρές όσο και σε μεγάλες επιχειρήσεις, και αν δίνει σαφείς οδηγίες ανεξαρτήτως πόρων ή δομής.
    - Προσαρμοστικότητα σε διαφορετικούς κλάδους και τομείς: Εξετάζει κατά πόσο το πρότυπο παρέχει οδηγίες ή παραδείγματα για κλάδους όπως χρηματοοικονομικά, ενέργεια, μεταφορές, δημόσιο τομέα κ.λπ.

2. **Διεθνής αναγνώριση (international recognition):**
    - Γεωγραφική αναγνώριση: Εξετάζει κατά πόσο το πρότυπο έχει ευρωπαϊκή/παγκόσμια αναγνώριση από ρυθμιστικές αρχές, κυβερνήσεις ή διεθνείς οργανισμούς.

1. **Επίπεδο Ωριμότητας (Maturity Level):**.
    - Υποστήριξη διαφορετικών επιπέδων ωριμότητας οργανισμών: Εξετάζει κατά πόσο η μεθοδολογία μπορεί να εφαρμοστεί σε οργανισμούς με διάφορα επίπεδα ωριμότητας.
    - Προτεινόμενο μοντέλο ενίσχυσης ωριμότητας Οργανισμών: Εξετάζεται αν το πρότυπο καθορίζει στάδια ή επίπεδα εξέλιξης της ωριμότητας για τον οργανισμό ή τους προμηθευτές του.

2. **Μεθοδολογία Διαχείρισης Κινδύνων (Risk Management Methodology):**
    - Πληρότητα: Εξετάζει κατά πόσο υπάρχουν οι φάσεις αναγνώρισης, αξιολόγησης, αντιμετώπισης και παρακολούθησης και αν περιγράφονται με συνέπεια και σαφήνεια.
    - Μέτρηση απόδοσης: Εξετάζει κατά πόσο και αν υπάρχουν δείκτες μετρήσεις απόδοσης της διαδικασίας διαχείρισης κινδύνου.

3. **Επάρκεια Προτεινόμενων Μέτρων Ασφάλειας (Adequacy of Security Controls):**
    - Ποσότητα και κάλυψη μέτρων: Εξετάζεται κατά πόσο υπάρχει ικανοποιητικός αριθμός και ποικιλία μέτρων.
    - Σαφήνεια μέτρων: Εξετάζεται αν τα προτεινόμενα μέτρα είναι πρακτικά εφαρμόσιμα και κατανοητά.

4. **Πρακτική Εφαρμογή (Practical Implementation):**
    - Πληρότητα και Χρηστικότητα: Εξετάζεται η ευκολία κατανόησης και ενσωμάτωσης του προτύπου στην καθημερινή λειτουργία.
    - Υποστηρικτικό υλικό και οδηγίες υλοποίησης: Εξετάζεται κατά πόσο περιλαμβάνει οδηγούς, παραδείγματα, FAQs για επιπλέον υποστήριξη.

5. **Υποστήριξη και Συμβατότητα με Εργαλεία Διαχείρισης Κινδύνων (Tool Support & Compatibility):**
    - Αναφορά και συμβατότητα σε εργαλεία διαχείρισης κινδύνων: Εξετάζεται κατά πόσο προβλέπεται τεχνική διαλειτουργικότητα με υφιστάμενα εργαλεία διαχείρισης κινδύνων.
    - Κόστος εργαλείων: Εξετάζεται αν απαιτούνται επιπρόσθετες επενδύσεις για λογισμικά ή υποδομές.

6. **Διαλειτουργικότητα με Άλλα Πλαίσια (Interoperability with Other Frameworks):**
    - Ευθυγράμμιση με άλλα πρότυπα: Εξετάζεται κατά πόσο είναι σχεδιασμένο να «συμπληρώνει» ή να εναρμονίζεται με άλλα πρότυπα.
    - Υποστήριξη πολλαπλών υποδομών: Εξετάζεται κατά πόσο είναι κατάλληλο για διαφορετικές υποδομές και αρχιτεκτονικές.

7. **Επίπεδο Εμπιστοσύνης Μεταξύ των Εμπλεκόμενων Μερών (Trust Mechanisms):**
    - Μέθοδοι Αξιολόγησης τρίτων: Εξετάζεται κατά πόσο παρέχει μεθόδους αξιολόγησης τρίτων.
    - Διαφάνεια: Εξετάζεται αν απαιτείται ή ενθαρρύνεται η σαφής τεκμηρίωση ρόλων, όρων συνεργασίας και συμβολαίων.

- Διαμοιρασμός πληροφοριών: Εξετάζεται κατά πόσο απαιτούνται μηχανισμοί για την ανταλλαγή κρίσιμων πληροφοριών ασφαλείας (π.χ. ευπάθειες, απειλές, περιστατικά, πολιτικές) μεταξύ των εμπλεκόμενων μερών της εφοδιαστικής αλυσίδας.

8. **Κόστος - Όφελος (Cost-Benefit Consideration):** Αξιολογεί αν το πρότυπο ενσωματώνει ή επιτρέπει την εκτίμηση του κόστους εφαρμογής.
   - Αξιολόγηση κόστους εφαρμογής μέτρων: Εξετάζεται κατά πόσο το πρότυπο επιτρέπει την εκτίμηση του κόστους εφαρμογής των μέτρων.
   - Υποστήριξη λήψης αποφάσεων βάσει κόστους-οφέλους: Εξετάζεται αν το πρότυπο περιλαμβάνει κατευθύνσεις ή εργαλεία για την αξιολόγηση των επενδύσεων σε σχέση με το αναμενόμενο όφελος για την ασφάλεια.

Η επιλογή των συγκεκριμένων κατηγοριών και κριτηρίων, έγινε ώστε να καλύπτεται τόσο η στρατηγική και οργανωτική πλευρά των προτύπων, όσο και η πρακτική εφαρμογή τους από οργανισμούς ιδιωτικού και δημόσιου τομέα.

### 5.2.3 Ποσοτική κλίμακα αξιολόγησης

Για την αντικειμενική και συνεπή αξιολόγηση των δύο προτύπων, υιοθετήθηκε μια ποσοτική κλίμακα τριών επιπέδων. Η κλίμακα αυτή εφαρμόστηκε σε δέκα θεματικές κατηγορίες αξιολόγησης, καθεμία από τις οποίες περιλαμβάνει έναν ή περισσότερους επιμέρους δείκτες αξιολόγησης (κριτήρια). Ο συνολικός αριθμός των επιμέρους κριτηρίων διαφοροποιείται ανά κατηγορία, ανάλογα με τη φύση και το εύρος της.

Η αξιολόγηση κάθε επιμέρους κριτηρίου πραγματοποιήθηκε με βάση την ακόλουθη ποσοτική κλίμακα:

| | |
|---|---|
| **1** | Καθόλου ή ελάχιστα ικανοποιητικά |
| **2** | Σε ικανοποιητικό βαθμό |
| **3** | Σε μεγάλο ή πλήρες βαθμό |

*Σχήμα 7: Κλίμακα βαθμολογίας κριτηρίων*

Η χρήση της κλίμακας αυτής επιτρέπει τη συγκριτική αποτύπωση της επάρκειας και της ωριμότητας κάθε προτύπου σε επιμέρους τομείς, διατηρώντας παράλληλα απλότητα στην ερμηνεία και συγκρισιμότητα μεταξύ των πλαισίων.

Ο συνολικός βαθμός για κάθε πρότυπο προκύπτει ως άθροισμα των βαθμών που συγκεντρώνει σε όλα τα επιμέρους κριτήρια. Ο τελικός αριθμός διαμορφώνεται από το άθροισμα των Μέσων Όρων (ΜΟ) του μέγιστου πλήθους κριτηρίων (ανώτατη τιμή βαθμολογίας ανά κατηγορία κριτήριων).

| | |
|---|---|
| 0 - 10 | Χαμηλή επάρκεια |
| 11 - 20 | Μέτρια έως ικανοποιητική επάρκεια |
| 21 - 30 | Υψηλή επάρκεια |

*Σχήμα 8: Κλίμακα συνολικής βαθμολογίας*

Πιο συγκεκριμένα:

- **Χαμηλή επάρκεια:** Το πρότυπο εμφανίζει σημαντικά κενά ή περιορισμούς στις περισσότερες κατηγορίες αξιολόγησης. Ενδείκνυται κυρίως για ειδικές περιπτώσεις ή ως συμπληρωματικό εργαλείο.
- **Μέτρια έως ικανοποιητική επάρκεια:** Το πρότυπο καλύπτει βασικές απαιτήσεις και μπορεί να εφαρμοστεί με επιτυχία σε αρκετά περιβάλλοντα, ενδεχομένως με ανάγκη για πρόσθετες προσαρμογές ή ενίσχυση σε κρίσιμους τομείς.
- **Υψηλή επάρκεια:** Το πρότυπο θεωρείται ολοκληρωμένο, εφαρμόσιμο σε ποικίλα επιχειρησιακά πλαίσια και συμβατό με κανονιστικές απαιτήσεις. Προσφέρει ευρεία κάλυψη και υποστήριξη για την ενίσχυση της ασφάλειας της εφοδιαστικής αλυσίδας.

