



ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ – ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Πρόγραμμα Μεταπτυχιακών Σπουδών «Πληροφορική»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	Αξιολόγηση Κινδύνων Ασφάλειας Πληροφοριών και Οργανωτικής Ετοιμότητας Κρίσιμων Υποδομών Πληροφορικής Information Security Risk and Organizational Readiness Assessment of Critical IT Infrastructures
Ονοματεπώνυμο Φοιτητή	Γεώργιος Καπέρδας
Πατρώνυμο	Δημήτριος
Αριθμός Μητρώου	ΜΠΠΛ2413
Επιβλέπουσα	Δέσποινα Πολέμη, Καθηγήτρια

Ημερομηνία Παράδοσης **Σεπτέμβριος 2026**

Τριμελής Εξεταστική Επιτροπή

Δέσποινα Πολέμη
Καθηγήτρια

Κωνσταντίνος Πατσάκης
Καθηγητής

Παναγιώτης Κοτζανικολάου
Καθηγητής

Περίληψη

Η διατριβή αναπτύσσει και εφαρμόζει συστηματική, επαναλήψιμη μέθοδο αξιολόγησης κινδύνων ασφάλειας πληροφοριών και οργανωτικής ετοιμότητας σε συνθετικό, ανωνυμοποιημένο αρχέτυπο δημόσιου ERP (govERP), χωρίς χρήση πραγματικών λειτουργικών ή ευαίσθητων δεδομένων. Η μέθοδος έχει δύο συμπληρωματικά σκέλη: ανάλυση επικινδυνότητας με MONARC, στηριγμένη στα ISO/IEC 27001:2022 και ISO/IEC 27002:2022 και στο Interoperable EU Risk Management Toolbox του ENISA, και αποτίμηση τεκμηριωτικής ετοιμότητας προς αξιολόγηση/πιστοποίηση με CUSTODES. Η NIS2, ο Ν. 5160/2024 και η ΚΥΑ 1689/2025 χρησιμοποιούνται ως πλαίσιο αναφοράς, χωρίς ισχυρισμό νομικής υπαγωγής του αρχέτυπου. Η εφαρμογή παράγει ιχνηλάσιμο μητρώο κινδύνων, ανάλυση αποκλίσεων, αποτίμηση οργανωτικής ετοιμότητας και προσχέδιο Security Target για τη διεπαφή ηλεκτρονικής τιμολόγησης. Οι υψηλότερες προτεραιότητες συγκεντρώνονται κυρίως σε ταυτότητα, πρόσβαση, ανθρώπινες πρακτικές και τεκμηρίωση. Οι δύο άξονες λειτουργούν συμπληρωματικά, χωρίς αριθμητική μετατροπή βαθμολογίας κινδύνου σε επίπεδο διασφάλισης. Η διαδικασία αποδείχθηκε εκτελέσιμη, αναπαραγώγιμη και ιχνηλάσιμη στο συγκεκριμένο αρχέτυπο, ενώ η εξωτερική εγκυρότητα δεν εξετάστηκε. Στη συγκεκριμένη έκδοση και στις συνεδρίες της πλατφόρμας, η συνύπαρξη διαφορετικών καταλόγων απειλών δυσχέρανε την ανάκτηση ορισμένων συναφών στόχων ασφάλειας.

Λέξεις-κλειδιά: ασφάλεια πληροφοριών, αξιολόγηση κινδύνων, οργανωτική ετοιμότητα, ταξινομίες απειλών, υποδομές υψηλής κρίσιμότητας, ISO/IEC 27001, NIS2, MONARC, CUSTODES, ENISA.

Abstract

This MSc thesis develops and applies a systematic, repeatable method for assessing information-security risks and organizational readiness in a synthetic, anonymized public-sector ERP archetype (govERP), without using real operational or sensitive data. The method has two complementary strands: risk assessment with MONARC, grounded in ISO/IEC 27001:2022, ISO/IEC 27002:2022 and ENISA's Interoperable EU Risk Management Toolbox; and an assessment of documentation readiness for conformity assessment and certification using CUSTODES. The NIS2 Directive, Greek Law 5160/2024 and Joint Ministerial Decision 1689/2025 are used as regulatory references, without implying legal applicability to the archetype. The application produces a traceable risk register, a gap analysis, an organizational-readiness assessment and a draft Security Target for the e-invoicing interface. The highest priorities concern identity, access, human practices and documentation. Risk assessment and certification readiness are complementary, but no risk score is converted into an assurance level. The process was executable, reproducible and traceable on the stated archetype; external validity was not tested. In the specific platform version and sessions examined, the coexistence of different threat catalogues made some relevant security objectives harder to retrieve.

Keywords: information security, risk assessment, organizational readiness, threat taxonomies, high-criticality infrastructures, ISO/IEC 27001, NIS2, MONARC, CUSTODES, ENISA.

Πίνακας Περιεχομένων

Περίληψη	3
Abstract.....	3
1. Εισαγωγή.....	15
1.1 Πλαίσιο και σημασία του προβλήματος.....	15
1.2 Κρίσιμες υποδομές πληροφορικής και δημόσια ψηφιακή διοίκηση	15
1.3 Σκοπός και στόχοι της εργασίας.....	16
1.4 Ερευνητικά ερωτήματα	16
1.5 Οριοθέτηση και περιορισμοί της μελέτης	17
1.6 Μεθοδολογική προσέγγιση — συνοπτικά	18
1.7 Διάρθρωση της διατριβής	18
2. Θεωρητικό Υπόβαθρο Ανάλυσης Επικινδυνότητας Ασφάλειας Πληροφοριών: Πρότυπα, Μεθοδολογίες και Εργαλεία Ανοιχτού Κώδικα	19
2.1 Εισαγωγή και οριοθέτηση	19
2.2 Εννοιολογικά θεμέλια.....	19
2.2.1 Ορισμοί	19
2.2.2 Η τριάδα CIA και ο κύκλος διαχείρισης κινδύνων	20
2.2.3 Ποιοτική, ποσοτική και ημι-ποσοτική προσέγγιση.....	20
2.3 Πρότυπα	21
2.3.1 ISO/IEC 27001:2022 και Amd 1:2024	21
2.3.2 ISO/IEC 27002:2022.....	22
2.3.3 ISO/IEC 27005:2022.....	22
2.3.4 ISO/IEC 27017:2015.....	23
2.3.5 Η οικογένεια NIST	23
2.3.6 NIS2, Νόμος 5160/2024 και ΚΥΑ 1689/2025	23
2.3.7 Σύνθεση και πίνακας αντιστοίχισης	24
2.4 Μεθοδολογίες	25
2.4.1 Η διεργασία του ISO/IEC 27005 ως μεθοδολογία	25
2.4.2 Το NIST RMF ως διαδικαστική μεθοδολογία	25
2.4.3 Λοιπές αναγνωρισμένες μεθοδολογίες	25
2.4.4 ENISA Interoperable EU Risk Management Toolbox.....	25
2.4.5 Κριτήρια επιλογής μεθοδολογίας για το αρχέτυπο govERP	25
2.5 Εργαλεία ανοιχτού κώδικα.....	26
2.5.1 Κριτήρια αξιολόγησης	26
2.5.2 MONARC	26
2.5.3 CISO Assistant.....	26
2.5.4 verinice και Eramba	27
2.5.5 Συγκριτικός πίνακας και τεκμηρίωση της MONARC ως κύριου εργαλείου	27
2.6 Οργανωτική ετοιμότητα και ωριμότητα ασφάλειας	27
2.7 Σύνοψη και μετάβαση στο Κεφάλαιο 3.....	28

3. Θεωρητικό Υπόβαθρο Συμμόρφωσης και Προσέγγισης προς Πιστοποίηση	29
3.1 Συμμόρφωση, αξιολόγηση συμμόρφωσης και πιστοποίηση	29
3.2 Διαπίστευση και φορείς αξιολόγησης	29
3.3 Πρότυπα αξιολόγησης ασφάλειας (Common Criteria — ISO/IEC 15408, 18045).....	30
3.4 Πρότυπα της σειράς ISO/IEC 17000 για την αξιολόγηση συμμόρφωσης.....	31
3.5 Ευρωπαϊκό πλαίσιο πιστοποίησης κυβερνοασφάλειας (Cybersecurity Act, EUCC)	31
3.6 Το έργο CUSTODES	32
3.7 Κανονιστικό πλαίσιο αναφοράς (Οδηγία NIS2, Ν. 5160/2024)	33
3.8 Σχέση ανάλυσης επικινδυνότητας και ετοιμότητας προς πιστοποίηση	33
4. Πρακτική Ανάλυση Επικινδυνότητας σε Αρχέτυπο govERP	35
4.1 Ορισμός και οριοθέτηση του αντιπροσωπευτικού αρχετύπου govERP.....	35
4.1.1 Το δημόσιο σημείο αναφοράς: το πρόγραμμα Gov-ERP και το σύστημα ΟΠΣΥΔΔ... 35	
4.1.2 Αρχή αφαίρεσης και μη-επανάταυτοποίησης	35
4.1.3 Ο φορέας του αρχετύπου: αντιπροσωπευτική ΓΔΟΥ σε φάση λειτουργικής ένταξης. 36	
4.1.4 Οριοθέτηση: πυρήνας ανάλυσης, κλάδος ηλεκτρονικής τιμολόγησης, εκτός πεδίου.. 36	
4.1.5 Συστατικά στοιχεία του αρχετύπου και τεκμηρίωση πηγών	37
4.2 Εργαστηριακό περιβάλλον και εγκατάσταση του MONARC	39
4.2.1 Επιλογή περιβάλλοντος εκτέλεσης	39
4.2.2 Εγκατάσταση, επαλήθευση και θωράκιση	39
4.2.3 Αναπαραγωγιμότητα, φορητότητα και κύκλος ζωής.....	40
4.3 Μεθοδολογική βάση: μεθοδολογία CUSTODES και ENISA toolbox	40
4.3.1 Το ISO/IEC 27005:2022 ως πρότυπο-πλαίσιο	40
4.3.2 Η μέθοδος και το εργαλείο MONARC	40
4.3.3 Εναρμόνιση με το οικοσύστημα ENISA	40
4.3.4 Η μεθοδολογική συγγένεια με το CUSTODES και η γέφυρα προς το Κεφάλαιο 5	40
4.4 Μοντελοποίηση περιουσιακών στοιχείων και εξαρτήσεων	41
4.4.1 Από τα συστατικά του αρχετύπου στα αντικείμενα του εργαλείου	41
4.4.2 Πρωτεύοντα αγαθά και αποτίμηση επιπτώσεων	42
4.4.3 Υποστηρικτικά αγαθά, δέντρο εξαρτήσεων και πρώτη επανάληψη αναγνώρισης.....	44
4.5 Αναγνώριση απειλών και ευπαθειών: εσκεμμένες, τυχαίες και περιβαλλοντικές απειλές . 45	
4.5.1 Το τοπίο απειλών της πρώτης επανάληψης και η τριμερής τυπολογία	45
4.5.2 Ευθυγράμμιση με το ENISA Threat Landscape 2025 και πιθανοφάνειες απειλών	46
4.5.3 Έλεγχος πληρότητας: το κενό άρνησης υπηρεσίας και ο στοχευμένος εμπλουτισμός	47
4.5.4 Ευπάθειες: κάλυψη της βάσης γνώσης και παράδοση στην αποτίμηση	48
4.6 Υπολογισμός και αποτίμηση επιπέδων κινδύνου σε τεχνικό, λειτουργικό και θεσμικό επίπεδο.....	48
4.6.1 Βαθμονόμηση ευπαθειών: η παραδοχή ωριμότητας.....	49
4.6.2 Υπολογισμός, επαλήθευση και συνολική εικόνα	49
4.6.3 Τριεπίπεδη αποτίμηση: τεχνικό, λειτουργικό και θεσμικό επίπεδο.....	53
4.7 Αντιστοίχιση μέτρων κατά ISO/IEC 27002:2022	54

4.7.1 Το πλαίσιο αναφοράς και ο μηχανισμός αντιστοίχισης	55
4.7.2 Η εικόνα της χαρτογράφησης	55
4.7.3 Χειροκίνητη αντιστοίχιση του εμπλουτισμού.....	56
4.7.4 Ιεράρχηση της αντιμετώπισης και παράδοση στην ανάλυση αποκλίσεων	56
4.8 Ανάλυση αποκλίσεων έναντι του ISO/IEC 27001	57
4.8.1 Μεθοδολογική βάση και μέσο αποτύπωσης.....	57
4.8.2 Οι απαιτήσεις του συστήματος διαχείρισης (ρήτρες 4–10).....	57
4.8.3 Οι δικλίδες του Παραρτήματος Α και η οριστική εικόνα χαρτογράφησης	57
4.8.4 Η εθνική όψη: το πλαίσιο απαιτήσεων της ΚΥΑ 1689/2025	58
4.9 Εκτίμηση οργανωτικής ετοιμότητας και ωριμότητας	58
4.9.1 Από τα κελιά του μητρώου στην οργανωτική ανάγνωση.....	58
4.9.2 Το ανθρωποκεντρικό εύρημα και οι δικλίδες της κατηγορίας «Άνθρωποι»	58
4.9.3 Τρεις διαστάσεις ετοιμότητας και η ωριμότητα της φάσης ένταξης	58
4.9.4 Σύνοψη κεφαλαίου και παράδοση στον άξονα πιστοποίησης	59
5. Πρακτική Προσέγγιση προς Πιστοποίηση με CUSTODES.....	60
5.1 Η πλατφόρμα CUSTODES και το περιβάλλον εργασίας	60
5.1.1 Το έργο και η προσέγγισή του	60
5.1.2 Επίπεδο του εγχειρήματος και οργάνωση της εργασίας	60
5.1.3 Το περιβάλλον εργασίας της πλατφόρμας	60
5.2 Ορισμός υποσυστήματος ως αντικείμενου αξιολόγησης	62
5.2.1 Από το ευρύ πεδίο της ανάλυσης στον στόχο αξιολόγησης.....	62
5.2.2 Το όριο του στόχου αξιολόγησης: εντός, εκτός και διεπαφές.....	62
5.2.3 Περιουσιακά στοιχεία και ιδιότητες προς προστασία.....	62
5.2.4 Το προφίλ κινδύνου-εισόδου από το Κεφάλαιο 4	63
5.3 Στόχοι και απαιτήσεις ασφάλειας	64
5.3.1 Ορισμός του προβλήματος ασφάλειας	64
5.3.2 Στόχοι ασφάλειας για τον στόχο αξιολόγησης και το περιβάλλον	66
5.3.3 Λειτουργικές απαιτήσεις ασφάλειας.....	68
5.3.4 Απαιτήσεις διασφάλισης και όριο ετοιμότητας.....	69
5.4 Μέτρα, αποδεικτικά στοιχεία και προφίλ προστασίας.....	69
5.4.1 Από τις απαιτήσεις στα μέτρα: η αντιστοίχιση προς το ISO/IEC 27002:2022.....	69
5.4.2 Μητρώο αποδεικτικών στοιχείων ετοιμότητας	70
5.4.3 Προφίλ προστασίας και προσχέδιο στόχου ασφάλειας.....	71
5.5 Ενδεικτικό workflow προσέγγισης προς πιστοποίηση	72
5.5.1 Η λογική του workflow	72
5.5.2 Η αποτύπωση στην πλατφόρμα του έργου	72
5.6 Συγκριτική αποτίμηση των δύο προσεγγίσεων και των εργαλείων	74
5.6.1 Δύο ερωτήματα, δύο παραδείγματα — μία σχέση παραλληλίας.....	74
5.6.2 Η συμπληρωματικότητα στην πράξη: τι έδωσε ο ένας άξονας στον άλλον	74
5.6.3 Τα εργαλεία: MONARC και πλατφόρμα CUSTODES	74
6. Συμπεράσματα	77
Αξιολόγηση Κινδύνων Ασφάλειας Πληροφοριών και Οργανωτικής Ετοιμότητας Κρίσιμων Υποδομών Πληροφορικής	6

6.1 Απαντήσεις στα ερευνητικά ερωτήματα	77
6.2 Κύρια ευρήματα και συνεισφορά της εργασίας	78
6.3 Περιορισμοί της μελέτης	79
6.4 Προτάσεις για μελλοντική έρευνα	80
6.4.1 Ενσωμάτωση της κλιματικής διάστασης στην αξιολόγηση ετοιμότητας	80
6.4.2 Διερεύνηση των ευρύτερων μακροοικονομικών και θεσμικών επιπτώσεων περιστατικών σε πληροφοριακά συστήματα της δημόσιας διοίκησης	81
6.4.3 Προσαρμοστική και αυτοματοποιημένη απόκριση σε εξελισσόμενες και μη προβλέψιμες απειλές	81
Βιβλιογραφία	82
Παράρτημα Α' — Αναλογική μετάφραση των κλιμάκων συνεπειών ROLFP σε δημόσιο πλαίσιο	87
Παράρτημα Β' — Συγκεντρωτικές αποτιμήσεις επιπτώσεων των πέντε πρωτευόντων αγαθών	88
Παράρτημα Γ' — Πλήρες μητρώο των 90 μοναδικών αξιολογήσεων κινδύνου	89
Παράρτημα Δ' — Τεκμήρια αναπαραγωγιμότητας και αρχεία τεκμηρίωσης	97
Παράρτημα Ε' — Ηλεκτρονικό παράρτημα: υπολογιστικό φύλλο ανάλυσης αποκλίσεων	98
Παράρτημα ΣΤ' — Προσχέδιο Στόχου Ασφάλειας (Security Target) για τη διεπαφή ηλεκτρονικής τιμολόγησης και εκκαθάρισης του αρχετύπου govERP	99
ST.1 Εισαγωγή του στόχου ασφάλειας	99
ST.1.1 Αναφορά του στόχου ασφάλειας	99
ST.1.2 Αναφορά του στόχου αξιολόγησης	99
ST.1.3 Επισκόπηση του στόχου αξιολόγησης	99
ST.1.4 Περιγραφή του στόχου αξιολόγησης	99
ST.2 Δηλώσεις συμμόρφωσης	100
ST.3 Ορισμός του προβλήματος ασφάλειας	100
ST.3.1 Απειλές	100
ST.3.2 Παραδοχές για το περιβάλλον λειτουργίας	101
ST.3.3 Οργανωσιακές πολιτικές ασφάλειας	102
ST.4 Στόχοι ασφάλειας	102
ST.4.1 Στόχοι για τον στόχο αξιολόγησης	102
ST.4.2 Στόχοι για το περιβάλλον λειτουργίας	102
ST.4.3 Τεκμηρίωση στόχων (rationale)	103
ST.5 Απαιτήσεις ασφάλειας	103
ST.5.1 Λειτουργικές απαιτήσεις (SFR) — επίπεδο οικογένειας	103
ST.5.2 Απαιτήσεις διασφάλισης (SAR) — διαθεσιμότητα υλικού	104
ST.5.3 Τεκμηρίωση απαιτήσεων (rationale)	104
ST.6 Συνοπτική προδιαγραφή του στόχου αξιολόγησης	104
ST.7 Ιχνηλασιμότητα προσχεδίου	105

Κατάλογος Εικόνων

Εικόνα 4.1. Επαλήθευση έκδοσης MONARC 2.13.4 (οθόνη About) επί του τελικού μοντέλου των 90 μοναδικών κινδύνων (05/07/2026)· η αντίστοιχη λήψη της ημέρας εγκατάστασης (04/07) περιλαμβάνεται στα τεκμήρια του Παραρτήματος Δ΄.....	39
Εικόνα 4.2. Οθόνη αποτίμησης επιπτώσεων (Edit impacts) του πρωτεύοντος αγαθού P1 — οι καταχωρισμένες τιμές ταυτίζονται κελί προς κελί με τον Πίνακα 4.8.....	43
Εικόνα 4.3. Ο διάλογος δημιουργίας ειδικού κινδύνου («+ Create a specific risk») με τα δύο υποχρεωτικά πεδία επιλογής από τους καθολικούς καταλόγους της βάσης γνώσης — στο στιγμιότυπο, η δημιουργία της προσθήκης E2: απειλή MDA18 (Data from untrustworthy sources) και ευπάθεια 978 (ασφαλής αυθεντικοποίηση αποστολέα)· τεκμήριο της διαδικασίας εμπλουτισμού της §4.5.3....	47
Εικόνα 4.4. Απόσπασμα-άγκυρα του μητρώου κινδύνων σε φθίνουσα κατάταξη (προβολή «1–90 of 90»)· το πλήρες μητρώο των 90 μοναδικών αξιολογήσεων παρατίθεται ως Πίνακας Γ΄.1, ενώ η πλήρης σειρά των έξι στιγμιότυπων στα τεκμήρια του Παραρτήματος Δ΄.	50
Εικόνα 4.5. Το μοναδικό κελί της αποδεκτής (πράσινης) ζώνης — αντίγραφα ασφαλείας υπό το P4, απειλή κλοπής/καταστροφής μέσων, μέγιστος κίνδυνος 8, ακριβώς στο κατώφλι αποδοχής. Πάνω: η κεφαλίδα της όψης P4 («27 information risks»)· κάτω: το τέλος της φθίνουσας κατάταξης με το πράσινο κελί.....	51
Εικόνα 4.6. Το ίδιο καθολικό αντικείμενο N1 (κανάλι ΚΕΔ/PEPPOL) υπό το P3a (πάνω — A=36, μη αποδεκτή ζώνη) και υπό το P3b (κάτω — A=24) — οπτικό τεκμήριο της ανά-γονέα κληρονόμησης επιπτώσεων επί κοινών T/V.....	52
Εικόνα 4.7. Οι όψεις των υποστηρικτικών αγαθών S3 — λογισμικό διεπαφής e-invoicing (πάνω) και S2 — ΣΔΒΔ (κάτω), με τις γραμμές των εμπλουτισμών σε πλάγια σήμανση ειδικού κινδύνου: E2 επί του S3 (I=36) και E3 επί των S3/S2 (I=24) — §4.5.3, λήψεις 05/07/2026.	53
Εικόνα 4.8. Το φύλλο κινδύνου (Risk sheet) γραμμής του συμπλέγματος 64 (Employees / Forging of rights) με ορατή την προ-αντιστοίχιση μέτρων του ISO/IEC 27002:2022 (5.17, 6.3) — οπτική γέφυρα προς την §4.7.....	54
Εικόνα 5.1. Το μοντέλο οντοτήτων της πλατφόρμας και τα τέσσερα δομικά στοιχεία που καταχωρίστηκαν.	61

Εικόνα 5.2. Η αλυσίδα ιχνηλασιμότητας από την επίπτωση του Κεφαλαίου 4 έως την αποτύπωση στην πλατφόρμα.	70
Εικόνα 5.3. Οι δύο οντολογίες σε αντιπαραβολή: το ίδιο λεξιλόγιο, διαφορετική οργάνωση.	75

Κατάλογος Πινάκων

Πίνακας 2.1. Βασικοί όροι της ανάλυσης επικινδυνότητας.	20
Πίνακας 2.2. Ενδεικτική ερμηνευτική αντιστοίχιση φάσεων διαχείρισης κινδύνου με επιλεγμένα πρότυπα και πλαίσια.	24
Πίνακας 2.3. Ενδεικτική συγκριτική αποτίμηση εργαλείων ανάλυσης κινδύνου και GRC.	27
Πίνακας 4.1. Τα οκτώ συστατικά στοιχεία του αρχετύπου gonERP και η συνοπτική περιγραφή τους.	37
Πίνακας 4.2. Θεμελίωση κάθε συστατικού του αρχετύπου σε δημόσια πηγή· με Δ σημαίνονται όσα στηρίζονται σε γενική πρακτική συστημάτων ERP και όχι σε σύστημα-ειδική αναφορά.	37
Πίνακας 4.3. Ασφαλείς πηγές του αρχετύπου και η χρήση τους.	38
Πίνακας 4.4. Πηγές που αποκλείονται από τη συγκρότηση του αρχετύπου.	38
Πίνακας 4.5. Αντιστοίχιση των σταδίων του ISO/IEC 27005:2022, των φάσεων του MONARC και των ενοτήτων του κεφαλαίου.	41
Πίνακας 4.6. Από τα συστατικά της §4.1.5 στα αντικείμενα του MONARC: πρωτεύοντα και υποστηρικτικά αγαθά.	42
Πίνακας 4.7. Τα πέντε πρωτεύοντα αγαθά (P1, P2, P3a, P3b, P4) και οι αποτιμήσεις επιπτώσεων C/I/A.	43
Πίνακας 4.8. Αναλυτική αποτίμηση επιπτώσεων του πρωτεύοντος αγαθού P1 κατά τις κλίμακες ROLFP, με τη μέγιστη τιμή ανά κριτήριο.	43
Πίνακας 4.9. Προσαρτήσεις υποστηρικτικών αγαθών ανά πρωτεύον και αριθμός κινδύνων κάθε υποδέντρου στην πρώτη επανάληψη.	44
Πίνακας 4.10. Οι δεκατρείς απειλές της πρώτης επανάληψης, με προέλευση, τοποθετήσεις, τιμή πιθανοφάνειας T και άγκυρα τεκμηρίωσης έναντι του ENISA Threat Landscape 2025.	46
Πίνακας 4.11. Οι τρεις γραμμές εμπλουτισμού E1–E3: απειλή, ευπάθεια, τοποθέτηση και τεκμηρίωση.	48
Πίνακας 4.12. Οι τρεις βαθμίδες βαθμονόμησης ευπαθειών Q-Θ, Q-T και Q-Λ, με το πεδίο εφαρμογής και το σκεπτικό τους.	49
Πίνακας 4.13. Τα δέκα συχνότερα μέτρα του ISO/IEC 27002:2022 στη χαρτογράφηση, με τη θεματική τους και τον αριθμό γραμμών του μητρώου.	55

Πίνακας 4.14. Χειροκίνητη αντιστοίχιση των γραμμών εμπλουτισμού σε μέτρα του ISO/IEC 27002:2022, με το σκεπτικό επιλογής.	56
Πίνακας 4.15. Κάλυψη των τεσσάρων κατηγοριών μέτρων του Παραρτήματος Α του ISO/IEC 27001:2022 από τη χαρτογράφηση. ...	57
Πίνακας 5.1. Περιουσιακά στοιχεία του στόχου αξιολόγησης και αντιστοιχία με το μοντέλο MONARC του Κεφαλαίου 4.	63
Πίνακας 5.2. Το ποσοτικοποιημένο προφίλ κινδύνου του κλάδου της διεπαφής, όπως αποτιμήθηκε στην §4.6 (τιμές επαληθευμένες προγραμματιστικά επί της εξαγωγής του εργαλείου). Σημειώνεται για πληρότητα ότι οι E1 και E3 εκτείνονται και πέραν του ορίου του στόχου αξιολόγησης: το E1 πλήττει με A = 36 και το κανάλι διαλειτουργικότητας N2 υπό τη ροή εκκαθάρισης (P1), ενώ το E3 διαχέεται με I = 24 και μέσω της βάσης δεδομένων (S2) — υποστηρικτικού αγαθού του περιβάλλοντος λειτουργίας — στα P2, P3b και P4.	64
Πίνακας 5.3. Απειλές κατά του στόχου αξιολόγησης και θεμελίωσή τους στην ανάλυση του Κεφαλαίου 4.	65
Πίνακας 5.4. Παραδοχές για το περιβάλλον λειτουργίας του στόχου αξιολόγησης.	66
Πίνακας 5.5. Οργανωσιακές πολιτικές ασφάλειας που δεσμεύουν τον στόχο αξιολόγησης.	66
Πίνακας 5.6. Στόχοι ασφάλειας για τον στόχο αξιολόγησης και για το περιβάλλον λειτουργίας του.	67
Πίνακας 5.7. Λειτουργικές απαιτήσεις ασφάλειας σε επίπεδο οικογένειας και αντιστοίχιση στους στόχους.	68
Πίνακας 5.8. Οι κλάσεις διασφάλισης και το διαθέσιμο υλικό.	69
Πίνακας 5.9. Αντιστοίχιση στόχων/απαιτήσεων του στόχου αξιολόγησης προς μέτρα του ISO/IEC 27002:2022 και σημεία συνάντησης με την αντιστοίχιση του Κεφαλαίου 4.	70
Πίνακας 5.10. Μητρώο αποδεικτικών στοιχείων ετοιμότητας.	71
Πίνακας 5.11. Τα οκτώ βήματα της προσέγγισης προς πιστοποίηση.	72
Πίνακας 5.12. Τα δομικά στοιχεία που καταχωρίστηκαν στην πλατφόρμα και η αντιστοιχία τους με τον Πίνακα 5.1.	73
Πίνακας 5.13. Οι επτά λειτουργικές απαιτήσεις που παρήγαγε η πλατφόρμα και τα ζεύγη αποτίμησης ανά απαίτηση.	73
Πίνακας 5.14. Αντιπαραβολή των δύο εργαλείων κατά τις διαστάσεις της §5.6.3.	75

Πίνακας Α΄.1. Αναλογική μετάφραση των κλιμάκων συνεπειών ROLFP της βάσης γνώσης MONARC σε δημόσιο πλαίσιο.....	87
Πίνακας Β΄.1. Συγκεντρωτικές αποτιμήσεις C//A των πέντε πρωτευόντων αγαθών και η κύρια αγκύρωση της μέγιστης τιμής.	88
Πίνακας Γ΄.1. Πλήρες μητρώο των 90 μοναδικών αξιολογήσεων κινδύνου, από την εξαγωγή CSV v2 της 05/07/2026.....	89
Πίνακας Δ΄.1. Τεκμήρια αναπαραγωγιμότητας και αρχεία τεκμηρίωσης του μοντέλου.	97
Πίνακας ΣΤ΄.1. Στοιχεία αναφοράς του προσχεδίου Στόχου Ασφάλειας.	99
Πίνακας ΣΤ΄.2. Στοιχεία αναφοράς του στόχου αξιολόγησης.	99
Πίνακας ΣΤ΄.3. Δηλώσεις συμμόρφωσης του προσχεδίου προς τα Common Criteria, προς προφίλ προστασίας και προς πακέτο διασφάλισης.	100
Πίνακας ΣΤ΄.4. Απειλές κατά του στόχου αξιολόγησης — αναπαραγωγή του Πίνακα 5.3.	100
Πίνακας ΣΤ΄.5. Παραδοχές για το περιβάλλον λειτουργίας — αναπαραγωγή του Πίνακα 5.4.	101
Πίνακας ΣΤ΄.6. Οργανωσιακές πολιτικές ασφάλειας — αναπαραγωγή του Πίνακα 5.5.....	102
Πίνακας ΣΤ΄.7. Στόχοι ασφάλειας για τον στόχο αξιολόγησης — το σκέλος Ο.* του Πίνακα 5.6.....	102
Πίνακας ΣΤ΄.8. Στόχοι ασφάλειας για το περιβάλλον λειτουργίας — το σκέλος ΟΕ.* του Πίνακα 5.6, με τις παραδοχές που καλύπτει καθένας.	102
Πίνακας ΣΤ΄.9. Τεκμηρίωση στόχων: αντιστοίχιση κάθε απειλής, παραδοχής και πολιτικής του ορισμού του προβλήματος ασφάλειας προς τους στόχους που την καλύπτουν.	103
Πίνακας ΣΤ΄.10. Λειτουργικές απαιτήσεις ασφάλειας ανά οικογένεια και ο στόχος που υπηρετεί καθεμία — συνοπτική προβολή του Πίνακα 5.7 σε δύο στήλες.	103
Πίνακας ΣΤ΄.11. Απαιτήσεις διασφάλισης και διαθέσιμο υλικό ανά κλάση — αναπαραγωγή του Πίνακα 5.8.	104
Πίνακας ΣΤ΄.12. Συνοπτική προδιαγραφή: ποιο λειτουργικό στοιχείο του στόχου αξιολόγησης υλοποιεί κατά κύριο λόγο κάθε οικογένεια απαιτήσεων.	105

Πίνακας ΣΤ΄.13. Ιχνηλασιμότητα του προσχεδίου: κάθε τμήμα του Στόχου Ασφάλειας προς την πηγή του στο Κεφάλαιο 5 και την άγκυρά του στο Κεφάλαιο 4.....	105
--	-----

Συντομεύσεις

ANSSI	Agence nationale de la sécurité des systèmes d'information
AVA_VAN	Οικογένεια ανάλυσης ευπαθειών της κλάσης AVA (ISO/IEC 15408-3)
B2G	Business-to-Government — τιμολόγηση προς φορείς του Δημοσίου
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
CRA	Cyber Resilience Act — Κανονισμός (ΕΕ) 2024/2847
CSF	Cybersecurity Framework (NIST)
CUSTODES	CUStomizable and Trustable cOntinuous assurance and certification methoDology for composiTE systemS — πλατφόρμα ετοιμότητας πιστοποίησης
EAL	Evaluation Assurance Level — επίπεδο διασφάλισης αξιολόγησης
ENISA	European Union Agency for Cybersecurity — Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια
ERP	Enterprise Resource Planning — σύστημα διαχείρισης επιχειρησιακών πόρων
EUCC	European Common Criteria-based Cybersecurity Certification Scheme
FAU	Κλάση λειτουργικών απαιτήσεων ελέγχου ασφάλειας (Security Audit)
GRC	Governance, Risk and Compliance
HRM	Human-Centric Risk Management
IAM	Identity and Access Management — διαχείριση ταυτότητας και πρόσβασης
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
ITSEF	Information Technology Security Evaluation Facility — εργαστήριο αξιολόγησης
MEHARI	Méthode Harmonisée d'Analyse de Risques
MITIGATE	Multidimensional, IntegraTEd, risk assessment framework and dynamic, collaborative Risk ManaGement tools for critical information infrastructures
MONARC	Method for an Optimised aNALysis of Risks — Μέθοδος Βελτιστοποιημένης Ανάλυσης Κινδύνων
NIS2	Οδηγία (ΕΕ) 2022/2555 για υψηλό κοινό επίπεδο κυβερνοασφάλειας
NIST	National Institute of Standards and Technology
OLIR	Online Informative References (NIST)
PEPPOL	Pan-European Public Procurement On-Line — δίκτυο δρομολόγησης παραστατικών
PP	Protection Profile — προφίλ προστασίας
RMF	Risk Management Framework (NIST SP 800-37 Rev. 2)
SAR	Security Assurance Requirements — απαιτήσεις διασφάλισης ασφάλειας
SFR	Security Functional Requirements — λειτουργικές απαιτήσεις ασφάλειας
SOG-IS	Senior Officials Group Information Systems Security
ST	Security Target — στόχος ασφάλειας
STRIDE	Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege
ToE	Target of Evaluation — στόχος αξιολόγησης
TVRA	Threat, Vulnerability, Risk Analysis
ΓΔΟΥ	Γενική Διεύθυνση Οικονομικών Υπηρεσιών
ΚΕΔ	Κέντρο Διαλειτουργικότητας
ΚΥΑ	Κοινή Υπουργική Απόφαση
ΟΠΣΥΔΔ	Ολοκληρωμένο Πληροφοριακό Σύστημα Δημοσιονομικής Διαχείρισης
ΣΔΒΔ	Σύστημα Διαχείρισης Βάσεων Δεδομένων
ΤΠΕ	Τεχνολογίες Πληροφορικής και Επικοινωνιών
ΥΑΣΠΕ	Υπεύθυνος Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών
ΦΕΚ	Φύλλο Εφημερίδας της Κυβερνήσεως

Σημείωση ανάγνωσης: οι αριθμοί των βιβλιογραφικών παραπομπών είναι ενεργοί σύνδεσμοι προς τις αντίστοιχες εγγραφές. Για επιστροφή στο σημείο ανάγνωσης: Alt με αριστερό βέλος στο Acrobat, ή Μετάβαση → Πίσω στην Προεπισκόπηση.

1. Εισαγωγή

1.1 Πλαίσιο και σημασία του προβλήματος

Ο ψηφιακός μετασχηματισμός της δημόσιας διοίκησης έχει καταστήσει τα πληροφοριακά συστήματα σημαντικό πυλώνα της κρατικής λειτουργίας και της παροχής δημόσιων υπηρεσιών [1]. Συστήματα που υποστηρίζουν την οικονομική διαχείριση, τις προμήθειες και τις διοικητικές διαδικασίες — όπως τα ολοκληρωμένα συστήματα διαχείρισης επιχειρησιακών πόρων (Enterprise Resource Planning, ERP) — μπορούν, ανάλογα με τον ρόλο τους και τις επιπτώσεις πιθανής διακοπής τους, να αντιμετωπιστούν λειτουργικά ως υποδομές υψηλής κρίσιμότητας ΤΠΕ. Η διαθεσιμότητα, η ακεραιότητα και η εμπιστευτικότητα των πληροφοριών και υπηρεσιών που διαχειρίζονται επηρεάζουν τη συνέχεια και την αξιοπιστία των σχετικών δημόσιων λειτουργιών, έννοιες που συνδέονται άμεσα με τη λογική των Συστημάτων Διαχείρισης Ασφάλειας Πληροφοριών (Information Security Management System, ISMS) [2], [3].

Παράλληλα, το τοπίο των κυβερνοαπειλών έχει οδηγήσει σε αυστηρότερο ευρωπαϊκό και εθνικό κανονιστικό πλαίσιο. Η Οδηγία (ΕΕ) 2022/2555 (NIS2) προβλέπει ότι οι βασικές και σημαντικές οντότητες λαμβάνουν κατάλληλα και αναλογικά τεχνικά, επιχειρησιακά και οργανωτικά μέτρα για τη διαχείριση κινδύνων κυβερνοασφάλειας [4]. Η ενσωμάτωσή της στο ελληνικό δίκαιο με τον Ν. 5160/2024 εισάγει αντίστοιχα μέτρα και υποχρεώσεις σε εθνικό επίπεδο [5]. Σε εφαρμογή της παρ. 2 του άρθρου 15 του Ν. 5160/2024, η ΚΥΑ 1689/2025 «Εθνικό Πλαίσιο Απαιτήσεων Κυβερνοασφάλειας Βασικών και Σημαντικών Οντοτήτων» εξειδικεύει τα μέτρα διαχείρισης κινδύνων σε είκοσι δύο απαιτήσεις [6]. Για την παρούσα εργασία, οι πηγές αυτές αξιοποιούνται ως πλαίσιο αναφοράς για την ανάγκη συστηματικής αξιολόγησης κινδύνων και οργανωτικής ετοιμότητας, χωρίς να τεκμηριώνεται νομική υπαγωγή συγκεκριμένου πραγματικού συστήματος.

1.2 Κρίσιμες υποδομές πληροφορικής και δημόσια ψηφιακή διοίκηση

Για τους σκοπούς της παρούσας εργασίας, και χωρίς να αποδίδεται τυπικός νομικός χαρακτηρισμός σε συγκεκριμένο σύστημα, ως κρίσιμη ή υψηλής κρίσιμότητας υποδομή πληροφορικής νοείται ένα πληροφοριακό σύστημα του οποίου η διακοπή, αλλοίωση ή μη διαθεσιμότητα θα μπορούσε να έχει σημαντικές επιπτώσεις σε ουσιώδεις δημόσιες, κοινωνικές ή οικονομικές λειτουργίες. Η λειτουργική αυτή θεώρηση είναι συμβατή με την ευρωπαϊκή έμφαση στην ανθεκτικότητα κρίσιμων οντοτήτων και στην αξιολόγηση των επιπτώσεων περιστατικών στην παροχή βασικών υπηρεσιών [7].

Τα τελευταία χρόνια, ο ψηφιακός μετασχηματισμός της ελληνικής δημόσιας διοίκησης έχει μεταβάλει τον τρόπο με τον οποίο το κράτος παρέχει υπηρεσίες και διαχειρίζεται εσωτερικές λειτουργίες. Η Βίβλος Ψηφιακού Μετασχηματισμού 2020–2025 αποτυπώνει παρεμβάσεις σε τεχνολογικές υποδομές του κράτους και στον τρόπο αξιοποίησης της ψηφιακής τεχνολογίας στους τομείς της οικονομίας και της δημόσιας διοίκησης [1]. Στο πλαίσιο αυτό, ιδιαίτερη σημασία έχουν συστήματα που δεν απευθύνονται κατ' ανάγκη άμεσα στον πολίτη, αλλά υποστηρίζουν θεμελιώδεις εσωτερικές λειτουργίες, όπως η δημοσιονομική διαχείριση, οι δημόσιες προμήθειες και η οικονομική πληροφόρηση.