Η ερμηνεία των βαθμών δεν είναι απόλυτη αλλά ενδεικτική. Η τελική επιλογή προτύπου πρέπει να βασίζεται στις ανάγκες και τους πόρους του κάθε οργανισμού, καθώς και στην κριτική αξιολόγηση των θεματικών κατηγοριών που έχουν μεγαλύτερη σημασία για το εκάστοτε επιχειρησιακό πλαίσιο.

### 5.2.4 Συνολική διαδικασία αξιολόγησης

Η διαδικασία αξιολόγησης περιλαμβάνει τα εξής στάδια:

- **Μελέτη προτύπων**: Μελέτη του περιεχομένου των δύο προτύπων ώστε να αποτυπωθούν οι βασικές απαιτήσεις και οι στόχοι.
- **Καθορισμός κατηγοριών κριτηρίων**: Δημιουργήθηκαν 10 υψηλού επιπέδου αφαίρεσης θεματικές κατηγορίες αξιολόγησης.
- **Καθορισμός κριτηρίων**: Για κάθε κατηγορία κριτηρίων ορίστηκαν κριτηρία με στόχο την εμβάθυνση και λεπτομερή ανάλυση των δυνατοτήτων και στοιχείων κάθε προτύπου.
- **Ποιοτική τεκμηρίωση ανά κριτήριο**: Κάθε κριτήριο συνοδεύεται από αναλυτική ποιοτική περιγραφή των δυνατοτήτων κάθε προτύπου, με παραπομπές σε επίσημες και δευτερογενείς πηγές.
- **Ποσοτική βαθμολόγηση**: Καθορίστηκε και εφαρμόστηκε ποσοτική κλίμακα τριών επιπέδων κάλυψης για κάθε κριτήριο (1 έως 3) με σκοπό τον υπολογισμό του τελικού βαθμού, στον οποίο κάθε πρότυπο καλύπτει το εκάστοτε κριτήριο.
- **Οπτική απεικόνιση**: Για κάθε πρότυπο δημιουργήθηκε πίνακας υπολογισμού βαθμού και ακολούθησε η δημιουργία ενός ακόμα συνολικού πίνακα σύγκρισης και η τελική εξαγωγή συμπερασμάτων μέσω διαγραμμάτων.

Ο συνολικός πίνακας συγκριτικής αξιολόγησης λειτουργεί ως βασικό εργαλείο για την εξαγωγή συμπερασμάτων και την ενίσχυση της τεκμηριωμένης επιλογής προτύπων από οργανισμούς που επιθυμούν να υιοθετήσουν ένα καλά οργανωμένο και σύμφωνο με διεθνή Κανονισμούς πλαίσιο διαχείρισης κινδύνων στην εφοδιαστική τους αλυσίδα.

## 5.3 Συγκριτική Αξιολόγηση

Στην παρούσα ενότητα, πραγματοποιείται η συγκριτική αξιολόγηση των δύο προτύπων ανά κατηγορία κριτηρίων. Συγκεκριμένα για κάθε κατηγορία παρατίθενται δύο πινακάκια βαθμολόγησης, ένα για κάθε πρότυπο.

### 1. Πεδίο εφαρμογής

Το NIST SP 800 – 161r1 προσφέρει εκτενή κάλυψη ανεξαρτήτως μεγέθους, παρέχοντας καθοδήγηση τόσο για μικρούς όσο και για μεγάλους φορείς, συμπεριλαμβανομένων των ομοσπονδιακών υπηρεσιών. Παράλληλα, προσαρμόζεται σε διάφορους τομείς με αναφορές σε διαφορετικά επίπεδα λειτουργίας και ρυθμιστικές απαιτήσεις. Όπως αναφέρεται ακριβώς μέσα στο πρότυπο, δεν υπάρχει μία καθολική προσέγγιση (not one-size-fits-all), αλλά μια προσαρμόσιμη στρατηγική.

| | Κριτήριο | Τεκμηρίωση | Βαθμός |
|---|---|---|---|
| Πεδίο εφαρμογής | **Κάλυψη διαφορετικών οργανωτικών μεγεθών** | Αναγνωρίζει διαφορετικά μεγέθη οργανισμών, συμπεριλαμβανομένων μικρομεσαίων επιχειρήσεων, παρέχοντας προσαρμόσιμη στρατηγική. *NIST SP 800 - 161r1: section 1.1* | **3** |
| | **Προσαρμοστικότητα σε διαφορετικούς κλάδους και τομείς** | Υποστηρίζει εφαρμογή σε πολλούς τομείς, με έμφαση στην ομοσπονδιακή χρήση. *NIST SP 800 - 161r1: section 1.1, 1.2* | **3** |

*Σχήμα 9: Κριτήριο 1- NIST SP 800 - 161R1*

Το ίδιο ισχύει και για το ISO 27036. Συγκεκριμένα στο 2ο μέρος του προτύπου αναφέρεται ότι εφαρμόζεται σε όλους τους οργανισμούς ανεξαρτήτως είδους, μεγέθους και φύσεως.

| | Κριτήριο | Τεκμηρίωση | Βαθμός |
|---|---|---|---|
| Πεδίο εφαρμογής | **Κάλυψη διαφορετικών οργανωτικών μεγεθών** | Εφαρμόζεται σε διαφορετικά μεγέθη οργανισμών. *ISO 27036 - 2: Scope* | **3** |
| | **Προσαρμοστικότητα σε διαφορετικούς κλάδους και τομείς** | Προσφέρει κατευθυντήριες οδηγίες σε οργανισμούς ενεξαρτήτως είδους, μεγέθους, φύσεως. *ISO 27036 - 2: Scope* | **3** |

*Σχήμα 10: Κριτήριο 1- ISO 27036*

### 2. Διεθνής αναγνώριση

Το NIST SP 800-161r1 αναγνωρίζεται κυρίως στις Ηνωμένες Πολιτείες και από οργανισμούς που συνεργάζονται με την αμερικανική κυβέρνηση ή κρίσιμες υποδομές, αλλά

έχει επίσης διεθνή τεχνική απήχηση ως πρακτική καθοδήγηση για τον εντοπισμό και τη διαχείριση κινδύνων κυβερνοασφάλειας στην αλυσίδα εφοδιασμού.

| | Κριτήριο | Τεκμηρίωση | Βαθμός |
|---|---|---|---|
| Διεθνής αναγνώριση | **Γεωγραφική αναγνώριση** | Το πρότυπο εφαρμόζεται σε ΗΠΑ, όμως μπορει να υιοθετηθεί από κάθε οργανισμό για την ενίσχυση της ασφάλειας της Εφοδιαστικής Αλυσίδας.<br>*NIST SP 800 - 161r1* | **2** |

*Σχήμα 11: Κριτήριο 2- NIST SP 800 - 161R1*

Αντίθετα, το ISO/IEC 27036 έχει ευρεία διεθνή αναγνώριση ως πρότυπο για την ασφάλεια πληροφοριών στις σχέσεις με προμηθευτές και χρησιμοποιείται σε οργανισμούς παγκοσμίως, συχνά σε συνδυασμό με το ISO 27001 για την κάλυψη απαιτήσεων της εφοδιαστικής αλυσίδας.

| | Κριτήριο | Τεκμηρίωση | Βαθμός |
|---|---|---|---|
| Διεθνής αναγνώριση | **Γεωγραφική αναγνώριση** | Είναι διεθνής με ευρεία αναγνώριση.<br>*ISO 27036* | **3** |

*Σχήμα 12: Κριτήριο 2- ISO 27036*

Ενώ το ISO 27036 θεωρείται παγκόσμιο πρότυπο, το NIST SP 800-161r1 έχει τεχνική και στρατηγική αξία διεθνώς, αλλά δεν αποτελεί επίσημο ή πιστοποιήσιμο διεθνές πρότυπο.