Το έργο Gov-ERP, με πλήρη τίτλο «Μεταρρύθμιση του Δημοσιονομικού Συστήματος στην Κεντρική Διοίκηση και τη λοιπή Γενική Κυβέρνηση», τεκμηριώνεται από επίσημες πηγές ως έργο του Ταμείου Ανάκαμψης και Ανθεκτικότητας «Ελλάδα 2.0» [8], [9]. Σύμφωνα με τη σελίδα του έργου στο Greece 2.0, αντικείμενό του είναι η αναμόρφωση και βελτίωση του συστήματος χρηματοοικονομικής και δημοσιονομικής διαχείρισης του Δημοσίου, με έμφαση, μεταξύ άλλων, στην ενοποίηση πληροφοριακών συστημάτων, τη βελτίωση της διαφάνειας, της λογοδοσίας και της χρηματοοικονομικής πληροφόρησης [9]. Επιπλέον, νεότερη πράξη τροποποίησης της απόφασης ένταξης του έργου τεκμηριώνει τη συνέχιση της θεσμικής του αποτύπωσης στο πλαίσιο του Ταμείου Ανάκαμψης [10].

Το πραγματικό Gov-ERP χρησιμοποιείται μόνο ως δημόσιο σημείο αναφοράς. Η πρακτική ανάλυση αφορά το συνθετικό, ανωνυμοποιημένο αρχέτυπο govERP. Η σύμβαση γραφής είναι σταθερή: «Gov-ERP» για το πραγματικό έργο και «govERP» για το αρχέτυπο. Έτσι εξετάζονται

κίνδυνοι και οργανωτική ετοιμότητα χωρίς αποκάλυψη πραγματικής αρχιτεκτονικής, δεδομένων, ευπαθειών ή στοιχείων ασφάλειας φορέα.

1.3 Σκοπός και στόχοι της εργασίας

Σκοπός της εργασίας είναι ο σχεδιασμός, η εφαρμογή και η αξιολόγηση μιας συστηματικής και επαναλήψιμης μεθόδου αξιολόγησης κινδύνων ασφάλειας πληροφοριών για μια αντιπροσωπευτική υποδομή υψηλής κρισιμότητας ΤΠΕ της δημόσιας διοίκησης, καθώς και της οργανωτικής ετοιμότητας του αντιπροσωπευτικού οργανωτικού πλαισίου που τη λειτουργεί. Η μεθοδολογία θεμελιώνεται στα πρότυπα ISO/IEC 27001:2022, το οποίο ορίζει απαιτήσεις για ISMS [2], και ISO/IEC 27002:2022, το οποίο παρέχει καθοδήγηση για δικλίδες ασφάλειας πληροφοριών (information security controls) [3], με το ISO/IEC 27005:2022 ως ειδικό πρότυπο-πλαίσιο καθοδήγησης για τη διαχείριση κινδύνων ασφάλειας πληροφοριών [11]. Μεθοδολογικά υποστηρίζεται από το Interoperable EU Risk Management Toolbox (εργαλειοθήκη διαλειτουργικής διαχείρισης κινδύνων) του ENISA [12], από το MONARC ως εργαλείο/μέθοδο επαναλήψιμης αξιολόγησης κινδύνου [13], και από την προσέγγιση CUSTODES για τεκμηριωτική ετοιμότητα προς αξιολόγηση/πιστοποίηση σύνθετων συστημάτων ΤΠΕ [14], [15]. Το σκέλος της ετοιμότητας προς πιστοποίηση τοποθετείται στο ευρύτερο πλαίσιο της αξιολόγησης συμμόρφωσης και των προτύπων αξιολόγησης ασφάλειας (Common Criteria/ISO/IEC 15408 [16], ISO/IEC 18045 [17] και σειρά ISO/IEC 17000 [18], συμπεριλαμβανομένων των ISO/IEC 17025 και ISO/IEC 17065), τα οποία αναπτύσσονται θεωρητικά στο Κεφάλαιο 3, ενώ η αποτίμηση της οργανωτικής ετοιμότητας συναρτάται και προς τις απαιτήσεις διαχείρισης κινδύνου της NIS2, του Ν. 5160/2024 και της ΚΥΑ 1689/2025 [6]. Ως προς τις εκδόσεις των προτύπων αξιολόγησης, η εργασία αγκυρώνεται συνειδητά στα ISO/IEC 15408:2022 και ISO/IEC 18045:2022, στα οποία θεμελιώνεται κανονιστικά το ευρωπαϊκό σχήμα EUCC - οι αναθεωρημένες εκδόσεις του 2026 μνημονεύονται και αιτιολογούνται στο Κεφάλαιο 3.

Επιμέρους στόχοι της εργασίας είναι οι ακόλουθοι:

- Αποσαφήνιση του θεωρητικού και κανονιστικού υποβάθρου της διαχείρισης κινδύνου και της αξιολόγησης συμμόρφωσης.
- Εκτέλεση στοχευμένης και οριοθετημένης ανάλυσης επικινδυνότητας σε αντιπροσωπευτικό αρχέτυπο govERP, με το εργαλείο MONARC, αξιοποιώντας το toolbox του ENISA.
- Ανάλυση αποκλίσεων έναντι του ISO/IEC 27001, σε αντιστοίχιση με τις απαιτήσεις διαχείρισης κινδύνου της NIS2, του Ν. 5160/2024 και της ΚΥΑ 1689/2025, και εκτίμηση της οργανωτικής ετοιμότητας και ωριμότητας του αντιπροσωπευτικού οργανωτικού πλαισίου λειτουργίας του αρχέτυπου.
- Υλοποίηση πρακτικής προσέγγισης τεκμηριωτικής ετοιμότητας προς αξιολόγηση/πιστοποίηση με την πλατφόρμα CUSTODES.
- Συγκριτική αποτίμηση των χρησιμοποιούμενων εργαλείων και πλατφορμών υποστήριξης της ανάλυσης κινδύνου και της προσέγγισης προς πιστοποίηση.

Το επιδιωκόμενο αποτέλεσμα είναι μια τεκμηριωμένη και επαναλήψιμη προσέγγιση που συνδέει την τεχνική ανάλυση κινδύνου με την οργανωτική και τεκμηριωτική ετοιμότητα προς αξιολόγηση/πιστοποίηση.

1.4 Ερευνητικά ερωτήματα

Η διατριβή οργανώνεται γύρω από ένα κεντρικό και τέσσερα επιμέρους ερευνητικά ερωτήματα:

Πώς μπορεί ένα πληροφοριακό σύστημα ΤΠΕ υψηλής κρισιμότητας της δημόσιας διοίκησης, όπως ένα δημόσιο ERP, να αξιολογηθεί συστηματικά και επαναλήψιμα ως προς τους κινδύνους ασφάλειας πληροφοριών, και πώς μπορεί να αποτιμηθεί η οργανωτική ετοιμότητα του αντιπροσωπευτικού οργανωτικού πλαισίου που το λειτουργεί, με την Οδηγία NIS2, τον Ν. 5160/2024 και την ΚΥΑ 1689/2025 ως κανονιστικό πλαίσιο αναφοράς, χωρίς να τεκμαίρεται νομική υπαγωγή του αρχέτυπου;

Τα επιμέρους ερωτήματα είναι:

- **EE1:** Ποιοι είναι οι κύριοι κίνδυνοι ασφάλειας πληροφοριών ενός αντιπροσωπευτικού αρχετύπου δημόσιου ERP, και πώς αναγνωρίζονται και αξιολογούνται συστηματικά με βάση διεθνή πρότυπα και το Interoperable EU Risk Management Toolbox του ENISA, μέσω του εργαλείου MONARC;
- **EE2:** Πώς μπορεί μια δομημένη ανάλυση αποκλίσεων έναντι του ISO/IEC 27001:2022 — με την Οδηγία NIS2, τον Ν. 5160/2024 και την ΚΥΑ 1689/2025 ως συμπληρωματικό πλαίσιο αναφοράς — να αξιοποιηθεί για την αποτίμηση της οργανωτικής ετοιμότητας και ωριμότητας του αντιπροσωπευτικού οργανωτικού πλαισίου λειτουργίας του αρχετύπου, και ποιες κατηγορίες παρεμβάσεων βελτίωσης υποδεικνύει;
- **EE3:** Πώς μπορεί να αποτιμηθεί η συμμορφωσιακή και τεκμηριωτική ετοιμότητα ενός οριοθετημένου υποσυστήματος υψηλής κρίσιμότητας του αρχετύπου προς αξιολόγηση/πιστοποίηση μέσω της πλατφόρμας CUSTODES, σε σχέση με τα Common Criteria/ISO/IEC 15408, το ISO/IEC 18045, το ευρωπαϊκό σχήμα EUCC και τα συναφή πρότυπα αξιολόγησης συμμόρφωσης ISO/IEC 17025 και ISO/IEC 17065;
- **EE4:** Σε ποιον βαθμό η ανάλυση επικινδυνότητας (MONARC) και η προσέγγιση τεκμηριωτικής ετοιμότητας προς πιστοποίηση (CUSTODES) λειτουργούν συμπληρωματικά για μια ολιστική αποτίμηση της ασφάλειας, και ποια είναι τα μεθοδολογικά τους πλεονεκτήματα και όρια;

Τα EE1–EE2 θεμελιώνονται στο Κεφάλαιο 2 και απαντώνται στο Κεφάλαιο 4. Το EE3 θεμελιώνεται στο Κεφάλαιο 3 και απαντάται στο Κεφάλαιο 5, ενώ το EE4 συντίθεται στα Κεφάλαια 5 και 6.

1.5 Οριοθέτηση και περιορισμοί της μελέτης

Η παρούσα διατριβή οριοθετείται από ορισμένες συνειδητές μεθοδολογικές επιλογές, η σημαντικότερη εκ των οποίων αφορά το ίδιο το αντικείμενο της μελέτης. Η ανάλυση δεν εφαρμόζεται σε ένα πραγματικό, εν λειτουργία πληροφοριακό σύστημα, αλλά σε ένα αντιπροσωπευτικό και ανωνυμοποιημένο αρχέτυπο δημόσιου συστήματος ERP. Η επιλογή αυτή αποτελεί μεθοδολογική και δεοντολογική απόφαση.

Ο πρώτος λόγος είναι δεοντολογικός. Ένα πραγματικό σύστημα ERP που υποστηρίζει κρίσιμες λειτουργίες της δημόσιας διοίκησης μπορεί να αποτελεί ευαίσθητη υποδομή. Η εκπόνηση και δημοσίευση λεπτομερούς ανάλυσης κινδύνων, ευπαθειών ή τεχνικών εξαρτήσεων ενός αναγνωρίσιμου τέτοιου συστήματος θα μπορούσε να αυξήσει τον κίνδυνο έκθεσης. Με την εργασία σε ανωνυμοποιημένο αρχέτυπο επιτρέπεται επιστημονική ανάλυση χωρίς αποκάλυψη στοιχείων που αφορούν την ασφάλεια συγκεκριμένου φορέα.

Ο δεύτερος λόγος είναι πρακτικός. Οι δημόσια διαθέσιμες πηγές για το πραγματικό Gov-ERP τεκμηριώνουν το αντικείμενο και τη θεσμική ένταξη του έργου, αλλά δεν παρέχουν δημόσια τεχνικά και λειτουργικά δεδομένα επαρκή για ασφαλή εμπειρική ανάλυση πραγματικής παραγωγικής εγκατάστασης [9], [10]. Η κατασκευή ενός αρχετύπου, βασισμένου σε δημόσιες πηγές, τεκμηριωμένες παραδοχές και διεθνή πρότυπα, καθιστά δυνατή μια αυστηρή και επαναλήψιμη ανάλυση χωρίς εξάρτηση από μη διαθέσιμα ή ευαίσθητα δεδομένα.

Η εργασία είναι μεθοδολογική εφαρμογή και όχι έλεγχος, δοκιμή διείσδυσης, επίσημο audit ή πιστοποίηση φορέα. Δείχνει ότι η διαδικασία εκτελείται και αναπαράγεται στο συγκεκριμένο αρχέτυπο· δεν αποδεικνύει εξωτερική εγκυρότητα ή μεταφερσιμότητα. Η σύνδεση κινδύνου και στόχου ασφάλειας επιδεικνύεται μία φορά και χρειάζεται μελλοντική επανάληψη σε άλλα περιβάλλοντα.

Επιπλέον περιορισμοί προκύπτουν από τα ίδια τα εργαλεία. Στο πρακτικό σκέλος της προσέγγισης προς πιστοποίηση, η διαθέσιμη λειτουργικότητα της πλατφόρμας CUSTODES, όπως αξιοποιείται στην εργασία, χρησιμοποιείται για να καταδείξει μια ροή εργασίας (workflow) βασισμένη σε τεκμήρια, στόχους ασφάλειας, απαιτήσεις ασφάλειας, δικλίδες και αποδεικτικά στοιχεία [15]. Δεν συνιστά εξαντλητική αξιολόγηση ασφάλειας ούτε τελική πιστοποίηση πραγματικού συστήματος. Αντίστοιχα, η ανάλυση επικινδυνότητας με MONARC στηρίζεται στις παραδοχές που ορίζουν το αρχέτυπο· οι παραδοχές αυτές δηλώνονται ρητά ώστε τα αποτελέσματα να είναι ερμηνεύσιμα και επαναλήψιμα.

Οι εκδόσεις, το καθεστώς ισχύος και ο ρόλος κάθε προτύπου τεκμηριώνονται στα αντίστοιχα θεωρητικά κεφάλαια με επίσημες πηγές και, όπου είναι διαθέσιμο και επιτρεπτό, με το αδειοδοτημένο κείμενο του προτύπου. Για τα Common Criteria και το EUCC αξιοποιούνται επιπλέον οι δημόσιες επίσημες πηγές του αντίστοιχου σχήματος και της Ευρωπαϊκής Ένωσης.

1.6 Μεθοδολογική προσέγγιση — συνοπτικά

Σε μεθοδολογικό επίπεδο, η εργασία υιοθετεί τη στρατηγική της μελέτης περίπτωσης και εκτυλίσσεται σε πέντε διαδοχικά βήματα, τα οποία αναπτύσσονται αναλυτικά στα επόμενα κεφάλαια. Πρώτον, καθορίζονται το αντικείμενο, οι στόχοι και τα όρια της μελέτης. Δεύτερον, συγκεντρώνονται και μελετώνται οι πηγές: διεθνή πρότυπα, κανονιστικό πλαίσιο, εκθέσεις και εργαλεία του ENISA, η τεκμηρίωση του MONARC και η διαθέσιμη τεκμηρίωση του έργου CUSTODES. Τρίτον, ορίζεται και μοντελοποιείται το αντιπροσωπευτικό αρχέτυπο govERP σε ελεγχόμενο περιβάλλον ανάλυσης, με δομικά στοιχεία αντλημένα αποκλειστικά από δημόσια διαθέσιμες και τεκμηριωμένες πηγές. Τέταρτον, εκτελείται η πρακτική ανάλυση: ανάλυση επικινδυνότητας με MONARC και, στη συνέχεια, προσέγγιση τεκμηριωτικής ετοιμότητας προς πιστοποίηση με την πλατφόρμα CUSTODES. Πέμπτον, τα δύο σκέλη και τα αντίστοιχα εργαλεία αποτιμώνται συγκριτικά, ώστε να αναδειχθούν τα μεθοδολογικά τους πλεονεκτήματα και όρια. Η ίδια η διαδικασία αξιολογείται με πέντε ρητά κριτήρια: αν εκτελείται σε πραγματικό εργαστηριακό περιβάλλον· αν τα βήματά της επαναλαμβάνονται από τις ίδιες τεκμηριωμένες εισόδους και δηλωμένες παραδοχές, αναπαράγοντας τα ίδια αριθμητικά αποτελέσματα· και αν κάθε αριθμητική τιμή και κρίσιμη αναλυτική επιλογή ανάγονται στην προέλευσή τους. Τα δύο τελευταία αφορούν την εσωτερική συνέπεια των παραγόμενων τεκμηρίων και την ανθεκτικότητα της βασικής θεματικής ιεράρχησης όταν μεταβάλλεται η κύρια παραδοχή βαθμονόμησης. Τα κριτήρια αφορούν την ποιότητα και την ευρωστία της συγκεκριμένης εφαρμογής· δεν συνιστούν έλεγχο εξωτερικής εγκυρότητας ή μεταφερσιμότητας, οι οποίες δεν εξετάζονται εμπειρικά (§1.5). Η αναλυτική θεμελίωση, οι κλίμακες και οι παραδοχές κάθε βήματος παρουσιάζονται στα Κεφάλαια 2 έως 5.

1.7 Διάρθρωση της διατριβής

Η διατριβή διατηρεί την εγκεκριμένη δομή έξι κεφαλαίων και δύο συμπληρωματικούς άξονες: θεωρία και εφαρμογή της ανάλυσης κινδύνου, και θεωρία και εφαρμογή της ετοιμότητας προς αξιολόγηση/πιστοποίηση.

Το Κεφάλαιο 2 παρουσιάζει τις έννοιες, τα πρότυπα, τις μεθοδολογίες και τα εργαλεία της διαχείρισης κινδύνου, με επιλογή του MONARC. Το Κεφάλαιο 3 καλύπτει αξιολόγηση συμμόρφωσης, Common Criteria/ISO/IEC 15408, ISO/IEC 18045, τη σειρά ISO/IEC 17000 [16]–[18], το Cybersecurity Act και το EUCC [19], [20], καθώς και τις μεθοδολογικές γέφυρες προς CUSTODES. Η ΚΥΑ 1689/2025 διατηρείται ως εθνικό πλαίσιο αναφοράς [6]. Μη δημόσιο υλικό του έργου δεν αναπαράγεται.

Το Κεφάλαιο 4 ορίζει το govERP, εκτελεί την ανάλυση με MONARC, αντιστοιχίζει δικλίδες και αποτιμά αποκλίσεις και οργανωτική ετοιμότητα. Το Κεφάλαιο 5 εστιάζει στη διεπαφή ηλεκτρονικής τιμολόγησης/εκκαθάρισης και εξετάζει την τεκμηριωτική της ετοιμότητα με CUSTODES, χωρίς αξίωση πιστοποίησης.

Τέλος, το έκτο κεφάλαιο συνοψίζει τα κύρια ευρήματα, απαντά στα ερευνητικά ερωτήματα, καταγράφει τους περιορισμούς της μελέτης και διατυπώνει προτάσεις για μελλοντική έρευνα. Ακολουθούν η βιβλιογραφία και τα παραρτήματα.

2. Θεωρητικό Υπόβαθρο Ανάλυσης Επικινδυνότητας Ασφάλειας Πληροφοριών: Πρότυπα, Μεθοδολογίες και Εργαλεία Ανοιχτού Κώδικα

2.1 Εισαγωγή και οριοθέτηση

Το παρόν κεφάλαιο πραγματεύεται την ανάλυση επικινδυνότητας ασφάλειας πληροφοριών ως οργανωμένη διεργασία εκτίμησης και αντιμετώπισης κινδύνων. Στο πλαίσιο της εργασίας, ο όρος περιλαμβάνει την αναγνώριση αγαθών, απειλών και ευπαθειών, την ανάλυση συνέπειας και πιθανοφάνειας, την αξιολόγηση των επιπέδων κινδύνου έναντι προκαθορισμένων κριτηρίων, καθώς και τη σύνδεση των κινδύνων με κατάλληλες δικλίδες ασφάλειας.

Ο τίτλος «Ανάλυση Επικινδυνότητας» χρησιμοποιείται με ευρεία έννοια: καλύπτει την αναγνώριση, ανάλυση, αξιολόγηση και αντιμετώπιση κινδύνων, σύμφωνα με ISO/IEC 27005:2022 και ISO 31000:2018 [11], [21].

Το Κεφάλαιο 2 απαντά στο «πώς αναγνωρίζεται και αντιμετωπίζεται ο κίνδυνος». Η αξιολόγηση συμμόρφωσης, η πιστοποίηση, η διαπίστευση, τα ISO/IEC 15408 και 18045, η σειρά ISO/IEC 17000, το EUCC και το CUSTODES εξετάζονται στο Κεφάλαιο 3.

Ως προς την ορολογία, υιοθετούνται συνεπείς αποδόσεις σε όλο το κεφάλαιο. Ο όρος «control» αποδίδεται ως «δικλίδα ασφάλειας πληροφοριών (information security control)» στην πρώτη χρήση και εν συνεχεία ως «δικλίδα». Σημειώνεται ότι η ελληνική έκδοση του προτύπου από τον ΕΛΟΤ αποδίδει τον ίδιο όρο ως «έλεγχο προστασίας πληροφοριών»: η παρούσα εργασία διατηρεί την απόδοση «δικλίδα», ώστε ο όρος να διακρίνεται από τα κανονιστικά μέτρα του ν. 5160/2024 και της ΚΥΑ 1689/2025 και να μην ταυτίζεται λεκτικά με το «μέτρο» του ίδιου του ορισμού της ρήτρας 3.1.8. Ο όρος «risk register» αποδίδεται ως «μητρώο κινδύνων». Προτιμάται ο όρος «συνέπεια (consequence)» έναντι του όρου «επίπτωση (impact)», σε ευθυγράμμιση με το ISO 31000 και το ISO/IEC 27005:2022. Το χαρακτηριστικό «Security domains» αποδίδεται ως «πεδία ασφάλειας».

2.2 Εννοιολογικά θεμέλια

2.2.1 Ορισμοί

Η εννοιολογική βάση της ανάλυσης επικινδυνότητας αντλείται από το λεξιλόγιο της οικογένειας προτύπων ISO/IEC 27000, το ISO/IEC 27005:2022 [11], το ISO 31000:2018 [21] και το ISO 31073:2022 (Risk management — Vocabulary), το οποίο αντικατέστησε τον ISO Guide 73:2009 [22]. Σύμφωνα με το ISO 31000:2018, ο κίνδυνος (risk) ορίζεται ως «το αποτέλεσμα της αβεβαιότητας επί των στόχων» (the effect of uncertainty on objectives), αποτέλεσμα που μπορεί να είναι θετικό, αρνητικό ή και τα δύο. Η διαχείριση κινδύνων (risk management) ορίζεται ως οι συντονισμένες δραστηριότητες με τις οποίες ο οργανισμός κατευθύνεται και ελέγχεται ως προς τον κίνδυνο.

Στο ISO 31073:2022 η «συνέπεια (consequence)» ορίζεται ως το αποτέλεσμα ενός συμβάντος που επηρεάζει τους στόχους, ενώ η «πιθανοφάνεια (likelihood)» αποτυπώνει τη δυνατότητα επέλευσης. Η εκτίμηση κινδύνου (risk assessment) συγκροτείται από την αναγνώριση (risk identification), την ανάλυση (risk analysis) και την αξιολόγηση (risk evaluation) του κινδύνου. Η αντιμετώπιση κινδύνου (risk treatment) είναι η διεργασία επιλογής και υλοποίησης επιλογών τροποποίησης του κινδύνου.

Στο ειδικότερο πλαίσιο της ασφάλειας πληροφοριών, ως αγαθό νοείται οτιδήποτε έχει αξία για τον οργανισμό [3] — και, ως εκ τούτου, χρήζει προστασίας. Τα αγαθά μπορούν να είναι πρωτεύοντα, όπως πληροφορίες και επιχειρησιακές διεργασίες, ή υποστηρικτικά, όπως λογισμικό, υλισμικό, δίκτυα, προσωπικό, εγκαταστάσεις και οργανωτική δομή. Η απειλή αποτελεί δυνητική αιτία ανεπιθύμητου συμβάντος, ενώ η ευπάθεια είναι αδυναμία αγαθού ή δικλίδας που μπορεί να αξιοποιηθεί από μία ή περισσότερες απειλές. Οι έννοιες αυτές είναι κρίσιμες για την παρούσα εργασία, διότι η πρακτική ανάλυση του Κεφαλαίου 4 θα στηριχθεί στη μοντελοποίηση αγαθών, απειλών, ευπαθειών, συνεπειών και πιθανοφάνειας.

Πίνακας 2.1. Βασικοί όροι της ανάλυσης επικινδυνότητας.

Όρος	Ορισμός (κατά το πρότυπο)	Ρόλος στην εργασία
Αγαθό (asset)	Οποδήποτε έχει αξία για τον οργανισμό (ISO/IEC 27002:2022, 3.1.2).	Στοιχείο που χρήζει προστασίας· αντικείμενο μοντελοποίησης στο MONARC και στο αρχέτυπο govERP (Κεφ. 4).
Πρωτεύον / υποστηρικτικό αγαθό	Πρωτεύοντα: πληροφορίες και επιχειρησιακές διεργασίες· υποστηρικτικά: λογισμικό, υλισμικό, δίκτυα, προσωπικό, εγκαταστάσεις (ISO/IEC 27002:2022, 3.1.2, Σημ. 1· καθοδήγηση 5.9).	Ιεραρχική δομή αγαθών στο MONARC.
Απειλή (threat)	Δυνητική αιτία ανεπιθύμητου συμβάντος που μπορεί να βλάψει σύστημα ή οργανισμό.	Αναγνώριση απειλών στην ανάλυση του Κεφ. 4.
Ευπάθεια (vulnerability)	Αδυναμία αγαθού ή δικλίδας που μπορεί να αξιοποιηθεί από απειλή.	Αναγνώριση ευπαθειών στην ανάλυση του Κεφ. 4.
Ιδιοκτήτης κινδύνου (risk owner)	Πρόσωπο ή οντότητα στο οποίο έχουν ανατεθεί η ευθύνη και η εξουσία για τη διαχείριση συγκεκριμένου κινδύνου (ISO 31000:2018 και ISO 31073:2022 [21], [22]).	Αρμόδιος έγκρισης σχεδίου αντιμετώπισης και αποδοχής υπολειπόμενου κινδύνου.
Μητρώο κινδύνων (risk register)	Τεκμηριωμένο σύνολο αναγνωρισμένων κινδύνων με τα χαρακτηριστικά τους (πηγή, συνέπεια, πιθανοφάνεια, επίπεδο, ιδιοκτήτης, αντιμετώπιση).	Παράγεται στο πρακτικό μέρος (Κεφ. 4).
Δήλωση Εφαρμοσιμότητας (SoA)	Τεκμηριωμένο αποτέλεσμα που δηλώνει, ανά δικλίδα, ένταξη/εξαίρεση με αιτιολόγηση και κατάσταση υλοποίησης (ISO/IEC 27001:2022, 6.1.3).	Αναλυτικό τεκμήριο τεκμηρίωσης, όχι πιστοποιητική δήλωση.

Στο ειδικότερο λεξιλόγιο της ασφάλειας πληροφοριών, η «δικλίδα ασφάλειας πληροφοριών (information security control)» ορίζεται στο ISO/IEC 27002:2022 (ρήτρα 3.1.8) ως «μέτρο που διατηρεί ή/και τροποποιεί τον κίνδυνο» (measure that maintains and/or modifies risk) [3]. Ο ορισμός αυτός είναι ουσιώδης· όπως επεξηγεί η Εισαγωγή του προτύπου (ρήτρα 0.3), μια πολιτική ασφάλειας μπορεί μόνο να διατηρεί τον κίνδυνο, ενώ η συμμόρφωση προς αυτήν μπορεί να τον τροποποιεί [3]. Ο «υπολειπόμενος κίνδυνος (residual risk)» είναι ο κίνδυνος που απομένει μετά την αντιμετώπιση, και το ISO/IEC 27005:2022 σημειώνει ότι μπορεί να περιλαμβάνει και μη αναγνωρισμένο κίνδυνο [11].

2.2.2 Η τριάδα CIA και ο κύκλος διαχείρισης κινδύνων

Η θεμελιώδης τριάδα της ασφάλειας πληροφοριών συγκροτείται από την εμπιστευτικότητα (confidentiality), την ακεραιότητα (integrity) και τη διαθεσιμότητα (availability) — την τριάδα CIA. Η αναγνώριση και αξιολόγηση κινδύνων διενεργείται σε σχέση με τις τρεις αυτές ιδιότητες των αγαθών πληροφορίας. Ο κύκλος διαχείρισης κινδύνων δεν είναι εφάπαξ έργο αλλά συνεχής, επαναληπτική διεργασία: καθιέρωση πλαισίου, εκτίμηση, αντιμετώπιση, αποδοχή υπολειπόμενου κινδύνου, καθώς και διαρκής επικοινωνία και διαβούλευση, παρακολούθηση και επανεξέταση, σε ευθυγράμμιση με το μοντέλο PDCA.

2.2.3 Ποιοτική, ποσοτική και ημι-ποσοτική προσέγγιση

Η ανάλυση κινδύνων μπορεί να είναι ποιοτική (qualitative), ποσοτική (quantitative) ή ημι-ποσοτική (semi-quantitative). Η ποιοτική προσέγγιση χρησιμοποιεί περιγραφικές κλίμακες (π.χ. χαμηλό/μεσαίο/υψηλό) και είναι ταχεία και κατανοητή, αλλά ευάλωτη σε υποκειμενικότητα. Η ποσοτική προσέγγιση αποδίδει αριθμητικές, συνήθως νομισματικές τιμές σε συνέπειες και πιθανοφάνειες, προσφέροντας ακρίβεια αλλά απαιτώντας αξιόπιστα δεδομένα που σπανίως είναι

διαθέσιμα στο πεδίο της κυβερνοασφάλειας. Η ημι-ποσοτική προσέγγιση συνδυάζει αριθμητικές κλίμακες με ποιοτικές κρίσεις, επιτρέποντας συγκρισιμότητα και ιεράρχηση χωρίς την απαίτηση πλήρων ποσοτικών δεδομένων.

Για το συνθετικό αρχέτυπο govERP — αρχέτυπο δημόσιου συστήματος ERP υψηλής κρισιμότητας — επιλέγεται η ημι-ποσοτική προσέγγιση. Η επιλογή τεκμηριώνεται από τρεις παράγοντες. Πρώτος είναι η έλλειψη επαρκών ιστορικών ποσοτικών δεδομένων για αξιόπιστη πλήρως ποσοτική ανάλυση. Δεύτερος, η ανάγκη για συγκρίσιμα και επαναλήψιμα αποτελέσματα μεταξύ διαφορετικών αγαθών και διεργασιών, την οποία η αμιγώς ποιοτική προσέγγιση δεν εξασφαλίζει. Τρίτος, η συμβατότητα με το MONARC: αν και αυτοχαρακτηρίζεται ως ποιοτική μέθοδος, υπολογίζει τον κίνδυνο επί διακριτών αριθμητικών κλιμάκων συνέπειας, απειλής και ευπάθειας, επιτρέποντας ημι-ποσοτική αξιοποίηση (βλ. §2.5.2).

2.3 Πρότυπα

2.3.1 ISO/IEC 27001:2022 και Amd 1:2024

Το ISO/IEC 27001:2022 ορίζει τις απαιτήσεις για ένα Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ/ISMS) και τοποθετεί τη διαχείριση κινδύνων στον πυρήνα του [2]. Οι ουσιαστικές απαιτήσεις διαχείρισης κινδύνων εντοπίζονται στις ρήτρες 6.1.2 (εκτίμηση κινδύνων) και 6.1.3 (αντιμετώπιση κινδύνων).

Η ρήτρα 6.1.2 απαιτεί από τον οργανισμό να καθιερώσει και να διατηρεί κριτήρια κινδύνου ασφάλειας πληροφοριών που περιλαμβάνουν, ως δύο διακριτά στοιχεία (ρήτρα 6.1.2 α): τα κριτήρια αποδοχής κινδύνου (the risk acceptance criteria) και τα κριτήρια για τη διενέργεια εκτιμήσεων κινδύνου ασφάλειας πληροφοριών (criteria for performing information security risk assessments). Η διάκριση αυτή είναι ρητή στο κανονιστικό κείμενο. Επιπλέον, η διεργασία πρέπει να παράγει συνεπή, έγκυρα και συγκρίσιμα αποτελέσματα, να αναγνωρίζει τους κινδύνους που συνδέονται με την απώλεια εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας, να προσδιορίζει τους ιδιοκτήτες κινδύνου, και να αναλύει και αξιολογεί τους κινδύνους έναντι των κριτηρίων.

Η ρήτρα 6.1.3 ορίζει ότι ο οργανισμός καθορίζει και εφαρμόζει διεργασία αντιμετώπισης κινδύνου ασφάλειας πληροφοριών, η οποία περιλαμβάνει έξι σκέλη (α έως στ):

- (α) επιλογή κατάλληλων επιλογών αντιμετώπισης κινδύνου, λαμβάνοντας υπόψη τα αποτελέσματα της εκτίμησης κινδύνων·
- (β) προσδιορισμό όλων των δικλίδων που είναι αναγκαίες για την υλοποίηση των επιλεγμένων επιλογών αντιμετώπισης· το πρότυπο σημειώνει ότι οι οργανισμοί μπορούν να σχεδιάζουν δικλίδες όπως απαιτείται ή να τις αναγνωρίζουν από οποιαδήποτε πηγή·
- (γ) σύγκριση των δικλίδων που προσδιορίστηκαν με εκείνες του Παραρτήματος Α και επαλήθευση ότι δεν έχει παραλειφθεί καμία αναγκαία δικλίδα·
- (δ) σύνταξη Δήλωσης Εφαρμοσιμότητας (Statement of Applicability — SoA) που περιέχει τις αναγκαίες δικλίδες, την αιτιολόγηση συμπερίληψής τους, την κατάσταση υλοποίησής τους και την αιτιολόγηση τυχόν εξαιρέσεων δικλίδων του Παραρτήματος Α·
- (ε) διαμόρφωση σχεδίου αντιμετώπισης κινδύνου ασφάλειας πληροφοριών (risk treatment plan)· και
- (στ) λήψη της έγκρισης των ιδιοκτητών κινδύνου επί του σχεδίου αντιμετώπισης και της αποδοχής των υπολειπόμενων κινδύνων ασφάλειας πληροφοριών.

Το Παράρτημα Α του ISO/IEC 27001:2022 είναι κανονιστικό (normative) και παραθέτει το σύνολο των 93 δικλίδων αναφοράς, σε αντιστοιχία με το ISO/IEC 27002:2022. Η σύγκριση των επιλεγμένων δικλίδων με το Παράρτημα Α λειτουργεί ως μηχανισμός επαλήθευσης πληρότητας, και όχι ως αφετηρία επιλογής δικλίδων: η επιλογή είναι καθοδηγούμενη από τον κίνδυνο (risk-driven), όχι από κατάλογο. Στην παρούσα εργασία, η Δήλωση Εφαρμοσιμότητας αντιμετωπίζεται ως αναλυτικό τεκμήριο τεκμηρίωσης των αποφάσεων αντιμετώπισης κινδύνου, και όχι ως τεκμήριο πιστοποίησης — η διάσταση της πιστοποίησης εξετάζεται στο Κεφάλαιο 3.

Η Τροποποίηση ISO/IEC 27001:2022/Amd 1:2024 (Climate action changes) επιφέρει ακριβώς δύο αλλαγές κειμένου: μία προσθήκη στη ρήτρα 4.1 («Ο οργανισμός θα προσδιορίσει εάν η κλιματική αλλαγή αποτελεί σχετικό ζήτημα») και μία σημείωση στη ρήτρα 4.2 ότι τα ενδιαφερόμενα μέρη μπορούν να έχουν απαιτήσεις σχετιζόμενες με την κλιματική αλλαγή [23]. Η τροποποίηση

δεν προσθέτει νέες δικλίδες και δεν μεταβάλλει τις ρήτρες 5 έως 10. Για την ανάλυση επικινδυνότητας, η σημασία της έγκειται στο ότι η κλιματική αλλαγή πρέπει πλέον να εξετάζεται ρητά ως ζήτημα του πλαισίου, με συνέπειες κυρίως στη διαθεσιμότητα.

2.3.2 ISO/IEC 27002:2022

Το ISO/IEC 27002:2022 (τρίτη έκδοση) αντικαθιστά το ISO/IEC 27002:2013 και παρέχει καθοδήγηση για τις δικλίδες που αντιστοιχούν στο κανονιστικό Παράρτημα Α του ISO/IEC 27001:2022 [3]. Περιλαμβάνει 93 δικλίδες, οργανωμένες σε τέσσερα θέματα (themes): 37 Οργανωτικές (Organizational), 8 Ανθρώπινες (People), 14 Φυσικές (Physical) και 34 Τεχνολογικές (Technological). Η αναδιάρθρωση αυτή αντικατέστησε τους δεκατέσσερις τομείς ελέγχου της έκδοσης 2013.

Καθεμία δικλίδα συνοδεύεται από πέντε χαρακτηριστικά (attributes), τα οποία επιτρέπουν διαφορετικές «όψεις» του συνόλου των δικλίδων: Τύπος δικλίδας (Control type — προληπτική/ανιχνευτική/διορθωτική)· Ιδιότητες ασφάλειας πληροφοριών (Information security properties — εμπιστευτικότητα/ακεραιότητα/διαθεσιμότητα)· Έννοιες κυβερνοασφάλειας (Cybersecurity concepts)· Επιχειρησιακές ικανότητες (Operational capabilities)· και Πεδία ασφάλειας (Security domains). Η διάταξη κάθε δικλίδας ακολουθεί έξι στοιχεία: τίτλο δικλίδας, πίνακα χαρακτηριστικών, τη δικλίδα (Control), τον σκοπό (Purpose), την καθοδήγηση (Guidance) και λοιπές πληροφορίες (Other information).

Ως προς το χαρακτηριστικό «Έννοιες κυβερνοασφάλειας», το ISO/IEC 27002:2022 αντιστοιχίζει κάθε δικλίδα στις πέντε έννοιες του ISO/IEC TS 27110 — Identify, Protect, Detect, Respond, Recover — οι οποίες αντιστοιχούν εννοιολογικά στις βασικές λειτουργίες του NIST CSF [24]. Το κείμενο του ISO/IEC 27002:2022 αποδίδει τις πέντε αυτές έννοιες στο ISO/IEC TS 27110, και όχι απευθείας στο NIST CSF· επιπλέον, ενώ το NIST CSF 2.0 διαθέτει έξι λειτουργίες (με την προσθήκη της Govern), το χαρακτηριστικό που βασίζεται στο ISO/IEC TS 27110 αντανάκλα μόνο τις πέντε προαναφερθείσες έννοιες.

Σύμφωνα με τη ρήτρα 0.2 του ISO/IEC 27002:2022, οι απαιτήσεις ασφάλειας πληροφοριών προέρχονται από τρεις πηγές: την εκτίμηση κινδύνων του οργανισμού· τις νομικές, κανονιστικές και συμβατικές απαιτήσεις· και τις αρχές, τους στόχους και τις επιχειρησιακές ανάγκες του οργανισμού. Στο παρόν κεφάλαιο, οι νομικές απαιτήσεις λαμβάνονται υπόψη αποκλειστικά ως μία από τις τρεις αυτές πηγές απαιτήσεων ασφάλειας πληροφοριών, και όχι ως αντικείμενο ανάλυσης συμμόρφωσης, η οποία θα ενέπιπτε στο πεδίο του Κεφαλαίου 3.

Στο πλαίσιο της παρούσας εργασίας, το ISO/IEC 27002:2022 δεν χρησιμοποιείται ως μηχανιστική checklist συμμόρφωσης, αλλά ως ρεπερτόριο δικλίδων καθοδηγούμενο από τον κίνδυνο: οι δικλίδες επιλέγονται για να αντιμετωπίσουν αναγνωρισμένους κινδύνους και συνδέονται με αυτούς μέσω του μητρώου κινδύνων. Ενδεικτικές δικλίδες με ιδιαίτερη σημασία για το αρχέτυπο govERP είναι η 5.9 (Απογραφή πληροφοριών και άλλων συνδεδεμένων αγαθών), η 5.23 (Ασφάλεια πληροφοριών για τη χρήση υπηρεσιών νέφους), η 8.9 (Διαχείριση διαμόρφωσης), η 8.26 (Απαιτήσεις ασφάλειας εφαρμογών) και οι 5.29/5.30 (Ασφάλεια πληροφοριών κατά τη διατάραξη / ετοιμότητα ΤΠΕ για επιχειρησιακή συνέχεια).

2.3.3 ISO/IEC 27005:2022

Το ISO/IEC 27005:2022 (τέταρτη έκδοση, Οκτώβριος 2022) αντικαθιστά το ISO/IEC 27005:2018 και αποτελεί το ειδικό πρότυπο καθοδήγησης της οικογένειας ISO/IEC 27000 για τη διαχείριση κινδύνων ασφάλειας πληροφοριών [11]. Είναι ευθυγραμμισμένο με το ISO/IEC 27001:2022 και τις γενικές αρχές του ISO 31000:2018, και υποστηρίζει την εκπλήρωση των απαιτήσεων των ρητρών 6.1, 8.2 και 8.3 του ISO/IEC 27001. Ενώ το ISO/IEC 27001 ορίζει «τι» πρέπει να επιτύχει η διεργασία, το ISO/IEC 27005 παρέχει αναλυτικότερη καθοδήγηση για το «πώς» σε επίπεδο διεργασίας — δομή, κριτήρια, σενάρια και επιλογές αντιμετώπισης — χωρίς να επιβάλλει μία μοναδική τεχνική, κλίμακα ή μέθοδο υλοποίησης. Δεν πρέπει, ωστόσο, να παρουσιάζεται ως το αποκλειστικό πρότυπο διαχείρισης κινδύνων: στο ίδιο κεφάλαιο αξιοποιούνται συμπληρωματικά και άλλα πλαίσια (NIST, ENISA) και μεθοδολογίες (EBIOS RM, OCTAVE, MEHARI, MONARC).

Η διεργασία του ISO/IEC 27005:2022 συγκροτείται από πέντε στάδια: καθιέρωση πλαισίου (context establishment), αναγνώριση κινδύνων, ανάλυση κινδύνων, αξιολόγηση κινδύνων και

αντιμετώπιση κινδύνων, με παράλληλες δραστηριότητες επικοινωνίας/διαβούλευσης και παρακολούθησης/επανεξέτασης. Η έκδοση του 2022 συμπύκνωσε τη δομή της προηγούμενης έκδοσης, εισήγαγε την έννοια του σεναρίου κινδύνου (risk scenario) και τη διάκριση μεταξύ προσέγγισης αναγνώρισης βασισμένης σε συμβάντα (event-based) και βασισμένης σε αγαθά (asset-based). Επίσης ενσωμάτωσε ρητή αναφορά στη Δήλωση Εφαρμοσιμότητας, ενισχύοντας τη σύνδεση με τα ISO/IEC 27001 και ISO/IEC 27002.

Σημαντική αλλαγή είναι η αναδιάταξη της αποδοχής κινδύνου: η αυτοτελής ρήτρα αποδοχής κινδύνου της έκδοσης 2018 καταργήθηκε, και το πρότυπο τοποθετεί πλέον την αποδοχή του υπολειπόμενου κινδύνου ως διακριτό σημείο απόφασης μετά την αντιμετώπιση. Η έκδοση 2022 τονίζει την ευθύνη των ιδιοκτητών κινδύνου στη δημιουργία και έγκριση του σχεδίου αντιμετώπισης και στην αποδοχή των υπολειπόμενων κινδύνων, και ενίσχυσε την καθοδήγηση τεκμηρίωσης για τις διεργασίες και τα αποτελέσματα της διαχείρισης κινδύνου.

2.3.4 ISO/IEC 27017:2015

Το ISO/IEC 27017:2015 παρέχει πρόσθετη καθοδήγηση για παρόχους και πελάτες υπηρεσιών νέφους [25]. Βασίζεται στο ISO/IEC 27002:2013, επεκτείνει 37 δικλίδες και προσθέτει επτά CLD δικλίδες για ρόλους, αφαίρεση αγαθών, διαχωρισμό και σκλήρυνση εικονικών περιβαλλόντων, ασφάλεια διαχειριστών, παρακολούθηση υπηρεσιών και ευθυγράμμιση εικονικών/φυσικών δικτύων. Κεντρική αρχή είναι ο επιμερισμός ευθύνης παρόχου και πελάτη· στη δομή του 2022 η θεματική αποτυπώνεται κυρίως στη 5.23.

Η ανάλυση στηρίζεται στο ISO/IEC 27017:2015, την έκδοση που ίσχυε κατά τον σχεδιασμό και την εκτέλεση της μελέτης. Στις 27 Ιουλίου 2026 δημοσιεύθηκε η δεύτερη έκδοση, ISO/IEC 27017:2026, ευθυγραμμισμένη με το ISO/IEC 27002:2022, η οποία αντικαθιστά και αποσύρει την έκδοση του 2015 [26]. Η εργασία διατηρεί την ιχνηλασιμότητα προς την έκδοση που πράγματι χρησιμοποιήθηκε και δεν επιχειρεί αντιστοίχιση δικλίδα προς δικλίδα με τη νέα, η οποία θα προϋπέθετε πρόσβαση στο πλήρες κείμενό της. Η επικαιροποίηση των αντιστοιχίσεων CLD καταγράφεται ως κατεύθυνση μελλοντικής εργασίας.

2.3.5 Η οικογένεια NIST

Το πλαίσιο του NIST προσφέρει συμπληρωματική, διαδικαστικά προσανατολισμένη οπτική στη διαχείριση κινδύνων. Το NIST SP 800-37 Rev. 2 ορίζει το Risk Management Framework (RMF) με επτά βήματα: Prepare (Προετοιμασία), Categorize (Κατηγοριοποίηση), Select (Επιλογή δικλίδων), Implement (Υλοποίηση), Assess (Αξιολόγηση), Authorize (Εξουσιοδότηση) και Monitor (Παρακολούθηση) [27]. Το NIST SP 800-30 Rev. 1 παρέχει τη μεθοδολογία διενέργειας εκτίμησης κινδύνου σε τέσσερα στάδια: Prepare, Conduct, Communicate και Maintain [28].

Το NIST Cybersecurity Framework (CSF) 2.0, που δημοσιεύθηκε στις 26 Φεβρουαρίου 2024, οργανώνεται γύρω από έξι λειτουργίες: Govern (Διακυβέρνηση), Identify, Protect, Detect, Respond και Recover [29]. Η λειτουργία Govern προστέθηκε νέα στην έκδοση 2.0, αναβαθμίζοντας τη διακυβέρνηση της κυβερνοασφάλειας σε αυτοτελή, διατομεακή λειτουργία και αναγνωρίζοντας τον ρόλο της διαχείρισης κινδύνων σε όλες τις υπόλοιπες λειτουργίες. Οι έξι λειτουργίες δεν συνιστούν αυστηρό, διαδοχικό κύκλο ζωής αλλά ταυτόχρονες και διαρκείς δραστηριότητες· η παράθεσή τους σε φάσεις στους πίνακες που ακολουθούν είναι ερμηνευτική.

Υφίσταται τεκμηριωμένη γέφυρα μεταξύ του ISO/IEC 27002 και του NIST: το χαρακτηριστικό «Έννοιες κυβερνοασφάλειας» του ISO/IEC 27002:2022 αντιστοιχίζει κάθε δικλίδα στις πέντε έννοιες του ISO/IEC TS 27110, οι οποίες αντιστοιχούν εννοιολογικά στις βασικές λειτουργίες του NIST CSF [24]. Πρέπει, ωστόσο, να τονιστεί ότι η αντιστοίχιση μέσω του ISO/IEC TS 27110 περιλαμβάνει πέντε έννοιες (Identify/Protect/Detect/Respond/Recover), ενώ το NIST CSF 2.0 περιλαμβάνει έξι λειτουργίες, με την προσθήκη της Govern. Συνεπώς, η εννοιολογική αντιστοίχιση αφορά τις πέντε επιχειρησιακές λειτουργίες και δεν καλύπτει τη λειτουργία διακυβέρνησης.

2.3.6 NIS2, Νόμος 5160/2024 και ΚΥΑ 1689/2025

Το κανονιστικό πλαίσιο καθιστά τη διαχείριση κινδύνων κυβερνοασφάλειας νομική υποχρέωση για τις βασικές και σημαντικές οντότητες που εμπίπτουν στο πεδίο εφαρμογής του. Στην παρούσα

εργασία αξιοποιείται ως πλαίσιο αναφοράς, χωρίς να τεκμηριώνεται συγκεκριμένη νομική υπαγωγή του ανωνυμοποιημένου αρχετύπου govERP. Η Οδηγία (ΕΕ) 2022/2555 (NIS2), στο άρθρο 21, επιβάλλει στις βασικές και σημαντικές οντότητες τη λήψη κατάλληλων και αναλογικών τεχνικών, επιχειρησιακών και οργανωτικών μέτρων διαχείρισης κινδύνων κυβερνοασφάλειας, βάσει προσέγγισης «όλων των κινδύνων» (all-hazards approach) [4], ενώ το άρθρο 20 θεσπίζει την ευθύνη των διοικητικών οργάνων για την έγκριση και εποπτεία των μέτρων αυτών. Η Οδηγία ενσωματώθηκε στην ελληνική έννομη τάξη με τον Νόμο 5160/2024 (ΦΕΚ Α' 195/27-11-2024), του οποίου το άρθρο 15 («Μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας») μεταφέρει τις οριζόντιες απαιτήσεις διαχείρισης κινδύνων του άρθρου 21 της Οδηγίας, σε συνδυασμό με το άρθρο 14 για τη διακυβέρνηση [5].

Η ΚΥΑ 1689/2025 εξειδικεύει τις υποχρεώσεις σε είκοσι δύο απαιτήσεις [6]. Στο Κεφάλαιο 2 λειτουργεί ως κανονιστικό πλαίσιο διαχείρισης κινδύνων, η απόδειξη συμμόρφωσης εξετάζεται στο Κεφάλαιο 3 και η αντιστοίχιση δικλίδων στο Κεφάλαιο 4.

2.3.7 Σύνθεση και πίνακας αντιστοίχισης

Παρά τις διαφορές ορολογίας και δομής, τα εξεταζόμενα πρότυπα και πλαίσια συγκλίνουν σε έναν κοινό κύκλο ζωής κινδύνου. Ο Πίνακας 2.2 αντιστοιχίζει τις φάσεις του κύκλου αυτού στα ISO/IEC 27005:2022, NIST RMF (SP 800-37 Rev. 2) / SP 800-30 Rev. 1, NIST CSF 2.0 και στο άρθρο 21 της NIS2 / άρθρο 15 του Ν. 5160/2024. Η αντιστοίχιση είναι λειτουργική και ερμηνευτική, όχι επίσημη αντιστοίχιση που εκδίδεται από ISO, NIST ή ENISA· ειδικότερα, οι λειτουργίες του NIST CSF 2.0 παρατίθενται ως ταυτόχρονες/διαρκείς και όχι ως υποχρεωτική ακολουθία.

Πίνακας 2.2. Ενδεικτική ερμηνευτική αντιστοίχιση φάσεων διαχείρισης κινδύνου με επιλεγμένα πρότυπα και πλαίσια.

Φάση κύκλου κινδύνου	ISO/IEC 27005:2022	NIST RMF / SP 800-30	NIST CSF 2.0	NIS2 άρ. 20–21 / Ν. 5160/2024 άρ. 14–15
Καθιέρωση πλαισίου / διακυβέρνηση	Context establishment	Prepare	Govern	Πολιτικές ανάλυσης κινδύνων & διακυβέρνηση
Αναγνώριση κινδύνων	Risk identification	Categorize · Conduct	Identify	Αναγνώριση αγαθών/κινδύνων
Ανάλυση κινδύνων	Risk analysis	Conduct (συνέπεια/πιθανοφάνεια)	Identify	Εκτίμηση κινδύνων
Αξιολόγηση κινδύνων	Risk evaluation	Conduct (καθορισμός κινδύνου)	Identify	Αξιολόγηση & ιεράρχηση
Αντιμετώπιση κινδύνων	Risk treatment	Select · Implement · Assess · Authorize	Protect · Detect · Respond · Recover	Τεχνικά/οργανωτικά/επιχειρησιακά μέτρα
Αποδοχή υπολειπόμενου κινδύνου	μετά την αντιμετώπιση (ευθύνη ιδιοκτήτη κινδύνου)	Authorize	Govern	Έγκριση διοίκησης
Παρακολούθηση & επανεξέταση	Monitoring & review	Monitor · Maintain	Govern (διαρκής)	Παρακολούθηση & αναφορά

2.4 Μεθοδολογίες

2.4.1 Η διεργασία του ISO/IEC 27005 ως μεθοδολογία

Το ISO/IEC 27005:2022 παρέχει ένα καθοδηγητικό μοντέλο διεργασίας, χωρίς να επιβάλλει μία μοναδική τεχνική ή μέθοδο αποτίμησης· επιτρέπει, αντιθέτως, την επιλογή της καταλληλότερης μεθόδου ανάλογα με το πλαίσιο του οργανισμού. Λειτουργεί έτσι ως μετα-μεθοδολογικό πλαίσιο: ορίζει τα πέντε στάδια και τις παράλληλες δραστηριότητες, αφήνοντας στον αναλυτή την επιλογή τεχνικών αναγνώρισης (event-based ή asset-based) και κλιμάκων μέτρησης.

2.4.2 Το NIST RMF ως διαδικαστική μεθοδολογία

Σε αντίθεση με την ευελιξία του ISO/IEC 27005, το NIST RMF (SP 800-37 Rev. 2) προσφέρει μια αυστηρά διαδικαστική μεθοδολογία επτά βημάτων, ισχυρά συνδεδεμένη με τον κατάλογο δικλίδων του NIST SP 800-53 και προσαρμοσμένη στην εξουσιοδότηση λειτουργίας συστημάτων [27]. Το NIST SP 800-30 Rev. 1 παρέχει αναλυτική καθοδήγηση για τη διενέργεια εκτίμησης κινδύνου — απειλές, ευπάθειες, πιθανοφάνεια και συνέπεια — και υποστηρίζει τις αποφάσεις διαχείρισης κινδύνου σε πολλαπλά στάδια του RMF [28].

2.4.3 Λοιπές αναγνωρισμένες μεθοδολογίες

Η EBIOS Risk Manager (EBIOS RM) αναπτύχθηκε από τη γαλλική ANSSI και δημοσιεύθηκε τον Οκτώβριο 2018 [30]. Δομείται σε πέντε εργαστήρια (workshops): καθορισμός πλαισίου και βάσης ασφάλειας, πηγές κινδύνου, στρατηγικά σενάρια, επιχειρησιακά σενάρια και αντιμετώπιση. Είναι σεναριο-κεντρική (scenario-based) και εστιάζει σε εσκεμμένες απειλές και στην οικοσυστημική χαρτογράφηση. Η μέθοδος MONARC δεν αποτελεί παράγωγο της EBIOS RM: είναι ευρέως βασισμένη στο ISO/IEC 27005, αξιοποιεί όμως βάσεις γνώσης προερχόμενες από την κλασική μέθοδο EBIOS.

Η OCTAVE Allegro είναι ποιοτική μεθοδολογία εστιασμένη στα αγαθά πληροφορίας, οργανωμένη σε οκτώ βήματα εντός τεσσάρων φάσεων, με έμφαση στην επιχειρησιακή οπτική [31]. Η MEHARI, αναπτυγμένη από το γαλλικό CLUSIF, προσφέρει δομημένο μοντέλο κινδύνου με βάσεις γνώσης για την αξιολόγηση της ποιότητας των δικλίδων, υποστηρίζοντας τόσο ποιοτική όσο και ημι-ποσοτική αποτίμηση [32]. Συγκριτικά, η EBIOS RM είναι σεναριο-κεντρική και κατάλληλη για σύνθετους οργανισμούς, η OCTAVE Allegro είναι αγαθο-κεντρική και ευέλικτη για μικρότερους οργανισμούς, και η MEHARI παρέχει αναλυτικές βάσεις γνώσης δικλίδων. Και οι τρεις είναι κατά βάση ποιοτικές.

Η Human-Centric Risk Management (HRM) ενσωματώνει συμπεριφορές, δεξιότητες και οργανωσιακή κουλτούρα στη διαχείριση κινδύνων [33]. Συμπληρώνει τις τεχνικοκεντρικές μεθόδους και συνδέεται με τις δικλίδες της κατηγορίας «Άνθρωποι» του ISO/IEC 27002:2022.

Η MITIGATE είναι συνεργατική, evidence-driven μέθοδος για κινδύνους εφοδιαστικής αλυσίδας, με έμφαση στη διάδοση και στις αλυσιδωτές επιπτώσεις μεταξύ οργανισμών [34], [35]. Αναφέρεται συγκριτικά και δεν εφαρμόζεται στο gonERP.

2.4.4 ENISA Interoperable EU Risk Management Toolbox

Το Interoperable EU Risk Management Toolbox του ENISA είναι εργαλείο διαλειτουργικότητας και σύγκρισης, όχι αυτοτελής μέθοδος [12]. Παρέχει κοινές μετρικές για ερμηνεία και συνάθροιση αποτελεσμάτων, ενώ το συνοδευτικό Compendium καταγράφει πλαίσια όπως ISO/IEC 27005, NIST, EBIOS και MONARC [36]. Στην εργασία χρησιμοποιείται για συγκριτική βαθμονόμηση των κλιμάκων του Κεφαλαίου 4.

2.4.5 Κριτήρια επιλογής μεθοδολογίας για το αρχέτυπο gonERP

Για το gonERP υιοθετείται τριμερής προσέγγιση: ISO/IEC 27005 ως θεωρητικό πλαίσιο, MONARC ως εργαλείο μοντελοποίησης και υπολογισμού, και ENISA toolbox ως κοινή αναφορά

κλιμάκων. Το MONARC επιλέχθηκε επειδή υποστηρίζει πρωτεύοντα/υποστηρικτικά αγαθά, ιχνηλασιμότητα ανά τριάδα αγαθού–απειλής–ευπάθειας, επαναλήψιμους υπολογισμούς και πλήρη εξαγωγή του μοντέλου. Η προσέγγιση είναι ημι-ποσοτική και η διάσταση πιστοποίησης παραμένει στο Κεφάλαιο 3.

2.5 Εργαλεία ανοιχτού κώδικα

2.5.1 Κριτήρια αξιολόγησης

Τα εργαλεία ανοιχτού κώδικα αξιολογούνται με βάση την άδεια χρήσης και τη βιωσιμότητα του έργου, τη μεθοδολογική ευθυγράμμιση με το ISO/IEC 27005, την υποστήριξη ημι-ποσοτικής ανάλυσης και μητρώου κινδύνων, τις δυνατότητες εισαγωγής/εξαγωγής και διαλειτουργικότητας, τη συντήρηση και την κοινότητα, και την καταλληλότητα για το αρχέτυπο govERP.

2.5.2 MONARC

Η MONARC (Method for an Optimised aNalysis of Risks) αναπτύσσεται και συντηρείται από το Luxembourg House of Cybersecurity και διατίθεται ως λογισμικό ανοιχτού κώδικα [13]. Σύμφωνα με το επίσημο αποθετήριο, ο κώδικας διατίθεται υπό την άδεια GNU Affero General Public License v3, ενώ τα αντικείμενα δεδομένων που συνοδεύουν τη MONARC (απειλές, αγαθά, ευπάθειες, βάσεις αναφοράς) διατίθενται υπό την άδεια CC0 1.0 Universal. Η μέθοδος αυτοχαρακτηρίζεται ως επαναληπτική και ποιοτική, ευρέως βασισμένη στο ISO/IEC 27005, και οργανώνεται σε τέσσερις φάσεις — καθιέρωση πλαισίου, μοντελοποίηση πλαισίου, αξιολόγηση και αντιμετώπιση κινδύνων, υλοποίηση και παρακολούθηση — τις οποίες η επίσημη τεκμηρίωση παρουσιάζει ως λειτουργικά ανάλογες προς τον κύκλο PDCA [37]. Διακρίνει τα πρωτεύοντα αγαθά (primary assets) από τα υποστηρικτικά (supporting assets) σε ιεραρχική δομή.

Ο υπολογισμός του κινδύνου στη MONARC γίνεται με βάση κλίμακες απειλής και ευπάθειας, ενώ οι συνέπειες αποτιμώνται τόσο επί της τριάδας CIA όσο και επί των κριτηρίων ROLFP (Reputation, Operational, Legal, Financial, Person — φήμη, λειτουργία, νομικές συνέπειες, οικονομικές συνέπειες και επίπτωση σε φυσικά πρόσωπα). Οι κλίμακες του εργαλείου είναι διακριτές αριθμητικές· στην παρούσα εργασία αξιοποιούνται ως ημι-ποσοτική επιχειρησιακή αποτύπωση, χωρίς οι τιμές να εκλαμβάνονται ως ακριβείς στατιστικές πιθανότητες ή χρηματικές μετρήσεις. Το εργαλείο υποστηρίζει βάσεις γνώσης επαναχρησιμοποιήσιμων αγαθών και εξαγωγή σε μορφή CSV, στοιχεία που το καθιστούν κατάλληλο ως κύριο εργαλείο για το αρχέτυπο govERP.

2.5.3 CISO Assistant

Το CISO Assistant της intuitem διατίθεται σε Community Edition υπό την άδεια AGPL v3, ενώ οι εκδόσεις Pro/Enterprise διατίθενται υπό εμπορική άδεια της intuitem [38]. Αποτελεί ολοκληρωμένη πλατφόρμα GRC (Governance, Risk and Compliance) που καλύπτει διαχείριση κινδύνων, διαχείριση ελέγχων/συμμόρφωσης και αναφορές. Διαθέτει ενσωματωμένη λειτουργία εκτίμησης κινδύνου και υποστηρίζει άνω των 100 πλαισίων κατά τον χρόνο συγγραφής, με αυτόματη αντιστοίχιση δικλίδων (μεταξύ άλλων ISO 27001, NIST CSF, NIS2, DORA, GDPR)· οι αντιστοιχίσεις (crosswalks) μεταξύ πλαισίων ακολουθούν τη σύμβαση του προγράμματος NIST OLIR (Online Informative References) [39]. Παρέχει επίσης δυνατότητες εισαγωγής/εξαγωγής.

Στην παρούσα εργασία, το CISO Assistant εξετάζεται ως συμπληρωματικό εργαλείο GRC και ως παράδειγμα εργαλείου που υποστηρίζει risk assessment και αντιστοιχίσεις μεταξύ πλαισίων. Δεν αποτελεί το κύριο εργαλείο της πρακτικής ανάλυσης επικινδυνότητας, η οποία υλοποιείται με MONARC, ούτε το κύριο εργαλείο της προσέγγισης προς πιστοποίηση, η οποία εξετάζεται μέσω CUSTODES. Μπορεί ωστόσο να αξιοποιηθεί στη συγκριτική αποτίμηση εργαλείων και στη συζήτηση της οργανωτικής ετοιμότητας.

2.5.4 verinice και Eramba

Το verinice διατίθεται υπό AGPLv3, υποστηρίζει ISO/IEC 27001/27002/27005 και BSI IT-Grundschutz, αλλά η κλασική γενιά του βρίσκεται σε συντήρηση [40]. Το Eramba καλύπτει GRC, πολιτικές και κινδύνους [41], όμως η Community Edition είναι source-available με ιδιόκτητους περιορισμούς και δεν θεωρείται ανοικτού κώδικα. Και τα δύο χρησιμοποιούνται μόνο συγκριτικά.

2.5.5 Συγκριτικός πίνακας και τεκμηρίωση της MONARC ως κύριου εργαλείου

Πίνακας 2.3. Ενδεικτική συγκριτική αποτίμηση εργαλείων ανάλυσης κινδύνου και GRC.

Κριτήριο	MONARC	CISO Assistant	verinice	Eramba
Μοντέλο διάθεσης / άδεια	AGPL v3 (δεδομένα CC0 1.0)	AGPL v3 (Community)	AGPLv3 (classic: συντήρηση)	Community (source-available, ιδιόκτητοι όροι)
Φορέας / συντήρηση	Luxembourg House of Cybersecurity	intuitem	SerNet	Eramba
Ευθυγράμμιση ISO/IEC 27005	Ναι (ισχυρή μεθοδολογική ευθυγράμμιση)	Ναι (ενσωματωμένη εκτίμηση)	Ναι	Μερική
Ημι-ποσοτική ανάλυση	Ναι (CIA + ROLFP)	Ναι	Ναι	Περιορισμένη
Πρωτεύοντα/υποστηρικτικά αγαθά	Ναι	Όχι ρητά	Ναι (δέντρο αγαθών)	Όχι
Αντιστοίχιση πλαισίων	Περιορισμένη	Υψηλή (NIST OLIR, 100+ πλαίσια)	Μέτρια	Μέτρια
Εξαγωγή / εισαγωγή	CSV	Πλήρης (API/CLI)	CSV/XML/XLS	Ναι
Καταλληλότητα για govERP	Υψηλή (κύριο)	Συμπληρωματική (GRC)	Μέτρια	Συγκριτική αναφορά

Η MONARC επιλέγεται ως κύριο εργαλείο διότι συνδυάζει την ισχυρή μεθοδολογική ευθυγράμμιση με τη διεργασία του ISO/IEC 27005, την ημι-ποσοτική μέθοδο με κριτήρια CIA και ROLFP, τη ρητή διάκριση πρωτευόντων/υποστηρικτικών αγαθών, και τη διάθεση υπό ελεύθερη άδεια με επαναχρησιμοποιήσιμες βάσεις γνώσης. Το CISO Assistant αξιοποιείται συμπληρωματικά, ιδίως για τη διάσταση GRC και τις αντιστοιχίσεις πλαισίων· δεν αποτελεί το κύριο εργαλείο της πρακτικής ανάλυσης επικινδυνότητας, η οποία υλοποιείται με MONARC.

2.6 Οργανωτική ετοιμότητα και ωριμότητα ασφάλειας

Οργανωτική ετοιμότητα είναι η ύπαρξη ρόλων, διεργασιών, πόρων, δικλίδων και τεκμηρίων που επιτρέπουν συστηματική διαχείριση κινδύνων. Ωριμότητα είναι ο βαθμός στον οποίο οι πρακτικές αυτές είναι θεσμοθετημένες, επαναλήψιμες, μετρήσιμες και βελτιώνονται. Οι έννοιες είναι συγγενείς αλλά όχι ταυτόσημες.

Το εννοιολογικό αυτό ζεύγος θεμελιώνεται στα πρότυπα και στο κανονιστικό πλαίσιο των προηγούμενων ενοτήτων. Το ISO/IEC 27001:2022 απαιτεί ηγεσία και δέσμευση της διοίκησης, επάρκεια πόρων και ικανοτήτων, αξιολόγηση επίδοσης και συνεχή βελτίωση (ρήτρες 5, 7, 9 και 10) [2]. Η Οδηγία NIS2 και ο Ν. 5160/2024 καθιστούν τα διοικητικά όργανα υπεύθυνα για την έγκριση και την εποπτεία των μέτρων διαχείρισης κινδύνων και για τη σχετική κατάρτιση (άρθρο 20 της Οδηγίας· άρθρο 14 του νόμου) [4], [5], ενώ το εθνικό πλαίσιο της ΚΥΑ 1689/2025 εξειδικεύει τα σχετικά οργανωτικά μέτρα [6]. Την ανθρώπινη διάσταση αναδεικνύουν οι δικλίδες

του θέματος «Άνθρωποι» του ISO/IEC 27002:2022 [3] και, σε ερευνητικό επίπεδο, η ανθρωποκεντρική μεθοδολογία HRM της §2.4.3 [33].

Η §4.9 αποτιμά τρεις διαστάσεις: διακυβέρνηση και λογοδοσία, ανθρώπινη ικανότητα και λειτουργικές διαδικασίες. Η τεκμηρίωση και η συνεχής παρακολούθηση λειτουργούν εγκάρσια σε όλες.

Ως προς την ωριμότητα, το Κεφάλαιο 4 (§4.9) εφαρμόζει τριεπίπεδη ερμηνευτική ανάγνωση των αποτελεσμάτων της ανάλυσης κινδύνου σε θεσμικό, τεχνικό και λειτουργικό επίπεδο. Η κλίμακα αυτή αποτελεί αναλυτικό εργαλείο που κατασκευάστηκε για τους σκοπούς της παρούσας διατριβής, στηριγμένο στις προαναφερθείσες διαστάσεις διακυβέρνησης, εφαρμογής, τεκμηρίωσης και βελτίωσης· δεν παρουσιάζεται ως επίσημο μοντέλο ωριμότητας των ISO/IEC 27001, ISO/IEC 27002 ή της NIS2, καθώς τα κείμενα αυτά δεν ορίζουν τυποποιημένο μοντέλο επιπέδων ωριμότητας.

Τέλος, οριοθετείται η σχέση με το Κεφάλαιο 3: η ετοιμότητα που εξετάζεται εδώ αφορά την ικανότητα διαχείρισης κινδύνων. Η ετοιμότητα προς αξιολόγηση και πιστοποίηση — δηλαδή η ικανότητα απόδειξης συμμόρφωσης έναντι καθορισμένων απαιτήσεων — εκφεύγει του παρόντος κεφαλαίου, εξετάζεται θεωρητικά στο Κεφάλαιο 3 και εφαρμόζεται στο Κεφάλαιο 5.

2.7 Σύνοψη και μετάβαση στο Κεφάλαιο 3

Το κεφάλαιο θεμελίωσε τη διεργασία κινδύνου, τα βασικά πρότυπα, το NIST, το κανονιστικό πλαίσιο, τις κύριες μεθοδολογίες και τα εργαλεία. Για το govERP επιλέχθηκαν ISO/IEC 27005 ως πλαίσιο, MONARC ως εργαλείο και ENISA toolbox ως κοινή αναφορά κλιμάκων, με ημι-ποσοτικό χαρακτήρα. Η οργανωτική ετοιμότητα της §2.6 τροφοδοτεί την §4.9.

Το κεφάλαιο απάντησε στο ερώτημα «πώς αναλύουμε τον κίνδυνο». Το Κεφάλαιο 3 μεταβαίνει στο ερώτημα «πώς αποδεικνύουμε συμμόρφωση και ετοιμότητα πιστοποίησης», όπου εξετάζεται αναλυτικά το εθνικό πλαίσιο των είκοσι δύο απαιτήσεων της ΚΥΑ 1689/2025 και όπου εντάσσεται η μεθοδολογία CUSTODES ως μεθοδολογία ετοιμότητας πιστοποίησης.

3. Θεωρητικό Υπόβαθρο Συμμόρφωσης και Προσέγγισης προς Πιστοποίηση

3.1 Συμμόρφωση, αξιολόγηση συμμόρφωσης και πιστοποίηση

Η αξιολόγηση συμμόρφωσης εξετάζει αν καθορισμένες απαιτήσεις πληρούνται και με ποια τεκμήρια. Στην εργασία θεμελιώνει το Κεφάλαιο 5, όπου αποτιμάται η ετοιμότητα ενός οριοθετημένου υποσυστήματος χωρίς εκτέλεση πιστοποίησης.

Conformity assessment αποδίδεται ως «αξιολόγηση συμμόρφωσης», attestation ως «βεβαίωση», certification ως «πιστοποίηση» και accreditation ως «διαπίστευση». Ο οργανισμός αξιολόγησης είναι CAB και το αντικείμενο των Common Criteria ToE. Η γενική αξιολόγηση συμμόρφωσης διακρίνεται από την ειδική τεχνική αξιολόγηση κατά Common Criteria.

Κατά το ISO/IEC 17000:2020, συμμόρφωση είναι η εκπλήρωση καθορισμένης απαίτησης, ενώ αξιολόγηση συμμόρφωσης είναι η απόδειξη ότι καθορισμένες απαιτήσεις πληρούνται [18]. Αντικείμενο της αξιολόγησης μπορεί να είναι προϊόν, διεργασία, υπηρεσία, σύστημα, εγκατάσταση, φορέας ή πρόσωπο. Η λειτουργική προσέγγιση του προτύπου περιλαμβάνει την επιλογή του αντικειμένου και των απαιτήσεων, τον προσδιορισμό μέσω δοκιμής, ελέγχου ή επιθεώρησης, την ανασκόπηση, την απόφαση, τη βεβαίωση και, όπου προβλέπεται, την επιτήρηση [18]. Οι απαιτήσεις προέρχονται συνήθως από πρότυπα, τεχνικές προδιαγραφές ή κανονιστικά κείμενα.

Οι δραστηριότητες αξιολόγησης διακρίνονται ανάλογα με τον φορέα που τις διενεργεί. Η αξιολόγηση πρώτου μέρους γίνεται από τον ίδιο τον πάροχο του αντικειμένου, ενώ η δεύτερου μέρους από οργανισμό με συμφέρον χρήστη, όπως ο αγοραστής. Η αξιολόγηση τρίτου μέρους γίνεται από φορέα ανεξάρτητο από τον πάροχο και τον χρήστη [18]. Η πιστοποίηση είναι βεβαίωση τρίτου μέρους για αντικείμενο αξιολόγησης συμμόρφωσης, ενώ η διαπίστευση αφορά την επάρκεια των ίδιων των φορέων αξιολόγησης [18]. Η ανεξάρτητη βεβαίωση μειώνει την ανάγκη επανάληψης του ίδιου ελέγχου και υποστηρίζει την εμπιστοσύνη στην εσωτερική αγορά [42] και στο ευρωπαϊκό πλαίσιο πιστοποίησης κυβερνοασφάλειας [19].

Στην κυβερνοασφάλεια, η αξιολόγηση εξετάζει αν ένα αντικείμενο διαθέτει τις δηλωμένες λειτουργίες ασφάλειας και αν υπάρχουν επαρκή τεκμήρια για το αντίστοιχο επίπεδο διασφάλισης. Ο Κανονισμός (ΕΕ) 2019/881 θέσπισε ευρωπαϊκό πλαίσιο πιστοποίησης για προϊόντα, υπηρεσίες και διεργασίες ΤΠΕ [19]. Ένα πιστοποιητικό επιβεβαιώνει ότι η προβλεπόμενη αξιολόγηση ολοκληρώθηκε επιτυχώς έναντι συγκεκριμένου σχήματος και ορίου· δεν εγγυάται, συνεπώς, την απουσία κάθε ευπάθειας ούτε καταργεί την ανάγκη διαχείρισης κινδύνων [19]. Η διατριβή περιορίζεται στην ετοιμότητα προς αξιολόγηση και πιστοποίηση, οργανώνοντας το αντικείμενο, τις απαιτήσεις και τα αναμενόμενα τεκμήρια, χωρίς να υποκαθιστά αξιολόγηση από αρμόδιο και διαπιστευμένο φορέα.

3.2 Διαπίστευση και φορείς αξιολόγησης

Η διαπίστευση είναι βεβαίωση τρίτου μέρους για την επάρκεια, την αμεροληψία και τη συνεπή λειτουργία ενός φορέα αξιολόγησης της συμμόρφωσης [18]. Αφορά τον φορέα που διενεργεί την αξιολόγηση ή εκδίδει την πιστοποίηση, όχι το ίδιο το προϊόν ή την υπηρεσία. Το ISO/IEC 17011:2017 καθορίζει τις απαιτήσεις για τους φορείς διαπίστευσης [43]. Στην Ευρωπαϊκή Ένωση, ο Κανονισμός (ΕΚ) 765/2008 προβλέπει έναν εθνικό φορέα διαπίστευσης ανά κράτος μέλος, με μη κερδοσκοπική και μη ανταγωνιστική λειτουργία και με αξιολόγηση από ομοτίμους· στην Ελλάδα ο ρόλος αυτός ασκείται από το Εθνικό Σύστημα Διαπίστευσης (Ε.ΣΥ.Δ.) [42].

Στο ευρωπαϊκό πλαίσιο κυβερνοασφάλειας διακρίνονται οι εθνικές αρχές πιστοποίησης, οι φορείς αξιολόγησης της συμμόρφωσης και οι εθνικοί φορείς διαπίστευσης. Οι εθνικές αρχές πιστοποίησης της κυβερνοασφάλειας (National Cybersecurity Certification Authorities — NCCA) εποπτεύουν την εφαρμογή των ευρωπαϊκών σχημάτων, ενώ οι φορείς αξιολόγησης διενεργούν τις προβλεπόμενες δραστηριότητες και, όπου έχουν σχετική αρμοδιότητα, εκδίδουν πιστοποιητικά. Η επάρκειά τους αναγνωρίζεται μέσω διαπίστευσης από τον εθνικό φορέα, σύμφωνα με τις απαιτήσεις του εφαρμοζόμενου σχήματος, και η ευρωπαϊκή υποδομή διαπίστευσης υποστηρίζει την αμοιβαία εμπιστοσύνη στα αποτελέσματα [42], [19].

Στο σχήμα EUCC, η τεχνική αξιολόγηση πραγματοποιείται από εργαστήρια αξιολόγησης ασφάλειας τεχνολογίας πληροφοριών (Information Technology Security Evaluation Facilities — ITSEF). Τα εργαστήρια αυτά διαπιστεύονται κατά ISO/IEC 17025 [44], ενώ τα πιστοποιητικά εκδίδονται από φορείς πιστοποίησης διαπιστευμένους κατά ISO/IEC 17065 [45]. Το σχήμα επιβάλλει πρόσθετες ειδικές απαιτήσεις και, για το επίπεδο διασφάλισης «υψηλό», συμπληρωματικές προϋποθέσεις έγκρισης [20]. Παρά τους διαφορετικούς ρόλους τους, οι εμπλεκόμενοι φορείς οφείλουν να τεκμηριώνουν επάρκεια προσωπικού, αμεροληψία, ακεραιότητα και συνεπή λειτουργία [43]–[45].

Το govERP δεν αξιολογείται από ITSEF και δεν πιστοποιείται. Το Κεφάλαιο 5 οργανώνει μόνο τα στοιχεία μιας μελλοντικής προετοιμασίας.

3.3 Πρότυπα αξιολόγησης ασφάλειας (Common Criteria — ISO/IEC 15408, 18045)

Τα Common Criteria for Information Technology Security Evaluation (CC) αποτελούν διεθνές πλαίσιο αξιολόγησης της ασφάλειας προϊόντων ΤΠΕ. Η σειρά ISO/IEC 15408:2022, με το Μέρος 1 να παρέχει το γενικό μοντέλο και την επισκόπηση της σειράς [16], αντιστοιχεί στα CC:2022 Release 1 [46]. Η CCRA [47] οριοθετεί το πεδίο της αμοιβαίας αναγνώρισης. Η κοινή μεθοδολογία αξιολόγησης CEM:2022 [48] αντιστοιχεί στο ISO/IEC 18045:2022 [17]. Το 2026 δημοσιεύθηκαν αναθεωρημένες εκδόσεις της σειράς ISO/IEC 15408 και του ISO/IEC 18045. Η εργασία διατηρεί την αγκύρωση στις εκδόσεις 2022, επειδή ο Εκτελεστικός Κανονισμός (ΕΕ) 2024/3144 ορίζει τα ISO/IEC 15408:2022/CC:2022 και ISO/IEC 18045:2022/CEM:2022 ως εφαρμοστέα βάση του EUCC [20]. Η μεταβατική περίοδος έως τις 31 Δεκεμβρίου 2027 αφορά τις προγενέστερες εκδόσεις που απαριθμεί ο ίδιος Κανονισμός [20]. Η συμφωνία CCRA καλύπτει πιστοποιητικά που δηλώνουν συμμόρφωση προς συνεργατικό προφίλ προστασίας (cPP), με δραστηριότητες διασφάλισης επιλεγμένες έως και EAL4 και ALC_FLR σύμφωνα με το Παράρτημα Κ. Καλύπτει επίσης αξιολογήσεις EAL1 έως EAL2 μαζί με ALC_FLR όταν δεν χρησιμοποιείται cPP [47]. Στην Ευρώπη, το EUCC διαδέχεται τη σχετική λειτουργία των εθνικών σχημάτων SOG-IS [20], [49].

Η έκδοση 2022 οργανώνεται σε πέντε μέρη: τα Μέρη 1 έως 3 παρουσιάζουν αντίστοιχα τις βασικές έννοιες και το μοντέλο αξιολόγησης, τις λειτουργικές απαιτήσεις και τις απαιτήσεις διασφάλισης. Το Μέρος 4 παρέχει το πλαίσιο προδιαγραφής μεθόδων αξιολόγησης και το Μέρος 5 τα προκαθορισμένα πακέτα απαιτήσεων [16], [46]. Κεντρική έννοια είναι ο στόχος αξιολόγησης (ToE), δηλαδή το προϊόν ή το τμήμα προϊόντος που εξετάζεται. Ό,τι βρίσκεται εκτός του ToE ανήκει στο περιβάλλον λειτουργίας και οι σχετικές υποχρεώσεις δηλώνονται ως παραδοχές. Η διάκριση αυτή καθορίζει με σαφήνεια τι καλύπτει και τι δεν καλύπτει το αποτέλεσμα της αξιολόγησης.

Η προδιαγραφή αρχίζει με το πρόβλημα ασφάλειας, το οποίο περιλαμβάνει απειλές, οργανωσιακές πολιτικές και παραδοχές, και από αυτό προκύπτουν στόχοι ασφάλειας για τον ToE και το περιβάλλον λειτουργίας του. Οι στόχοι εξειδικεύονται σε λειτουργικές απαιτήσεις ασφάλειας (Security Functional Requirements — SFR) από το Μέρος 2 και σε απαιτήσεις διασφάλισης ασφάλειας (Security Assurance Requirements — SAR) από το Μέρος 3 [16], [46]. Η τυποποιημένη αυτή δομή επιτρέπει τη σύγκριση απαιτήσεων και αποτελεσμάτων μεταξύ διαφορετικών προϊόντων και αξιολογήσεων.