## 3. Επίπεδο Ωριμότητας

Το NIST SP 800-161r1 ενσωματώνει τη χρήση των **NIST Cybersecurity Framework Tiers (1–4)** ως σαφές εργαλείο για την κατηγοριοποίηση και σταδιακή εξέλιξη των δυνατοτήτων ενός οργανισμού στη διαχείριση κινδύνων στην εφοδιαστική αλυσίδα. Τα Tiers επιτρέπουν στον οργανισμό να αυτοαξιολογηθεί, να παρακολουθεί την πρόοδο του και να υλοποιεί βέλτιστες πρακτικές, βάσει ωριμότητας.

| | Κριτήριο | Τεκμηρίωση | Βαθμός |
|---|---|---|---|
| Επίπεδο Ωριμότητας | **Υποστήριξη διαφορετικών επιπέδων ωριμότητας Οργανισμών** | Εφαρμόζεται σε οργανισμούς με διαφορετικά επίπεδα ωριμότητας (Foundational, Sustaining, Enabling)<br>*NIST SP 800 - 161r1: section 1.1* | **3** |
| | **Προτεινόμενο μοντέλο ενίσχυσης ωριμότητας Οργανισμών** | Προτείνει τη χρήση των CSF Tiers.<br>*NIST SP 800 - 161r1: section 3.5* | **3** |

*Σχήμα 13: Κριτήριο 3 - NIST SP 800 - 161R1*

Αντίθετα, το ISO/IEC 27036 παρέχει γενικές οδηγίες και καλές πρακτικές, χωρίς να περιλαμβάνει μοντέλο ωριμότητας ή μετρήσιμα επίπεδα εξέλιξης, καθιστώντας το λιγότερο κατάλληλο ως εργαλείο στρατηγικού σχεδιασμού ανάπτυξης ικανοτήτων.

| | Κριτήριο | Τεκμηρίωση | Βαθμός |
|---|---|---|---|
| Επίπεδο Ωριμότητας | **Υποστήριξη διαφορετικών επιπέδων ωριμότητας Οργανισμών** | Προσφέρει ευελιξία και δυνατότητα προοδευτικής εφαρμογής στις σχέσεις με προμηθευτές. *ISO 27036 - 2: Scope* | 3 |
| | **Προτεινόμενο μοντέλο ενίσχυσης ωριμότητας Οργανισμών** | Δεν προσφέρεται συγκεκριμένος κατευθυντήριος χάρτης ή μοντέλο υλοποίησης για την επίτευξη της μέγιστης ικανότητας και ωριμότητας. *ISO 27036 - 2: Scope* | 1 |

*Σχήμα 14: Κριτήριο 3- ISO 27036*

## 4. Διαδικασία Διαχείρισης Κινδύνου

Το NIST SP 800 – 161r1 διαθέτει ολοκληρωμένη μεθοδολογία διαχείρισης κινδύνου καλύπτοντας με συνέπεια τις φάσεις του πλαισίου διαχείρισης κινδύνων (ορισμός, αξιολόγηση, απόκριση και παρακολούθηση) κατά μήκος της εφοδιαστικής αλυσίδας. Επιπλέον, προτείνει την χρήση δεικτών απόδοσης (π.χ. supply chain risk metrics, performance outcomes, tiered implementation) οι οποίοι διευκολύνουν τη μέτρηση της αποτελεσματικότητας των μέτρων και τη συνεχή βελτίωση.

| | Κριτήριο | Τεκμηρίωση | Βαθμός |
|---|---|---|---|
| Μεθοδολογία Διαχείρισης Κινδύνων | **Πληρότητα** | Αναλύονται όλες οι φάσεις της διαδικασίας διαχείρισης κινδύνων και προτείνονται μέτρα ασφαλείας για την αντιμετώπιση των σχετικών κιδύνων. *NIST SP 800 - 161r1: Appendix G, NASA SWEP* | 3 |
| | **Μέτρηση απόδοσης** | Προτείνεται η χρήση KPIs και KRIs , χωρίς όμως να προτείνει συγκεκριμένο μοντέλο καθορισμού δεικτών απόδοσης. *NIST SP 800 - 161r1: Appendix G* | 2 |

*Σχήμα 15: Κριτήριο 4- NIST SP 800 - 161R1*

Αντίθετα, το ISO/IEC 27036-2 υιοθετεί μια πιο γενική, διοικητική προσέγγιση, ευθυγραμμισμένη με το ISO/IEC 27005, χωρίς όμως να διαχωρίζει ξεκάθαρα τις φάσεις του risk management κύκλου, ενώ απουσιάζει μία αναφορά ή πρόταση μέτρησης απόδοσης της διαδικασίας.

| | Κριτήριο | Τεκμηρίωση | Βαθμός |
|---|---|---|---|
| Μεθοδολογία Διαχείρισης Κινδύνων | **Πληρότητα** | Βασίζεται στο ISO 27005, προσφέροντας μια πιο γενική διοικητική προσέγγιση στις σχέσεις με τους προμηθευτές και όχι στην διαχείριση κινδύνου κατα μήκους της εφοδιαστικής αλυσίδας. *Supply Chain Cybersecurity – Good Practices for Risk Management, ENISA* | 2 |
| | **Μέτρηση απόδοσης** | Δεν γίνεται αναφορά σε KPIs ή metrics. *ISO 27036* | 1 |

*Σχήμα 16: Κριτήριο 4 -ISO 27036*

Το ISO παρέχει χρήσιμες γενικές οδηγίες για την αναγνώριση και διαχείριση των κινδύνων που προκύπτουν από τις σχέσεις με τους προμηθευτές, αλλά δεν εισέρχεται στο ίδιο βάθος λειτουργικής αξιολόγησης, όπως το NIST, καθιστώντας το λιγότερο κατάλληλο για οργανισμούς που απαιτούν μετρήσιμα αποτελέσματα και συνεχή παρακολούθηση.

## 5. Επάρκεια Προτεινόμενων Μέτρων Ασφάλειας

το NIST SP 800-161r1 ενσωματώνει και εξειδικεύει μέτρα ασφάλειας για τη διαχείριση κινδύνων στην εφοδιαστική αλυσίδα εντός του ίδιου του εγγράφου (μέσω παραπομπής στο SP 800-53 Rev. 5), με πλήρεις πίνακες και οδηγίες εφαρμογής σε κάθε φάση της σχέσης.

| | Κριτήριο | Τεκμηρίωση | Βαθμός |
|---|---|---|---|
| Επάρκεια Προτεινόμενων Μέτρων Ασφάλειας | **Ποσότητα και κάλυψη μέτρων** | Εκτεταμένος κατάλογος μέτρων ασφαλείας, καλύπτωντας τεχνικά και οργανωτικά μέτρα. *NIST SP 800 - 161r1: Appendix A, NASA SWEP* | 3 |
| | **Σαφήνεια μέτρων** | Τα μέτρα παρέχονται με ορισμούς, πρακτικές κατευθύνσεις. *NIST SP 800 - 161r1: Appendix A, NASA SWEP* | 3 |

*Σχήμα 17: Κριτήριο 5 - NIST SP 800 - 161R1*

Το ISO/IEC 27036 εστιάζει στη διαχείριση των σχέσεων με προμηθευτές από διοικητική και οργανωτική οπτική, και όπου απαιτούνται μέτρα ασφαλείας, παραπέμπει στον Annex A του ISO/IEC 27001:2022 και κυρίως στο ISO/IEC 27002:2022, όπου γίνεται η αναλυτική περιγραφή των ελέγχων και των πρακτικών εφαρμογής τους.

| | Κριτήριο | Τεκμηρίωση | Βαθμός |
|---|---|---|---|
| Επάρκεια Προτεινόμενων Μέτρων Ασφάλειας | **Ποσότητα και κάλυψη μέτρων** | Προτείνει την εφαρμογή μέτρων ασφαλείας βασισμένων σε άλλα πρότυπα (π.χ. ISO 27001/27002). *ISO 27036 , NASA SWEP* | 2 |
| | **Σαφήνεια μέτρων** | Τα μέτρα παρέχονται με ορισμούς, πρακτικές κατευθύνσεις. *NIST SP 800 - 161r1: Appendix A, NASA SWEP* | 3 |

*Σχήμα 18: Κριτήριο 5- ISO 27036*

## 6. Πρακτική Εφαρμογή

Το πρότυπο NIST SP 800-161r1 προσφέρει μια πλήρη και λεπτομερή μεθοδολογία για την πρακτική εφαρμογή της ασφάλειας στην εφοδιαστική αλυσίδα, παρέχοντας εκτενή υποστηρικτικά έγγραφα, παραδείγματα και εργαλεία, όπως τα μέτρα του NIST SP 800-53, που καλύπτουν τόσο τεχνικές όσο και οργανωτικές πτυχές. Επιπλέον υπάρχουν πολλά έγγραφα τα οποία λειτουργούν ως οδηγοί για την υλοποίηση του περιεχομένου του προτύπου και αναγράφονται στο ANNEX B του εγγράφου του ENISA: Good practices for supply chain cybersecurity.

| | Κριτήριο | Τεκμηρίωση | Βαθμός |
|---|---|---|---|
| Πρακτική Εφαρμογή | **Πληρότητα και χρηστικότητα** | Το έγγραφο είναι πλήρες και αναλυτικό προσφέροντας παραδείγματα υλοποίησης όπου χρειάζεται. *NIST SP 800 - 161r1* | 3 |
| | **Υποστηρικτικό υλικό και οδηγίες υλοποίησης** | Υπάρχουν συνοδευτικές υποστηρικτικές πηγές υλοποίησης C-SCRM. *Good practices for supply chain cybersecurity ,ENISA* | 3 |

*Σχήμα 19: Κριτήριο 6- NIST SP 800 - 161R1*

Αντίθετα, το ISO/IEC 27036-2 λειτουργεί κυρίως ως γενικό πλαίσιο κατευθυντήριων οδηγιών και πολιτικών, με περιορισμένο υποστηρικτικό υλικό μέσα στο ίδιο το πρότυπο, το οποίο προτείνεται να συμπληρώνεται από άλλα σχετικά ISO πρότυπα (όπως τα ISO 27001, 27002 και 27005) για να επιτευχθεί ολοκληρωμένη εφαρμογή. Παρόλα αυτά υπάρχουν υποστηρικτικές πηγές που το συμπληρώνουν και αναγράφονται στο ANNEX B του εγγράφου του ENISA: Good practices for supply chain cybersecurity.

| | Κριτήριο | Τεκμηρίωση | Βαθμός |
|---|---|---|---|
| Πρακτική Εφαρμογή | **Πληρότητα και χρηστικότητα** | Δεν μπορεί να χαρακτηριστεί πλήρες με την έννοια της τεχνικής πληρότητας ή της αναλυτικής καθοδήγησης.<br>*ISO 27036* | 2 |
| | **Υποστηρικτικό υλικό και οδηγίες υλοποίησης** | Υπάρχουν υποστηρικτικές πηγές.<br>*Good practices for supply chain cybersecurity ,ENISA* | 3 |

*Σχήμα 20: Κριτήριο 6- ISO 27036*

Συνεπώς, το NIST παρέχει πιο συγκεκριμένες και πρακτικές οδηγίες για άμεση υλοποίηση, ενώ το ISO 27036-2 είναι πιο ευέλικτο και εναρμονίζεται εύκολα με ευρύτερα συστήματα διαχείρισης ασφάλειας, απαιτώντας όμως επιπλέον πηγές για την πληρότητα της εφαρμογής.

## 7. Υποστήριξη και Συμβατότητα με Εργαλεία Διαχείρισης Κινδύνων

Το NIST SP 800-161r1 προσφέρει ενσωματωμένα, εξειδικευμένα υποστηρικτικά templates, όπως το C-SCRA Template, το C-SCRM Strategy and Implementation Plan, και το C-SCRM Policy, τα οποία διευκολύνουν την πρακτική υλοποίηση και την ενσωμάτωση του C-SCRM σε ολόκληρο τον οργανισμό. Τα templates αυτά παρέχονται μέσα στο πρότυπο συνοδευόμενα από πρακτικά παραδείγματα οπότε δεν επιφέρουν επιπλέον κόστος στον οργανισμό.

| | Κριτήριο | Τεκμηρίωση | Βαθμός |
|---|---|---|---|
| Υποστήριξη και Συμβατότητα με Εργαλεία Διαχείρισης Κινδύνων | **Αναφορά και συμβατότητα σε εργαλεία διαχείρισης κινδύνων** | Παρέχει υποδείγματα (templates) για την δημιουργία στρατηγικής και σχέδιο υλοποίησης (C-SCRM Strategy & Plan), Πολιτική (C-SCRM Policy) και τη διαδικασία αξιολόγησης προμηθευτών (C-SCRA Template)<br>*NIST SP 800 - 161r1: Appendex G* | 3 |
| | **Κόστος εργαλείων** | Τα templates υπάρχουν μέσα στο πρότυπο συνοδευόμενα από παραδείγματα.<br>*NIST SP 800 - 161r1: Appendex G* | 3 |

*Σχήμα 21: Κριτήριο 7- NIST SP 800 - 161R1*

Παρότι το ISO/IEC 27036 δεν παρέχει εξειδικευμένα εργαλεία για την ανάλυση κινδύνων στην εφοδιαστική αλυσίδα, εντούτοις ευθυγραμμίζεται πλήρως με το ISO/IEC 27001. Η ευθυγράμμιση αυτή επεκτείνεται και στη σύνδεση του 27036 με το ISO 27005, επιτρέποντας τη χρήση αναγνωρισμένων εργαλείων διαχείρισης κινδύνων όπως τα CRAMM, EBIOS, MEHARI και MONARC κ.α. Τα εργαλεία αυτά, αν και γενικού σκοπού, μπορούν να προσαρμοστούν στην αξιολόγηση προμηθευτών και στην εκτίμηση των απειλών που απορρέουν από τρίτα μέρη, ενισχύοντας έτσι τη χρηστικότητα του ISO. Τέλος, τα εργαλεία αυτά δεν είναι όλα open source οπότε η χρήση και κατ' επέκταση παραμετροποίησή τους δύναται να οδηγήσει σε επιπλέον κόστος.

| | Κριτήριο | Τεκμηρίωση | Βαθμός |
|---|---|---|---|
| Υποστήριξη και Συμβατότητα με Εργαλεία Διαχείρισης Κινδύνων | **Αναφορά και συμβατότητα σε εργαλεία διαχείρισης κινδύνων** | Παραπέμπει στο ISO/IEC 27001 για την απαίτηση υλοποίησης ISMS. Επομένως η χρήση εργαλείων διαχείρισης κινδύνου κατά iso 27005 είναι θεμιτή και συμβατή μετά από σχετική παραμετροποίηση. *ISO 27036 - 3, 4* | **3** |
| | **Κόστος εργαλείων** | Τα εργαλεία διαχείρισης κινδύνου που είναι συμβατά με ISO 27005 δεν είναι όλα δωρεάν και θα χρειαστούν παραμετροποίηση οπότε η χρήση τους θα επιφέρει κόστος. | **2** |

*Σχήμα 22: Κριτήριο 7- ISO 27036*

Συνεπώς, ενώ το ISO 27036 παρέχει ευελιξία μέσω προσαρμογής υπαρχόντων εργαλείων διαχείρισης κινδύνων, το NIST προσφέρει πληρότητα μέσω έτοιμων και καθοδηγούμενων πρακτικών λύσεων, προσδίδοντας μεγαλύτερη επιχειρησιακή υποστήριξη και ευκολία στην εφαρμογή.

## 8. Διαλειτουργικότητα

το NIST SP 800-161r1 υποστηρίζει την εφαρμογή της C-SCRM τόσο σε IT όσο και σε OT περιβάλλοντα, περιλαμβάνοντας και IoT υποδομές, και ενσωματώνει πρότυπα όπως το NIST SP 800-53 και το NIST SP 800-37, καθώς και διεθνή πρότυπα όπως τα ISO 27001 και ISO 27002.