Η προδιαγραφή οργανώνεται κυρίως μέσω του προφίλ προστασίας (Protection Profile — PP) και του στόχου ασφάλειας (Security Target — ST). Το PP περιγράφει ανάγκες ασφάλειας για έναν τύπο ToE, ανεξάρτητα από συγκεκριμένη υλοποίηση, και περιλαμβάνει τις αναμενόμενες SFR και SAR. Μπορεί έτσι να χρησιμοποιηθεί από κοινότητα χρηστών, ρυθμιστική αρχή ή ομάδα κατασκευαστών ως κοινό σημείο αναφοράς [16], [46]. Το ST αφορά συγκεκριμένο ToE και συγκεκριμένη υλοποίηση, αποτελεί τη βασική προδιαγραφή έναντι της οποίας διενεργείται η αξιολόγηση και δηλώνει, όπου εφαρμόζεται, συμμόρφωση προς προφίλ προστασίας.

Τα Common Criteria περιλαμβάνουν επτά προκαθορισμένα επίπεδα διασφάλισης αξιολόγησης (Evaluation Assurance Levels — EAL1 έως EAL7) στο Μέρος 5 [46]. Η αύξηση του επιπέδου συνεπάγεται περισσότερη τεκμηρίωση, αυστηρότερο έλεγχο του σχεδιασμού και βαθύτερη ανάλυση ευπαθειών. Το EAL εκφράζει το εύρος και την αυστηρότητα των ενεργειών διασφάλισης: δεν δηλώνει από μόνο του περισσότερες λειτουργίες ασφάλειας ούτε επιτρέπει απλή κατάταξη διαφορετικών προϊόντων. Η οικογένεια AVA_VAN της κλάσης AVA αξιολογεί την

ανθεκτικότητα του ΤοΕ απέναντι σε επιτιθέμενους με καθορισμένο δυναμικό επίθεσης. Το EUCC χρησιμοποιεί την οικογένεια αυτή για τη σύνδεση των τεχνικών αξιολογήσεων με τα επίπεδα διασφάλισής του.

Το ISO/IEC 18045 και η CEM καθορίζουν τις ελάχιστες ενέργειες που εκτελεί ο αξιολογητής για κάθε συνιστώσα διασφάλισης, ώστε τα αποτελέσματα διαφορετικών εργαστηρίων να είναι συγκρίσιμα [48], [17]. Για την εργασία, το ζεύγος ISO/IEC 15408 και 18045 παρέχει τη δομή που εφαρμόζεται στο Κεφάλαιο 5: ορισμό του ΤοΕ, πρόβλημα ασφάλειας, στόχους, απαιτήσεις και τεκμήρια. Η εφαρμογή παραμένει σε επίπεδο ετοιμότητας και δεν αποτελεί τεχνική αξιολόγηση κατά Common Criteria· η επόμενη ενότητα εξετάζει τις απαιτήσεις επάρκειας των φορέων που θα εκτελούσαν και θα πιστοποιούσαν μια τέτοια αξιολόγηση.

3.4 Πρότυπα της σειράς ISO/IEC 17000 για την αξιολόγηση συμμόρφωσης

Τα Common Criteria/CEM ορίζουν το τεχνικό περιεχόμενο, ενώ η σειρά ISO/IEC 17000 παρέχει την ορολογία και τις απαιτήσεις επάρκειας των φορέων αξιολόγησης. Το ISO/IEC 17000:2020 αποτελεί τη βάση των εννοιών της §3.1 [18].

Στο EUCC, η επάρκεια των ITSEF στηρίζεται στο ISO/IEC 17025:2017 [44], [20]. Το ISO/IEC TS 23532-1:2021 συμπληρώνει το πρότυπο με απαιτήσεις ειδικές για εργαστήρια που αξιολογούν προϊόντα κατά ISO/IEC 15408 και ISO/IEC 18045 [50]. Η διαπίστευση των φορέων πιστοποίησης βασίζεται στο ISO/IEC 17065:2012, ενώ το ISO/IEC 17011:2017 καθορίζει τις απαιτήσεις για τους εθνικούς φορείς διαπίστευσης [43], [45], [20].

Άλλα μέλη της σειράς καλύπτουν διαφορετικές μορφές αξιολόγησης, όπως το ISO/IEC 17020:2026 για φορείς επιθεώρησης [51]. Το ISO/IEC 17021-1:2015 αφορά φορείς που ελέγχουν και πιστοποιούν συστήματα διαχείρισης [52], ενώ το ISO/IEC 27006-1:2024 εξειδικεύει τις απαιτήσεις για φορείς πιστοποίησης Συστημάτων Διαχείρισης Ασφάλειας Πληροφοριών κατά ISO/IEC 27001 [53]. Η πιστοποίηση συστήματος διαχείρισης ακολουθεί, επομένως, την οδό ISO/IEC 27001 και ISO/IEC 17021-1/27006-1. Η πιστοποίηση προϊόντος κατά Common Criteria ακολουθεί την οδό ISO/IEC 15408/18045, με εργαστήριο κατά ISO/IEC 17025 και φορέα πιστοποίησης κατά ISO/IEC 17065.

Η σειρά 17000 ρυθμίζει τους φορείς και την επάρκειά τους, τα Common Criteria/CEM το τεχνικό αντικείμενο, και το EUCC συνδέει τα δύο επίπεδα.

3.5 Ευρωπαϊκό πλαίσιο πιστοποίησης κυβερνοασφάλειας (Cybersecurity Act, EUCC)

Ο Κανονισμός (ΕΕ) 2019/881, γνωστός ως Cybersecurity Act, θέσπισε το ευρωπαϊκό πλαίσιο πιστοποίησης κυβερνοασφάλειας και έδωσε μόνιμη εντολή στον ENISA [19]. Το πλαίσιο επιτρέπει τη δημιουργία ευρωπαϊκών σχημάτων για προϊόντα, υπηρεσίες και διεργασίες ΤΠΕ και, μετά την τροποποίησή του με τον Κανονισμό (ΕΕ) 2025/37, για διαχειριζόμενες υπηρεσίες ασφάλειας. Στόχος είναι να περιοριστεί ο κατακερματισμός των εθνικών σχημάτων και να αναγνωρίζονται τα ευρωπαϊκά πιστοποιητικά σε όλα τα κράτη μέλη. Τα υποψήφια σχήματα καταρτίζονται από τον ENISA και αποκτούν δεσμευτική ισχύ μέσω εκτελεστικών πράξεων της Ευρωπαϊκής Επιτροπής [19].

Το άρθρο 52 του Κανονισμού ορίζει τα επίπεδα διασφάλισης «βασικό», «σημαντικό» και «υψηλό» [19]. Το επιλεγμένο επίπεδο πρέπει να είναι ανάλογο με τον κίνδυνο της σκοπούμενης χρήσης, ως προς την πιθανότητα και την επίπτωση περιστατικού. Στο «βασικό» επίπεδο η αξιολόγηση αντιμετωπίζει γνωστούς βασικούς κινδύνους και μπορεί να περιορίζεται σε ανασκόπηση τεχνικής τεκμηρίωσης. Στο «σημαντικό» προστίθενται έλεγχοι γνωστών ευπαθειών και δοκιμές λειτουργιών ασφάλειας, ενώ το «υψηλό» εξετάζει ανθεκτικότητα απέναντι σε επιτιθέμενους με σημαντικές δεξιότητες και πόρους [19]. Στο «βασικό» επίπεδο μπορεί να επιτρέπεται αυτοαξιολόγηση και δήλωση συμμόρφωσης ΕΕ, εφόσον το προβλέπει το συγκεκριμένο σχήμα, ενώ η ευρωπαϊκή πιστοποίηση παραμένει καταρχήν εθελοντική εκτός αν ενωσιακή ή εθνική νομοθεσία ορίσει διαφορετικά [19].

Το πρώτο σχήμα που θεσπίστηκε βάσει του πλαισίου είναι το European Common Criteria-based Cybersecurity Certification Scheme (EUCC). Υιοθετήθηκε με τον Εκτελεστικό Κανονισμό (ΕΕ) 2024/482 και εφαρμόζεται από τις 27 Φεβρουαρίου 2025 [20]. Το EUCC διαδέχεται τα σχετικά εθνικά σχήματα που λειτουργούσαν στο πλαίσιο SOG-IS, έχει οριζόντιο χαρακτήρα και βασίζεται στο υποψήφιο σχήμα που εκπόνησε ο ENISA και δημοσίευσε το 2021 [20], [49].

Το EUCC αφορά την πιστοποίηση προϊόντων ΤΠΕ και προφίλ προστασίας. Στο πλαίσιο του σχήματος, οι αρμόδιοι φορείς πιστοποίησης εκδίδουν πιστοποιητικά στα επίπεδα «σημαντικό» και «υψηλό» βάσει των ISO/IEC 15408 και 18045 [20]. Το «σημαντικό» συνδέεται με τις συνιστώσες AVA_VAN.1 ή AVA_VAN.2 και το «υψηλό» με τις AVA_VAN.3 έως AVA_VAN.5 [20]. Η αντιστοίχιση προσδιορίζει το βάθος της ανάλυσης ευπαθειών και το δυναμικό επίθεσης έναντι του οποίου εξετάζεται η ανθεκτικότητα, χωρίς τα επίπεδα του EUCC να ταυτίζονται μηχανικά με τα πακέτα EAL. Η τεχνική αξιολόγηση γίνεται από ITSEF διαπιστευμένο κατά ISO/IEC 17025 και η πιστοποίηση από φορέα διαπιστευμένο κατά ISO/IEC 17065 [20].

Το EUCC καλύπτει τη διατήρηση της διασφάλισης μετά την αρχική πιστοποίηση και προβλέπει καθορισμένη περίοδο ισχύος, με ανώτατο κατά κανόνα όριο πέντε ετών, υποχρεώσεις διαχείρισης και γνωστοποίησης ευπαθειών και διαδικασίες για αλλαγές και ενημερώσεις του προϊόντος [20]. Οι ρυθμίσεις για σειρές προϊόντων, για τη διάκριση μειζόνων και ελασσόνων αλλαγών και για τη συνέχεια διασφάλισης εξειδικεύθηκαν περαιτέρω με τον Εκτελεστικό Κανονισμό (ΕΕ) 2025/2462 [20]. Η διατήρηση, η επανεκτίμηση ή η επαναξιολόγηση εξαρτώνται από την επίδραση της αλλαγής στη δηλωμένη διασφάλιση. Τα πιστοποιητικά, οι εκθέσεις πιστοποίησης και τα σχετικά στοιχεία δημοσιεύονται μέσω του ENISA [20].

Το γενικό πλαίσιο του Cybersecurity Act καλύπτει προϊόντα, υπηρεσίες και διεργασίες, ενώ το EUCC αφορά προϊόντα ΤΠΕ και προφίλ προστασίας [20]. Η διεπαφή που εξετάζεται στο Κεφάλαιο 5 είναι αντικείμενο τύπου υπηρεσίας και σύνθεσης συστατικών και μπορεί να οριοθετηθεί ως ToE για σκοπούς προδιαγραφής και ανάλυσης. Η χρήση της ορολογίας των Common Criteria δεν αρκεί, όμως, για να θεμελιώσει επιλεξιμότητα σε συγκεκριμένο ευρωπαϊκό σχήμα. Η εργασία αξιοποιεί τις έννοιες ToE, Security Target, SFR και SAR για να οργανώσει το όριο, τους στόχους, τις απαιτήσεις και τα τεκμήρια. Δεν υποστηρίζει ότι η διεπαφή είναι αυτομάτως επιλέξιμη για πιστοποίηση EUCC· το σχήμα λειτουργεί ως σημείο αναφοράς και όχι ως ισχυρισμός πραγματικής πιστοποίησης.

3.6 Το έργο CUSTODES

Το CUSTODES («A Certification approach for dynamic, agile and reUSable assessment fOr composite systems of ICT products, services, and processes») είναι έργο Horizon Europe με Grant Agreement 101120684. Συντονίζεται από το RISE και υλοποιείται από κοινοπραξία δεκαεπτά οργανισμών [14]. Αναπτύσσει προσέγγιση αξιολόγησης συμμόρφωσης για σύνθετα προϊόντα και υπηρεσίες ΤΠΕ, με επαναχρησιμοποίηση πληροφοριών πιστοποίησης από επιμέρους δομικούς λίθους και υποστήριξη πολλαπλών επιπέδων διασφάλισης. Περιλαμβάνει επίσης προστατευμένο περιβάλλον εκτέλεσης για τη διαχείριση τεκμηρίων και της αλυσίδας φύλαξης [14]. Η προσέγγιση δοκιμάζεται σε τρεις πιλοτικές εφαρμογές και αποτελεί τη μεθοδολογική και εργαλειολογική αναφορά του Κεφαλαίου 5. Δεν χρησιμοποιείται για τον υπολογισμό κινδύνου, ο οποίος εκτελείται με MONARC στο Κεφάλαιο 4 [14].

Η ανάγκη που εξετάζει το CUSTODES προκύπτει από τη σύνθεση πραγματικών συστημάτων από συστατικά διαφορετικής προέλευσης και κύκλου ζωής. Η αξιολόγηση ενός τέτοιου συνόλου απαιτεί να συνδυάζονται και να επικαιροποιούνται πληροφορίες αξιολόγησης για τους επιμέρους δομικούς λίθους. Η επαναχρησιμοποίηση μπορεί να περιορίσει την επανάληψη ελέγχων, αλλά προϋποθέτει ότι είναι γνωστά η προέλευση, η ισχύς και οι συνθήκες εφαρμογής κάθε τεκμηρίου. Το έργο τοποθετεί αυτή την προσέγγιση στο πλαίσιο του Cybersecurity Act και τη δοκιμάζει μέσω πιλοτικών εφαρμογών σε σύνθετα προϊόντα και υπηρεσίες [19], [14]. Η δυναμική αξιολόγηση δεν καταργεί την ανάγκη ανάλυσης κινδύνου· προϋποθέτει ενημερωμένη εικόνα των απειλών, των ευπαθειών και των αλλαγών του αντικειμένου.

Στη διατριβή, το CUSTODES χρησιμοποιείται για την ετοιμότητα οριοθετημένου υποσυστήματος: προσχέδιο Security Target, απαιτήσεις, αντιστοιχίσεις και αναμενόμενα τεκμήρια. Το αποτέλεσμα δεν είναι πιστοποιητικό ή έκθεση διαπιστευμένου φορέα.

3.7 Κανονιστικό πλαίσιο αναφοράς (Οδηγία NIS2, N. 5160/2024)

Η §2.3.6 εξέτασε τη NIS2, τον Ν. 5160/2024 και την ΚΥΑ 1689/2025 από τη σκοπιά της διαχείρισης κινδύνων. Στην παρούσα ενότητα το ίδιο πλαίσιο εξετάζεται από τη σκοπιά της απόδοξης συμμόρφωσης και του ρόλου που μπορεί να έχει η πιστοποίηση. Η Οδηγία (ΕΕ) 2022/2555 αφορά «βασικές και σημαντικές οντότητες» [4], αλλά το συνθετικό αρχέτυπο gonERP δεν ταξινομείται νομικά σε μία από αυτές τις κατηγορίες. Η NIS2 χρησιμοποιείται μόνο ως πλαίσιο αναφοράς, επειδή η δημόσια διοίκηση περιλαμβάνεται στους τομείς υψηλής κρισιμότητας του Παραρτήματος Ι [4].

Το άρθρο 21 της NIS2 απαιτεί κατάλληλα και αναλογικά τεχνικά, επιχειρησιακά και οργανωτικά μέτρα διαχείρισης κινδύνων· κατά το άρθρο 20, τα μέτρα αυτά εγκρίνονται από τα διοικητικά όργανα, τα οποία εποπτεύουν την εφαρμογή τους και μπορούν να θεωρηθούν υπεύθυνα για παραβάσεις [4]. Η συμμόρφωση πρέπει να μπορεί να τεκμηριώνεται, καθώς η Οδηγία προβλέπει εκ των προτέρων και εκ των υστέρων εποπτικά μέτρα για τις βασικές οντότητες και εκ των υστέρων μέτρα για τις σημαντικές. Οι αρμόδιες αρχές μπορούν να ζητούν πολιτικές, αποτελέσματα ελέγχων, στοιχεία εφαρμογής μέτρων και άλλα τεκμήρια [4]. Η υποχρέωση δεν εξαντλείται, επομένως, στην ύπαρξη καταλόγου μέτρων, αλλά περιλαμβάνει οργανωτική έγκριση, εφαρμογή και δυνατότητα απόδοξης.

Το άρθρο 24 συνδέει ρητά τις απαιτήσεις διαχείρισης κινδύνου με την ευρωπαϊκή πιστοποίηση. Τα κράτη μέλη μπορούν να απαιτούν πιστοποιημένα προϊόντα, υπηρεσίες ή διεργασίες ΤΠΕ για την απόδειξη συμμόρφωσης με συγκεκριμένες απαιτήσεις του άρθρου 21, σύμφωνα με ευρωπαϊκά σχήματα του Κανονισμού (ΕΕ) 2019/881 [19], [4]. Η διάταξη δεν καθιστά κάθε πιστοποίηση υποχρεωτική, αλλά αναγνωρίζει ότι μπορεί να χρησιμοποιηθεί ως μέσο απόδοξης όταν το κράτος μέλος ή άλλο εφαρμοστέο ενωσιακό πλαίσιο το απαιτεί.

Η NIS2 ενσωματώθηκε στην ελληνική έννομη τάξη με τον Ν. 5160/2024 [5]. Το άρθρο 15 του νόμου μεταφέρει τις βασικές υποχρεώσεις μέτρων και τη δυνατότητα χρήσης πιστοποιημένων προϊόντων, υπηρεσιών ή διεργασιών για την απόδειξη συμμόρφωσης. Η ΚΥΑ 1689/2025 εξειδικεύει το εθνικό πλαίσιο σε είκοσι δύο απαιτήσεις κυβερνοασφάλειας [6]. Για τη διατριβή, οι απαιτήσεις αυτές παρέχουν πλαίσιο αναφοράς για την οργανωτική ετοιμότητα του αρχετύπου και για τα μέτρα και τεκμήρια που θα έπρεπε να μπορεί να παρουσιάσει μια υπόχρεη οντότητα, χωρίς να αποτελούν μέθοδο πιστοποίησης ή να μετατρέπουν το αρχέτυπο σε νομικά υπαγόμενη οντότητα. Η πιστοποίηση παραμένει αναγνωρισμένο μέσο απόδοξης μόνο όπου το εφαρμοστέο πλαίσιο επιλέγει να την απαιτήσει.

3.8 Σχέση ανάλυσης επικινδυνότητας και ετοιμότητας προς πιστοποίηση

Η ανάλυση κινδύνου είναι συνεχής οργανωτική διεργασία που ιεραρχεί κινδύνους και υποστηρίζει αντιμετώπιση. Η αξιολόγηση συμμόρφωσης εξετάζει οριοθετημένο αντικείμενο έναντι καθορισμένων απαιτήσεων και παράγει τεκμηριωμένο αποτέλεσμα. Διαφέρουν ως προς χρόνο, φορέα και θεσμική αλυσίδα: τα ISMS πιστοποιούνται μέσω ISO/IEC 17021-1 και 27006-1 [52], [53], ενώ τα προϊόντα Common Criteria αξιολογούνται κατά ISO/IEC 17025 και πιστοποιούνται κατά 17065 [44], [45].

Οι δύο προσεγγίσεις μπορούν να συνδεθούν χωρίς να συγχέονται, καθώς το επίπεδο διασφάλισης ενός ευρωπαϊκού σχήματος πρέπει να είναι ανάλογο με τον κίνδυνο της σκοπούμενης χρήσης [19] και, στο EUCC, συνδέεται με το βάθος της ανάλυσης ευπαθειών μέσω της AVA_VAN [20]. Το CUSTODES εξετάζει δυναμικές και σύνθετες αξιολογήσεις που χρειάζονται ενημερωμένη εικόνα των συστατικών, των ευπαθειών και των αλλαγών τους [14], οπότε η ανάλυση κινδύνου μπορεί να τροφοδοτεί την επιλογή στόχων και απαιτήσεων. Δεν υπάρχει, όμως, αυτόματη αριθμητική μετατροπή μιας τιμής κινδύνου σε επίπεδο διασφάλισης· η επιλογή απαιτεί χωριστή αιτιολόγηση ως προς το αντικείμενο, το περιβάλλον απειλής και το εφαρμοζόμενο σχήμα.

Το έργο CYRENE παρέχει ευρωπαϊκό παράδειγμα σύνδεσης των δύο προσεγγίσεων σε υπηρεσίες εφοδιαστικής αλυσίδας [54]. Το δημόσιο παραδοτέο D2.1 του CYRENE οργανώνει την υπηρεσία σε επιχειρησιακή, τεχνική και τομεακή όψη. Κάθε όψη μπορεί να οριοθετηθεί ως διακριτός ΤοΕ και να αναλυθεί μέσω διεργασιών, εταίρων, υποδομών και περιουσιακών στοιχείων, με αναφορά στις έννοιες των Common Criteria [54]. Η μεθοδολογία περιλαμβάνει τον

προσδιορισμό απαιτήσεων για τους διαφορετικούς ToE και τη δυνατότητα αυτοαξιολόγησης έναντι αυτών, χωρίς να εξομοιώνει την αυτοαξιολόγηση με πιστοποίηση τρίτου μέρους. Το μεταγενέστερο δημόσιο D3.1 συνδυάζει διαδικασία αξιολόγησης συμμόρφωσης με πολυεπίπεδη, τεκμηριοκεντρική εκτίμηση κινδύνου εφοδιαστικής αλυσίδας [55]. Το CYRENE αποτελεί, επομένως, εφαρμοσμένο μεθοδολογικό παράδειγμα κοινής χρήσης της ανάλυσης κινδύνου και της αξιολόγησης συμμόρφωσης, όχι αντιστοίχιση ρήτρας προς ρήτρα μεταξύ προτύπων.

Η μέθοδος Threat, Vulnerability, Risk Analysis (TVRA) του ETSI TS 102 165-1 παρέχει πιο άμεση διαδικαστική σύνδεση [56]. Περιλαμβάνει τον ορισμό του ToE και του περιβάλλοντός του, τους στόχους και τις λειτουργικές απαιτήσεις ασφάλειας, την απογραφή φυσικών, ανθρώπινων και λογικών αγαθών και την αναγνώριση απειλών και ευπαθειών. Το δυναμικό επίθεσης εκτιμάται μέσω παραμέτρων όπως ο απαιτούμενος χρόνος, η τεχνογνωσία, η γνώση του αντικειμένου, η ευκαιρία και ο εξοπλισμός. Χρησιμοποιείται μαζί με το επίπεδο απειλής για την πιθανοφάνεια, ενώ η επίπτωση αποτιμάται χωριστά [56]. Ακολουθούν ο υπολογισμός κινδύνου, η επιλογή αντιμέτρων και η επανάληψη της ανάλυσης ώστε να ληφθούν υπόψη οι αλλαγές που προκαλούν τα αντίμετρα. Το CYRENE χρησιμοποιεί την TVRA στο δικό του πλαίσιο αξιολόγησης και τη συνδέει με απαιτήσεις του ISO/IEC 15408 [54]. Στο συγκεκριμένο αυτό πλαίσιο, οι απαιτήσεις διασφάλισης που παράγονται από την TVRA χρησιμοποιούνται ως ένδειξη του EAL που θα μπορούσε να υποστηρίξει η υλοποίηση του βασικού προτύπου ασφάλειας [54]. Η σχέση δεν αποτελεί γενικό κανόνα ούτε αυτόματη μετατροπή αριθμητικής τιμής κινδύνου σε επίπεδο διασφάλισης. Η τρέχουσα έκδοση της TVRA είναι η V5.3.1 του 2025, ενώ το D2.1 του CYRENE βασίστηκε στην προγενέστερη V5.2.3 [54], [56].

Στην εφαρμογή, το Κεφάλαιο 4 ιεραρχεί κινδύνους με MONARC και το Κεφάλαιο 5 μεταφέρει επιλεγμένα αποτελέσματα στη διεπαφή ηλεκτρονικής τιμολόγησης, ορίζοντας ToE, στόχους, απαιτήσεις και τεκμήρια. Η μεταφορά είναι ιχνηλάσιμη. Ο κίνδυνος καθοδηγεί προτεραιότητες, αλλά δεν αποδεικνύει συμμόρφωση, δεν καθορίζει μηχανικά επίπεδο διασφάλισης και δεν υποκαθιστά αρμόδιο φορέα. Η ετοιμότητα ToE δεν υποκαθιστά τη συνεχή διαχείριση κινδύνων.

Το κεφάλαιο συνέδεσε τις έννοιες αξιολόγησης συμμόρφωσης, διαπίστευσης, Common Criteria, σειράς 17000, Cybersecurity Act, EUCC, CUSTODES και NIS2. Οι συνδέσεις εφαρμόζονται στο Κεφάλαιο 5 και συντίθενται στο Κεφάλαιο 6 για το EE4.

4. Πρακτική Ανάλυση Επικινδυνότητας σε Αρχέτυπο govERP

4.1 Ορισμός και οριοθέτηση του αντιπροσωπευτικού αρχτύπου govERP

Το κεφάλαιο εφαρμόζει τη μεθοδολογία του Κεφαλαίου 2 σε οριοθετημένο αντικείμενο. «Gov-ERP» δηλώνει το πραγματικό δημόσιο πρόγραμμα ως σημείο αναφοράς και «govERP» το συνθετικό αρχέτυπο που αναλύεται.

4.1.1 Το δημόσιο σημείο αναφοράς: το πρόγραμμα Gov-ERP και το σύστημα ΟΠΣΥΔΔ

Οι δημόσιες πηγές διακρίνουν τρία επίπεδα αναφοράς. Πρώτο είναι το πρόγραμμα «Μεταρρύθμιση του Δημοσιονομικού Συστήματος στην Κεντρική Διοίκηση και τη λοιπή Γενική Κυβέρνηση (gov-ERP)». Το έργο εντάσσεται στο «Ελλάδα 2.0», στη Δράση 4.2.8 (16705), με Κωδικό ΟΠΣ ΤΑ 5136212, φορέα ευθύνης το Υπουργείο Εθνικής Οικονομίας και Οικονομικών και φορέα υλοποίησης την Κοινωνία της Πληροφορίας Μ.Α.Ε. Η έναρξη τοποθετείται την 1/10/2021 και ο προϋπολογισμός του Ταμείου Ανάκαμψης ανέρχεται σε 29.087.097 €, επί συνολικού προϋπολογισμού 35.274.247,76 € [9]. Δεύτερο επίπεδο είναι το Ολοκληρωμένο Πληροφοριακό Σύστημα Δημοσιονομικής Διαχείρισης (ΟΠΣΥΔΔ), το οποίο περιγράφεται και ως «Κεντρικό και Ενιαίο Σύστημα Δημοσιονομικής Πολιτικής» [57], [58]. Τρίτο επίπεδο είναι το ΟΠΣΔΠ του Γενικού Λογιστηρίου του Κράτους, του οποίου το ΟΠΣΥΔΔ αποτελεί μετεξέλιξη και τεχνολογική αναβάθμιση [57], [59].

Το δημόσια τεκμηριωμένο λειτουργικό εύρος καλύπτει την κατάρτιση και εκτέλεση του Προϋπολογισμού, τις πληρωμές, το Μεσοπρόθεσμο Πλαίσιο Δημοσιονομικής Στρατηγικής, τη λογιστική, τις προμήθειες, τις αναφορές, τα πάγια και τον Προϋπολογισμό Επιδόσεων [57], [60]. Το σύστημα υποστηρίζει επίσης το Λογιστικό Πλαίσιο Γενικής Κυβέρνησης του π.δ. 54/2018, με λογιστική πλήρους δεδουλευμένης βάσης και αναφορά στα IPSAS [58]. Ο διεθνής διαγωνισμός τέθηκε σε δημόσια διαβούλευση το 2021, με συνολικό προϋπολογισμό 51,522 εκατ. ευρώ και δύο Τμήματα [59]. Η υλοποίηση στηρίζεται στη Συμφωνία-Πλαίσιο 1872/06-05-2022 και στις εκτελεστικές συμβάσεις για τις επιχειρησιακές μελέτες και για τον σχεδιασμό, την υλοποίηση και τη λειτουργία του ΟΠΣΥΔΔ [61]. Η διαλειτουργία με οριζόντια συστήματα του Δημοσίου προβλέπεται μέσω του Κέντρου Διαλειτουργικότητας (ΚΕΔ) [62]. Η ηλεκτρονική τιμολόγηση αναφέρεται ρητά στον τίτλο της Δράσης [9] και, από τον Σεπτέμβριο του 2025, εφαρμόζεται υποχρεωτικά στις προμήθειες του Δημοσίου με τις προβλεπόμενες εξαιρέσεις. Τα τιμολόγια διαβιβάζονται στις αναθέτουσες αρχές μέσω του ΚΕΔ [63], [64].

Τον Ιούλιο 2026 αναφερόταν σταδιακή θέση σε λειτουργία επιμέρους υποσυστημάτων [65]. Οι δημόσιες πηγές διαφωνούν για την ολοκλήρωση, μεταξύ 30/06/2026 και Οκτωβρίου 2026 [9], [62], [65]. Η απόκλιση δεν επηρεάζει το συνθετικό μοντέλο. Η γραφή «Gov-ERP» διατηρείται για το πραγματικό πρόγραμμα.

4.1.2 Αρχή αφαίρεσης και μη-επαναταυτοποίησης

Η σχέση πραγματικού προγράμματος και συνθετικού αρχτύπου είναι μονόδρομη. Από το Gov-ERP/ΟΠΣΥΔΔ αντλούνται μόνο δημοσιευμένα στοιχεία ταυτότητας, αποστολής, λειτουργικού εύρους, θεσμικού πλαισίου και χρηματοδότησης. Ο φορέας, η οργανωτική κατάσταση, η αρχιτεκτονική, τα αγαθά και η στάση ασφάλειας του govERP είναι αφαιρετικές κατασκευές. Δεν περιέχουν εσωτερικά ή επιχειρησιακά ευαίσθητα δεδομένα και δεν επιτρέπουν άμεση ή έμμεση επαναταυτοποίηση.

Η εργασία δεσμεύεται ρητά από τις ακόλουθες δύο δηλώσεις, οι οποίες διατρέχουν το σύνολο των Κεφαλαίων 4 και 5:

Δήλωση πεδίου και καθεστώτος. Η παρούσα εργασία εφαρμόζει τη μεθοδολογία της σε αντιπροσωπευτικό σενάριο κύκλου ζωής υιοθέτησης και λειτουργικής ένταξης δημόσιου ERP δημοσιονομικής και χρηματοοικονομικής διαχείρισης. Το πραγματικό πρόγραμμα Gov-ERP αξιοποιείται αποκλειστικά ως δημόσια τεκμηριωμένο σύστημα

αναφοράς για την κατανόηση του γενικού περιβάλλοντος και όχι ως αντικείμενο επίσημης αξιολόγησης, ελέγχου (audit), πιστοποίησης ή τεχνικού ελέγχου. Ο φορέας εφαρμογής, η οργανωτική κατάσταση και η επιμέρους επιχειρησιακή ροή αποτυπώνονται αφαιρετικά και αντιπροσωπευτικά, χωρίς χρήση εσωτερικών, διαβαθμισμένων ή επιχειρησιακά ευαίσθητων δεδομένων.

Δήλωση χρήσης επαγγελματικής εμπειρίας. Η επαγγελματική εμπειρία του συγγραφέα σε ρόλο βασικού χρήστη (Key User) δημόσιου πληροφοριακού συστήματος αξιοποιείται μόνο για την κατανόηση του πεδίου, τη διαμόρφωση γενικευμένων σεναρίων κινδύνου και την επιλογή αντιπροσωπευτικών περιουσιακών στοιχείων, απειλών, μέτρων και απαιτήσεων τεκμηρίωσης. Δεν περιλαμβάνονται ονόματα φορέων, οργανωτικές λεπτομέρειες, πραγματικά δεδομένα, εσωτερικά έγγραφα ή σχέδια (blueprints), στιγμιότυπα οθόνης, πίνακες δικαιωμάτων πρόσβασης, αρχεία καταγραφής, ευπάθειες, περιστατικά ή οποιαδήποτε πληροφορία θα μπορούσε να οδηγήσει σε ταυτοποίηση πραγματικού συστήματος, υπηρεσίας ή προσώπων.

Το govERP δεν ταξινομείται νομικά ως βασική ή σημαντική οντότητα κατά NIS2 και N. 5160/2024. Το πλαίσιο χρησιμοποιείται μόνο ως φακός οργανωτικής ετοιμότητας, σύμφωνα με την §3.7.

4.1.3 Ο φορέας του αρχετύπου: αντιπροσωπευτική ΓΔΟΥ σε φάση λειτουργικής ένταξης

Ο φορέας του σεναρίου είναι αντιπροσωπευτική ΓΔΟΥ της Κεντρικής Διοίκησης, βάσει του οριζόντιου προτύπου των ν. 4270/2014 και 4622/2019 [66], [67]. Το αρχέτυπο ακολουθεί το κοινό διοικητικό πρότυπο και όχι τις ειδικές εξαιρέσεις που ο ν. 4622/2019 προβλέπει για Υπουργεία στα οποία υπάγονται οι Ένοπλες Δυνάμεις ή τα σώματα ασφαλείας [67], και δεν ταυτίζεται με συγκεκριμένο Υπουργείο. Η εγκύκλιος 14044/27-01-2026 τεκμηριώνει ότι το σύστημα αναφοράς καλύπτει το σύνολο των λειτουργιών οικονομικής υπηρεσίας και διαλειτουργεί με ΔΙΑΥΓΕΙΑ, ΚΗΜΔΗΣ και ΕΣΗΔΗΣ [68]. Το αρχέτυπο αναπαράγει το χαρακτηριστικό αυτό ως δηλωμένη παραδοχή.

Η ΓΔΟΥ τοποθετείται σε φάση υιοθέτησης και λειτουργικής ένταξης, με κινδύνους μετάπτωσης, δικαιωμάτων, εκπαίδευσης και παράλληλης λειτουργίας. Η παραδοχή 80–150 χρηστών βασίζεται σε τυπική διοικητική διάρθρωση [66], [67], δεν αντιστοιχεί σε πραγματικό φορέα και επηρεάζει μόνο τις σεναριακές κλίμακες. Το μοντέλο περιλαμβάνει ιδιοκτήτη συστήματος, υπεύθυνο ασφάλειας, διαχειριστές, βασικούς/τελικούς χρήστες και ανώνυμα τρίτα μέρη υποστήριξης και φιλοξενίας.

4.1.4 Οριοθέτηση: πυρήνας ανάλυσης, κλάδος ηλεκτρονικής τιμολόγησης, εκτός πεδίου

Εντός πεδίου βρίσκεται η γενικευμένη ροή εκκαθάρισης δαπανών. Περιλαμβάνει τη δέσμευση πίστωσης, την παραλαβή παραστατικού, τον έλεγχο, την εκκαθάριση, την ενταλματοποίηση, την πληρωμή και τη λογιστική αποτύπωση. Η ροή αντιστοιχεί στο δημόσια τεκμηριωμένο εύρος του συστήματος αναφοράς [57], [68]. Στο πεδίο περιλαμβάνονται επίσης οι σχετικές διεργασίες, οι χρήστες και οι ρόλοι τους, οι σταθμοί εργασίας, ο έλεγχος πρόσβασης και οι διεπαφές με συστήματα-πηγές.

Η διεπαφή ηλεκτρονικής τιμολόγησης αποτελεί διακριτό κλάδο του αρχετύπου. Μέσω αυτής παραλαμβάνονται τιμολόγια κατά EN 16931, τα οποία δρομολογούνται μέσω PEPPOL και ΚΕΔ και τροφοδοτούν τη ροή εκκαθάρισης [63], [64]. Στο Κεφάλαιο 4 η διεπαφή εξετάζεται ως μέρος του ευρύτερου πεδίου κινδύνου, με δικά της αγαθά και εκθέσεις. Στο Κεφάλαιο 5 το ίδιο υποσύστημα οριοθετείται στενότερα ως αντικείμενο της μελέτης ετοιμότητας προς αξιολόγηση. Έτσι, οι κίνδυνοι που αποτιμώνται στην §4.6 μεταφέρονται ιχνηλάσιμα στο προφίλ απειλών του επόμενου κεφαλαίου.

Εκτός πεδίου βρίσκονται η εσωτερική υλοποίηση και η υποδομή φιλοξενίας, οι οποίες αντιμετωπίζονται ως εξαρτήσεις τρίτου μέρους. Εξαιρούνται επίσης ο μεσοπρόθεσμος δημοσιονομικός σχεδιασμός [57], η διαχείριση εσόδων και το φορολογικό σκέλος, η διαχείριση Αξιολόγηση Κινδύνων Ασφάλειας Πληροφοριών και Οργανωτικής Ετοιμότητας Κρίσιμων Υποδομών Πληροφορικής 36

δημοσίου χρέους και ταμειακών διαθεσίμων [61], η μισθοδοσία μέσω της Ενιαίας Αρχής Πληρωμής [69] και τα λοιπά μη διασυνδεδεμένα συστήματα του φορέα. Οι εξαιρέσεις διατηρούν την ανάλυση εστιασμένη στον δημοσιονομικό πυρήνα. Ο χαρακτηρισμός της υποδομής ως υψηλής κρισιμότητας είναι λειτουργικός και δεν συνιστά νομική υπαγωγή.

4.1.5 Συστατικά στοιχεία του αρχτύπου και τεκμηρίωση πηγών

Ο Πίνακας 4.1 συνοψίζει τα κύρια συστατικά του govERP. Η §4.4 τα μετατρέπει σε πρωτεύοντα και υποστηρικτικά αγαθά και προσθέτει εξαρτήσεις όπως εξυπηρετητές, σταθμούς εργασίας, δίκτυο, αντίγραφα ασφαλείας και προσωπικό.

Πίνακας 4.1. Τα οκτώ συστατικά στοιχεία του αρχτύπου govERP και η συνοπτική περιγραφή τους.

#	Συστατικό στοιχείο	Συνοπτική περιγραφή
1	Ροή δημοσιονομικής εκκαθάρισης	Η γενικευμένη διεργασία εκκαθάρισης δαπανών (πυρήνας ανάλυσης)
2	Λειτουργική ενότητα ERP	Οι εφαρμογές εκτέλεσης προϋπολογισμού, λογιστικής, προμηθειών, παγίων, αποθηκών, αναφορών
3	Αποθετήριο οικονομικών εγγραφών	Το αφαιρετικό αποθετήριο λογιστικών/δημοσιονομικών δεδομένων δεδουλευμένης βάσης, συμπεριλαμβανομένων των στοιχείων προμηθευτών/δικαιούχων (βασικά δεδομένα, τραπεζικοί λογαριασμοί)
4	Διαχείριση ταυτότητας και ρόλων	Λογαριασμοί, ρόλοι, δικαιώματα, αρχή ελάχιστου προνομίου
5	Ίχνη ελέγχου και τεκμήρια	Καταγραφή ενεργειών, ιχνηλασιμότητα, αποδεικτικό υλικό
6	Διεπαφή ηλεκτρονικής τιμολόγησης	Το κανάλι παραλαβής ηλεκτρονικών τιμολογίων μέσω ΚΕΔ (κλάδος-γέφυρα προς Κεφ. 5)
7	Στοιχείο διαλειτουργικότητας	Οι λοιπές διασυνδέσεις με οριζόντια συστήματα της Δημόσιας Διοίκησης και η διεπαφή εκτέλεσης πληρωμών προς το ταμειακό κύκλωμα
8	Υποστήριξη αναδόχου / τρίτου μέρους	Υπηρεσίες υλοποίησης, συντήρησης και φιλοξενίας ως εξαρτήσεις

Ο Πίνακας 4.2 συνδέει κάθε συστατικό με δημόσια πηγή. Όπου η θεμελίωση προκύπτει από γενική πρακτική ERP και όχι από σύστημα-ειδική αναφορά, επισημαίνεται ως αντιπροσωπευτική κατασκευή (Δ).

Πίνακας 4.2. Θεμελίωση κάθε συστατικού του αρχτύπου σε δημόσια πηγή· με Δ σημαίνονται όσα στηρίζονται σε γενική πρακτική συστημάτων ERP και όχι σε σύστημα-ειδική αναφορά.