Το πρότυπο είναι ιδιαίτερα ευέλικτο ως προς την ενσωμάτωση με πολλαπλά περιβάλλοντα τεχνολογικών υποδομών, υποστηρίζοντας συνδυαστικά ICT και OT τομείς, γεγονός που το καθιστά εξαιρετικά κατάλληλο για σύνθετα περιβάλλοντα.

| | Κριτήριο | Τεκμηρίωση | Βαθμός |
|---|---|---|---|
| Διαλειτουργικότητα | **Ευθυγράμμιση με άλλα πρότυπα** | Ευθυγραμμίζεται με ISO 27000, NIST CSF, SP 800-53. *NIST SP 800 - 161r1* | **3** |
| | **Υποστήριξη πολλαπλών υποδομών** | Διευρυμένη εφαρμοσιμότητα του προτύπου σε περιβάλλοντα τόσο Information Technology (IT) όσο και Operational Technology (OT) συμπεριλαμβανομένων και των συστημάτων Internet of Things (IoT). | **3** |

*Σχήμα 23: Κριτήριο 8- NIST SP 800 - 161R1*

Το ISO/IEC 27036 ανήκει στην οικογένεια προτύπων ISO 27000 και συνεπώς ευθυγραμμίζεται πλήρως με τα συναφή πρότυπα, όπως το ISO/IEC 27001, ISO/IEC 27002 και το ISO/IEC 27005. Επιπλέον, σημαντικό μέρος του (ιδίως το ISO/IEC 27036-3 και 27036-4) επικεντρώνεται σε εξειδικευμένα περιβάλλοντα, όπως οι εφοδιαστικές αλυσίδες ICT και τα Cloud οικοσυστήματα, προσφέροντας έτσι ευρεία υποστήριξη σε διαφορετικά τεχνολογικά περιβάλλοντα και ενισχύοντας την προσαρμοστικότητά του σε σύγχρονες υποδομές.

| | Κριτήριο | Τεκμηρίωση | Βαθμός |
|---|---|---|---|
| Διαλειτουργικότητα | **Ευθυγράμμιση με άλλα πρότυπα** | Ανήκει στην οικογένεια ISO 27000.<br>*ISO 27036 - 1* | **3** |
| | **Υποστήριξη πολλαπλών υποδομών** | Το ISO 27036 part 3 εξειδικευεται για ICT αλυσίδες εφοδιασμού, ενώ το part 4 σε cloud service providers.<br>*ISO 27036 - 3, 4* | **3** |

*Σχήμα 24: Κριτήριο 8- ISO 27036*

Και τα δύο πρότυπα επιδεικνύουν ισχυρή ευθυγράμμιση με πρότυπα και υποστήριξη πολλαπλών τεχνολογικών υποδομών.

## 9. Επίπεδο Εμπιστοσύνης Μεταξύ των Εμπλεκόμενων Μερών

Μέσω του C-SCRA (Cybersecurity Supply Chain Risk Assessment), το NIST SP 800 - 161r1 προσφέρει ένα δομημένο πλαίσιο για την αποτίμηση προμηθευτών και προϊόντων, ενσωματώνοντας μηχανισμούς που ενισχύουν την εμπιστοσύνη (confidence-building mechanisms) και προωθούν τη διαφάνεια ως ουσιώδες στοιχείο της C-SCRM. Παράλληλα, η ανταλλαγή πληροφοριών περιγράφεται ως κρίσιμος παράγοντας επιτυχίας ενισχύοντας έτσι την ανθεκτικότητα, τόσο σε τεχνικό όσο και σε οργανωτικό επίπεδο (π.χ. συνεργασία με FASC και άλλους φορείς), ενώ η οικογένεια μέτρων PT υπογραμμίζει τη διαφάνεια στη διαχείριση δεδομένων.

| | Κριτήριο | Τεκμηρίωση | Βαθμός |
|---|---|---|---|
| Επίπεδο Εμπιστοσύνης Μεταξύ των Εμπλεκόμενων Μερών | **Μέθοδοι αξιολόγισης Τρίτων** | Το Cybersecurity Supply Chain Risk Assessment (C-SCRA) λειτουργεί σαν καθοδήγηση για την αξιολόγηση προϊόντων, υπηρεσιών ή προμηθευτών τρίτων. Επιπλέον, αναφέρεται και ως κρίσιμος παράγοντας επιτυχίας (Confidence-Building Mechanisms)<br>*NIST SP 800 - 161r1: Appendix D, section 3* | **3** |
| | **Διαφάνεια** | Αναφέρεται ως πρακτική C-SCRM και στην οικογένεια μέτρων ασφαλείας PT (Personally identifiable information processing and Transparency)<br>*NIST SP 800 - 161r1: Appendix A, section 3* | **3** |
| | **Διαμοιρασμός πληροφοριών** | Αναφέρεται ως πρακτική C-SCRM (διαμοιρασμός με FASC και άλλα μέρη) για την ενίσχυση της ανθεκτικότητας.<br>*NIST SP 800 - 161r1: section 3* | **3** |

*Σχήμα 25: Κριτήριο 9- NIST SP 800 - 161R1*

Αντίθετα, το ISO/IEC 27036 αναγνωρίζει μεν τη σημασία της διαφάνειας και του διαμοιρασμού πληροφοριών ως απαιτήσεις, ωστόσο το κάνει σε πιο αφηρημένο και περιγραφικό επίπεδο. Ο διαμοιρασμός πληροφοριών περιορίζεται σε γενικές απαιτήσεις ανταλλαγής πληροφοριών που σχετίζονται με αλλαγές στην ασφάλεια και περιστατικά, χωρίς να εξειδικεύονται διαδικασίες, ρόλοι, μορφές πληροφόρησης ή μηχανισμοί ελέγχου της εγκυρότητας. Η διαφάνεια καλύπτεται μόνο εντός του πλαισίου διαχείρισης

σχέσεων με τους προμηθευτές, χωρίς ιδιαίτερη εστίαση στην ενίσχυση της εμπιστοσύνης ή της λογοδοσίας.

| | Κριτήριο | Τεκμηρίωση | Βαθμός |
|---|---|---|---|
| Επίπεδο Εμπιστοσύνης Μεταξύ των Εμπλεκόμενων Μερών | **Μέθοδοι αξιολόγισης Τρίτων** | Αναφέρεται σε πολλά σημεία ως απαίτηση χωρίς να αναλύει ή να προτείνει μία μέθοδο αξιολόγησης τρίτων. *ISO 27036 - Part 2* | 2 |
| | **Διαφάνεια** | Ορίζονται διαδικασίες που εξασφαλίζουν τη διαφάνεια στις σχέσεις με τους προμηθευτές. *ISO 27036 - Part 2* | 3 |
| | **Διαμοιρασμός πληροφοριών** | Αναφέρεται μόνο στην ανταλλαγή πληροφοριών ως απαίτηση (αλλαγές στην ασφάλεια των πληροφοριών, και περιστατικά) μεταξύ των εμπλεκόμενων μερών. *ISO 27036 - Part 2* | 2 |

*Σχήμα 26: Κριτήριο 9- ISO 27036*

Κατά συνέπεια, το NIST παρουσιάζει μεγαλύτερο επίπεδο πρακτικής καθοδήγησης και λειτουργικής πληρότητας σε σχέση με το ISO, το οποίο παραμένει περισσότερο θεωρητικό και γενικό.

## 10. Κόστος - Όφελος

Το NIST SP 800-161r1 παρέχει μία αναλυτική προσέγγιση στη διαχείριση κόστους και πόρων στο πλαίσιο της C-SCRM. Εξετάζει την ισορροπία μεταξύ του κόστους εφαρμογής μέτρων ασφαλείας και του κινδύνου μη εφαρμογής τους, τονίζοντας την ανάγκη λήψης αποφάσεων βάσει ανάλυσης κόστους-οφέλους. Επισημαίνει τη σημασία της επαναχρησιμοποίησης τεκμηρίωσης και πιστοποιήσεων για τη μείωση κόστους, τη διαφοροποίηση μεταξύ λειτουργικών και επενδυτικών δαπανών, καθώς και την ανάγκη ύπαρξης σαφώς προσδιορισμένου προϋπολογισμού C-SCRM σε ετήσιο ή πολυετές επίπεδο. Παρουσιάζει επίσης τρόπους βελτιστοποίησης μέσω shared services, cost-sharing μηχανισμών και επιδόσεων (performance-linked funding). Είναι ένας από τους κρίσιμους παράγοντες επιτυχίας της C-SCRM και οδηγεί στην αποφυγή περιττών επαναξιολογήσεων και αυξημένη υπευθυνότητα διαχείρισης πόρων.

| | Κριτήριο | Τεκμηρίωση | Βαθμός |
|---|---|---|---|
| Κόστος - όφελος | **Αξιολόγηση κόστους εφαρμογής μέτρων ασφάλειας** | Αναλυτική προσέγγιση στη διαχείριση κόστους και πόρων στο πλαίσιο της C-SCRM<br>*NIST SP 800 - 161r1 & NISTIR 8286B report* | 3 |
| | **Υποστήριξη λήψης αποφάσεων βάση κόστους - οφέλους** | Καθοδήγηση για την αξιολόγηση του κόστους υλοποίησης και του κινδύνου μη υιοθέτησης μέτρων, μέσω του cybersecurity risk register, το οποίο τροφοδοτεί το ευρύτερο Enterprise Risk Register, συνυπολογίζοντας την εκτιμώμενη επίδραση και κόστος των επιλογών απόκρισης στον κίνδυνο σε σχέση με τους επιχειρησιακούς στόχους.<br>*NIST SP 800 - 161r1* | 3 |

*Σχήμα 27: Κριτήριο 10- NIST SP 800 - 161R1*

Το ISO/IEC 27036, αν και δεν παρέχει αναλυτικό μοντέλο κόστους-οφέλους, αναγνωρίζει ωστόσο την επίδραση των απαιτήσεων ασφάλειας στο κόστος, το σχέδιο και το χρονοδιάγραμμα ενός έργου. Συγκεκριμένα, στο πλαίσιο του προγραμματισμού έργων, απαιτεί να λαμβάνονται υπόψη οι επιπτώσεις των απαιτήσεων ασφάλειας στις σχετικές παραμέτρους. Παρά τη θετική αυτή αναφορά, δεν προσφέρει μεθοδολογία για την αποτίμηση του κόστους μέτρων ή για σύγκριση επένδυσης - ωφέλειας, ούτε και καθοδήγηση για την υποστήριξη αποφάσεων βάσει ανάλυσης κόστους-απόδοσης.

| | Κριτήριο | Τεκμηρίωση | Βαθμός |
|---|---|---|---|
| Κόστος - όφελος | **Αξιολόγηση κόστους εφαρμογής μέτρων ασφάλειας** | Μερική κάλυψη (π.χ., αναγνώριση κόστους ως παράγοντα, χωρίς ανάλυση).<br>*ISO 27036 - 2* | 1 |
| | **Υποστήριξη λήψης αποφάσεων βάση κόστους - οφέλους** | Δεν παρέχει ρητές οδηγίες ή μεθοδολογίες για ανάλυση κόστους-οφέλους (cost-benefit analysis) ως εργαλείο υποστήριξης λήψης αποφάσεων για την εφαρμογή ελέγχων ή την επιλογή στρατηγικών διαχείρισης κινδύνου.<br>*ISO 27036 - 2* | 1 |

*Σχήμα 28: Κριτήριο 10- ISO 27036*

Συνεπώς, το NIST υπερτερεί σημαντικά, προσφέροντας ένα πλήρες, μετρήσιμο και ευέλικτο πλαίσιο κόστους-οφέλους, απαραίτητο για οργανισμούς που επιθυμούν να συνδέσουν τις απαιτήσεις κυβερνοασφάλειας εφοδιαστικής αλυσίδας με ρεαλιστικό και βιώσιμο οικονομικό σχεδιασμό. Το ISO, αν και θέτει τη σωστή κατεύθυνση, παραμένει σε επίπεδο απαίτησης χωρίς επαρκή καθοδήγηση εφαρμογής.

## 5.4 Συνολικός Πίνακας Αξιολόγησης NIST SP 800-161r1 vs ISO 27036

Με βάση την παραπάνω ανάλυση και βαθμολόγηση κάθε προτύπου για κάθε ένα από τα υπο – κριτήρια των κατηγοριών κριτηρίων καταλήγει ο πίνακας:

*Πίνακας 2: Συγκεντρωτικός πίνακας Συγκριτικής Αξιολόγησης*

| Κατηγορία Κριτηρίων | NIST SP 800 -161r1 | ISO 27036 |
|---|---|---|
| Πεδίο Εφαρμογής | 3 | 3 |
| Διεθνής Αναγνώριση | 2 | 3 |
| Επίπεδο Ωριμότητας | 3 | 2 |
| Μεθοδολογία Διαχείρισης Κινδύνων | 2.5 | 1.5 |
| Επάρκεια Προτεινόμενων Μέτρων Ασφάλειας | 3 | 2.5 |
| Πρακτική Εφαρμογή | 3 | 2.5 |
| Υποστήριξη και Συμβατότητα με Εργαλεία Διαχείρισης Κινδύνων | 3 | 2.5 |
| Διαλειτουργικότητα | 3 | 3 |
| Επίπεδο Εμπιστοσύνης Μεταξύ των Εμπλεκόμενων Μερών | 3 | 2.3 |
| Κόστος - Όφελος | 3 | 1 |
| Τελικός Βαθμός | 28.5 | 23,3 |

## 5.5 Ευρήματα Αξιολόγησης

Η συγκριτική αξιολόγηση μεταξύ των προτύπων **NIST SP 800-161r1** και **ISO/IEC 27036** ανέδειξε ουσιώδεις διαφορές στη δομή, τον σκοπό και την εφαρμοστική προσέγγισή τους στη διαχείριση κινδύνων της εφοδιαστικής αλυσίδας στον κυβερνοχώρο.

Το NIST SP 800-161r1 συγκεντρώνει την υψηλότερη συνολική βαθμολογία (28.5 έναντι 23.3), επιδεικνύοντας σημαντική υπεροχή στις περισσότερες κατηγορίες. Πρόκειται για ένα πλαίσιο που εστιάζει στην πρακτική υλοποίηση της διαχείρισης κινδύνου, εντάσσοντας τη C-SCRM στην ευρύτερη Διαχείριση Κινδύνου σε έναν Οργανισμό ενισχύοντας την ανθεκτικότητά του.

Αντίθετα, το ISO/IEC 27036 ακολουθεί μια πιο συμβατική προσέγγιση προτύπου, εστιάζοντας κυρίως στη διαχείριση των σχέσεων μεταξύ αγοραστών και προμηθευτών και στις απαιτήσεις και διαδικασίες που πρέπει να καθορίζονται μέσω των συμβάσεων. Παράλληλα, προσφέρει επαρκή προσαρμοστικότητα και διεθνή αναγνώριση, αλλά υστερεί σε πρακτικές καθοδήγησης για τον καθορισμό ενός ολοκληρωμένου πλαισίου Διαχείρισης Κινδύνων κατά μήκος της εφοδιαστικής αλυσίδας.