Συστατικό	Δημόσια θεμελίωση
Ροή εκκαθάρισης	Λειτουργικό εύρος εκτέλεσης/πληρωμών [57]· κάλυψη «του συνόλου των λειτουργιών οικονομικής υπηρεσίας» [68]· κύκλος δαπάνης ν. 4270/2014 [66]
Λειτουργική ενότητα ERP	Ενότητες λογιστικής, προμηθειών, παγίων, αναφορών [57]· σταδιακή θέση σε λειτουργία υποσυστημάτων λογιστικής, αποθηκών, μητρώων παγίων [65]
Αποθετήριο εγγραφών	ΛΠΓΚ/π.δ. 54/2018, δεδουλευμένη βάση, IPSAS [58]· καταγραφή δεσμεύσεων, υποχρεώσεων, παγίων [62]

Συστατικό	Δημόσια θεμελίωση
Ταυτότητα & ρόλοι	Θεσμικός διαχωρισμός καθηκόντων διατάκτη/προϊσταμένου οικονομικών υπηρεσιών (ν. 4270/2014, άρθ. 65) [66]· Δ μηχανισμός ελέγχου πρόσβασης κατά γενική πρακτική
Ίχνη ελέγχου	Στόχοι διαφάνειας και λογοδοσίας του έργου [9]· Δ υλοποίηση κατά γενική πρακτική
Διεπαφή e-invoicing	Ρητή αναφορά στον τίτλο της Δράσης [9]· υποχρεωτικό B2G μέσω ΚΕΔ [63], [64]
Διαλειτουργικότητα	Διασύνδεση με ΔΙΑΥΓΕΙΑ/ΚΗΜΔΗΣ/ΕΣΗΔΗΣ [68]· ΚΕΔ [62]· τήρηση Θησαυροφυλακίου/Ταμειακού Προγραμματισμού από το σύστημα-προκάτοχο [69]· Δ ως αντιπροσωπευτική εξειδίκευση της διεπαφής πληρωμών
Ανάδοχος / τρίτο μέρος	Συμφωνία-Πλαίσιο και εκτελεστικές συμβάσεις υλοποίησης/λειτουργίας [61], [59]

Τέλος, η πειθαρχία πηγών του αρχετύπου κωδικοποιείται στους Πίνακες 4.3 και 4.4, οι οποίοι δεσμεύουν το σύνολο των Κεφαλαίων 4 και 5:

Πίνακας 4.3. Ασφαλείς πηγές του αρχετύπου και η χρήση τους.

Ασφαλείς πηγές (χρησιμοποιούνται)	Χρήση
Δημόσιες πηγές Gov-ERP/ΟΠΣΥΔΔ [9]–[65], [68], [69]	Τεκμηρίωση σημείου αναφοράς και ρεαλιστικότητας αρχετύπου
Πρότυπα ISO/IEC 27005, 27001, 27002 (μέσω δημόσιων/δευτερογενών πηγών)	Μεθοδολογία ανάλυσης, μέτρα, αντιστοιχίσεις (Κεφ. 2, §§4.6–4.8)
Βάση γνώσης MONARC (άδεια CC0)	Κατάλογοι αγαθών, απειλών, ευπαθειών (§§4.4–4.5)
NIS2 / Ν. 5160/2024 (ως πλαίσιο αναφοράς)	Ετοιμότητα, χωρίς νομική ταξινόμηση (§3.7, §§4.8–4.9)
Δημόσια περιγραφή έργου CUSTODES	Μεθοδολογική συγγένεια ετοιμότητας πιστοποίησης (Κεφ. 3, Κεφ. 5)
Γενικευμένη επαγγελματική εμπειρία	Μόνο ως practitioner-informed πλαισίωση (Δήλωση §4.1.2)

Πίνακας 4.4. Πηγές που αποκλείονται από τη συγκρότηση του αρχετύπου.

Μη ασφαλείς πηγές (αποκλείονται ρητά)
Εσωτερικά σχέδια/blueprints, αρχιτεκτονικά διαγράμματα ή παραδοτέα πραγματικού συστήματος
Πραγματικές ροές, παραμετροποιήσεις ή οργανωτικές λεπτομέρειες συγκεκριμένης υπηρεσίας
Ονόματα φορέων, υπηρεσιών, ρόλων ή προσώπων· πίνακες δικαιωμάτων πρόσβασης
Αρχεία καταγραφής, περιστατικά, ευπάθειες, στιγμιότυπα οθόνης πραγματικών συστημάτων
Πραγματικά οικονομικά δεδομένα· κάθε εσωτερικό ή διαβαθμισμένο έγγραφο

Με το πεδίο, τις πηγές και τις παραδοχές καθορισμένα, η ανάλυση προχωρά στο εργαστηριακό περιβάλλον (§4.2), στη μεθοδολογική βάση (§4.3) και στη μοντελοποίηση των αγαθών (§4.4).

4.2 Εργαστηριακό περιβάλλον και εγκατάσταση του MONARC

Η ενότητα καταγράφει το περιβάλλον εκτέλεσης, την εγκατάσταση, την επαλήθευση και τα τεκμήρια αναπαραγωγιμότητας του MONARC.

4.2.1 Επιλογή περιβάλλοντος εκτέλεσης

Ο σταθμός εργασίας ήταν ARM, ενώ οι βασικές διαδρομές MONARC ήταν x86. Η επίσημη εικονική μηχανή και η λύση Windows ARM/WSL2 παρουσίασαν περιορισμούς, ενώ η κοινοτική εικόνα Docker δεν ήταν επίσημη και υστερούσε έκδοση. Διατηρήθηκε μόνο ως εναλλακτική τοπικής επίδειξης μέσω εισαγωγής JSON.

Επιλέχθηκε εικονική μηχανή x86/amd64 Hetzner CX23 στη Γερμανία, με Ubuntu Server 22.04 LTS, ως συνηρητικό και δοκιμασμένο περιβάλλον. Υπήρχε επίσης επίσημη διαδικασία Ubuntu 24.04, άρα η επιλογή δεν οφειλόταν σε ασυμβατότητα [13], [70]. Το MONARC εγκαταστάθηκε επίσημα και φιλοξένησε μόνο συνθετικά δεδομένα.

4.2.2 Εγκατάσταση, επαλήθευση και θωράκιση

Η εγκατάσταση ολοκληρώθηκε στις 4 Ιουλίου 2026 με την επίσημη διαδικασία [70]. Αλλάχθηκαν τα προεπιλεγμένα διαπιστευτήρια, επιβεβαιώθηκε η έκδοση 2.13.4 και η πρόσβαση περιορίστηκε με SSH κλειδί και τείχος προστασίας στις αναγκαίες θύρες.

ID	Asset	Impact	Threat	Vulnerability	Current risk	Treatment	Residual risk
		C I A	Label Prob.	Label Existing controls Qualif.	C I A		
118	Employees	2 4 3	Forging of rights 4	No protection of confidential authentication information	4 32 64 48	Not treated	6
121	Employees	2 4 3	Forging of rights 4	Lack of teleworking rules	4 32 64 48	Not treated	6
131	IT organization	2 4 3	Forging of rights 4	Logical access authorisations are not checked regularly	4 32 64 48	Not treated	6
41	System administrator	3 4 3	Forging of rights 4	No protection of confidential authentication information	4 48 64 48	Not treated	6
44	System administrator	3 4 3	Forging of rights 4	Lack of teleworking rules	4 48 64 48	Not treated	6
108	User workstations	2 4 3	Forging of rights 4	Authorisation management is flawed	4 32 64 48	Not treated	6

Εικόνα 4.1. Επαλήθευση έκδοσης MONARC 2.13.4 (οθόνη About) επί του τελικού μοντέλου των 90 μοναδικών κινδύνων (05/07/2026)· η αντίστοιχη λήψη της ημέρας εγκατάστασης (04/07) περιλαμβάνεται στα τεκμήρια του Παραρτήματος Δ'.

Δημιουργήθηκε η ανάλυση «govERP — Ανάλυση Επικινδυνότητας». Η βάση γνώσης παρέμεινε αγγλική και τα προσαρμοσμένα αντικείμενα ονοματοδοτήθηκαν ελληνικά [13]. Πριν από τη μοντελοποίηση επιβεβαιώθηκε το referential ISO/IEC 27002:2022 με 93 μέτρα, προϋπόθεση της §4.7.

4.2.3 Αναπαραγωγιμότητα, φορητότητα και κύκλος ζωής

Κύριο τεκμήριο αναπαραγωγιμότητας είναι η πλήρης εξαγωγή JSON [13]. Περιλαμβάνει βιβλιοθήκη, προσαρμοσμένα αντικείμενα, επιπτώσεις, βάση γνώσης και βήματα μεθόδου. Ο έλεγχος επιβεβαίωσε MONARC 2.13.4, πέντε πρωτεύοντα αγαθά, 190 τοποθετήσεις στην πρώτη επανάληψη και 93 μέτρα. Η εξαγωγή εισάγεται σε συμβατή εγκατάσταση και αποτελεί αυτοτελές αποτύπωμα του μοντέλου, ανεξάρτητο από τον αναλώσιμο εξυπηρετητή [70].

Με το περιβάλλον επαληθευμένο, η επόμενη ενότητα ορίζει τον μεθοδολογικό συνδυασμό της εφαρμογής.

4.3 Μεθοδολογική βάση: μεθοδολογία CUSTODES και ENISA toolbox

Η εφαρμογή συνδυάζει ISO/IEC 27005 ως πλαίσιο, MONARC για μοντελοποίηση και υπολογισμό, και ENISA toolbox για βαθμονόμηση. Το CUSTODES δεν υπολογίζει κίνδυνο· οργανώνει τη μετάβαση των αποτελεσμάτων στο Κεφάλαιο 5.

4.3.1 Το ISO/IEC 27005:2022 ως πρότυπο-πλαίσιο

Το ISO/IEC 27005:2022 ορίζει τη δομή και την ορολογία της διεργασίας [11]. Η εφαρμογή ακολουθεί αναγνώριση βάσει αγαθών, ξεκινώντας από τα συστατικά της §4.1.5, ενώ η εκτέλεση και τεκμηρίωση πραγματοποιούνται με MONARC.

4.3.2 Η μέθοδος και το εργαλείο MONARC

Το MONARC αποτελεί το κύριο εργαλείο εφαρμογής και παρουσιάστηκε θεωρητικά στις §§2.5.2 και 2.5.5 [13]. Η μέθοδος οργανώνεται σε τέσσερις φάσεις: καθορισμό πλαισίου, μοντελοποίηση πλαισίου, εκτίμηση και αντιμετώπιση κινδύνων, και υλοποίηση και παρακολούθηση [13]. Στην εργασία, τα παραδοτέα των §§4.4–4.8 περιλαμβάνουν τις εξαγωγές JSON/CSV και τα στιγμιότυπα του εργαλείου και της υποδομής. Οι εξαγωγές επιτρέπουν προγραμματιστικό έλεγχο και είναι πληρέστερες από τις τυποποιημένες αναφορές της διεπαφής. Η μοντελοποίηση χρησιμοποιεί δέντρο αντικειμένων. Οι επιπτώσεις ορίζονται στα πρωτεύοντα αγαθά και κληρονομούνται από τα υποστηρικτικά που τα στηρίζουν, με δυνατότητα χειροκίνητης προσαρμογής. Η δομή αντιστοιχεί στη διάκριση πρωτευόντων και υποστηρικτικών αγαθών του ISO/IEC 27005 και στον πίνακα της §4.1.5. Στο εργαλείο ο τύπος «Service» χρησιμοποιείται για πρωτεύον αγαθό που αντιστοιχεί σε διεργασία, ενώ ο τύπος «Information» χρησιμοποιείται για πληροφορία. Η ορολογική αυτή διαφορά δεν μεταβάλλει το περιεχόμενο της ανάλυσης. Οι κίνδυνοι πληροφορίας αποτιμώνται ως προς CIA και οι λειτουργικές συνέπειες μέσω ROLFP. Η τριεπίπεδη ανάγνωση σε τεχνικό, λειτουργικό και θεσμικό επίπεδο αποτελεί ερμηνευτική σύμβαση της εργασίας και ορίζεται στην §4.6. Η βάση γνώσης του MONARC παρέχει αγαθά, απειλές, ευπάθειες και referentials υπό CC0. Η πρώτη επανάληψη χρησιμοποιεί τις προτάσεις της βάσης και ακολουθείται από έλεγχο και εμπλουτισμό με ευθύνη του αναλυτή [13].

4.3.3 Εναρμόνιση με το οικοσύστημα ENISA

Το ENISA toolbox χρησιμοποιείται ως κοινή αναφορά και όχι ως αυτοτελής μέθοδος [12]. Οι κλίμακες MONARC συγκρίνονται με τις κλίμακες του toolbox, ενώ το Compendium εντάσσει το MONARC σε ευρωπαϊκό πλαίσιο διαλειτουργικότητας μαζί με ISO/IEC 27005, NIST και άλλες μεθόδους [36]. Η αναγνώριση απειλών αξιοποιεί επίσης το ENISA Threat Landscape 2025 [71].

4.3.4 Η μεθοδολογική συγγένεια με το CUSTODES και η γέφυρα προς το Κεφάλαιο 5

Το CUSTODES αποτελεί τη μεθοδολογική αναφορά του άξονα ετοιμότητας [14], όχι μέρος του υπολογισμού του Κεφαλαίου 4. Η συμβολή του είναι σχεδιαστική: η διεπαφή ηλεκτρονικής τιμολόγησης διατηρείται ως διακριτός κλάδος, ώστε οι τιμές της §4.6 να τροφοδοτήσουν το ToE,

το προφίλ απειλών και τις απαιτήσεις του Κεφαλαίου 5. Η ακολουθία είναι «κίνδυνος → αντικείμενο αξιολόγησης → απαιτήσεις» (§3.8). Χρησιμοποιείται μόνο δημόσια τεκμηρίωση [14].

Η συνολική αντιστοίχιση προτύπου, μεθόδου και δομής του κεφαλαίου συνοψίζεται στον Πίνακα 4.5:

Πίνακας 4.5. Αντιστοίχιση των σταδίων του ISO/IEC 27005:2022, των φάσεων του MONARC και των ενοτήτων του κεφαλαίου.

Στάδιο ISO/IEC 27005:2022	Φάση MONARC	Ενότητες εργασίας
Καθιέρωση πλαισίου	1. Καθορισμός πλαισίου	§4.1 (αρχέτυπο), §4.2 (περιβάλλον), §4.3 (μέθοδος)
Αναγνώριση κινδύνων	2. Μοντελοποίηση πλαισίου	§4.4 (αγαθά/εξαρτήσεις), §4.5 (απειλές/ευπάθειες)
Ανάλυση & αξιολόγηση κινδύνων	3. Εκτίμηση και αντιμετώπιση — σκέλος εκτίμησης	§4.6 (επίπεδα κινδύνου)
Αντιμετώπιση κινδύνων	3. Εκτίμηση και αντιμετώπιση — σκέλος αντιμετώπισης	§4.7 (μέτρα ISO/IEC 27002:2022), §4.8 (αποκλίσεις έναντι ISO/IEC 27001)
Παρακολούθηση & επανεξέταση	4. Υλοποίηση και παρακολούθηση	§4.9 (αποτίμηση οργανωτικής ετοιμότητας για μελλοντική υλοποίηση και παρακολούθηση)*

Σημείωση: Η αντιστοίχιση της §4.9 είναι ερμηνευτική. Η ενότητα δεν υλοποιεί ούτε παρακολουθεί δικλίδες, αλλά αποτιμά την οργανωτική ικανότητα που θα απαιτούσε μελλοντική υλοποίηση και παρακολούθηση.

Η §4.4 εφαρμόζει το παραπάνω σχήμα στη μοντελοποίηση των αγαθών και των εξαρτήσεων.

4.4 Μοντελοποίηση περιουσιακών στοιχείων και εξαρτήσεων

Η ενότητα περιγράφει τη μοντελοποίηση που εκτελέστηκε στις 4 Ιουλίου 2026. Ο πίνακας της §4.1.5 μετατρέπεται σε αντικείμενα του MONARC, αποτιμώνται οι επιπτώσεις των πρωτευόντων αγαθών και συγκροτείται το δέντρο εξαρτήσεων. Ακολουθεί η πρώτη αναγνώριση κινδύνων από τη βάση γνώσης. Τα αριθμητικά μεγέθη ελέγχθηκαν τόσο στη διεπαφή όσο και στην εξαγωγή της §4.2.3.

4.4.1 Από τα συστατικά του αρχέτυπου στα αντικείμενα του εργαλείου

Το MONARC επιτρέπει έναν μόνο τύπο για κάθε πρωτεύον αγαθό: Information ή Service. Η διεπαφή ηλεκτρονικής τιμολόγησης έχει διπλή φύση, επειδή περιλαμβάνει τόσο τη διεργασία παραλαβής και επικύρωσης όσο και το περιεχόμενο του τιμολογίου. Για τον λόγο αυτό μοντελοποιήθηκε ως δύο πρωτεύοντα αγαθά. Το P3a, τύπου Service, εκφράζει τη διεργασία παραλαβής και επικύρωσης. Το P3b, τύπου Information, εκφράζει το περιεχόμενο του τιμολογίου. Η διάσπαση διαχωρίζει τη διαθεσιμότητα του καναλιού από την ακεραιότητα και την αυθεντικότητα του περιεχομένου. Τα δύο αγαθά παράγουν από κοινού το προφίλ κινδύνου που μεταφέρεται στο Κεφάλαιο 5. Ο Πίνακας 4.6 αποδίδει την αντιστοίχιση συστατικών και αντικειμένων.

Με αυτή τη διάσπαση, τα οκτώ συστατικά της §4.1.5 αποτυπώνονται σε πέντε πρωτεύοντα και δεκαπέντε υποστηρικτικά αντικείμενα. Επτά υποστηρικτικά αντικείμενα δημιουργήθηκαν ειδικά για την ανάλυση (S1–S5, N1, N2) και οκτώ προέρχονται από τη βιβλιοθήκη της βάσης γνώσης.

Πίνακας 4.6. Από τα συστατικά της §4.1.5 στα αντικείμενα του MONARC: πρωτεύοντα και υποστηρικτικά αγαθά.

Συστατικό (§4.1.5)	Αντικείμενα εργαλείου
1 — Ροή δημοσιονομικής εκκαθάρισης	P1 (Service)
2 — Λειτουργική ενότητα ERP	S1 — Εφαρμογή ERP (ενότητες), S2 — ΣΔΒΔ/Βάση δεδομένων
3 — Αποθετήριο οικονομικών εγγραφών	P2 (Information)
4 — Διαχείριση ταυτότητας και ρόλων	S4 — Μηχανισμός ταυτότητας & ρόλων (IAM)· η οργανωσιακή διάσταση (πολιτικές, θεσμικός διαχωρισμός) μέσω του αντικειμένου IT organization
5 — Ίχνη ελέγχου και τεκμήρια	P4 (Information) + S5 — Μηχανισμός καταγραφής (logging)
6 — Διεπαφή ηλεκτρονικής τιμολόγησης	P3a (Service) + P3b (Information) + S3 — Λογισμικό διεπαφής e-invoicing & επικύρωση + N1 — Κανάλι ΚΕΔ/PEPPOL, πιστοποιητικά & κλειδιά υπογραφής
7 — Στοιχείο διαλειτουργικότητας	N2 — Διεπαφές ΔΙΑΥΓΕΙΑ/ΚΗΜΔΗΣ/ΕΣΗΔΗΣ & ταμειακού κυκλώματος
8 — Υποστήριξη αναδόχου/τρίτου μέρους	Specific software maintenance (υπηρεσίες αναδόχου)· Server management (υποδομή τρίτου παρόχου)
Οριζόντια υποστηρικτικά (§4.1.5, τελ. παράγραφος)	Network and Telecom, User workstations, Employees, System administrator, Backup management

4.4.2 Πρωτεύοντα αγαθά και αποτίμηση επιπτώσεων

Στο MONARC η επίπτωση κάθε κριτηρίου CIA προκύπτει από τις πέντε διαστάσεις ROLFP: φήμη, λειτουργία, νομικές συνέπειες, οικονομικές συνέπειες και επίπτωση σε φυσικά πρόσωπα [13]. Κάθε διάσταση αποτιμάται σε κλίμακα 0–4 και η τελική τιμή του κριτηρίου είναι το μέγιστο. Έτσι, κάθε τιμή συνδέεται με τη βαρύτερη συνέπεια που αιτιολογήθηκε για το συγκεκριμένο αγαθό.

Οι προεπιλεγμένες περιγραφές ROLFP χρησιμοποιούν ιδιωτικοοικονομικό λεξιλόγιο, όπως «εταιρεία», «πελάτες» και «έσοδα από πωλήσεις». Για το govERP μεταφράστηκαν αναλογικά σε δημόσιο θεσμικό πλαίσιο. Ενδεικτικά, η καταδίκη εταιρείας αποδόθηκε ως πειθαρχική ή ποινική ευθύνη οργάνου ή υπαλλήλου, οι πελάτες ως πολίτες, προμηθευτές και δικαιούχοι, και τα έσοδα ως διαχειριζόμενες πιστώσεις. Η διατακτική κλίμακα 0–4 και οι αριθμητικές τιμές δεν μεταβλήθηκαν. Ο πλήρης πίνακας είναι ο Πίνακας Α'.1 του Παραρτήματος Α'. Για τα κελιά που καθορίζουν το μέγιστο χρησιμοποιήθηκε χωριστό θεσμικό ή τεχνικό επιχείρημα. Όταν δύο γειτονικές βαθμίδες ήταν αμφότερες εύλογες και δεν επηρέαζαν το μέγιστο, επιλέχθηκε η τιμή που στηριζόταν σαφέστερα στους ορισμούς της κλίμακας.

Με αυτό το πλαίσιο, οι αποτιμήσεις των πέντε πρωτευόντων αγαθών παρουσιάζονται στον Πίνακα 4.7:

Πίνακας 4.7. Τα πέντε πρωτεύοντα αγαθά (P1, P2, P3a, P3b, P4) και οι αποτιμήσεις επιπτώσεων C//A.

ID	Πρωτεύον αγαθό	Τύπος	Συστατικό	C	I	A
P1	Ροή δημοσιονομικής εκκαθάρισης	Service	#1	2	4	3
P2	Δημοσιονομικές/λογιστικές εγγραφές & στοιχεία προμηθευτών-δικαιούχων	Information	#3	3	4	3
P3a	Διεργασία παραλαβής και επικύρωσης ηλεκτρονικού τιμολογίου	Service	#6	2	3	3
P3b	Περιεχόμενο ηλεκτρονικού τιμολογίου	Information	#6	3	4	2
P4	Ίχνη ελέγχου & τεκμήρια	Information	#5	2	4	2

Για το P1, η ακεραιότητα είναι το κρίσιμότερο κριτήριο. Η παράκαμψη ελέγχου ή η μη εξουσιοδοτημένη αλλαγή ποσού ή σειράς εγκρίσεων παραβιάζει τον διαχωρισμό καθηκόντων του άρθρου 65 του ν. 4270/2014 [66], επομένως I=4. Η διακοπή της ροής μπορεί να ακινητοποιήσει ολόκληρη οργανική μονάδα, οπότε A=3. Η εμπιστευτικότητα της διεργασίας αποτιμάται χαμηλότερα, με C=2. Ο αναλυτικός πίνακας του P1 είναι ο Πίνακας 4.8.

Πίνακας 4.8. Αναλυτική αποτίμηση επιπτώσεων του πρωτεύοντος αγαθού P1 κατά τις κλίμακες ROLFP, με τη μέγιστη τιμή ανά κριτήριο.

P1	Reputation	Operational	Legal	Financial	Personal	Max
Confidentiality	0	0	2	1	0	2
Integrity	2	2	4	3	0	4
Availability	1	3	1	2	0	3

The screenshot shows the 'Edit impacts' dialog for the primary asset P1 (Public financial statement flow). The dialog contains a table of consequences with the following data:

	Reputation	Operational	Legal	Financial	Personal	Max
Confidentiality	0	0	2	1	0	2
Integrity	2	2	4	3	0	4
Availability	1	3	1	2	0	3

The background interface shows a risk analysis dashboard with a list of risks and their current and residual risk levels. The risks are categorized by type (Information, Operational) and their impact on the primary asset P1.

Εικόνα 4.2. Οθόνη αποτίμησης επιπτώσεων (Edit impacts) του πρωτεύοντος αγαθού P1 — οι καταχωρισμένες τιμές ταυτίζονται κελί προς κελί με τον Πίνακα 4.8.

Οι τελικές τιμές και οι κύριες αγκυρώσεις και των πέντε πρωτευόντων αγαθών παρατίθενται συγκεντρωτικά στο Παράρτημα Β'.

Για το P2, το επίπεδο εμπιστευτικότητας C=3 συνδέεται με στοιχεία προμηθευτών και δικαιούχων, όπως βασικά δεδομένα και τραπεζικοί λογαριασμοί. Η επιλογή στηρίζεται στις Αξιολόγηση Κινδύνων Ασφάλειας Πληροφοριών και Οργανωτικής Ετοιμότητας Κρίσιμων Υποδομών Πληροφορικής 43

περιγραφές της κλίμακας και στο πλαίσιο προστασίας προσωπικών δεδομένων [72], [73]. Το επίπεδο 4 αφορά διαβαθμισμένες πληροφορίες, τις οποίες το αρχέτυπο δεν περιλαμβάνει. Η ακεραιότητα είναι $I=4$, επειδή αλλοίωση λογιστικών εγγραφών ή στοιχείων πληρωμής μπορεί να οδηγήσει σε πλαστογραφία ή αχρεώστητη καταβολή. Η μη διαθεσιμότητα ακινητοποιεί τη λογιστική λειτουργία, οπότε $A=3$.

Τα P3a και P3b αποτυπώνουν διαφορετικές όψεις της ηλεκτρονικής τιμολόγησης. Για το P3a, η διαθεσιμότητα είναι $A=3$, επειδή η πτώση της διεπαφής διακόπτει ένα κρίσιμο κανάλι εισροής αλλά όχι το σύνολο των υπηρεσιών. Για το P3b, η ακεραιότητα είναι $I=4$, επειδή πλαστό ή αλλοιωμένο τιμολόγιο μπορεί να τροφοδοτήσει δημόσια πληρωμή. Οι ιδιότητες αυθεντικότητας και μη αποποίησης μεταφέρονται στο αντικείμενο του Κεφαλαίου 5. Η υψηλή έκθεση της δημόσιας διοίκησης σε επιθέσεις άρνησης υπηρεσίας [71] δεν αυξάνει την επίπτωση του P3a. Αποτυπώνεται στην πιθανοφάνεια της απειλής, ώστε να αποφεύγεται διπλομέτρηση.

Τέλος, για το P4 η ακεραιότητα ταυτίζεται με τη λογοδοσία ($I=4$): η αλλοίωση ιχνών ελέγχου ισοδυναμεί με συγκάλυψη ή παραποίηση αποδεικτικού υλικού και καταστρέφει τη δυνατότητα καταλογισμού. Η εμπιστευτικότητα ($C=2$) συνυπολογίζει ότι τα ίχνη αποτυπώνουν ενέργειες ταυτοποιήσιμων υπαλλήλων, ενώ η προσωρινή μη διαθεσιμότητα καθυστερεί ελέγχους χωρίς να διακόπτει λειτουργία ($A=2$).

4.4.3 Υποστηρικτικά αγαθά, δέντρο εξαρτήσεων και πρώτη επανάληψη αναγνώρισης

Τα δεκαπέντε υποστηρικτικά αγαθά τοποθετήθηκαν κάτω από τα πρωτεύοντα που στηρίζουν. Τα αγαθά που εξυπηρετούν περισσότερα από ένα πρωτεύοντα ορίστηκαν ως Global και αξιολογούνται μία φορά για ολόκληρη την ανάλυση [13]. Μόνο ο μηχανισμός καταγραφής S5 ορίστηκε ως Local, επειδή ανήκει ειδικά στον κλάδο των ιχνών ελέγχου. Ο Πίνακας 4.9 δείχνει τις προσαρτήσεις και τον αριθμό κινδύνων κάθε υποδέντρου. Οι μετρητές επαληθεύτηκαν έναντι των αναμενόμενων αθροισμάτων.

Πίνακας 4.9. Προσαρτήσεις υποστηρικτικών αγαθών ανά πρωτεύον και αριθμός κινδύνων κάθε υποδέντρου στην πρώτη επανάληψη.

Πρωτεύον	Προσαρτημένα υποστηρικτικά	Κίνδυνοι 1ης επανάληψης
P1	S1, S4, N2, Network and Telecom, Server management, User workstations, Employees, System administrator, IT organization, Specific software maintenance	61
P2	S1, S2, S4, Server management, Network and Telecom, Backup management, System administrator, Specific software maintenance	43
P3a	S3, S4, N1, Network and Telecom, Server management, User workstations, Employees	42
P3b	S3, S2, N1, Backup management	18
P4	S5, S2, S4, Backup management, System administrator	26

Οι επιπτώσεις ορίζονται στα πρωτεύοντα αγαθά και κληρονομούνται από τα υποστηρικτικά σε κάθε τοποθέτηση. Για παράδειγμα, το S3 κληρονομεί 2/3/3 κάτω από το P3a και 3/4/2 κάτω από το P3b. Ο ίδιος μηχανισμός ισχύει για το N1. Οι 190 εγγραφές του πίνακα είναι τοποθετήσεις ανά γονέα, ενώ οι μοναδικές αξιολογήσεις της πρώτης επανάληψης είναι 85. Κάθε Global αγαθό αξιολογείται μία φορά και το Local S5 χωριστά. Η διάκριση αυτή μειώνει τις επαναλαμβανόμενες αξιολογήσεις [13].

Με την τοποθέτηση των αγαθών, η βάση γνώσης πρότεινε τα προκαθορισμένα σύνολα κινδύνων για κάθε τύπο. Προτάθηκαν έξι γραμμές ανά αγαθό λογισμικού, τέσσερις ανά δικτυακό αντικείμενο, οκτώ για διαχείριση εξυπηρετητών και σταθμούς εργασίας, έξι για προσωπικό και διαχειριστές, οκτώ για την οργάνωση πληροφορικής, πέντε για συντήρηση τρίτου μέρους και δύο Αξιολόγηση Κινδύνων Ασφάλειας Πληροφοριών και Οργανωτικής Ετοιμότητας Κρίσιμων Υποδομών Πληροφορικής 44

για αντίγραφα ασφαλείας. Η πρώτη αυτή επανάληψη είναι αφετηρία και όχι τελικός έλεγχος πληρότητας [13]. Η §4.5 συγκρίνει τις προτάσεις με το ευρωπαϊκό τοπίο απειλών και προσθέτει ό,τι λείπει.

Τα στιγμιότυπα του N1 κάτω από τα P3a και P3b τεκμηριώνουν την κληρονόμηση ανά γονέα. Το συγκεντρωτικό μητρώο της §4.6 δείχνει τις 90 τελικές γραμμές, ενώ η πρώτη εξαγωγή JSON διατηρεί την αρχική κατάσταση των 85.

Η πρώτη επανάληψη ολοκληρώθηκε με πέντε πρωτεύοντα αγαθά, δεκαπέντε υποστηρικτικά και 85 μοναδικές γραμμές κινδύνου. Η §4.5 ελέγχει τις απειλές και τις ευπάθειες αυτού του μοντέλου.

4.5 Αναγνώριση απειλών και ευπαθειών: εσκεμμένες, τυχαίες και περιβαλλοντικές απειλές

Η ενότητα παρουσιάζει την αναγνώριση που εκτελέστηκε στις 5 Ιουλίου 2026. Οι απειλές της πρώτης επανάληψης ταξινομούνται κατά προέλευση, συγκρίνονται με το ENISA Threat Landscape 2025 και λαμβάνουν τιμές πιθανοφάνειας. Ακολουθεί έλεγχος πληρότητας, στοχευμένος εμπλουτισμός και εξέταση των ευπαθειών. Τα αριθμητικά μεγέθη ελέγχθηκαν στην εξαγωγή και όχι μόνο στη διεπαφή.

4.5.1 Το τοπίο απειλών της πρώτης επανάληψης και η τριμερής τυπολογία

Κάθε γραμμή κινδύνου στο MONARC συνδέει ένα αγαθό, μία απειλή και μία ευπάθεια. Με την τοποθέτηση των υποστηρικτικών αγαθών δημιουργήθηκε επομένως και ο αρχικός κατάλογος απειλών. Στις 190 τοποθετήσεις, που αντιστοιχούν σε 85 μοναδικές γραμμές, συμμετείχαν 13 από τις 30 απειλές της βάσης γνώσης [13]. Οι υπόλοιπες δεν προτάθηκαν από τους τύπους αγαθών του μοντέλου. Ο έλεγχος της §4.5.3 εντόπισε μία τεκμηριωμένη ανάγκη προσθήκης.

Το πρόθεμα του αναγνωριστικού δηλώνει την προέλευση της απειλής [13], [11]. Το MD αντιστοιχεί σε εσκεμμένη, το MA σε τυχαία, το MDA σε εσκεμμένη ή τυχαία και το ME σε περιβαλλοντική προέλευση. Στις εσκεμμένες απειλές ανήκουν η κατάχρηση ταυτότητας και δικαιωμάτων (MD14), η υποκλοπή (MD15), η άρνηση ενεργειών (MD24) και η κλοπή ή καταστροφή μέσων και εξοπλισμού (MD36). Η MD14 είναι η συχνότερη, με 53 τοποθετήσεις. Στις τυχαίες ανήκουν το σφάλμα χρήσης (MA11), η δυσλειτουργία λογισμικού (MA15) και η αστοχία εξοπλισμού (MA16). Στις απειλές διττής προέλευσης ανήκουν η αποκάλυψη πληροφοριών (MDA20), το κακόβουλο λογισμικό (MDA13), η κατάχρηση δικαιωμάτων (MDA17), η απώλεια διαθεσιμότητας προσωπικού (MDA28), η ανάκτηση από απορριφθέντα μέσα (MDA12) και η απώλεια συντηρησιμότητας (MDA25).

Οι περιβαλλοντικές απειλές ME11–ME18 δεν μοντελοποιήθηκαν ως αυτοτελή σενάρια στο επίπεδο του φορέα. Η φυσική υποδομή φιλοξενείται από κεντρικό πάροχο και βρίσκεται εκτός του άμεσου ελέγχου της ΓΔΟΥ. Η επιχειρησιακή ευθύνη αντιμετώπισης των φυσικών και περιβαλλοντικών συμβάντων ανήκει επομένως στον πάροχο. Ο κίνδυνος δεν εξαφανίζεται. Αποτυπώνεται ως εξάρτηση από τρίτο μέρος και ως ζήτημα επιχειρησιακής συνέχειας μέσω των αγαθών διαχείρισης εξυπηρετητών και συντήρησης. Η οριοθέτηση αποτελεί συνειδητή επιλογή του μοντέλου.

Το χωριστό μητρώο Operational Risks του MONARC παρέμεινε κενό. Η βάση γνώσης δεν προτείνει αυτόματα γραμμές σε αυτό το μητρώο και η εφαρμογή αποτίμησε τις διεργασίες τύπου Service μέσω των επιπτώσεων και των κινδύνων πληροφορίας του υποστηρικτικού δέντρου. Η επιλογή επαληθεύτηκε τόσο στη ρίζα όσο και στα πέντε πρωτεύοντα αγαθά και τεκμηριώνεται στο στιγμιότυπο του Παραρτήματος Δ'. Αποτελεί περιορισμό της εφαρμογής: οι λειτουργικοί κίνδυνοι αποτυπώνονται έμμεσα και όχι σε χωριστό μητρώο του εργαλείου.

Το κενό μητρώο τεκμηριώνεται οπτικά στο σχετικό στιγμιότυπο (kef4_operational_keno — βλ. Παράρτημα Δ').

4.5.2 Ευθυγράμμιση με το ENISA Threat Landscape 2025 και πιθανοφάνειες απειλών

Η αναγνώριση συγκρίθηκε με το ENISA Threat Landscape 2025 [71]. Η δημόσια διοίκηση ήταν ο πλέον στοχευόμενος τομέας, με 38% των συμβάντων, και η εικόνα της κυριαρχούνταν από DDoS χακτιβιστικής προέλευσης. Η κοινωνική μηχανική και το phishing αποτελούσαν το κύριο σημείο εισόδου, περίπου στο 60% των παρατηρήσεων. Το 68,6% των εισβολών κατέληγε σε διαρροή δεδομένων. Ransomware, τραπεζικά trojans και infostealers αντιστοιχούσαν στο 87,3% του κακόβουλου κώδικα μετά από εισβολή, ενώ η κλοπή διαπιστευτηρίων αντιστοιχούσε στο 8,9% των εισβολών [71]. Με βάση αυτά τα στοιχεία, κάθε απειλή έλαβε τιμή πιθανοφάνειας 0–4. Οι τιμές είναι κρίσεις για το συνθετικό σενάριο και δεν υπολογίζονται απευθείας από τα ευρωπαϊκά ποσοστά. Ο Πίνακας 4.10 συγκεντρώνει τις απειλές και τις τιμές τους.

Πίνακας 4.10. Οι δεκατρείς απειλές της πρώτης επανάληψης, με προέλευση, τοποθετήσεις, τιμή πιθανοφάνειας T και άγκυρα τεκμηρίωσης έναντι του ENISA Threat Landscape 2025.

Κωδ.	Απειλή	Προέλευση	Τοποθ.	T	Άγκυρα τεκμηρίωσης
MD14	Forging of rights	Εσκ.	53	4	Phishing/κοινωνική μηχανική κύριο σημείο εισόδου (~60%)· κλοπή διαπιστευτηρίων 8,9%· ΔΔ ο πλέον στοχευόμενος τομέας (38%)
MDA20	Disclosure	Εσκ./Τυχ.	25	3	68,6% των εισβολών κατέληξαν σε διαρροή δεδομένων
MD15	Eavesdropping	Εσκ.	24	2	Προϋποθέτει προνομιακή θέση/πρόσβαση δικτύου· δεν αναδεικνύεται ως κύριος φορέας
MA11	Error in use	Τυχ.	18	3	Τυπολογική· επιτεινόμενη στη φάση λειτουργικής ένταξης (νέο σύστημα, εκπαίδευση σε εξέλιξη — §4.1.3)
MD24	Denial of actions	Εσκ.	16	2	Εσωτερικής φύσης· ο insider ως φορέας στο 0,8%
MA16	Equipment malfunction or failure	Τυχ.	12	3	Τυπολογική· τυχαία τεχνική αστοχία, εκτός πεδίου μέτρησης του ETL
MDA13	Malware infection	Εσκ./Τυχ.	12	4	Ransomware/τραπεζικά trojans/infostealers 87,3% του κακόβουλου κώδικα κατόπιν εισβολής· η ΔΔ σταθερός στόχος
MDA17	Abuse of rights	Εσκ./Τυχ.	8	2	Εσωτερικής φύσης· ο insider ως φορέας στο 0,8%
MA15	Software malfunction	Τυχ.	6	3	Τυπολογική· επιτεινόμενη σε φάση παραμετροποίησης/ένταξης
MDA28	Breach of personnel availability	Εσκ./Τυχ.	5	2	Στελέχωση θέσεων-κλειδιών· κατά κανόνα τυχαίας εκδήλωσης
MDA12	Retrieval of recycled or discarded media	Εσκ./Τυχ.	5	2	Διαδικαστικής φύσης· περιστασιακή
MD36	Theft or destruction of media, documents or equipment	Εσκ.	4	2	Φυσική διάσταση· η κεντρική φιλοξενία τρίτου περιορίζει την έκθεση του φορέα
MDA25	Breach of information system maintainability	Εσκ./Τυχ.	2	2	Οργανωσιακής φύσης· η ουσία της αποτυπώνεται πρωτίστως στη βαθμονόμηση ευπαθειών (§4.6)

(Εσκ. = εσκεμμένη, Τυχ. = τυχαία προέλευση· «Τοποθ.» = τοποθετήσεις ανά γονέα, κατά τη διπλή ανάγνωση της §4.4.3 — άρθροισμα 190.)

Ο πίνακας συνοδεύεται από δύο επιφυλάξεις. Πρώτον, το ENISA Threat Landscape βασίζεται σε καταγεγραμμένα συμβάντα και τεκμηριώνει κυρίως εσκεμμένες ή διττής προέλευσης απειλές. Για τις τυχαίες τεχνικές απειλές MA15 και MA16 χρησιμοποιήθηκε τυπολογική αγκύρωση [11] και η παραδοχή της φάσης λειτουργικής ένταξης. Η παραμετροποίηση και η εκπαίδευση σε εξέλιξη αυξάνουν εύλογα τα σφάλματα χρήσης και τις δυσλειτουργίες λογισμικού. Δεύτερον, καμία απειλή Αξιολόγηση Κινδύνων Ασφάλειας Πληροφοριών και Οργανωτικής Ετοιμότητας Κρίσιμων Υποδομών Πληροφορικής 46

δεν έλαβε πιθανοφάνεια κάτω από 2. Η επιλογή είναι συντηρητική και συνεπής με τη βαθμονόμηση της §4.4.2.