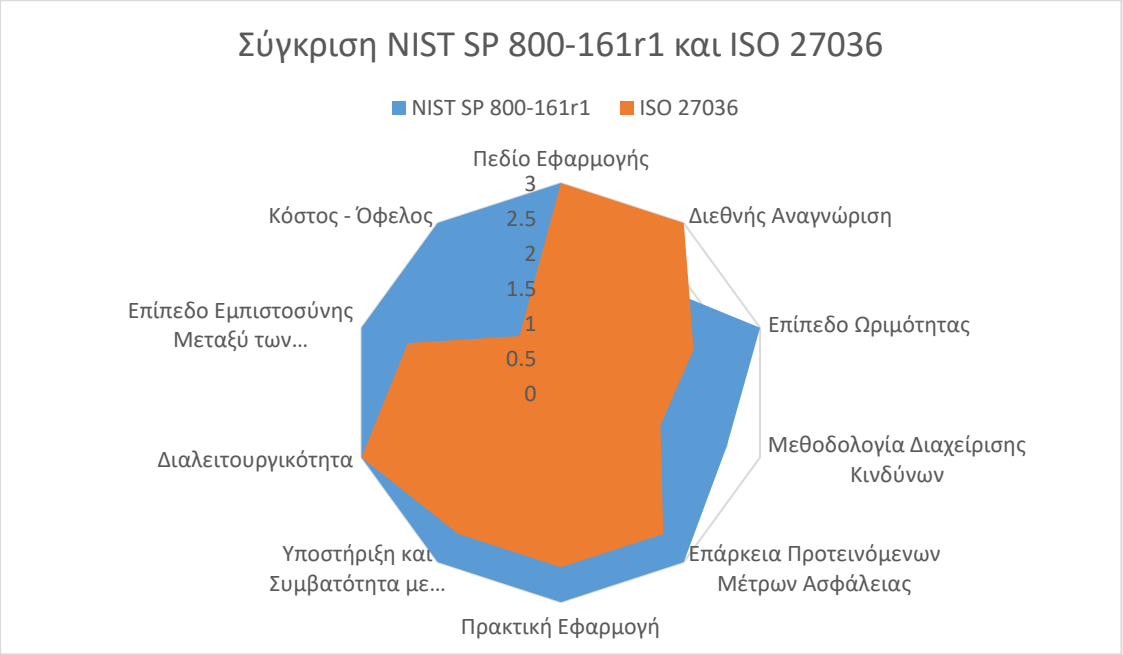
Συμπερασματικά, το NIST SP 800-161r1 παρουσιάζεται ως ένα πιο λειτουργικό πλαίσιο, ιδιαίτερα κατάλληλο για οργανισμούς με ώριμη προσέγγιση και τη διαχείριση μεγάλων σε έκταση αλυσίδων εφοδιασμού. Αντίθετα, το ISO/IEC 27036-2 δύναται να λειτουργήσει ως σημείο αναφοράς για τη σύναψη σχέσεων με προμηθευτές, αλλά απαιτεί συμπληρωματική υποστήριξη μέσω άλλων προτύπων ιδιαίτερα της οικογένειας ISO 27000, στην οποία και ανήκει.

Η διαφορά στην τελική βαθμολογία του κάθε προτύπου οφείλεται κυρίως σε τομείς όπως:

- **Κόστος - Όφελος:** Το πρότυπο NIST παρέχει σαφές πλαίσιο υποστήριξης λήψης αποφάσεων μέσω ανάλυσης κόστους - οφέλους, αξιοποιώντας τεκμηριωμένα στοιχεία για την εκτίμηση κόστους εφαρμογής των μέτρων και την αντιστοίχισή τους με το αναμενόμενο όφελος ασφάλειας. Αντίθετα, το ISO περιορίζεται σε γενικές αναφορές χωρίς συγκεκριμένη καθοδήγηση ή προσεγγίσεις.
- **Μεθοδολογία Διαχείρισης Κινδύνων:** Η προσέγγιση του NIST χαρακτηρίζεται από πληρότητα και λειτουργική συνοχή, ενσωματώνοντας έναν πλήρες κύκλο διαχείρισης κινδύνων και ενσωματώνοντας τεκμηριωμένα παραδείγματα σεναρίων κινδύνου και τρόπους ενσωμάτωσης σε ευρύτερα επιχειρησιακά μοντέλα. Το ISO, αν και θέτει βασικές αρχές, υστερεί σε βάθος καθοδήγησης και μεθοδικής ωριμότητας.
- **Επίπεδο Εμπιστοσύνης:** Το NIST εισάγει μηχανισμούς ενίσχυσης εμπιστοσύνης μεταξύ των εμπλεκομένων μερών της εφοδιαστικής αλυσίδας μέσω προδιαγεγραμμένων διαδικασιών ανταλλαγής πληροφοριών, αξιολόγησης τρίτων και υποστήριξης διαφάνειας με αναφορά σε συμβατικά και νομικά εργαλεία. Το ISO, αν και αναγνωρίζει τη σημασία διαφάνειας, δεν παρέχει εξίσου εξειδικευμένα μέσα εφαρμογής.

Παράλληλα, αξίζει να σημειωθεί ότι το πρότυπο **ISO/IEC 27036 υπερέχει στον δείκτη διεθνούς αναγνώρισης**, γεγονός που οφείλεται στην ιδιότητά του ως διεθνές πρότυπο με ευρύτερη χρήση και θεσμική ενσωμάτωση σε κανονιστικά πλαίσια κρατών και υπερεθνικών οργανισμών, ιδίως εντός Ευρωπαϊκής Ένωσης.

Το παραπάνω radar chart απεικονίζει με ευκρίνεια τις διαφορές μεταξύ των δύο προτύπων.




*Σχήμα 29: NIST SP 800-161r1 vs ISO 27036*

Η διαφορά των **5.2 μονάδων** μεταξύ των δύο προτύπων είναι ενδεικτική της τεχνικής και λειτουργικής πληρότητας του NIST. [29] [30] [31] [32] [33] [34] [35] [37] [9] [10] [11]

# 6. Επίλογος

Η παρούσα εργασία ανέδειξε τη στρατηγική σημασία της ασφάλειας της εφοδιαστικής αλυσίδας στην εποχή των αυξανόμενων ψηφιακών απειλών και της ολοένα και μεγαλύτερης εξάρτησης των οργανισμών από τρίτα μέρη. Η μελέτη απέδειξε πως η εφοδιαστική αλυσίδα θα μπορούσε να χαρακτηριστεί και ως ευάλωτος κρίκος, καθώς μπορεί να λειτουργήσει ως μέσο διάδοσης κυβερνοεπιθέσεων με εκτεταμένες και πολύ ζημιογόνες συνέπειες.

Μετά την έναρξη εφαρμογής της Οδηγίας NIS2, οι Οργανισμοί υποχρεούνται να υιοθετούν δομημένες πολιτικές για την αξιολόγηση, παρακολούθηση και διαχείριση των κινδύνων που σχετίζονται με τρίτα μέρη. Οι νέες απαιτήσεις που απορρέουν από την εν λόγω οδηγία καθιστούν σαφές πως η ασφάλεια της εφοδιαστικής αλυσίδας δεν αποτελεί πλέον επιλογή, αλλά κανονιστική συμμόρφωση.

Η συγκριτική μελέτη μεταξύ των προτύπων NIST SP 800-161r1 και ISO/IEC 27036 απέδειξε πως το NIST, με τον ολοκληρωμένο και επιχειρησιακά προσανατολισμένο χαρακτήρα του, παρέχει ένα πλήρες και δυναμικό πλαίσιο για την ενσωμάτωση της διαχείρισης κινδύνων προμηθευτών (C-SCRM) σε όλα τα επίπεδα της διοικητικής δομής ενός οργανισμού. Αντιθέτως, το ISO 27036 προσεγγίζει την ασφάλεια της εφοδιαστικής αλυσίδας από μια κανονιστική σκοπιά, προσφέροντας ένα πλέγμα απαιτήσεων και διαδικασιών που πρέπει να καθορίζονται μεταξύ αγοραστή και προμηθευτή, με έμφαση στην ευθύνη, συμβατική δέσμευση και κατανομή ρόλων.

Η σύγκλιση των δύο προτύπων μπορεί να αποτελέσει ένα πολυεπίπεδο πλαίσιο διαχείρισης κινδύνων, που θα συνδυάζει τη δομική συμμόρφωση του ISO με την επιχειρησιακή ευελιξία και πρακτική καθοδήγηση του NIST. Ειδικότερα σε περιβάλλοντα υψηλής κρισιμότητας, όπως η παροχή λογισμικού, τεχνολογικών υπηρεσιών ή η διαχείριση δεδομένων, απαιτείται συνδυαστική εφαρμογή των δύο προτύπων για την επίτευξη ουσιαστικής ανθεκτικότητας.

Με την ολοκλήρωση της παρούσας μελέτης, παρουσιάζεται η ανάγκη για περαιτέρω έρευνα, τόσο ως προς την εύρεση βέλτιστων πρακτικών εφαρμογής των προτύπων αυτών σε διάφορους τομείς, όσο και προς την ανάπτυξη μηχανισμών αξιολόγησης και πιστοποίησης για οργανισμούς και προμηθευτές. Εξίσου σημαντική είναι η ανάγκη για αυτόματη παρακολούθηση και ιχνηλασιμότητα της αλυσίδας, μέσα από ψηφιακά εργαλεία και πλατφόρμες διαχείρισης κινδύνων.

Συνοψίζοντας, η κυβερνοασφάλεια στην εφοδιαστική αλυσίδα αναδύεται ως ένας από τους πιο κρίσιμους τομείς της σύγχρονης ασφάλειας πληροφοριών. Η αποτελεσματική διαχείρισή της δεν βασίζεται σε ένα μόνο πρότυπο, αλλά στην ολιστική και διαλειτουργική υιοθέτηση πρακτικών, την καλλιέργεια κουλτούρας εμπιστοσύνης μεταξύ των εμπλεκομένων μερών και τη συνεχή προσαρμογή στις τεχνολογικές και κανονιστικές εξελίξεις. Μόνο μέσα από τέτοιου είδους πολυδιάστατες προσεγγίσεις μπορεί να διασφαλιστεί η ανθεκτικότητα και η ανταγωνιστικότητα των οργανισμών στο σημερινό ψηφιακό οικοσύστημα.

# Αρκτικόλεξα

| Αρκτικόλεξο | Πλήρης Ονομασία |
|---|---|
| APT | Advanced Persistent Threat |
| CEO | Chief Executive Officer |
| CERT | Computer Emergency Response Team |
| CISO | Chief Information Security Officer |
| CSF | Cybersecurity Framework |
| SLA | Service Level Agreement |
| C-SCRM | Cyber Supply Chain Risk Management |
| DoD | Department of Defense |
| ENISA | European Union Agency for Cybersecurity |
| ERM | Enterprise Risk Management |
| EU | European Union |
| ICT | Information and Communication Technologies |
| IoT | Internet of Things |
| IR | Interagency Report (NIST) |
| ISMS | Information Security Management System |
| ISO | International Organization for Standardization |
| IT | Information Technology |
| NIS2 | Network and Information Security Directive 2 |
| NIST | National Institute of Standards and Technology |
| OEM | Original Equipment Manufacturer |
| OT | Operational Technology |
| RFI/RFP | Request for Information / Proposal |
| SCADA | Supervisory Control and Data Acquisition |
| SCRM | Supply Chain Risk Management |
| SEWP | Solutions for Enterprise-Wide Procurement |
| SOC | Security Operations Center |
| SW | Software |
| VPN | Virtual Private Network |

# Πηγές

[1] Berry, J. (2023) The Importance of Cybersecurity in Supply Chain. ResearchGate. Available at: https://www.researchgate.net/publication/371086710_The_Importance_of_Cybersecurity_in_Supply_Chain

[2] Boyes, H. (2021) Cybersecurity in the supply chain. Springer.

[3] Greenberg, A. (2018) Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers. Doubleday.

[4] Rashid, A., Topping, C. and Michalec, O. (2022) 'Contrasting Global Approaches for Identifying and Managing Cybersecurity Risks in Supply Chains', arXiv preprint. Available at: https://arxiv.org/abs/2208.02244

[5] Wieland, A. (2021) Supply Chain Management: A Global Perspective. Cengage Learning.

[6] Arcadian-IoT (2024) Good Practices for Supply Chain Cybersecurity – ENISA Summary. Available at: https://arcadian-iot.eu/enisa-report-good-practices-for-supply-chain-cybersecurity

[7] CrowdStrike (2024) What Is a Supply Chain Attack?. Available at: https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/supply-chain-attack/

[8] CyberSaint (2024) How to Mitigate Cyber Risks in Your Third-Party Supply Chain. Available at: https://www.cybersaint.io/blog/how-to-mitigate-cyber-risks-in-your-third-party-supply-chain

[9] ENISA (2021) Threat Landscape for Supply Chain Attacks. European Union Agency for Cybersecurity. Available at: https://www.enisa.europa.eu

[10] ENISA (2022) Threat Landscape for Supply Chain Attacks. Available at: https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

[11] ENISA (2024) Threat Landscape 2023–2024. European Union Agency for Cybersecurity. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

[12] European Commission (2024) Cybersecurity in the Supply Chain: Key Statistics and Recommendations. Available at: https://ec.europa.eu/newsroom/cipr/items/722520/en

[13] European Union (2022) 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 (NIS2 Directive). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555

[14] EY (2023) How will NIS2 affect the supply chain security approach?. Available at: https://www.ey.com/en_pl/insights/law/nis2-supply-chain-security

[15] FireEye (2020) Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims. Available at: https://www.fireeye.com/blog

[16] InfoSecurity Europe (2024) Supply Chain Attacks Are on the Rise – Here's What You Need to Know. Available at: https://www.infosecurityeurope.com/en-gb/blog/threat-vectors/supply-chain-attacks-cyber-threat.html

[17] Kaspersky Lab (2019) Operation ShadowHammer. Available at: https://secure-list.com/operation-shadowhammer/89992/

[18] MarketWatch (2024) CDK Hack Underscores Vendor Risk. Available at: https://www.marketwatch.com/story/cdk-hack-underscores-vendor-risk-924228b5

[19] National Cyber Security Centre New Zealand (2021) Supply Chain Cyber Security. Available at: https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Supply-Chain-Cyber-Security.pdf

[20] NIST (2024) Best Practices in Cyber Supply Chain Risk Management. Available at: https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf

[21] Risk Ledger (2024) Why Hackers Target Our Corporate Supply Chains. Available at: https://riskledger.com/resources/why-hackers-target-supply-chains

[22] Symantec (2017) What You Need to Know About the Petya/NotPetya Ransomware Outbreak. Available at: https://www.broadcom.com/company/newsroom/press-releases

[23] TechRadar (2025) M&S hack may have been caused by security issues at Indian IT giant Tata Consultancy Services, 8 May. Available at: https://www.techradar.com/pro/security/m-and-s-hack-may-have-been-caused-by-security-issues-at-indian-it-giant-tata-consultancy-services

[24] The Scottish Sun (2025) Marks and Spencer boss reveals store was hit by cyberattack, 5 May. Available at: https://www.thescottishsun.co.uk/money/14846327/marks-and-spencer-boss-cyber-attack/

[25] Zetter, K. (2021) Inside the SolarWinds Hack. Wired. Available at: https://www.wired.com/story/solarwinds-hack-supply-chain/

[26] Greenberg, A. (2018) The Untold Story of NotPetya, the Most Devastating Cyberattack in History. Wired. Available at: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[27] Financial Times (2024) M&S undone by old-fashioned con: how retailer's cyber hell unfolded. Available at: https://www.ft.com/content/19dcd993-877e-43c5-aab4-c727e574e3f2

[28] Andreaviliotti.it (2024) The Landscape of Cybersecurity in the European Union 2024. Available at: https://www.andreaviliotti.it/post/the-landscape-of-cybersecurity-in-the-european-union-2024

[29] NIST, Special Publication 800-161 Rev. 1: Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, 2023. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/final

[30] ISO/IEC, 27036-1:2021 – Information security for supplier relationships – Part 1: Overview and concepts, Geneva, Switzerland: ISO, 2021.

[31] ISO/IEC, 27036-2:2021 – Information security for supplier relationships – Part 2: Requirements, Geneva, Switzerland: ISO, 2021.

[32] ISO/IEC, 27036-3:2013 – Information security for supplier relationships – Part 3: Guidelines for information and communication technology supply chain security, Geneva, Switzerland: ISO, 2013.

[33] ISO/IEC, 27036-4:2016 – Information security for supplier relationships – Part 4: Guidelines for security of cloud services, Geneva, Switzerland: ISO, 2016.

[34] ISO/IEC, 27036 – Information security for supplier relationships – at a glance.

[35] NASA SEWP, Supply Chain Risk Management (SCRM) Framework Crosswalk, 2022. [Online]. Available: https://www.sewp.nasa.gov/documents.shtml

[36] European Commission, “Commission Implementing Regulation (EU) 2024/7151 on Cybersecurity Requirements for Critical Entities and Networks under NIS2,” Official Journal of the European Union, L 295, pp. 10–25, 17 Oct. 2024. Available: https://digital-strategy.ec.europa.eu/en/library/nis2-commission-implementing-regulation-critical-entities-and-networks

[37] S. Quinn, N. Ivy, M. Barrett, G. Witte, and R. Gardner, “NIST Interagency Report (NISTIR) 8286B-upd1: Prioritizing Cybersecurity Risk for Enterprise Risk Management,” Nat. Inst. Stand. Technol., Gaithersburg, MD, USA, Tech. Rep. NISTIR 8286B-upd1, Feb. 2025. [Online]. Available: https://csrc.nist.gov/pubs/ir/8286/b/upd1/final