Ο οδηγός του πρώτου βήματος της φάσης καταγράφει ποιοτικά στοιχεία και δεν περιλαμβάνει αριθμητικά πεδία. Οι τιμές πιθανοφάνειας και οι βαθμίδες ευπάθειας καταχωρίστηκαν απευθείας στις 85 μοναδικές γραμμές του μητρώου. Το MONARC αποθηκεύει την τιμή στο επίπεδο του Global αγαθού και τη διαχέει στις τοποθετήσεις του. Έτσι διατηρείται ενιαία τιμή για την ίδια τριάδα αγαθού, απειλής και ευπάθειας [13]. Η εξαγωγή επιβεβαίωσε ότι και οι 16 τελικές απειλές είχαν ομοιόμορφη τιμή σε όλες τις εμφανίσεις τους.

4.5.3 Έλεγχος πληρότητας: το κενό άρνησης υπηρεσίας και ο στοχευμένος εμπλουτισμός

Η πρώτη επανάληψη δεν περιλάμβανε καμία απειλή άρνησης υπηρεσίας, παρότι το ENISA Threat Landscape 2025 αναδεικνύει τα DDoS ως κυρίαρχο εύρημα για τη δημόσια διοίκηση [71]. Στον τομέα αυτό το 96,2% της εικόνας απειλών αποδιδόταν σε χακτιβιστικά DDoS, ενώ μία ομάδα συγκέντρωνε το 66,7% της σχετικής δραστηριότητας. Συνολικά, οι επιθέσεις DDoS αντιστοιχούσαν στο 76,7% των καταγεγραμμένων συμβάντων [71]. Τα ποσοστά τεκμηριώνουν την επικαιρότητα της κατηγορίας και όχι τη συχνότητα επί του συγκεκριμένου αγαθού. Η πιθανοφάνεια του E1 βασίστηκε επιπλέον στο ότι τα εξωτερικά κανάλια είναι σημεία εισόδου υποχρεωτικών ροών. Η σχετική απειλή MDA16 υπήρχε στη βάση γνώσης, αλλά δεν είχε προταθεί από τους τύπους αγαθών της πρώτης επανάληψης.

Το κενό DDoS καλύφθηκε με την προσθήκη E1. Οι E2 και E3 προστέθηκαν σε χωριστό βήμα, όχι ως πρόσθετα κενά του ελέγχου πληρότητας. Αποτελούν προδηλωμένο εμπλουτισμό για το αντικείμενο του Κεφαλαίου 5 και καλύπτουν αυθεντικότητα, μη αποποίηση και ακεραιότητα. Κάθε προσθήκη δημιουργήθηκε ως specific risk και συνδέθηκε υποχρεωτικά με απειλή και ευπάθεια της βάσης γνώσης. Οι ειδικές γραμμές δεν λαμβάνουν αυτόματη χαρτογράφηση στο ISO/IEC 27002:2022. Η αντιστοίχισή τους γίνεται χειροκίνητα στην §4.7. Ο Πίνακας 4.11 αποδίδει τις τρεις προσθήκες.

Εικόνα 4.3. Ο διάλογος δημιουργίας ειδικού κινδύνου («+ Create a specific risk») με τα δύο υποχρεωτικά πεδία επιλογής από τους καθολικούς καταλόγους της βάσης γνώσης — στο στιγμιότυπο, η δημιουργία της προσθήκης E2: απειλή MDA18 (Data from untrustworthy sources) και ευπάθεια 978 (ασφαλής αυθεντικοποίηση αποστολέα)· τεκμήριο της διαδικασίας εμπλουτισμού της §4.5.3.

Πίνακας 4.11. Οι τρεις γραμμές εμπλουτισμού E1–E3: απειλή, ευπάθεια, τοποθέτηση και τεκμηρίωση.

E	Απειλή (ΒΓ)	Ευπάθεια (ΒΓ)	Τοποθέτηση	T	Τεκμηρίωση
E1	MDA16 — Saturation of the information system	991 — έκθεση αναμεταδοτών σε υπερβολικό όγκο αιτημάτων ή έντονη παρεμβολή (άρνηση υπηρεσίας)	N1, N2	4	Το κορυφαίο τομεακό εύρημα (DDoS 96,2% στη ΔΔ) αποκτά ρητή θέση στο μοντέλο, στα δύο κανάλια διασύνδεσης — διαθεσιμότητα P3a/P1
E2	MDA18 — Data from untrustworthy sources	978 — πρωτόκολλο που δεν επιτρέπει ασφαλή αυθεντικοποίηση του αποστολέα	S3	3	Πλαστά/μη έμπιστα εισερχόμενα παραστατικά στο κανάλι B2G· αυθεντικότητα και μη-αποποίηση — ευθεία είσοδος στο προφίλ απειλών του Κεφαλαίου 5
E3	MD23 — Corruption of data	262 — απουσία μέσων προστασίας και παρακολούθησης της ακεραιότητας δεδομένων	S2, S3	2	Στοχευμένη αλλοίωση περιεχομένου/εγγραφών· προϋποθέτει πρόσβαση και εξειδίκευση — δεύτερο σκέλος του προφίλ του Κεφαλαίου 5

Οι ευπάθειες επιλέχθηκαν με βάση το αντικείμενο κάθε προσθήκης. Η 991 περιγράφει τον κορεσμό αναμεταδοτών από υπερβολικά αιτήματα και αντιστοιχεί στον ρόλο των N1 και N2 ως καναλιών. Η 978 επιλέχθηκε για το E2 επειδή αφορά ασφαλή αυθεντικοποίηση αποστολέα. Η μη αποποίηση δεν εξαντλείται στην αυθεντικοποίηση, αλλά απαιτεί επίσης ακεραιότητα, κρυπτογραφικό τεκμήριο, προστατευμένα ίχνη και αξιόπιστη χρονική σήμανση. Η 262 επιλέχθηκε για το E3 επειδή αφορά προστασία και παρακολούθηση της ακεραιότητας δεδομένων. Οι εναλλακτικές 43 και 601 αφορούσαν αντίστοιχα αμιγώς ανιχνευτική λειτουργία και ακεραιότητα κώδικα. Το E1 δεν επεκτάθηκε στο γενικό αγαθό Network and Telecom, επειδή η ογκομετρική έκθεση του σεναρίου συγκεντρώνεται στα εξωτερικά σημεία διασύνδεσης. Η επέκταση παραμένει δυνατότητα μελλοντικής διεύρυνσης.

Μετά τον εμπλουτισμό, το μοντέλο περιλαμβάνει 16 απειλές, 90 μοναδικές γραμμές και 200 τοποθετήσεις. Η κατανομή είναι P1: 62, P2: 44, P3a: 45, P3b: 22 και P4: 27. Οι τρεις νέες απειλές ακολούθησαν την ίδια πειθαρχία βαθμονόμησης και συμπεριλήφθηκαν στον έλεγχο ομοιομορφίας.

4.5.4 Ευπάθειες: κάλυψη της βάσης γνώσης και παράδοση στην αποτίμηση

Στο MONARC κάθε γραμμή κινδύνου περιλαμβάνει και τη ζευγμένη ευπάθεια. Η πρώτη επανάληψη παρέδωσε επομένως απειλές και ευπάθειες από τον ίδιο δημόσια διανεμόμενο κατάλογο της βάσης γνώσης [13]. Οι περιγραφές είναι γενικές και εκφράζουν απουσία ή αδυναμία δικλίδας. Η ειδικότητα κάθε γραμμής προκύπτει από το αγαθό και από την κληρονομημένη επίπτωση του γονέα της. Οι ζεύξεις ελέγχθηκαν κατά την επισκόπηση της §4.5.2. Οι E1–E3 χρησιμοποίησαν επίσης ευπάθειες του καθολικού καταλόγου και όχι ελεύθερο κείμενο. Έτσι, το αρχικό και το προστιθέμενο τμήμα του μοντέλου στηρίζονται στην ίδια εκδοσιοποιημένη πηγή.

Μετά τον έλεγχο, καθεμία από τις 90 μοναδικές γραμμές διαθέτει αγαθό, κληρονομημένη επίπτωση, απειλή, πιθανοφάνεια και ευπάθεια. Η §4.6 βαθμονομεί την εκμεταλλευσιμότητα των ευπαθειών με ενιαία παραδοχή τριών βαθμίδων και υπολογίζει τα επίπεδα κινδύνου.

4.6 Υπολογισμός και αποτίμηση επιπέδων κινδύνου σε τεχνικό, λειτουργικό και θεσμικό επίπεδο

Η ενότητα βαθμονομεί τις ευπάθειες, υπολογίζει τον κίνδυνο και ερμηνεύει τα αποτελέσματα. Η ανάγνωση σε τεχνικό, λειτουργικό και θεσμικό επίπεδο αποτελεί σύμβαση της εργασίας και όχι νέο υπολογιστικό μοντέλο.

4.6.1 Βαθμονόμηση ευπαθειών: η παραδοχή ωριμότητας

Η δεύτερη αριθμητική είσοδος, μετά την πιθανοφάνεια, είναι η τιμή ευπάθειας στην κλίμακα 0–5 του MONARC [13]. Η τιμή εκφράζει την ευχέρεια εκμετάλλευσης στο συγκεκριμένο περιβάλλον. Επειδή το αρχέτυπο δεν επιτρέπει επιτόπιο έλεγχο ανά γραμμή, αποφεύχθηκαν 85 αποσπασματικές κρίσεις χωρίς κοινό μέτρο. Αντί αυτών εφαρμόστηκε ενιαία παραδοχή τριών βαθμίδων, συνδεδεμένη με τη φάση λειτουργικής ένταξης (§4.1.3). Οι τρεις βαθμίδες ορίζονται στον Πίνακα 4.12.

Πίνακας 4.12. Οι τρεις βαθμίδες βαθμονόμησης ευπαθειών Q-Θ, Q-T και Q-Λ, με το πεδίο εφαρμογής και το σκεπτικό τους.

Βαθμίδα	Τιμή	Πεδίο εφαρμογής	Σκεπτικό
Q-Θ — Θεσμικά κατοχυρωμένα	2	Ό,τι επιβάλλεται από το θεσμικό πλαίσιο ή την κεντρική σύμβαση: κύκλωμα εγκρίσεων και διαχωρισμός καθηκόντων (άρθ. 65 ν. 4270/2014 [66]), τυπικές εξουσιοδοτήσεις, συμβατικές υποχρεώσεις και συμφωνίες επιπέδου υπηρεσιών αναδόχου, κεντρικά αντίγραφα ασφαλείας ως υπηρεσία	Οι ισχυρότερες εγγυήσεις που διαθέτει ο φορέας στη φάση αυτή είναι οι θεσμικές και συμβατικές — προϋπάρχουν της ένταξης και δεν εξαρτώνται από την τοπική ωρίμανση
Q-T — Τεχνικά κεντρικής παροχής	3	Τεχνικά μέτρα της κεντρικής υποδομής: επικαιροποιήσεις και σκλήρυνση, διαχωρισμός δικτύων, διαχείριση επιπέδου υπηρεσιών	Υπάρχουν κεντρικά αλλά δεν είναι επαληθεύσιμα στο επίπεδο του φορέα — αντιπροσωπευτική ενδιάμεση παραδοχή, ρητά επισημασμένη ως τέτοια
Q-Λ — Λειτουργικά φορέα υπό διαμόρφωση	4	Ό,τι ωριμάζει με την ένταξη: εκπαίδευση χρηστών, χάρτα χρήσης, τοπική παρακολούθηση ιχνών, διαδικασίες περιστατικών και ανάκαμψης, κανόνες τηλεργασίας	Ακριβώς οι δικλίδες που η φάση ένταξης δεν έχει ακόμη σταθεροποιήσει — εδώ η έκθεση είναι μέγιστη

Η βαθμίδα Q-Θ εφαρμόστηκε στα αντίγραφα ασφαλείας και στη γραμμή συμφωνιών επιπέδου υπηρεσιών της συντήρησης τρίτου μέρους. Η Q-T εφαρμόστηκε στα S1–S5, στη διαχείριση εξυπηρετητών, στα Network and Telecom, N1 και N2, καθώς και στις λοιπές γραμμές συντήρησης. Η Q-Λ εφαρμόστηκε στο προσωπικό, στους διαχειριστές, στην οργάνωση πληροφορικής και στους σταθμούς εργασίας. Οι πέντε γραμμές E1–E3 έλαβαν την τιμή Q-T=3 των αγαθών στα οποία τοποθετήθηκαν. Προβλέφθηκε δυνατότητα τεκμηριωμένης απόκλισης ανά γραμμή, αλλά δεν χρειάστηκε. Οι επιπτώσεις και οι πιθανοφάνειες χρησιμοποιούν κλίμακα 0–4, ενώ οι ευπάθειες 0–5. Η μέγιστη τιμή ευπάθειας που χρησιμοποιήθηκε ήταν 4.

Η παραδοχή συνοδεύεται από δύο επιλογές διαφάνειας. Το πεδίο ελεύθερου κειμένου για υφιστάμενα μέτρα δεν συμπληρώθηκε σε κάθε γραμμή. Οι εγγυήσεις δηλώνονται κεντρικά μέσω των τριών βαθμίδων, ώστε κάθε τιμή να συνδέεται με ενιαίο σκεπτικό και να αποφεύγονται 85 επαναλήψεις. Η ίδια διαστρωμάτωση χρησιμοποιείται αργότερα ως σεναριακή ανάγνωση οργανωτικής ετοιμότητας. Η Q-Λ=4 δηλώνει το πεδίο που θεωρείται λιγότερο σταθεροποιημένο στη φάση ένταξης.

4.6.2 Υπολογισμός, επαλήθευση και συνολική εικόνα

Για κάθε πληττόμενο κριτήριο, το MONARC υπολογίζει τον τρέχοντα κίνδυνο ως $R = I \times T \times V$ και κατατάσσει τη γραμμή με τη μέγιστη τιμή [13]. Τα όρια διατηρήθηκαν στις προεπιλεγές 8 και 27. Τιμές έως 8 θεωρούνται αποδεκτές, 9–27 ενδιάμεσες και άνω του 27 μη αποδεκτές. Πρόκειται για κριτήρια του συνθετικού σεναρίου και όχι για εγκεκριμένη ανοχή πραγματικού φορέα, επειδή δεν υπάρχει αρμόδιος ιδιοκτήτης κινδύνου.

Ο υπολογισμός ελέγχθηκε με τρεις συμπληρωματικές διαδικασίες. Συγκρίθηκαν η πλήρης εξαγωγή JSON, η εξαγωγή CSV της προβολής του μητρώου και ανεξάρτητος επανυπολογισμός του R για όλα τα πληττόμενα κριτήρια των 200 τοποθετήσεων. Οι δύο εξαγωγές είναι διαφορετικές

αναπαραστάσεις του ίδιου μοντέλου. Ο επανυπολογισμός παρέχει τον ανεξάρτητο αριθμητικό έλεγχο. Οι έλεγχοι έδωσαν μηδέν αποκλίσεις, μηδέν κενές τιμές και ενιαίες πιθανοφάνειες για και τις 16 απειλές. Επιβεβαίωσαν επίσης ότι οι βαθμίδες συμφωνούν με την §4.6.1. Η σύγκριση των εξαγωγών πριν και μετά έδειξε ότι η μόνη μεταβολή ήταν οι πέντε προσθήκες της §4.5.3.

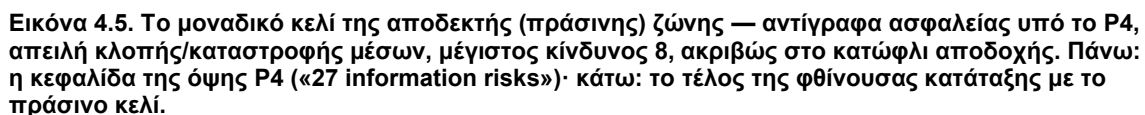
¹ Παρατηρήθηκε και καταγράφεται για λόγους αναπαραγωγιμότητας μία ιδιορρυθμία της διεπαφής στην έκδοση 2.13.4: τα εσωτερικά αναγνωριστικά και το εμφανιζόμενο πλαίσιο κληρονομημένης επίπτωσης της ίδιας μοναδικής γραμμής μεταβάλλονται μεταξύ διαδοχικών φορτώσεων της προβολής. Η ανάλυση ακύρωσε γι' αυτό κάθε γραμμή στο ζεύγος αγαθού–κειμένου ευπάθειας, με αυθεντική πηγή ανά τοποθέτηση την εξαγωγή της βάσης και όχι την εκάστοτε απόδοση της θόνης.

Σε επίπεδο τοποθετήσεων, 99 γραμμές είναι μη αποδεκτές, 100 ενδιάμεσες και μία αποδεκτή. Σε επίπεδο 90 μοναδικών γραμμών, με κριτήριο το μέγιστο των τοποθετήσεων, η κατανομή είναι 48 μη αποδεκτές και 42 ενδιάμεσες. Καμία μοναδική γραμμή δεν είναι πλήρως αποδεκτή. Η κορυφή περιλαμβάνει έντεκα γραμμές με τιμή 64, δηλαδή $I=4 \times T=4 \times V=4$. Οι γραμμές αφορούν την απειλή Forging of rights ή κακόβουλο λογισμικό στα αγαθά προσωπικού, διαχειριστών, οργάνωσης πληροφορικής και σταθμών εργασίας. Τα αγαθά αυτά στηρίζουν τέσσερα από τα πέντε πρωτεύοντα αγαθά. Το μοναδικό αποδεκτό κελί είναι ο κίνδυνος κλοπής ή καταστροφής μέσων για τα αντίγραφα ασφαλείας κάτω από το P4, με τιμή 8. Η ίδια μοναδική γραμμή φθάνει σε 12 κάτω από το P2, επομένως δεν είναι συνολικά αποδεκτή σε όλες τις τοποθετήσεις της.

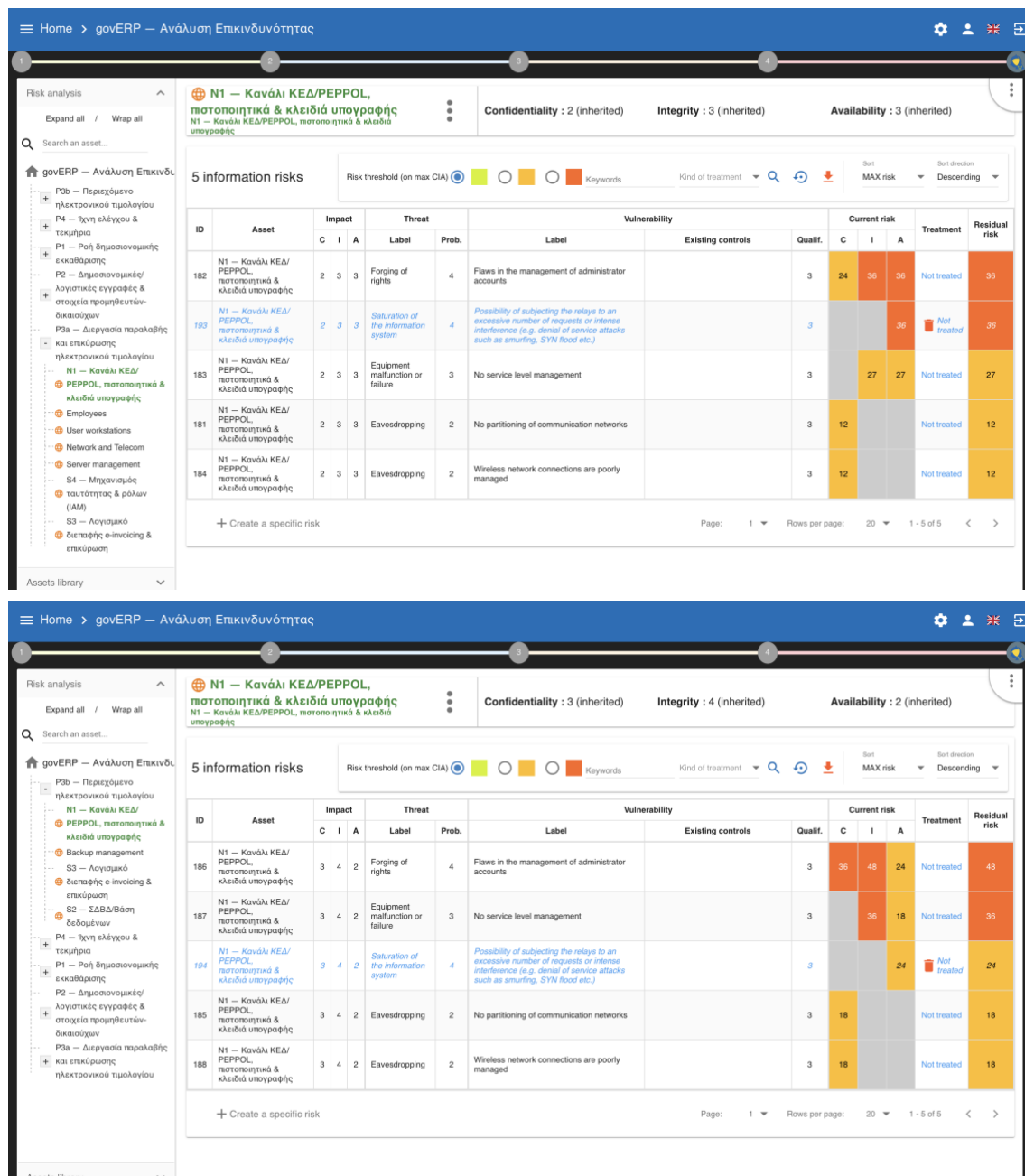
Για να ελεγχθεί η ευαισθησία του αποτελέσματος, επαναλήφθηκε ο υπολογισμός με μοναδική αλλαγή τη βαθμίδα Q-Λ από V=4 σε V=3. Οι επιπτώσεις, οι πιθανοφάνειες, τα κατώφλια και όλες οι άλλες τιμές παρέμειναν αμετάβλητες. Στις 90 μοναδικές γραμμές, η κατανομή μεταβλήθηκε από 48 μη αποδεκτές και 42 ενδιάμεσες σε 45 και 45 αντίστοιχα. Οι έντεκα γραμμές στην τιμή 64 εξαφανίστηκαν και η νέα μέγιστη τιμή 48 εμφανίστηκε σε 28 γραμμές. Από αυτές, 23 αφορούσαν Forging of rights και 5 κακόβουλο λογισμικό. Η θεματική προτεραιότητα ταυτότητας και πρόσβασης παραμένει, αλλά ο αποκλειστικά ανθρωποκεντρικός χαρακτήρας της αριθμητικής κορυφής εξαρτάται από τη βαθμονόμηση. Τα αποτελέσματα ερμηνεύονται επομένως ως σχετική ιεράρχηση υπό τις δηλωμένες παραδοχές.

ID	Asset	Impact			Threat	Prob.	Vulnerability			Current risk			Treatment	Residual risk
		C	I	A			Label	Existing controls	Qualif.	C	I	A		
118	Employees	2	4	3	Forging of rights	4	No protection of confidential authentication information		4	32	64	48	Not treated	64
121	Employees	2	4	3	Forging of rights	4	Lack of teleworking rules		4	32	64	48	Not treated	64
131	IT organization	2	4	3	Forging of rights	4	Logical access authorisations are not checked regularly		4	32	64	48	Not treated	64
41	System administrator	3	4	3	Forging of rights	4	No protection of confidential authentication information		4	48	64	48	Not treated	64
44	System administrator	3	4	3	Forging of rights	4	Lack of teleworking rules		4	48	64	48	Not treated	64
108	User workstations	2	4	3	Forging of rights	4	Authorisation management is flawed		4	32	64	48	Not treated	64
109	User workstations	2	4	3	Forging of rights	4	User authentication is not ensured		4	32	64	48	Not treated	64
110	User workstations	2	4	3	Forging of rights	4	The user workstation is not monitored		4	32	64	48	Not treated	64
114	User workstations	2	4	3	Malware infection	4	Programs can be downloaded and installed without monitoring		4	32	64	48	Not treated	64
112	User workstations	2	4	3	Malware infection	4	Update management (patches) is flawed		4	32	64	48	Not treated	64

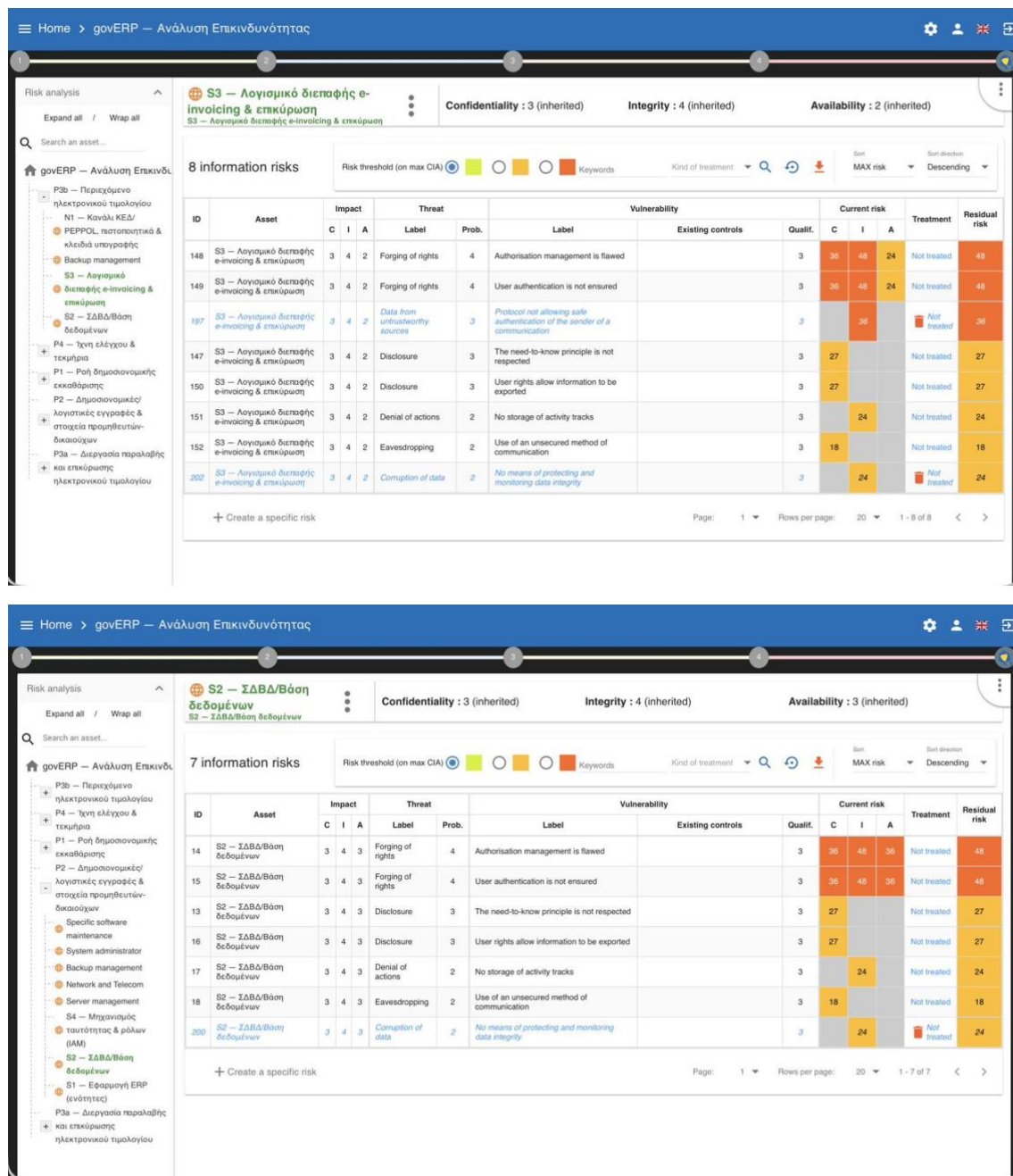
Εικόνα 4.4. Απόσπασμα-άγκυρα του μητρώου κινδύνων σε φθίνουσα κατάταξη (προβολή «1–90 of 90»): το πλήρες μητρώο των 90 μοναδικών αξιολογήσεων παρατίθεται ως Πίνακας Γ'.1, ενώ η πλήρης σειρά των έξι στιγμιοτύπων στα τεκμήρια του Παραρτήματος Δ'.



Αξιολόγηση Κινδύνων Ασφάλειας Πληροφοριών και Οργανωτικής Ετοιμότητας Κρίσιμων Υποδομών Πληροφορικής 51



Εικόνα 4.6. Το ίδιο καθολικό αντικείμενο N1 (κανάλι ΚΕΔ/ΡΕΡΡΟΛ) υπό το P3a (πάνω — A=36, μη αποδεκτή ζώνη) και υπό το P3b (κάτω — A=24) — οπτικό τεκμήριο της ανά-γονέα κληρονομήσης επιπτώσεων επί κοινών T/V.



Εικόνα 4.7. Οι όψεις των υποστηρικτικών αγαθών S3 — λογισμικό διεπαφής e-invoicing (πάνω) και S2 — ΣΔΒΔ (κάτω), με τις γραμμές των εμπλουτισμών σε πλάγια σήμανση ειδικού κινδύνου: E2 επί του S3 (I=36) και E3 επί των S3/S2 (I=24) — §4.5.3, λήψεις 05/07/2026.

4.6.3 Τριεπίπεδη αποτίμηση: τεχνικό, λειτουργικό και θεσμικό επίπεδο

Τα τρία επίπεδα που ακολουθούν είναι ερμηνευτικές αναγνώσεις των ίδιων αποτελεσμάτων. Χρησιμοποιούν την κατάταξη ανά γραμμή, τα υποδέντρα των πρωτευόντων αγαθών και τις διαστάσεις ROLFP. Δεν εισάγουν νέο υπολογισμό.

Στο τεχνικό επίπεδο εξετάζεται κάθε τριάδα αγαθού, απειλής και ευπάθειας έναντι των ορίων αποδοχής. Οι 48 μοναδικές γραμμές είναι μη αποδεκτές και οι 42 ενδιάμεσες. Η κορυφή αποτελείται από έντεκα γραμμές στην τιμή 64. Μόνο ένα κελί τοποθέτησης βρίσκεται στην αποδεκτή ζώνη. Η κατάταξη αυτή καθορίζει τη σειρά με την οποία εξετάζονται οι υποψήφιες δικλίδες στην §4.7.

Στο λειτουργικό επίπεδο τα αποτελέσματα ομαδοποιούνται ανά πρωτεύον αγαθό. Τα υποδέντρα P1 και P2 έχουν τον μεγαλύτερο αριθμό τοποθετήσεων, 62 και 44 αντίστοιχα. Η τιμή A=36 του N2 κάτω από το P1 δείχνει ότι η ροή εκκαθάρισης εξαρτάται από τη διαθεσιμότητα των διεπαφών. Το σημαντικότερο οριζόντιο αποτέλεσμα αφορά τα αγαθά προσωπικού, διαχειριστών, οργάνωσης πληροφορικής και σταθμών εργασίας. Στηρίζουν τέσσερα από τα πέντε πρωτεύοντα αγαθά και συνδέονται με δικλίδες ταυτότητας, πρόσβασης και ανθρώπινου παράγοντα. Το μέγεθος της πραγματικής μείωσης δεν μπορεί να εκτιμηθεί πριν από την επιλογή, υλοποίηση και επανεκτίμηση συγκεκριμένων δικλίδων. Για την ηλεκτρονική τιμολόγηση, το προφίλ που μεταφέρεται στο Κεφάλαιο 5 περιλαμβάνει το E1 στη μη αποδεκτή ζώνη, το E2 στη μη αποδεκτή και το E3 στην ενδιάμεση.

Risk analysis	
Expand all / Wrap all	
Search an asset...	
govERP — Ανάλυση Επικινδύνων	
P3b — Περιεχόμενο ηλεκτρονικού τιμολογίου	
P4 — Ίχνη ελέγχου & τεκμήρια	
P1 — Ροή δημοσιονομικής εκκαθάρισης	
N2 — Διεπαφές ΔΙΑΥΓΕΙΑ/ΚΗΜΔΗΖ/ΕΣΗΔΗΣ & τομειακού κυκλώματος	
Specific software maintenance	
IT organization	
System administrator	
Employees	
User workstations	
Server management	
Network and Telecom	
S4 — Μηχανισμός ταυτότητας & ρόλων (IAM)	
S1 — Εφαρμογή ERP (ενότητες)	
P2 — Δημοσιονομικές/λογιστικές εγγραφές & στοιχεία προμηθευτών/εταπλετών	
Assets library	

Employees Group of employees	
Confidentiality : 2 (inherited) Integrity : 4 (inherited) Availability : 3 (inherited)	
	C I A
Current risk	32 64 48
Residual risk	32 64 48
Asset	P1 — Ροή δημοσιονομικής εκκαθάρισης > Employees
Threat	Forging of rights
Threat probability	4 - Very likely: easy to execute, no mentionable investment or knowledge necessary
Vulnerability	No protection of confidential authentication information
Vulnerability qualification	4 - Strong vulnerability: Some measures have been already taken, even though they are ineffective or unadapted. Low maturity: Good practices aren't implemented, but there are some positive reactions without any thoughts.
Risk owner	
Risk context	
Existing controls	
Recommendations	
Search a recommendation	
Kind of treatment	Not treated
Vulnerability reduction	
Security referentials	ISO/IEC 27002:2022 5.17 - Authentication information 6.3 - Information security awareness, education and training

Εικόνα 4.8. Το φύλλο κινδύνου (Risk sheet) γραμμής του συμπλέγματος 64 (Employees / Forging of rights) με ορατή την προ-αντιστοίχιση μέτρων του ISO/IEC 27002:2022 (5.17, 6.3) — οπτική γέφυρα προς την §4.7.

Στο θεσμικό επίπεδο τα αποτελέσματα συνδέονται με λογοδοσία, νομικές συνέπειες και προστασία προσώπων. Για το P1, η αλλοίωση της ροής αντιβαίνει στον διαχωρισμό καθηκόντων του άρθρου 65 του ν. 4270/2014 [66]. Για το P2, η παραποίηση εγγραφών ή στοιχείων πληρωμής συνδέεται με πλαστογραφία και αχρεώστητη καταβολή, ενώ οι γραμμές αποκάλυψης σχετίζονται με την προστασία προσωπικών δεδομένων [72], [73]. Για το P4, η αλλοίωση ιχνών περιορίζει τη δυνατότητα καταλογισμού. Οι απαιτήσεις της ΚΥΑ 1689/2025 χρησιμοποιούνται ως πλαίσιο αναφοράς στις §§4.7–4.8. Η σύγκλιση αφορά θεματικές ταυτότητας, πρόσβασης, ανθρώπινου παράγοντα και ακεραιότητας ιχνών. Δεν υποδηλώνει νομική υπαγωγή του αρχετύπου.

Μετά τον υπολογισμό και την ερμηνεία, το μητρώο είναι ιεραρχημένο. Η §4.7 εξετάζει τις 85 προ-χαρτογραφημένες γραμμές και συμπληρώνει χειροκίνητα τις πέντε γραμμές E1–E3.

4.7 Αντιστοίχιση μέτρων κατά ISO/IEC 27002:2022

Η §4.7 εξετάζει τον σχεδιασμό αντιμετώπισης. Ως προς την ορολογία, το παρόν κεφάλαιο αποδίδει τον όρο «control» ως «μέτρο», ακολουθώντας τη διατύπωση του ίδιου του ορισμού της ρήτρας 3.1.8 του προτύπου· στο Κεφάλαιο 2 ο ίδιος όρος αποδόθηκε ως «δικλίδα ασφάλειας πληροφοριών». Οι δύο αποδόσεις είναι ισοδύναμες και δεν πρέπει να συγχέονται με τα κανονιστικά μέτρα του ν. 5160/2024 και της ΚΥΑ 1689/2025, τα οποία εξετάζονται χωριστά στην §4.9. Το ISO/IEC 27005 περιλαμβάνει τροποποίηση, διατήρηση, αποφυγή και επιμερισμό του κινδύνου [11]. Το μοντέλο υποδεικνύει τρεις υποψήφιες οδούς: δυνητική διατήρηση για το μοναδικό κελί εντός του σεναριακού ορίου, επιμερισμό για κινδύνους που ανατίθενται συμβατικά στον πάροχο και τροποποίηση για το μεγαλύτερο μέρος του μητρώου. Σε πραγματικό οργανισμό, Αξιολόγηση Κινδύνων Ασφάλειας Πληροφοριών και Οργανωτικής Ετοιμότητας Κρίσιμων Υποδομών Πληροφορικής 54

κάθε επιλογή θα απαιτούσε απόφαση ιδιοκτήτη κινδύνου. Η αποφυγή δεν είναι διαθέσιμη για την υποχρεωτική δημοσιονομική λειτουργία, αλλά μπορεί να εξεταστεί για επιμέρους τεχνικές λύσεις. Η ενότητα εστιάζει στην υποψήφια τροποποίηση και αντιστοιχίζει τους κινδύνους με δικλίδες του ISO/IEC 27002:2022 [3].

4.7.1 Το πλαίσιο αναφοράς και ο μηχανισμός αντιστοίχισης

Το ISO/IEC 27002:2022 περιλαμβάνει 93 μέτρα: 37 οργανωτικά, 8 για ανθρώπους, 14 φυσικά και 34 τεχνολογικά [3]. Η επιλογή του υποστηρίζει άμεσα την επόμενη ανάλυση αποκλίσεων, επειδή τα ίδια μέτρα αντιστοιχούν στο Παράρτημα Α του ISO/IEC 27001. Το MONARC ενσωματώνει το referential ISO/IEC 27002:2022 στη βάση γνώσης του [13]. Η διαθεσιμότητά του επαληθεύτηκε κατά την εγκατάσταση. Κάθε γραμμή που προτάθηκε από τη βάση γνώσης φέρει προ-αντιστοίχιση σε συγκεκριμένα μέτρα, ορατή στο φύλλο κινδύνου.

Η προ-αντιστοίχιση αποτελεί αφετηρία και όχι τελική απόφαση. Ο αναλυτής έλεγξε τη συνάφεια των προτεινόμενων μέτρων κατά την επισκόπηση της §4.5.2. Οι πέντε γραμμές E1–E3 δεν συνοδεύονταν από αυτόματη χαρτογράφηση και αντιστοιχίστηκαν χειροκίνητα στην §4.7.3. Όλες οι επιλογές προέρχονται από το ίδιο δημόσιο και εκδοσιοποιημένο referential. Έτσι διατηρείται κοινή γλώσσα μεταξύ του μητρώου κινδύνων και της ανάλυσης ISO/IEC 27001.

4.7.2 Η εικόνα της χαρτογράφησης

Από τις 90 μοναδικές γραμμές, οι 85 φέρουν προ-αντιστοίχιση. Οι γραμμές αυτές καλύπτουν 60 από τα 93 μέτρα του καταλόγου. Η έκταση της κάλυψης δείχνει πόσο πυκνά η βάση γνώσης χαρτογραφεί τους τύπους αγαθών του μοντέλου. Τα δέκα συχνότερα μέτρα παρουσιάζονται στον Πίνακα 4.13.

Πίνακας 4.13. Τα δέκα συχνότερα μέτρα του ISO/IEC 27002:2022 στη χαρτογράφηση, με τη θεματική τους και τον αριθμό γραμμών του μητρώου.

Μέτρο	Απόδοση τίτλου	Θεματική	Γραμμές
5.15	Έλεγχος πρόσβασης	Οργανωτική	18
5.17	Πληροφορίες αυθεντικοποίησης	Οργανωτική	16
5.18	Δικαιώματα πρόσβασης	Οργανωτική	14
5.16	Διαχείριση ταυτότητας	Οργανωτική	11
8.2	Προνομιακά δικαιώματα πρόσβασης	Τεχνολογική	9
8.24	Χρήση κρυπτογραφίας	Τεχνολογική	9
6.3	Ευαισθητοποίηση, εκπαίδευση και κατάρτιση	Ανθρώπων	8
8.12	Πρόληψη διαρροής δεδομένων	Τεχνολογική	8
5.14	Μεταφορά πληροφοριών	Οργανωτική	8
8.1	Τερματικές συσκευές χρηστών	Τεχνολογική	7

(Η απόδοση των τίτλων στα ελληνικά είναι του συγγραφέα· δεσμευτικοί παραμένουν οι αγγλικοί τίτλοι του προτύπου [3]. «Γραμμές» = μοναδικές γραμμές του μητρώου που φέρουν το μέτρο· επειδή κάθε γραμμή φέρει κατά κανόνα περισσότερα του ενός μέτρα, η στήλη δεν αθροίζεται στις 85 — οι δέκα κωδικοί συγκεντρώνουν συνολικά 108 αναφορές.)

Η οικογένεια ταυτότητας και πρόσβασης κυριαρχεί στη χαρτογράφηση. Τα 5.15, 5.16, 5.17, 5.18 και 8.2 συγκεντρώνουν 68 από τις 108 αναφορές της κορυφαίας δεκάδας. Η συχνότητα αυτή είναι συνεπής με το σύμπλεγμα κινδύνων 64 της §4.6.2. Οι δύο αναγνώσεις προκύπτουν από το ίδιο μοντέλο και δεν αποτελούν ανεξάρτητη επιβεβαίωση. Η παρουσία του 6.3 συνδέει την κατάταξη με την ανθρώπινη διάσταση της §4.9. Τα 8.24, 8.12, 5.14 και 8.1 αντανakλούν τους Αξιολόγηση Κινδύνων Ασφάλειας Πληροφοριών και Οργανωτικής Ετοιμότητας Κρίσιμων Υποδομών Πληροφορικής 55

κινδύνους εμπιστευτικότητας, διαβίβασης και σταθμών εργασίας. Η Εικόνα 4.8 δείχνει την προ-αντιστοίχιση των 5.17 και 6.3 σε γραμμή της κορυφής.

4.7.3 Χειροκίνητη αντιστοίχιση του εμπλουτισμού

Οι πέντε γραμμές των E1–E3 αντιστοιχίζονται χειροκίνητα, με την ίδια πειθαρχία που διέπει όλο το μοντέλο: επιλογή αποκλειστικά από τον κατάλογο του πλαισίου αναφοράς [3], με ρητή τεκμηρίωση της επιλογής και των απορρίψεων όπου χρειάζεται. Ο Πίνακας 4.14 καταγράφει τις αντιστοιχίσεις και το σκεπτικό τους.

Πίνακας 4.14. Χειροκίνητη αντιστοίχιση των γραμμών εμπλουτισμού σε μέτρα του ISO/IEC 27002:2022, με το σκεπτικό επιλογής.

Γραμμή εμπλουτισμού	Μέτρα	Σκεπτικό επιλογής
E1 — Κορεσμός συστήματος (MDA16) στα N1, N2	8.6 Διαχείριση χωρητικότητας · 8.16 Παρακολούθηση δραστηριοτήτων · 8.20 Ασφάλεια δικτύων	Η ανθεκτικότητα σε ογκομετρική εξάντληση πόρων απαιτεί τρία συμπληρωματικά σκέλη: πρόβλεψη και διαχείριση χωρητικότητας, έγκαιρη ανίχνευση ανώμαλης κίνησης, προστασία των δικτυακών υπηρεσιών στο όριο. Συμπληρωματικά λειτουργεί το 5.30 (ετοιμότητα ΤΠΕ για επιχειρησιακή συνέχεια), για το σκέλος της συνέχειας της διαθεσιμότητας
E2 — Δεδομένα από μη έμπιστες πηγές (MDA18) στο S3	8.24 Χρήση κρυπτογραφίας · 5.14 Μεταφορά πληροφοριών · 8.26 Απαιτήσεις ασφαλείας εφαρμογών	Η αυθεντικότητα και η μη-αποποίηση των εισερχόμενων παραστατικών θεμελιώνονται κρυπτογραφικά (ψηφιακές υπογραφές), πλαισιώνονται από τους κανόνες ασφαλούς διαβίβασης με τρίτους στο κανάλι B2G, και κατοχυρώνονται ως ρητή απαίτηση επικύρωσης εισόδων στο λογισμικό της διεπαφής
E3 — Αλλοίωση δεδομένων (MD23) στα S2, S3	8.15 Καταγραφή · 8.16 Παρακολούθηση δραστηριοτήτων · 8.13 Αντίγραφα ασφαλείας πληροφοριών	Η ευπάθεια 262 — απουσία μέσων προστασίας και παρακολούθησης της ακεραιότητας — απαντάται ευθέως στα δύο σκέλη της: καταγραφή και παρακολούθηση για την ανίχνευση της αλλοίωσης, αντίγραφα για την αποκατάσταση· οι κρυπτογραφικοί μηχανισμοί ακεραιότητας συνιστούν το κοινό σημείο με το E2 (8.24)

Το E1 υποδεικνύει συνδυασμό τροποποίησης και επιμερισμού. Η ογκομετρική άμυνα έναντι DDoS ασκείται κυρίως στο όριο του δικτύου από τον κεντρικό πάροχο, ενώ ο φορέας οφείλει να την κατοχυρώνει συμβατικά. Η επιλογή είναι συνεπής με τη §4.5.1 και τη βαθμίδα Q-Θ. Από τις χειροκίνητες αντιστοιχίσεις, τα 8.24 και 5.14 υπήρχαν ήδη στα 60 προ-χαρτογραφημένα μέτρα. Τα νέα μέτρα διευρύνουν το αποτύπωμα του μοντέλου. Η τελική καταμέτρηση γίνεται στο φύλλο της §4.8, το οποίο λειτουργεί ως προκαταρκτικός πίνακας εφαρμοσιμότητας και όχι ως εγκεκριμένη Δήλωση Εφαρμοσιμότητας.

4.7.4 Ιεράρχηση της αντιμετώπισης και παράδοση στην ανάλυση αποκλίσεων

Η ιεράρχηση οργανώνεται σε τρία μέτωπα. Πρώτο είναι η ταυτότητα και η πρόσβαση, επειδή συνδυάζουν τη μέγιστη τιμή κινδύνου, διάχυση σε τέσσερα από τα πέντε πρωτεύοντα αγαθά και 68 από τις 108 αναφορές της κορυφαίας δεκάδας δικλίδων. Το μέτωπο περιλαμβάνει τις 5.15–5.18, 8.2 και 6.3 και αφορά ανθρώπινες και λειτουργικές πρακτικές της βαθμίδας Q-Λ. Δεύτερο είναι η διαθεσιμότητα των καναλιών E1, με τις 8.6, 8.16, 8.20 και, συμπληρωματικά, την 5.30, καθώς και επιμερισμό προς τον πάροχο. Τρίτο είναι η ακεραιότητα και η αυθεντικότητα του περιεχομένου E2–E3, με τις 8.24, 5.14, 8.26, 8.15 και 8.13. Το τρίτο μέτωπο μεταφέρεται ως τεχνικό λεξιλόγιο στο Κεφάλαιο 5.

Η ανάλυση σταματά στην επιλογή και ιεράρχηση υποψήφιων μέτρων, επειδή δεν έχει υλοποιηθεί συγκεκριμένο σχέδιο αντιμετώπισης. Χωρίς τεκμήρια εφαρμογής και Αξιολόγηση Κινδύνων Ασφάλειας Πληροφοριών και Οργανωτικής Ετοιμότητας Κρίσιμων Υποδομών Πληροφορικής 56

αποτελεσματικότητας δεν υπάρχουν αιτιολογημένες νέες τιμές εισόδων για επανυπολογισμό του κινδύνου. Γι' αυτό δεν υπολογίζεται υπολειπόμενος κίνδυνος και δεν δηλώνεται ολοκληρωμένη αντιμετώπιση. Απουσιάζουν επίσης αναγνωρισμένοι ιδιοκτήτες κινδύνου, εγκεκριμένα κριτήρια αποδοχής και εγκρίσεις σχεδίου. Οι τιμές R αποτυπώνουν τον τρέχοντα σεναριακό κίνδυνο. Η §4.8 εξετάζει ποια μέτρα αντιστοιχούν σε απαιτήσεις, ποια θεωρούνται υφιστάμενα υπό την §4.6.1 και πού προκύπτουν αποκλίσεις.

4.8 Ανάλυση αποκλίσεων έναντι του ISO/IEC 27001

Η §4.7 προσδιόρισε τα μέτρα που υποδεικνύει το μοντέλο. Η §4.8 εξετάζει τη θέση του αρχετύπου απέναντι στο ISO/IEC 27001:2022 [2]. Οι ρήτρες 4–10 περιέχουν τις απαιτήσεις του συστήματος διαχείρισης και δεν επιδέχονται εξαίρεση. Το Παράρτημα Α περιλαμβάνει 93 μέτρα, τα οποία αντιστοιχούν στα μέτρα του ISO/IEC 27002:2022 [3]. Επειδή η §4.7 χρησιμοποίησε το ίδιο *referential*, τα αποτελέσματά της μεταφέρονται απευθείας στην ανάλυση αποκλίσεων.

4.8.1 Μεθοδολογική βάση και μέσο αποτύπωσης

Η ανάλυση αποκλίσεων αποτυπώνεται σε φύλλα για τη μεθοδολογία, τις ρήτρες 4–10, το Παράρτημα Α και την ΚΥΑ 1689/2025. Η κατάσταση κάθε μέτρου προκύπτει από τις βαθμίδες Q-Θ, Q-T και Q-Λ της §4.6.1 και οι αποκλίσεις χαρακτηρίζονται μερικές, επαλήθευσης ή ουσιώδεις. Η κοινή προέλευση εξασφαλίζει εσωτερική συνέπεια, όχι ανεξάρτητη επικύρωση. Η προτεραιότητα κληρονομείται από τα μέτωπα της §4.7.4.

4.8.2 Οι απαιτήσεις του συστήματος διαχείρισης (ρήτρες 4–10)

Οι 25 απαιτήσεις των ρητρών 4–10 αποτιμώνται με αφετηρία ότι δεν υπάρχει τεκμηριωμένο ISMS [2], άρα η προεπιλογή είναι «μη τεκμηριωμένο/ουσιώδης απόκλιση». Η εργασία παρέχει μόνο προκαταρκτικά τεκμήρια: μέθοδο και αναπαραγώγιμα αποτελέσματα για 6.1.2/8.2, πίνακα εφαρμοσιμότητας για 6.1.3 και υλικό οριοθέτησης για 4.1–4.3. Δεν αποδεικνύει εγκεκριμένα κριτήρια, ιδιοκτήτες κινδύνου, περιοδικότητα ή πλήρη SoA. Ο δημοσιονομικός διαχωρισμός καθηκόντων δεν ταυτίζεται με ρόλους ISMS, ενώ η 6.3 αφορά αλλαγές στο ίδιο το ISMS και όχι απευθείας τη μετάπτωση ERP.

4.8.3 Οι δικλίδες του Παραρτήματος Α και η οριστική εικόνα χαρτογράφησης

Η τελική καταμέτρηση έγινε στο μητρώο των 90 γραμμών. Οι 85 προ-χαρτογραφημένες γραμμές καλύπτουν 60 διακριτά μέτρα. Από τις χειροκίνητες αντιστοιχίσεις E1–E3, μόνο το 8.20 δεν υπήρχε ήδη. Η τελική κάλυψη είναι 61 από τα 93 μέτρα, δηλαδή 65,6%. Η αναλογία δείχνει το εύρος της χαρτογράφησης των σεναρίων και όχι ποσοστό υλοποίησης, αποτελεσματικότητας, ωριμότητας ή συμμόρφωσης. Η προσθήκη του 8.20 δείχνει ότι ο εμπλουτισμός κάλυψε κενό που δεν εμφανιζόταν στην πρώτη επανάληψη. Ο Πίνακας 4.15 δίνει την κάλυψη ανά κατηγορία.

Πίνακας 4.15. Κάλυψη των τεσσάρων κατηγοριών μέτρων του Παραρτήματος Α του ISO/IEC 27001:2022 από τη χαρτογράφηση.

Κατηγορία [3]	Μέτρα	Χαρτογραφημένα	Παρατήρηση
Οργανωτικά (5.x)	37	22	περιλαμβάνει και τα τέσσερα μέτρα του συμπλέγματος 64 (5.15–5.18)
Άνθρωποι (6.x)	8	7	μόνο το 6.6 εκτός — η υψηλότερη αναλογική κάλυψη κατηγορίας
Φυσικά (7.x)	14	9	κατά βάση σφαίρα του παρόχου φιλοξενίας (Q-T)
Τεχνολογικά (8.x)	34	23	22 από την προ-χαρτογράφηση + το 8.20 από το E1
Σύνολο	93	61	65,6% — τα 32 εκτός εμβέλειας σεναρίων

Η κατηγορία «Άνθρωποι» έχει την υψηλότερη αναλογική κάλυψη, με επτά από τις οκτώ δικλίδες. Το αποτέλεσμα προκύπτει από τα σενάρια του μοντέλου και δεν αποτελεί ανεξάρτητη μέτρηση. Η κατανομή των 93 μέτρων είναι 16 θεσμικά κατοχυρωμένα, 42 κεντρικής τεχνικής παροχής και 35 υπό διαμόρφωση. Στη ζώνη Q-Λ βρίσκονται και τα έξι μέτρα του πρώτου μετώπου. Τα 32 μη χαρτογραφημένα μέτρα δεν θεωρούνται περιττά. Σε πλήρες ISMS θα εξετάζονταν στη Δήλωση Εφαρμοσιμότητας, ενώ η χαρτογράφηση θα λειτουργούσε μόνο ως τεκμήριο ιεράρχησης.

4.8.4 Η εθνική όψη: το πλαίσιο απαιτήσεων της ΚΥΑ 1689/2025

Η ΚΥΑ 1689/2025 παρέχει την εθνική όψη της ανάλυσης αποκλίσεων [6]. Εξειδικεύει 22 απαιτήσεις για τις υπόχρεες βασικές και σημαντικές οντότητες. Το αρχέτυπο δεν ταξινομείται νομικά σε αυτές τις κατηγορίες και το πλαίσιο χρησιμοποιείται μόνο ως αναφορά. Οι πολιτικές πρόσβασης και η κατανομή αρμοδιοτήτων συνδέονται με το πρώτο μέτωπο. Η ασφάλεια δικτύων, εφοδιαστικής αλυσίδας και συνέχειας συνδέεται με το δεύτερο, ενώ η κρυπτογράφηση και τα αντίγραφα ασφαλείας με το τρίτο. Ο ΥΑΣΠΕ, οι έλεγχοι καταλληλότητας, η εκπαίδευση και η λογοδοσία της διοίκησης συνδέονται με την οργανωτική ετοιμότητα της §4.9. Η αρχή της αναλογικότητας της ΚΥΑ είναι συμβατή με τη διαβαθμισμένη ανάγνωση του σεναρίου, χωρίς να την επικυρώνει. Το τέταρτο φύλλο του βιβλίου αντιστοιχίζει τις 22 απαιτήσεις με τα μέτρα των [3] και [2]. Μετά τη διεθνή και την εθνική ανάγνωση, η §4.9 εξετάζει αν το αρχέτυπο διαθέτει την οργανωτική ικανότητα να περιορίσει τις αποκλίσεις.

4.9 Εκτίμηση οργανωτικής ετοιμότητας και ωριμότητας

4.9.1 Από τα κελιά του μητρώου στην οργανωτική ανάγνωση

Οι βαθμίδες Q-Θ, Q-T και Q-Λ χρησιμοποιούνται και για τη σεναριακή ετοιμότητα. Κριτήριο είναι αν η λειτουργία και το τεκμήριο ελέγχονται τοπικά, παρέχονται κεντρικά ή στηρίζονται σε θεσμική/συμβατική εγγύηση. Η κατανομή είναι 16, 42 και 35 μέτρα αντίστοιχα, ενώ και τα έξι μέτρα του πρώτου μετώπου βρίσκονται στη Q-Λ. Η ίδια παραδοχή επηρεάζει κινδύνους και κατάσταση μέτρων, άρα το μοντέλο δείχνει συνεπείς συνέπειες σεναρίου και όχι ανεξάρτητη μέτρηση φορέα.

4.9.2 Το ανθρωποκεντρικό εύρημα και οι δικλίδες της κατηγορίας «Άνθρωποι»

Οι έντεκα γραμμές της τιμής 64 αφορούν προσωπικό, διαχειριστές, οργάνωση πληροφορικής και σταθμούς εργασίας, με απειλές πλαστοπροσωπίας και κακόβουλου λογισμικού. Ενεργοποιούνται επτά από τις οκτώ δικλίδες «Άνθρωποι» του ISO/IEC 27002:2022 [3]. Επειδή οι δικλίδες αυτές απαιτούν επαναλαμβανόμενες πρακτικές, υπευθύνους και τεκμήρια, η ετοιμότητα εστιάζει σε πρόσωπα, ρόλους και καθημερινές διαδικασίες. Πρόκειται για εσωτερική ανάγνωση του μοντέλου, όχι ανεξάρτητη επικύρωση.

4.9.3 Τρεις διαστάσεις ετοιμότητας και η ωριμότητα της φάσης ένταξης

Η ετοιμότητα εξετάζεται σε τρεις διαστάσεις: διακυβέρνηση και λογοδοσία, ανθρώπινη ικανότητα και λειτουργικές διαδικασίες [6], [74]. Το αρχέτυπο έχει θεσμικό διαχωρισμό καθηκόντων, αλλά όχι πλήρες κύκλωμα ευθύνης ασφάλειας. Τα κεντρικά τεχνικά μέτρα αποκτούν οργανωτική αξία μόνο όταν τοπικοί ρόλοι μπορούν να ελέγξουν ειδοποιήσεις και ίχνη, να ενεργοποιήσουν διαδικασίες περιστατικών/συνέχειας και να τεκμηριώσουν τις ενέργειες. Το αρχέτυπο είναι θεσμικά πλαισιωμένο, τεχνικά εξαρτώμενο από κεντρικές υπηρεσίες και λειτουργικά υπό διαμόρφωση.

4.9.4 Σύνοψη κεφαλαίου και παράδοση στον άξονα πιστοποίησης

Το κεφάλαιο ορίζει το αρχέτυπο, εκτελεί την ανάλυση, αντιστοιχίζει μέτρα και αποτιμά αποκλίσεις και ετοιμότητα. Η κοινή παραδοχή ωριμότητας καθιστά τα αποτελέσματα συνεπή αλλά αλληλεξαρτώμενα. Κύρια προτεραιότητα είναι η ταυτότητα, η πρόσβαση και ο ανθρώπινος παράγοντας, ενώ η ηλεκτρονική τιμολόγηση αναδεικνύει διαθεσιμότητα, αυθεντικότητα και ακεραιότητα. Το Κεφάλαιο 5 παραλαμβάνει το προφίλ της διεπαφής. Η ανεξάρτητη επικύρωση θα απαιτούσε πραγματικό φορέα, πραγματικά τεκμήρια και επιτόπιο έλεγχο.

5. Πρακτική Προσέγγιση προς Πιστοποίηση με CUSTODES

Το Κεφάλαιο 5 εφαρμόζει τον δεύτερο άξονα της εργασίας σε στενά οριοθετημένο υποσύστημα του govERP. Με αναφορά στα ISO/IEC 15408 και 18045:2022 [16], [17] και στο CUSTODES [14], συγκροτεί προσχέδιο Security Target, απαιτήσεις και τεκμήρια ετοιμότητας. Δεν εκτελεί αξιολόγηση ούτε απονέμει πιστοποιητικό ή επίπεδο διασφάλισης. Οι §§5.1–5.5 ακολουθούν τη διαδρομή πλατφόρμα → ΤοΕ → πρόβλημα ασφάλειας → απαιτήσεις → μέτρα/τεκμήρια → workflow, και η §5.6 συγκρίνει τους δύο άξονες.

5.1 Η πλατφόρμα CUSTODES και το περιβάλλον εργασίας

5.1.1 Το έργο και η προσέγγισή του

Το CUSTODES είναι ερευνητικό έργο του προγράμματος Horizon Europe (Grant Agreement 101120684). Αντικείμενό του είναι μια προσέγγιση πιστοποίησης για σύνθετα συστήματα ΤΠΕ — προϊόντα, υπηρεσίες και διεργασίες — με δυναμική, ευέλικτη και επαναχρησιμοποιήσιμη αξιολόγηση [14].

Η δημόσια περιγραφή του δίνει έμφαση στη σύνθεση πληροφοριών πιστοποίησης από δομικούς λίθους και σε προστατευμένο περιβάλλον εκτέλεσης για την αλυσίδα φύλαξης τεκμηρίων [14].

Η προσέγγιση τοποθετείται στο θεσμικό πλαίσιο του Cybersecurity Act [19] και καλύπτει ένα κενό που περιγράφηκε στην §3.5. Το σχήμα EUCC, βασισμένο στα Common Criteria, πιστοποιεί μεμονωμένα προϊόντα ΤΠΕ [20]. Τα πραγματικά συστήματα, όμως, και ιδίως οι υπηρεσίες και οι διεπαφές, συντίθενται από συστατικά διαφορετικής προέλευσης και διαφορετικού κύκλου ζωής. Η αξιολόγησή τους απαιτεί σύνθεση, επαναχρησιμοποίηση και επικαιροποίηση αποτελεσμάτων. Γι' αυτό η προσέγγιση του έργου ταιριάζει σε αντικείμενο αξιολόγησης τύπου υπηρεσίας ή διεπαφής, όπως αυτό που ορίζεται στην §5.2.

Το CUSTODES χρησιμοποιείται μόνο στον άξονα ετοιμότητας και το MONARC μόνο στον άξονα κινδύνου. Η σχέση των δύο εξετάζεται στην §5.6. Σε όλο το κεφάλαιο χρησιμοποιείται αποκλειστικά δημόσια τεκμηρίωση του έργου [14].

5.1.2 Επίπεδο του εγχειρήματος και οργάνωση της εργασίας

Το κεφάλαιο διακρίνει δύο ερωτήματα που συχνά συγχέονται. Το πρώτο είναι μεθοδολογικό: *τι* πρέπει να συγκροτηθεί ώστε ένα υποσύστημα να φτάσει ώριμο σε μια μελλοντική αξιολόγηση. Περιλαμβάνει τον ορισμό και το όριο του αντικειμένου, το πρόβλημα ασφάλειας, τους στόχους, τις απαιτήσεις, τα μέτρα και τα τεκμήρια. Το δεύτερο είναι εργαλειακό: *πώς* τα παραπάνω καταχωρίζονται και υποστηρίζονται στην πλατφόρμα του έργου.

Οι ενότητες 5.2 έως 5.4 απαντούν στο πρώτο ερώτημα, με τεκμηρίωση από δημόσιες πηγές και με είσοδο το ποσοτικοποιημένο προφίλ κινδύνου του Κεφαλαίου 4. Η §5.5 απαντά στο δεύτερο, αξιοποιώντας την πρόσβαση δοκιμαστή (tester) που παραχωρήθηκε στην πλατφόρμα.

Η σειρά έχει σημασία. Η μεθοδολογική εργασία προηγείται της χρήσης του εργαλείου. Στην πλατφόρμα καταχωρίστηκε ήδη συγκροτημένη προδιαγραφή, ώστε να εξεταστεί κατά πόσο η πλατφόρμα μπορούσε να την αναπαραστήσει και να υποστηρίξει τη σχετική ροή εργασίας.

5.1.3 Το περιβάλλον εργασίας της πλατφόρμας

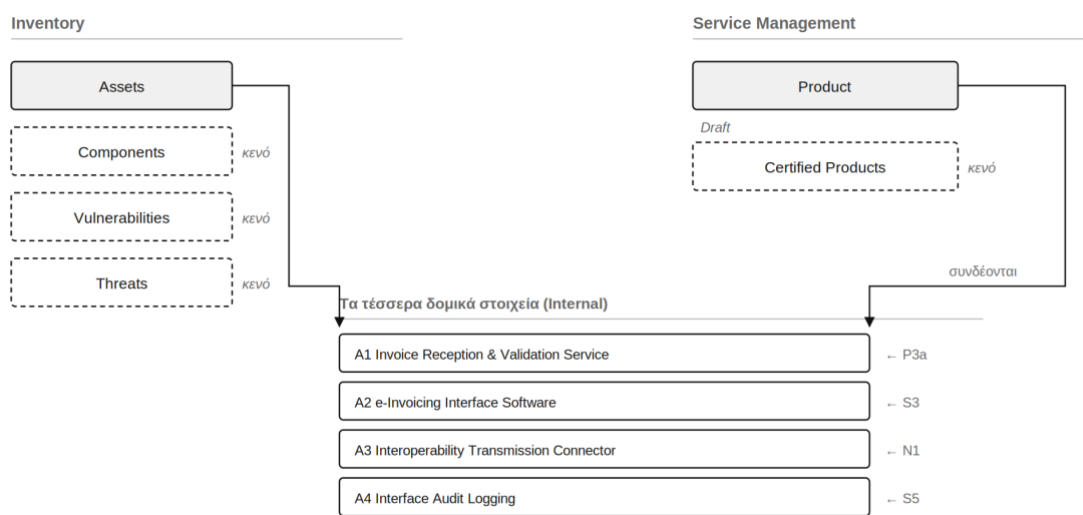
Η πρόσβαση δόθηκε από την ομάδα του έργου με λογαριασμό δοκιμαστή (tester), και η εργασία έγινε σε δύο φάσεις: αρχική καταχώριση στις 16 Ιουλίου 2026 και συνεδρία ολοκλήρωσης στις 4 Αυγούστου 2026. Αντικείμενό της ήταν να αποτυπωθεί η προδιαγραφή των §§5.2 έως 5.4 και να καταγραφεί τι υποστηρίζει η πλατφόρμα. Αξιολόγηση δεν εκτελέστηκε: η λειτουργία «Start Assessment» δεν ενεργοποιήθηκε σε κανένα στάδιο, κατά την οριοθέτηση του προοιμίου.

Η πλατφόρμα δεν εμφάνιζε αριθμό έκδοσης. Για τον λόγο αυτό, τα εμπειρικά ευρήματα οριοθετούνται ρητά στις συνεδρίες της 16ης Ιουλίου και της 4ης Αυγούστου 2026 και δεν

γενικεύονται σε προηγούμενες ή μεταγενέστερες καταστάσεις του λογισμικού. Τα τεχνικά αναγνωριστικά της συγκεκριμένης κατάστασης διατηρήθηκαν στο εσωτερικό audit trail.

Ο χώρος εργασίας οργανώνεται σε δύο ενότητες: το Inventory, που περιλαμβάνει τα Assets, τα Components, τα Vulnerabilities και τα Threats, και το Service Management, με τα Products και τα Certified Products. Το αντικείμενο αξιολόγησης καταχωρίζεται ως Product και τα δομικά του στοιχεία ως Assets συνδεδεμένα με αυτό. Στην παρούσα εργασία συμπληρώθηκαν το Product και τα Assets· τα Components, τα Vulnerabilities και τα Threats παρέμειναν κενά.

Η πλατφόρμα δέχθηκε και τα τέσσερα δομικά στοιχεία χωρίς CPE ή SBOM, μεταξύ τους και ένα δηλωμένο ως υπηρεσία. Επιβεβαιώθηκε έτσι εργαλειακά η δυνατότητα αναπαράστασης service/interface-type αντικειμένου, την οποία είχε ήδη υποστηρίξει η μεθοδολογική τεκμηρίωση (§5.2.1).



Άγκυρα στο μοντέλο κινδύνου του Κεφαλαίου 4

Εικόνα 5.1. Το μοντέλο οντοτήτων της πλατφόρμας και τα τέσσερα δομικά στοιχεία που καταχωρίστηκαν.

Η σύνδεση των στόχων ασφάλειας γίνεται μέσω κλειστού καταλόγου κατηγοριών απειλής, ο οποίος περιλαμβάνει τριάντα τρεις κατηγορίες και δεν είναι ενιαίος: οι πρώτες επτά δηλώνουν πλαίσιο STRIDE, με στόχους που φέρουν το πρόθεμα OT., ενώ οι υπόλοιπες είκοσι έξι δηλώνουν Cyber Resilience Act και αποδίδουν στόχους με πρόθεμα SO.. Το πλαίσιο κάθε κατηγορίας εμφανίζεται σε χωριστό πεδίο. Η συνέπεια της διπλής αυτής δομής για τη σύνταξη του στόχου ασφάλειας εξετάζεται στην §5.6.3.

Δεν χρησιμοποιήθηκαν το προστατευμένο περιβάλλον ανάλυσης κώδικα και ο διαμοιρασμός πιστοποίησης. Το πρώτο απαιτεί πραγματικό πηγαίο ή δυαδικό κώδικα, που το αρχέτυπο δεν διαθέτει, και το δεύτερο προϋποθέτει ολοκληρωμένη αξιολόγηση.

Η τεκμηρίωση του κεφαλαίου γίνεται με πρωτότυπα διαγράμματα. Οι εικόνες που ακολουθούν αποδίδουν σχηματικά τη δομή και τις σχέσεις που περιγράφει το κείμενο· δεν αναπαράγουν οθόνες της πλατφόρμας. Οι παρατηρήσεις τεκμηριώνονται από στιγμιότυπα που τηρήθηκαν κατά τις συνεδρίες ως εσωτερικό υλικό και είναι διαθέσιμα εφόσον ζητηθούν.

Δεν εξετάστηκε η σημασία της διάκρισης Internal/External ούτε ολόκληρος ο κατάλογος CRA. Όλα τα assets δηλώθηκαν Internal επειδή βρίσκονται εντός του ToE, χωρίς ταύτιση της εργαλειακής ετικέτας με τη διάκριση ToE/περιβάλλον των Common Criteria.

5.2 Ορισμός υποσυστήματος ως αντικειμένου αξιολόγησης

5.2.1 Από το ευρύ πεδίο της ανάλυσης στον στόχο αξιολόγησης

Το Κεφάλαιο 4 κάλυψε ολόκληρο το δημοσιονομικό πεδίο, ενώ η ετοιμότητα απαιτεί ακριβές όριο. Στα Common Criteria ο ΤοΕ είναι το αντικείμενο του οποίου οι ιδιότητες βεβαιώνονται και ό,τι μένει εκτός αποτελεί περιβάλλον με ρητές παραδοχές [16], [75]. Η ενότητα εφαρμόζει αυτή την οριοθέτηση στο gonERP.

Ως στόχος αξιολόγησης ορίζεται η **διεπαφή ηλεκτρονικής τιμολόγησης και εκκαθάρισης** του gonERP, δηλαδή το συστατικό #6 του πίνακα της §4.1.5. Το υποσύστημα αυτό παραλαμβάνει τα ηλεκτρονικά τιμολόγια των προμηθευτών, εκδίδόμενα κατά το ευρωπαϊκό πρότυπο EN 16931 και δρομολογούμενα μέσω PEPPOL και του Κέντρου Διαλειτουργικότητας. Τα επικυρώνει έναντι επιχειρησιακών και φορολογικών κανόνων αποδοχής και τροφοδοτεί τη ροή εκκαθάρισης [63], [64]. Η επιλογή ικανοποιεί και τα τέσσερα κριτήρια που είχαν τεθεί κατά τον σχεδιασμό της εργασίας για την ανάδειξη του στόχου αξιολόγησης. Πρόκειται, πρώτον, για σημείο γνήσιας κρίσιμότητας: είναι το κανάλι εισόδου των δημοσιονομικών υποχρεώσεων του φορέα και, ως δημοσίως εκτεθειμένο σημείο διασύνδεσης, συγκεντρώνει την επιφάνεια απάτης και αλλοίωσης του αρχετύπου. Διαθέτει, δεύτερον, καθαρό όριο με αριθμήσιμες διεπαφές — προϋπόθεση κάθε προδιαγραφής τύπου Common Criteria. Περιγράφεται, τρίτον, εξ ολοκλήρου από δημόσιες πηγές, χωρίς οποιαδήποτε προσφυγή σε στοιχεία πραγματικού φορέα, συνεπώς με τη μεθοδολογική αρχή του συνθετικού αρχετύπου (§4.1) — η πειθαρχία ασφαλών και μη ασφαλών πηγών της §4.1.5 δεσμεύει ρητά και το παρόν κεφάλαιο. Και είναι, τέταρτον, αρκετά πλούσιο ώστε να διατρέξει το πλήρες workflow της ετοιμότητας — από τα περιουσιακά στοιχεία στους στόχους, τις απαιτήσεις, τα μέτρα και τα τεκμήρια. Συντρέχει, τέλος, και λόγος συνέχειας: το Κεφάλαιο 4 μοντελοποίησε συνειδητά τη διεπαφή ως διακριτό κλάδο του δέντρου ανάλυσης (§4.3.4, §4.4), ακριβώς ώστε οι κίνδυνοι που αποτιμήθηκαν επ' αυτής να μεταφέρονται αυτούσιοι στο παρόν κεφάλαιο· η διαδρομή «κίνδυνος → στόχος αξιολόγησης → απαιτήσεις», που θεμελιώθηκε θεωρητικά στην §3.8, αποκτά εδώ πραγματικό, αριθμητικό περιεχόμενο (§5.2.4).

Ο ΤοΕ είναι υπηρεσία/διεπαφή και όχι προϊόν. Το EUCC αφορά προϊόντα ΤΠΕ [20], αλλά το CYRENE τεκμηριώνει υπηρεσία ως ΤοΕ [54], ενώ το CUSTODES υποστηρίζει σύνθετα αντικείμενα και η πλατφόρμα δέχθηκε την αναπαράσταση (§5.1.3). Το εγχείρημα παραμένει αποτίμηση ετοιμότητας με προσχέδιο Security Target, όχι πιστοποίηση.

5.2.2 Το όριο του στόχου αξιολόγησης: εντός, εκτός και διεπαφές

Εντός ΤοΕ βρίσκονται η παραλαβή, η μηχανή επικύρωσης, ο σύνδεσμος μετάδοσης, το συστατικό εκκαθάρισης/κατάστασης και το τοπικό logging. Εκτός μένουν ο πυρήνας ERP, το γενικό IAM, η δικτυακή υποδομή, οι σταθμοί εργασίας και το ΚΕΔ. Οι προσδοκίες από το περιβάλλον δηλώνονται ως παραδοχές στην §5.3.

Οι τέσσερις διεπαφές είναι: χειριστή, εσωτερική προς τον πυρήνα ERP, εξωτερική προς ΚΕΔ/PEPPOL και ελέγχου/καταγραφής.

Η τρίτη διεπαφή συγκεντρώνει το ενδιαφέρον του μοντέλου, επειδή εκεί η ευθύνη διασχίζει το όριο του οργανισμού. Εκεί εφαρμόζονται και οι απαιτήσεις έμπιστου καναλιού και μη-αποποίησης πέραν του ορίου, την οπτική των οποίων για τις διοργανωσιακές υπηρεσίες ανέπτυξε το CYRENE [54].

Το όριο παραμένει σφιχτό: περιλαμβάνει τη διεπαφή και το κανάλι της, όχι όλο το χρηματοοικονομικό υποσύστημα. Ευρύτερο όριο θα ήταν δυσανάλογο και στενότερο θα άφηνε εκτός την ακεραιότητα περιεχομένου και τη μη-αποποίηση υποβολής.

5.2.3 Περιουσιακά στοιχεία και ιδιότητες προς προστασία

Η απογραφή των περιουσιακών στοιχείων του στόχου αξιολόγησης δεν εκκινεί από μηδενική βάση: αποτελεί εστίαση του μοντέλου της §4.4 στο υποσύνολο της διεπαφής. Πρωτεύοντα στοιχεία είναι το περιεχόμενο των τιμολογίων, οι εγγραφές και η κατάσταση της εκκαθάρισης, και οι κανόνες επικύρωσης· υποστηρικτικά, το λογισμικό της διεπαφής, το κανάλι διασύνδεσης, τα

διαπιστευτήρια — πιστοποιητικά και κλειδιά υπογραφής — και τα ίχνη ελέγχου. Ο Πίνακας 5.1 αποτυπώνει την αντιστοιχία με το μοντέλο του Κεφαλαίου 4.

Πίνακας 5.1. Περιουσιακά στοιχεία του στόχου αξιολόγησης και αντιστοιχία με το μοντέλο MONARC του Κεφαλαίου 4.

Στοιχείο του στόχου αξιολόγησης	Κατηγορία	Αντιστοιχία στο μοντέλο του Κεφ. 4
Περιεχόμενο τιμολογίου (δεδομένα)	Πρωτεύον	P3b (Information)
Διεργασία παραλαβής, επικύρωσης και εκκαθάρισης (εγγραφές και κατάσταση συναλλαγών)	Πρωτεύον	P3a (Service)
Κανόνες επικύρωσης (επιχειρησιακοί και φορολογικοί)	Πρωτεύον	Ενσωματωμένοι στη διεργασία του P3a και στη διαμόρφωση του S3 — όχι διακριτό αγαθό στο εργαλείο
Λογισμικό διεπαφής ηλεκτρονικής τιμολόγησης και επικύρωσης	Υποστηρικτικό	S3 (Global)
Κανάλι διασύνδεσης (ΚΕΔ/PEPPOL), με τα πιστοποιητικά και τα κλειδιά υπογραφής του	Υποστηρικτικό	N1
Ίχνη ελέγχου της διεπαφής (τοπικό logging)	Υποστηρικτικό	S5 (Local) — στο μοντέλο του Κεφ. 4 προσαρτημένο υπό το P4 (συστατικό #5), εκτός του κλάδου P3a/P3b

Τρεις επιλογές του πίνακα χρήζουν σχολιασμού. Πρώτον, τα πιστοποιητικά και τα κλειδιά υπογραφής μοντελοποιήθηκαν στο Κεφάλαιο 4 εντός του N1, ως αναπόσπαστο μέρος του καναλιού· εδώ αναδεικνύονται ρητά, διότι στον άξονα της πιστοποίησης αποτελούν τον τεχνικό φορέα της μη-αποποίησης — της κεντρικής ιδιότητας του αντικειμένου. Δεύτερον, τα ίχνη ελέγχου απαιτούν διευκρίνιση ιχνηλασιμότητας. Η λειτουργία καταγραφής των ενεργειών της διεπαφής ανήκει στο εσωτερικό του στόχου αξιολόγησης και εκφράζεται στην §5.3 ως στόχος και απαίτηση ελεγκτικής καταγραφής. Στο μοντέλο του Κεφαλαίου 4, όμως, ο μηχανισμός καταγραφής (S5) εντάχθηκε μαζί με το οργανωσιακό μητρώο ιχνών (P4) στο συστατικό #5, όχι στον κλάδο της διεπαφής. Η αντιστοίχιση του πίνακα γίνεται συνεπώς σε επίπεδο ταυτότητας αγαθού, όχι θέσης στο δέντρο. Το οργανωσιακό σκέλος της τήρησης των ιχνών παραμένει στο περιβάλλον. Τρίτον, το υποσύστημα διαχείρισης ταυτότητας (S4 στο μοντέλο του Κεφαλαίου 4) παραμένει συνειδητά εκτός ορίου: στην §5.3 μετατρέπεται στην παραδοχή περιβάλλοντος Α.ΙΑΜ. Η επιλογή αυτή έχει μεθοδολογικό βάθος που αξίζει να δηλωθεί: το Κεφάλαιο 4 ανέδειξε ως κορυφαίο εγκάρσιο εύρημα το σύμπλεγμα κινδύνων των οριζόντιων ανθρώπινων και οργανωσιακών αγαθών (§4.6) — αγαθών που, στη γλώσσα του παρόντος κεφαλαίου, ανήκουν στο περιβάλλον του στόχου αξιολόγησης. Το εύρημα δεν εξαφανίζεται· αλλάζει θέση στο σχήμα: εκφράζεται ως παραδοχές και στόχοι για το περιβάλλον (§5.3), υπενθυμίζοντας ότι η διάκριση στόχου/περιβάλλοντος οριοθετεί την ευθύνη της αξιολόγησης, όχι τη σημασία των κινδύνων.

Κεντρικές ιδιότητες είναι ακεραιότητα, αυθεντικότητα και μη-αποποίηση, επειδή το τιμολόγιο αποτελεί δημοσιονομικό τεκμήριο. Ακολουθούν εμπιστευτικότητα, διαθεσιμότητα και λογοδοσία. Η ιεράρχηση είναι συνεπής με το προφίλ κινδύνου της επόμενης ενότητας· τα δύο απορρέουν από κοινή παραδοχή και δεν αποτελούν ανεξάρτητη επιβεβαίωση.

5.2.4 Το προφίλ κινδύνου-εισόδου από το Κεφάλαιο 4

Η οριοθέτηση δεν παραλαμβάνει από το Κεφάλαιο 4 μόνο στοιχεία· παραλαμβάνει και αριθμούς. Υπενθυμίζεται το πλαίσιο αποτίμησης της §4.6: κίνδυνος $R = I \times T \times V$ ανά πληττόμενο κριτήριο, με κατώφλια 8 και 27 — έως 8 αποδεκτός κίνδυνος, από 9 έως 27 ενδιάμεση ζώνη ανεκτού υπό παρακολούθηση, άνω του 27 μη αποδεκτός. Επί του κλάδου της διεπαφής, οι τρεις τεκμηριωμένες τριάδες εμπλουτισμού της §4.5 (E1–E3) απέδωσαν το προφίλ του Πίνακα 5.2.

Πίνακας 5.2. Το ποσοτικοποιημένο προφίλ κινδύνου του κλάδου της διεπαφής, όπως αποτιμήθηκε στην §4.6 (τιμές επαληθευμένες προγραμματιστικά επί της εξαγωγής του εργαλείου). Σημειώνεται για πληρότητα ότι οι E1 και E3 εκτείνονται και πέραν του ορίου του στόχου αξιολόγησης: το E1 πλήττει με $A = 36$ και το κανάλι διαλειτουργικότητας N2 υπό τη ροή εκκαθάρισης (P1), ενώ το E3 διαχέεται με $I = 24$ και μέσω της βάσης δεδομένων (S2) — υποστηρικτικού αγαθού του περιβάλλοντος λειτουργίας — στα P2, P3b και P4.

Τριάδα	Απειλή — ευπάθεια (βάση γνώσης MONARC)	Αγαθό-φορέας	Κίνδυνος υπό P3a	Κίνδυνος υπό P3b
E1	Κορεσμός/άρνηση υπηρεσίας (MDA16 — ευπ. 991: υπερβολικός όγκος αιτημάτων)	N1	$A = 36$ (μη αποδεκτή)	$A = 24$ (ενδιάμεση)
E2	Δεδομένα από μη έμπιστες πηγές (MDA18 — ευπ. 978: πρωτόκολλο χωρίς ασφαλή αυθεντικοποίηση αποστολέα)	S3	$I = 27$ (άνω όριο ενδιάμεσης)	$I = 36$ (μη αποδεκτή)
E3	Αλλοίωση δεδομένων (MD23 — ευπ. 262: απουσία μέσων προστασίας και παρακολούθησης ακεραιότητας)	S3	$I = 18$ (ενδιάμεση)	$I = 24$ (ενδιάμεση)

Η ανάγνωση του πίνακα αναδεικνύει δύο πόλους. Ο πρώτος είναι η **διαθεσιμότητα του καναλιού**: σε ολόκληρο το μοντέλο του Κεφαλαίου 4, η διαθεσιμότητα αποκτά παρουσία στη μη αποδεκτή ζώνη αποκλειστικά μέσω του E1 — εντός του ορίου του στόχου αξιολόγησης, στο N1 υπό τη διεργασία παραλαβής — εύρημα συνεπές με την τομεακή εικόνα απειλών που τεκμηρίωσε την πιθανοφάνειά του. Ο δεύτερος είναι η **ακεραιότητα και αυθεντικότητα του περιεχομένου**: το E2 τοποθετεί την αδυναμία ασφαλούς αυθεντικοποίησης του αποστολέα στη μη αποδεκτή ζώνη για το περιεχόμενο του τιμολογίου, με το E3 να συμπληρώνει την εικόνα στην ενδιάμεση ζώνη. Οι διατυπώσεις των ευπαθειών αντιστοιχούν ήδη στις απειλές που θα κωδικοποιήσει η §5.3. Ο κορεσμός από υπερβολικό όγκο αιτημάτων οδηγεί στην απειλή διακοπής υπηρεσίας. Η αδυναμία αυθεντικοποίησης του αποστολέα οδηγεί στις απειλές πλαστογράφησης και αποποίησης. Η απουσία παρακολούθησης ακεραιότητας οδηγεί στην απειλή αλλοίωσης.

Πέραν της ταυτοποίησης, οι τιμές δείχνουν και πού χρειάζονται οι ισχυρότερες απαιτήσεις. Τα κελιά της μη αποδεκτής ζώνης σημαίνουν τα σημεία όπου η ετοιμότητα οφείλει να είναι πιο απαιτητική, κατά τη θέση της §3.8.

Με ορισμένα το αντικείμενο, το όριο, τα περιουσιακά στοιχεία και το κληρονομημένο προφίλ κινδύνου, η επόμενη ενότητα διατυπώνει τυπικά το πρόβλημα ασφάλειας του στόχου αξιολόγησης — απειλές, παραδοχές και οργανωσιακές πολιτικές — και το μεταφράζει σε στόχους και απαιτήσεις ασφάλειας κατά ISO/IEC 15408.

5.3 Στόχοι και απαιτήσεις ασφάλειας

5.3.1 Ορισμός του προβλήματος ασφάλειας

Κατά τη λογική ροή της §3.3, η προδιαγραφή εκκινεί από τον ορισμό του προβλήματος ασφάλειας (Security Problem Definition). Αυτός περιλαμβάνει τις απειλές κατά του στόχου αξιολόγησης, τις παραδοχές για το περιβάλλον λειτουργίας του και τις οργανωσιακές πολιτικές που το δεσμεύουν [16]. Η διατύπωση που ακολουθεί δεν είναι θεωρητική κατασκευή. Κάθε απειλή αγκυρώνεται στο ποσοτικοποιημένο προφίλ της §5.2.4 ή στους κινδύνους της πρώτης επανάληψης του Κεφαλαίου

4 επί των αγαθών του κλάδου. Κάθε παραδοχή αντιστοιχεί σε στοιχείο που η οριοθέτηση της §5.2.2 τοποθέτησε στο περιβάλλον.

Οι απειλές κωδικοποιούνται κατά τη συμβατική πρακτική των Common Criteria, με το πρόθεμα T (threat). Κάθε μία περιγράφει τι μπορεί να πάθει το αντικείμενο και από ποιον, χωρίς να προδικάζει πώς θα αντιμετωπιστεί.

Πίνακας 5.3. Απειλές κατά του στόχου αξιολόγησης και θεμελίωσή τους στην ανάλυση του Κεφαλαίου 4.

Κωδικός	Περιγραφή	Θεμελίωση στο Κεφάλαιο 4
T.TAMPER	Αλλοίωση δεδομένων τιμολογίου ή εγγραφών εκκαθάρισης, εν κινήσει ή εν ηρεμία, με συνέπεια νόθευση της δημοσιονομικής ροής	E3 (αλλοίωση δεδομένων — απουσία μέσων προστασίας και παρακολούθησης ακεραιότητας): I = 24 υπό P3b, I = 18 υπό P3a· συνεργεί με το E2
T.FORGE	Υποβολή πλαστού ή παραποιημένου τιμολογίου από μη γνήσια πηγή	E2 (δεδομένα από μη έμπιστες πηγές — πρωτόκολλο χωρίς ασφαλή αυθεντικοποίηση αποστολέα): I = 36 υπό P3b — η βαρύτερη τιμή του κλάδου
T.REPUDIATE	Άρνηση της προέλευσης ή της υποβολής παραστατικού/συναλλαγής εκ των υστέρων	Η ίδια ευπάθεια του E2: η αδυναμία ασφαλούς αυθεντικοποίησης του αποστολέα υπονομεύει ευθέως τη δυνατότητα απόδειξης προέλευσης
T.DOS	Διακοπή ή υποβάθμιση της υπηρεσίας παραλαβής/εκκαθάρισης μέσω εξάντλησης πόρων του καναλιού	E1 (κορεσμός — υπερβολικός όγκος αιτημάτων): A = 36 υπό P3a — η μη αποδεκτή ζώνη διαθεσιμότητας εμφανίζεται σε όλο το μοντέλο αποκλειστικά μέσω του E1 (εντός ορίου: N1 υπό P3a· εκτός: N2 υπό P1)
T.DISCLOSE	Μη εξουσιοδοτημένη αποκάλυψη οικονομικών στοιχείων και δεδομένων προμηθευτών, εν κινήσει ή εν ηρεμία	Κίνδυνοι εμπιστευτικότητας της πρώτης επανάληψης επί των S3/N1· θεσμική διάσταση προστασίας δεδομένων κατά την ανάγνωση της §4.6.3
T.INTERCEPT	Υποκλοπή ή παρεμβολή στο κανάλι διασύνδεσης (επίθεση ενδιάμεσου)	Κίνδυνοι καναλιού της πρώτης επανάληψης επί του N1· τεχνική προϋπόθεση πραγμάτωσης των T.FORGE/T.DISCLOSE στο σημείο διασύνδεσης
T.LOG	Αλλοίωση, απώλεια ή καταστολή των ιχνών ελέγχου της διεπαφής	Θεσμική ανάγνωση της §4.6.3: η αλλοίωση ιχνών ισοδυναμεί με κατάλυση της δυνατότητας καταλογισμού· το σκέλος «παρακολούθησης» της ευπάθειας του E3

Οι παραδοχές για το περιβάλλον λειτουργίας φέρουν το πρόθεμα A (assumption) και καθρεφτίζουν την οριοθέτηση της §5.2.2. Τις απαρτιώνει ο Πίνακας 5.4.

Πίνακας 5.4. Παραδοχές για το περιβάλλον λειτουργίας του στόχου αξιολόγησης.

Κωδικός	Περιεχόμενο	Αγκύρωση
A.IAM	Το περιβάλλον παρέχει αξιόπιστη ταυτοποίηση και αυθεντικοποίηση των εσωτερικών χρηστών, καθώς και διαχείριση ρόλων	Το S4 και η οργανωσιακή του διάσταση εκτός ορίου (§5.2.2)
A.NETWORK	Η δικτυακή υποδομή και η περίμετρος του φορέα παρέχουν βασική προστασία και διαχωρισμό	Οριοθέτηση §5.2.2
A.PHYSICAL	Η φυσική και περιβαλλοντική προστασία της υποδομής φιλοξενίας εξασφαλίζεται	Μεταφορά των περιβαλλοντικών απειλών στον πάροχο (§4.5.1)
A.ADMIN	Οι διαχειριστές του συστήματος είναι έμπιστοι και επαρκώς καταρτισμένοι	Οριοθέτηση §5.2.2
A.TIME	Διατίθεται αξιόπιστη πηγή χρόνου για τη χρονοσήμανση	Υποστηρίζει τα O.AUDIT και O.NONREP

Οι παραδοχές αυτές δεν είναι ουδέτερες δηλώσεις ευκολίας. Οι A.IAM και A.ADMIN μεταφέρουν στο περιβάλλον το πρώτο μέτωπο του Κεφαλαίου 4, δηλαδή το σύμπλεγμα των οριζόντιων ανθρώπινων και οργανωσιακών κινδύνων. Γι' αυτό επιστρέφουν στην §5.3.2 ως στόχοι για το περιβάλλον, ώστε η μεταφορά να μη διαβαστεί ως εξαφάνιση του ευρήματος.

Τις οργανωσιακές πολιτικές ασφάλειας (πρόθεμα P — policy) συγκροτούν τέσσερις δεσμεύσεις, που απορρέουν από τη φύση του αντικειμένου και από το θεσμικό του πλαίσιο. Τις καταγράφει ο Πίνακας 5.5.

Πίνακας 5.5. Οργανωσιακές πολιτικές ασφάλειας που δεσμεύουν τον στόχο αξιολόγησης.

Κωδικός	Περιεχόμενο	Πηγή δέσμευσης
P.AUDIT	Κάθε ενέργεια παραλαβής, επικύρωσης, αποδοχής ή απόρριψης και εκκαθάρισης καταγράφεται, με ιχνηλασιμότητα ενεργούντος και χρόνου	Φύση του αντικειμένου ως καναλιού εισροής δημοσιονομικών υποχρεώσεων
P.CRYPTO	Χρησιμοποιούνται εγκεκριμένοι κρυπτογραφικοί μηχανισμοί για την υπογραφή και την προστασία των παραστατικών	Πλαίσιο ηλεκτρονικής τιμολόγησης B2G [63], [64]
P.RETENTION	Τα παραστατικά και τα ίχνη τηρούνται κατά το ισχύον πλαίσιο τήρησης δημοσίων οικονομικών αρχείων	Πλαίσιο τήρησης δημοσίων οικονομικών αρχείων
P.COMPLIANCE	Η λειτουργία της διεπαφής συμμορφώνεται με το θεσμικό πλαίσιο της ηλεκτρονικής τιμολόγησης στις συναλλαγές με το Δημόσιο	[63], [64]. Η Οδηγία NIS2 [4] και ο ν. 5160/2024 [5] λειτουργούν, κατά την §3.7, μόνο ως πλαίσιο αναφοράς: το αρχέτυπο δεν ταξινομείται νομικά ως βασική ή σημαντική οντότητα

5.3.2 Στόχοι ασφάλειας για τον στόχο αξιολόγησης και το περιβάλλον

Από το πρόβλημα ασφάλειας συνάγονται οι στόχοι ασφάλειας: συνοπτικές, αφηρημένες δηλώσεις του τι οφείλει να επιτυγχάνει ο στόχος αξιολόγησης και τι το περιβάλλον του [16]. Οι πρώτοι φέρουν το πρόθεμα O (objective), οι δεύτεροι το πρόθεμα OE. Ορίζονται επτά και πέντε αντίστοιχα.

Πίνακας 5.6. Στόχοι ασφάλειας για τον στόχο αξιολόγησης και για το περιβάλλον λειτουργίας του.

Κωδικός	Πεδίο	Περιεχόμενο	Έναντι / Από
O.INTEGRITY	ToE	Προστασία της ακεραιότητας των τιμολογίων και των εγγραφών εκκαθάρισης, εν κινήσει και εν ηρεμία	T.TAMPER, T.FORGE
O.NONREP	ToE	Μη-αποποίηση προέλευσης και υποβολής, μέσω ψηφιακών υπογραφών επί των παραστατικών	T.REPUDIATE, T.FORGE· υλοποίηση της P.CRYPTO
O.AUTH	ToE	Αυθεντικοποίηση της πηγής των εισερχόμενων παραστατικών και των άκρων του καναλιού διασύνδεσης	T.FORGE, T.INTERCEPT
O.CONFID	ToE	Προστασία της εμπιστευτικότητας των δεδομένων, εν κινήσει και εν ηρεμία	T.DISCLOSE, T.INTERCEPT
O.AUDIT	ToE	Παραγωγή και προστασία πλήρων εγγραφών ελέγχου για τις ενέργειες της διεπαφής	T.LOG· υλοποίηση της P.AUDIT
O.AVAIL	ToE	Διατήρηση της διαθεσιμότητας της υπηρεσίας παραλαβής και ικανότητα ανάκαμψης της ροής εκκαθάρισης	T.DOS
O.ACCESS	ToE	Εξουσιοδότηση της πρόσβασης στις λειτουργίες της διεπαφής κατά ρόλο	Εσωτερική κατάχρηση, σε συνεργασία με το περιβάλλον
OE.IAM	Περιβάλλον	Αξιόπιστη ταυτοποίηση και εξουσιοδότηση χρηστών	A.IAM
OE.NETWORK	Περιβάλλον	Προστασία της δικτυακής υποδομής	A.NETWORK
OE.PHYSICAL	Περιβάλλον	Φυσική και περιβαλλοντική προστασία της υποδομής φιλοξενίας, διά της συμβατικής μεταφοράς στον πάροχο	A.PHYSICAL
OE.TIME	Περιβάλλον	Αξιόπιστη πηγή χρόνου· υποστηρίζει τα O.AUDIT και O.NONREP	A.TIME
OE.ADMIN	Περιβάλλον	Έμπιστη και καταρτισμένη διαχείριση	A.ADMIN

Οι OE.IAM και OE.ADMIN μεταφράζουν στη γλώσσα του παρόντος κεφαλαίου το πρώτο μέτωπο της ιεράρχησης του Κεφαλαίου 4. Η οριοθέτηση δεν απαλλάσσει τον οργανισμό από την ευθύνη

του συμπλέγματος ταυτότητας–πρόσβασης–ανθρώπινου παράγοντα. Τη μετατρέπει σε ελέγξιμη προσδοκία από το περιβάλλον του στόχου αξιολόγησης.

Η πληρότητα του σχήματος ελέγχεται αμφίδρομα. Κάθε απειλή του Πίνακα 5.3 αντιστοιχεί σε τουλάχιστον έναν στόχο, κάθε πολιτική υλοποιείται από στόχο, και κάθε παραδοχή καλύπτεται από στόχο περιβάλλοντος. Η πλήρης αντιστοίχιση παρατίθεται στο ST.4.3 του Παραρτήματος ΣΤ'. Αποτελεί, κατά την §3.3, τον σκελετό τεκμηρίωσης (rationale) του στόχου ασφάλειας.

5.3.3 Λειτουργικές απαιτήσεις ασφάλειας

Οι στόχοι εξειδικεύονται σε λειτουργικές απαιτήσεις ασφάλειας (Security Functional Requirements — SFR). Αν ο στόχος λέει *π* πρέπει να επιτυγχάνεται, η απαίτηση το διατυπώνει στην τυποποιημένη γλώσσα του προτύπου, ώστε να μπορεί να ελεγχθεί από τρίτον. Οι απαιτήσεις επιλέγονται από τον κατάλογο κλάσεων, οικογενειών και συνιστωσών του Μέρους 2 του ISO/IEC 15408:2022 [16], [75].

Στο επίπεδο της ετοιμότητας η επιλογή γίνεται σε επίπεδο **οικογένειας**. Η ακριβής στοιχειοθέτηση σε συνιστώσες και η παραμετροποίησή τους ανήκουν στην πλήρη σύνταξη του στόχου ασφάλειας, σε μελλοντική προετοιμασία αξιολόγησης. η αντιστοίχιση οικογένειας–στόχου του Πίνακα 5.7 συνιστά τον πυρήνα της προδιαγραφής.

Πίνακας 5.7. Λειτουργικές απαιτήσεις ασφάλειας σε επίπεδο οικογένειας και αντιστοίχιση στους στόχους.

Οικογένεια (ISO/IEC 15408-2:2022)	Τι καλύπτει	Στόχος
FCO_NRO — μη-αποποίηση προέλευσης	Απόδειξη προέλευσης των παραστατικών, επαληθεύσιμη από τρίτους — ο πυρήνας της προδιαγραφής	O.NONREP
FDP_DAU — αυθεντικοποίηση δεδομένων	Εγγύηση γνησιότητας/εγκυρότητας αποθηκευμένων παραστατικών και εγγραφών	O.INTEGRITY, O.NONREP
FDP_SDI — ακεραιότητα αποθηκευμένων δεδομένων	Ανίχνευση αλλοίωσης δεδομένων εν ηρεμία	O.INTEGRITY
FDP_UIT / FDP_UCT — ακεραιότητα/εμπιστευτικότητα διακινούμενων δεδομένων	Προστασία των δεδομένων χρήστη κατά τη μεταφορά από/προς το κανάλι	O.INTEGRITY, O.CONFID
FCS_COP / FCS_CKM — κρυπτογραφικές πράξεις και διαχείριση κλειδιών	Υπογραφή, επαλήθευση, κρυπτογράφηση· κύκλος ζωής πιστοποιητικών και κλειδιών	O.NONREP, O.CONFID, O.AUTH
FTP_ITC — έμπιστο κανάλι μεταξύ λειτουργιών ασφάλειας	Αμοιβαία αυθεντικοποιημένο, προστατευμένο κανάλι προς την εξωτερική υποδομή διασύνδεσης — η οπτική CYRENE της διοργανωσιακής υπηρεσίας [54]	O.AUTH, O.CONFID
FIA_UID / FIA_UAU — ταυτοποίηση/αυθεντικοποίηση	Ταυτοποίηση και αυθεντικοποίηση πριν από κάθε ενέργεια στη διεπαφή (σε συνεργασία με OE.IAM)	O.AUTH, O.ACCESS
Κλάση FMT (ενδεικτικά FMT_SMF, FMT_SMR) — διαχείριση ασφάλειας	Καθορισμός λειτουργιών διαχείρισης κανόνων επικύρωσης, κλειδιών και ρόλων	O.ACCESS
FAU_GEN / FAU_STG — παραγωγή και αποθήκευση εγγραφών ελέγχου	Πλήρης, χρονοσημασμένη καταγραφή και προστασία των ιχνών από αλλοίωση/απώλεια	O.AUDIT
FPT_STM — αξιόπιστες χρονοσφραγίδες	Χρονοσήμανση εγγραφών και τεκμηρίων (με στήριξη του OE.TIME)	O.AUDIT, O.NONREP

Οικογένεια (ISO/IEC 15408-2:2022)	Τι καλύπτει	Στόχος
FRU_RSA / FPT_RCV — κατανομή πόρων / έμπιστη ανάκαμψη	Έλεγχος κατανομής πόρων της διεπαφής έναντι εξάντλησης· ανάκαμψη της ροής εκκαθάρισης σε συνεπή κατάσταση — το ογκομετρικό σκέλος παραμένει στο περιβάλλον/πάροχο (§4.7.3)	O.AVAIL

Η επιλογή έχει σαφή πυρήνα. Οι οικογένειες FCO_NRO, FCS_COP με FCS_CKM και FTP_ITC καλύπτουν τη μη-αποποίηση, την κρυπτογραφία και το έμπιστο κανάλι. Απαντούν στη βαρύτερη τιμή του προφίλ κινδύνου (E2, I = 36) και στην κεντρική ιδιότητα του αντικείμενου. Οι FAU_GEN και FAU_STG, μαζί με την FPT_STM, καλύπτουν τη λογοδοσία, την οποία η §4.6.3 ανέδειξε ως προϋπόθεση καταλογισμού. Πρόκειται για την τυποποιημένη έκφραση όσων το προφίλ της §5.2.4 υπέδειξε αριθμητικά.

5.3.4 Απαιτήσεις διασφάλισης και όριο ετοιμότητας

Οι απαιτήσεις διασφάλισης ασφάλειας (Security Assurance Requirements — SAR) του Μέρους 3 δεν αφορούν το τι κάνει το αντικείμενο, αλλά **πόσο αυστηρά ελέγχεται** ότι το κάνει. Εδώ δεν επιλέγονται ως πλήρες πακέτο προς αξιολόγηση, γιατί αυτό θα προϋπέθετε εκτέλεση αξιολόγησης, εκτός του επιπέδου του εγχειρήματος. Στο επίπεδο της ετοιμότητας η εργασία τεκμηριώνει τη διαθεσιμότητα του υλικού που θα εξετάζαν οι κλάσεις διασφάλισης, όπως αποτυπώνει ο Πίνακας 5.8.

Πίνακας 5.8. Οι κλάσεις διασφάλισης και το διαθέσιμο υλικό.

Κλάση	Τι εξετάζει	Πού υπάρχει το υλικό
ADV	Περιγραφή σχεδίασης και ορίου	§5.2
AGD	Οδηγίες λειτουργίας	Ροές χειριστή, κανόνες αποδοχής
ALC	Στοιχεία κύκλου ζωής	Εξάρτηση αναδόχου (συστατικό #8), συμβατική διάσταση
ATE	Βάση δοκιμών	Μοντελοποιημένες ροές επικύρωσης
AVA	Ανάλυση ευπαθειών	Μητρώο Κεφαλαίου 4

Η αντιστοίχιση συγκεκριμενοποιείται ως μητρώο τεκμηρίων στην §5.4.2.

Η εργασία δεν επιλέγει ούτε αξιώνει επίπεδο διασφάλισης, πακέτο SAR ή EAL. Η αποτίμηση περιορίζεται στη διαθεσιμότητα υλικού ανά κλάση διασφάλισης και στον εντοπισμό ελλείψεων τεκμηρίωσης. Οποιαδήποτε μελλοντική επιλογή επιπέδου θα απαιτούσε εφαρμοστέο σχήμα, οριστικοποιημένο ΤοΕ, τεκμήρια πραγματικού συστήματος και ανεξάρτητη αξιολόγηση.

Το προφίλ κινδύνου της §5.2.4 λειτουργεί αποκλειστικά ως ένδειξη κρίσιμότητας και προτεραιοποίησης. Καμία τιμή κινδύνου δεν μετατρέπεται σε επίπεδο διασφάλισης· η ανάλυση κινδύνου δείχνει πού βρίσκεται το διακύβευμα, αλλά δεν καθορίζει επίπεδο ή πακέτο αξιολόγησης.

5.4 Μέτρα, αποδεικτικά στοιχεία και προφίλ προστασίας

5.4.1 Από τις απαιτήσεις στα μέτρα: η αντιστοίχιση προς το ISO/IEC 27002:2022

Οι λειτουργικές απαιτήσεις της §5.3.3 είναι διατυπωμένες στη γλώσσα της αξιολόγησης προϊόντος. Τα μέτρα του ISO/IEC 27002:2022 [3] ανήκουν στη γλώσσα του συστήματος διαχείρισης, που χαρτογράφησε το Κεφάλαιο 4. Η αντιστοίχιση των δύο δεν είναι σχήμα ισοδυναμίας — οι δύο κατάλογοι έχουν διαφορετική φύση και κοκκομετρία — αλλά σχήμα **συνέχειας τεκμηρίωσης**: δείχνει ότι οι απαιτήσεις που ο στόχος ασφάλειας διατυπώνει τυπικά αντιστοιχούν σε μέτρα που η ανάλυση κινδύνου έχει ήδη αναδείξει, ιεραρχήσει και εντάξει στην

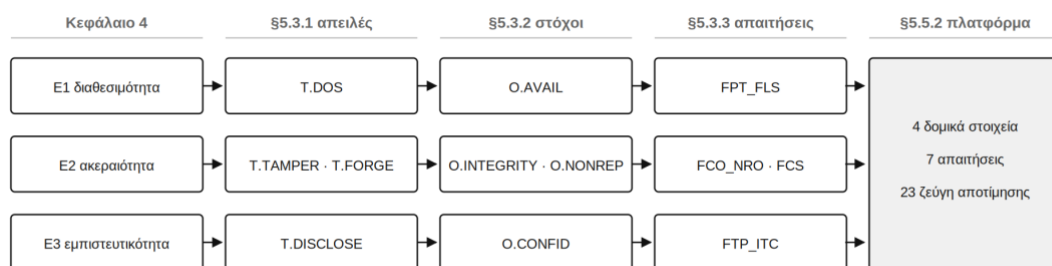
εικόνα κάλυψης του φορέα (§4.7, §4.8). Ο Πίνακας 5.9 αποτυπώνει την αντιστοίχιση, με ρητή σήμανση της συνάντησης με τη χειροκίνητη αντιστοίχιση του εμπλουτισμού της §4.7.3.

Πίνακας 5.9. Αντιστοίχιση στόχων/απαιτήσεων του στόχου αξιολόγησης προς μέτρα του ISO/IEC 27002:2022 και σημεία συνάντησης με την αντιστοίχιση του Κεφαλαίου 4.

Στόχος / απαιτήσεις	Μέτρα ISO/IEC 27002:2022	Συνάντηση με το Κεφάλαιο 4
O.NONREP, O.AUTH — FCO_NRO, FCS_COP/CKM	8.24 χρήση κρυπτογραφίας	Αντιστοιχίστηκε στο E2 (§4.7.3)· τρίτο μέτωπο ιεράρχησης
O.INTEGRITY — FDP_SDI, FDP_UIT	8.26 απαιτήσεις ασφάλειας εφαρμογών · 8.20/8.21 ασφάλεια/υπηρεσίες δικτύων	Το 8.26 αντιστοιχίστηκε στο E2 ως ρητή απαίτηση επικύρωσης εισόδων· το 8.20 στο E1
O.AUTH, O.CONFID — FTP_ITC, FDP_UCT	5.14 μεταφορά πληροφοριών · 5.19–5.23 σχέσεις προμηθευτών/αλυσίδα ΤΠΕ	Το 5.14 αντιστοιχίστηκε στο E2· τα 5.19–5.23 εκφράζουν τη διοργανωσιακή όψη του καναλιού — η γωνία CYRENE [54]
O.AUDIT — FAU_GEN/STG, FPT_STM	8.15 καταγραφή · 8.16 παρακολούθηση δραστηριοτήτων	Αντιστοιχίστηκαν στο E3 (§4.7.3)· το 8.16 και στο E1
O.AVAIL — FRU_RSA/FPT_RCV (λειτουργική συνέχεια)	8.6 διαχείριση χωρητικότητας · 8.13/8.14 αντίγραφα/πλεονασμός · 5.30 ετοιμότητα ΤΠΕ για επιχειρησιακή συνέχεια	Τα 8.6 και 5.30 από τη δέσμη του E1 (§4.7.3) — δεύτερο μέτωπο· το 8.13 από τη δέσμη του E3· ρητό το σκέλος επιμερισμού προς τον πάροχο
O.ACCESS — FIA_, FMT_	5.15–5.18 έλεγχος πρόσβασης/ταυτότητα · 8.2–8.5 προνομιακή πρόσβαση	Οικογένεια του πρώτου μετώπου — κατά κύριο λόγο στο περιβάλλον (OE.IAM/OE.ADMIN)
P.RETENTION, O.INTEGRITY — τεκμήρια	5.33 προστασία αρχείων · 8.12 πρόληψη διαρροής	Θεσμική ανάγνωση της §4.6.3 (ίχνη/τεκμήρια)

Η αντιστοίχιση συνδέεται με την §4.7.4. Τα μέτρα που εκεί συγκρότησαν το δεύτερο και το τρίτο μέτωπο αντιμετώπισης, δηλαδή τη διαθεσιμότητα των καναλιών και την ακεραιότητα του περιεχομένου, αντιστοιχούν εδώ σε τεχνικές απαιτήσεις του στόχου αξιολόγησης.

Η διαδρομή λειτουργεί και αντίστροφα: από κάθε γραμμή του προφίλ κινδύνου (§5.2.4), μέσω απειλής (§5.3.1) και στόχου (§5.3.2), σε απαίτηση (§5.3.3) και μέτρο. Η αλυσίδα αυτή αποτελεί η ίδια τεκμήριο ετοιμότητας.



Κάθε τιμή κινδύνου ανάγεται σε απαίτηση· καμία δεν μετατρέπεται σε επίπεδο διασφάλισης.

Εικόνα 5.2. Η αλυσίδα ιχνηλασιμότητας από την επίπτωση του Κεφαλαίου 4 έως την αποτύπωση στην πλατφόρμα.

5.4.2 Μητρώο αποδεικτικών στοιχείων ετοιμότητας

Η ετοιμότητα δεν επιδεικνύεται με διαβεβαιώσεις αλλά με απαριθμήσιμα τεκμήρια. Το μητρώο που ακολουθεί απογράφει τι έχει παραχθεί στο πλαίσιο της εργασίας, πού τεκμηριώνεται, και σε ποια κλάση διασφάλισης της §5.3.4 θα προσφερόταν ως πρώτη ύλη σε μια μελλοντική, πραγματική προετοιμασία αξιολόγησης.

Πίνακας 5.10. Μητρώο αποδεικτικών στοιχείων ετοιμότητας.

Τεκμήριο	Πηγή στην εργασία	Κλάση
Περιγραφή και όριο του στόχου αξιολόγησης, διεπαφές	§5.2.1–§5.2.2	ADV
Μητρώο περιουσιακών στοιχείων με ιχνηλασιμότητα στο μοντέλο κινδύνου	Πίνακας 5.1 ← §4.4	ADV / ASE
Μοντέλο απειλών με ποσοτική θεμελίωση	Πίνακας 5.3 ← Πίνακας 5.2 ← §4.6	ASE
Στόχοι, τεκμηρίωση αντιστοίχισης, απαιτήσεις σε επίπεδο οικογένειας	§5.3.2–§5.3.3	ASE
Πίνακας αντιστοίχισης απαιτήσεων → μέτρων, με εικόνα κάλυψης	Πίνακας 5.9 ← §4.7–§4.8	ASE / ALC
Κατάσταση μέτρων κατά την παραδοχή ωριμότητας και αποκλίσεις	§4.8 (φύλλο αποκλίσεων· τριβάθμια κατάσταση)	ALC
Σημειώσεις επικύρωσης της μοντελοποιημένης ροής (κανόνες αποδοχής, ακεραιότητα, μη-αποποίηση)	§5.5 — συμπληρώνεται με την ενσάρκωση στην πλατφόρμα	ATE
Ανάλυση ευπαθειών ως πρώτη ύλη: μητρώο 90 μοναδικών γραμμών, τριάδες εμπλουτισμού, εξαγωγές επαληθευμένες προγραμματιστικά	Κεφ. 4 (§4.5–§4.6, Παραρτήματα)	AVA
Αποτίμηση ετοιμότητας (τι υφίσταται — τι εκκρεμεί)	§5.4.2 (παρούσα) + §5.6	—

Υπάρχουν πέντε βασικά τεκμήρια: ορισμός ΤοΕ και ορίου, επαληθευμένο προφίλ κινδύνου, πρόβλημα ασφάλειας με *rationale*, απαιτήσεις σε επίπεδο οικογένειας και αντιστοίχιση μέτρων. Εκκρεμούν η εξειδίκευση των απαιτήσεων σε συνιστώσες, λειτουργική τεκμηρίωση AGD/ATE και πραγματικά τεκμήρια συστήματος. Η αποτίμηση ετοιμότητας είναι επομένως χάρτης υπάρχοντος και ελλείψεων, όχι βαθμολογία.

5.4.3 Προφίλ προστασίας και προσχέδιο στόχου ασφάλειας

Η §3.3 διέκρινε τα δύο τεχνουργήματα της προδιαγραφής: το προφίλ προστασίας (Protection Profile — PP), δήλωση αναγκών ανεξάρτητη υλοποίησης για έναν **τύπο** στόχου αξιολόγησης, και τον στόχο ασφάλειας (Security Target — ST), δήλωση εξαρτημένη υλοποίησης για **συγκεκριμένο** αντικείμενο [16]. Το υλικό των §§5.2–5.4 υπηρετεί και τα δύο, με διαφορετική ωριμότητα. Ως προς το δεύτερο, οι ενότητες συγκροτούν ήδη τα δομικά μέρη ενός προσχεδίου στόχου ασφάλειας: εισαγωγή και περιγραφή του αντικειμένου (§5.2.1–§5.2.2), περιουσιακά στοιχεία (§5.2.3), ορισμό προβλήματος ασφάλειας (§5.3.1), στόχους με τεκμηρίωση (§5.3.2), απαιτήσεις (§5.3.3–§5.3.4) και σύνοψη αντιστοίχισης προς μέτρα (§5.4.1). Η ενιαία τους αναδιάταξη παρατίθεται στο Παράρτημα ΣΤ', ώστε το προσχέδιο να υφίσταται και ως αυτοτελές τεχνουργήμα. Ως προς το πρώτο, αν αφαιρεθεί το συγκεκριμένο αρχέτυπο και διατηρηθούν οι απειλές, οι στόχοι και ο πυρήνας των απαιτήσεων, σκιαγραφείται ένα προφίλ προστασίας για την κατηγορία «διεπαφή ηλεκτρονικής τιμολόγησης και εκκαθάρισης δημόσιου ERP». Πρόκειται για δήλωση κοινών αναγκών, που θα μπορούσε να λειτουργήσει ως σημείο αναφοράς προδιαγραφών προμήθειας στο δημόσιο οικοσύστημα — τη λειτουργία δηλαδή που το πρότυπο επιφυλάσσει στα προφίλ προστασίας [16]. Η εργασία περιορίζεται στη σκιαγράφηση: η πλήρης σύνταξη και εγγραφή ενός προφίλ προστασίας συνιστά αυτοτελές εγχείρημα, πέραν της επίδειξης ετοιμότητας.

Τη θεσμική προοπτική της διαδρομής κλείνει η υπενθύμιση της υποδομής που θα υποδεχόταν ένα ώριμο αντικείμενο: αξιολόγηση από εργαστήριο ITSEF διαπιστευμένο κατά ISO/IEC 17025 [44] και πιστοποίηση από φορέα διαπιστευμένο κατά ISO/IEC 17065 [45], κατά τη θεσμική

αλυσίδα του σχήματος EUCC [20] που παρουσιάστηκε στις §§3.2–3.5. Η αναφορά παραμένει, ρητά, αναφορική: οριοθετεί το σημείο όπου η ετοιμότητα θα συναντούσε τον θεσμό, χωρίς η εργασία να εκτελεί κανένα βήμα της αλυσίδας αυτής.

5.5 Ενδεικτικό workflow προσέγγισης προς πιστοποίηση

5.5.1 Η λογική του workflow

Η διαδρομή των §§5.2 έως 5.4 ακολουθεί ρητή και επαναλήψιμη σειρά βημάτων, την οποία η ενότητα αυτή αποτυπώνει ως ενδεικτικό workflow οκτώ βημάτων στον Πίνακα 5.11. Η δυνατότητα γενίκευσής της δεν ελέγχθηκε και παραμένει ανοικτό ερώτημα (§6.3).

Πίνακας 5.11. Τα οκτώ βήματα της προσέγγισης προς πιστοποίηση.

#	Βήμα	Πού έγινε
1	Οριοθέτηση αντικείμενου και ορίου	§5.2.1–5.2.2
2	Απογραφή περιουσιακών στοιχείων, με ιχνηλασιμότητα στην ανάλυση κινδύνου	§5.2.3
3	Διατύπωση προβλήματος ασφάλειας: απειλές, παραδοχές, πολιτικές	§5.3.1
4	Συναγωγή στόχων για το αντικείμενο και το περιβάλλον	§5.3.2
5	Εξειδίκευση σε απαιτήσεις κατά ISO/IEC 15408	§5.3.3–5.3.4
6	Αντιστοίχιση σε μέτρα και εικόνα κάλυψης	§5.4.1
7	Συγκρότηση μητρώου τεκμηρίων	§5.4.2
8	Αποτίμηση ετοιμότητας και προσχέδιο στόχου ασφάλειας	§5.4.3, Παράρτημα ΣΤ´

Τα βήματα 1 έως 5 εκτελέστηκαν με δημόσια τεκμηρίωση, χωρίς εργαλείο. Τα βήματα 6 έως 8 συνδέουν την προδιαγραφή με την εικόνα του συστήματος διαχείρισης του Κεφαλαίου 4. Η σειρά έχει σημασία: η μεθοδολογική εργασία συγκροτήθηκε πρώτη και το εργαλείο κλήθηκε μετά.

5.5.2 Η αποτύπωση στην πλατφόρμα του έργου

Το αντικείμενο αξιολόγησης καταχωρίστηκε ως Product και παρέμεινε σε κατάσταση Draft, με τέσσερα δομικά στοιχεία συνδεδεμένα σε αυτό, όλα δηλωμένα ως Internal. Η επιλογή τους ακολουθεί τον Πίνακα 5.1 και διατηρεί την ιχνηλασιμότητα προς το μοντέλο του Κεφαλαίου 4· ο Πίνακας 5.12 δίνει την αντιστοιχία.

Πίνακας 5.12. Τα δομικά στοιχεία που καταχωρίστηκαν στην πλατφόρμα και η αντιστοιχία τους με τον Πίνακα 5.1.

Κωδ.	Όνομα στην πλατφόρμα	Αντιστοιχία	Άγκυρα Κεφ. 4
A1	Invoice Reception & Validation Service	Διεργασία παραλαβής, επικύρωσης και εκκαθάρισης	P3a (Service)
A2	e-Invoicing Interface Software	Λογισμικό της διεπαφής	S3 (Global)
A3	Interoperability Transmission Connector (KED/PEPPOL) incl. signing certificates & keys	Κανάλι διασύνδεσης, με πιστοποιητικά και κλειδιά υπογραφής	N1
A4	Interface Audit Logging	Τοπικό ίχνος καταγραφής της διεπαφής	S5 (Local)

Το περιεχόμενο του τιμολογίου (P3b) δεν καταχωρίστηκε ως χωριστό δομικό στοιχείο. Στην πλατφόρμα το asset είναι φορέας λειτουργικότητας, ενώ το P3b είναι πληροφορία που διακινείται μέσα από τα υπόλοιπα. Η επιλογή είναι συνειδητή και σημειώνεται εδώ, ώστε η απόκλιση από τον Πίνακα 5.1 να μη διαβαστεί ως παράλειψη.

Επιλέχθηκαν οι κατηγορίες STRIDE Repudiation και DenialOfService. Παρήγαγαν τέσσερις στόχους: OT.ACCOUNTABILITY και OT.AUDIT_PROTECTION για τέσσερα assets, και OT.KNOWN_STATE και OT.SELF_PROTECTION για τρία.

Από τους στόχους αυτούς προέκυψαν αυτόματα επτά λειτουργικές απαιτήσεις ασφάλειας, με πραγματικούς κωδικούς ISO/IEC 15408 και με αντίστροφη ιχνηλασιμότητα προς τον στόχο που τις γέννησε. Κάθε απαίτηση συνδυάστηκε με τα δομικά στοιχεία στα οποία εφαρμόζεται, παράγοντας ζεύγη αποτίμησης, όπως συγκεντρώνει ο Πίνακας 5.13.

Πίνακας 5.13. Οι επτά λειτουργικές απαιτήσεις που παρήγαγε η πλατφόρμα και τα ζεύγη αποτίμησης ανά απαίτηση.

Απαίτηση	Κάλυψη	Ζεύγη
FAU_GEN.1	Πλήρης	4
FAU_STG.1	Πλήρης	4
FPT_FLS.1	Μερική	3
FAU_SEL.1	Μερική	3
FDP_RIP.1	Μερική	3
FPT_TST_EXT.1	Μερική	3
FMT_SMF.1	Μερική	3
Σύνολο		23

Οι μετρητές της πλατφόρμας επιβεβαίωσαν τέσσερα assets, τέσσερις στόχους, επτά απαιτήσεις και είκοσι τρία σημεία αποτίμησης. Οι FAU_GEN.1 και FAU_STG.1 συμπίπτουν με οικογένειες του Παραρτήματος ΣΤ'. Η σύμπτωση είναι συγκλίνουσα ένδειξη και όχι ανεξάρτητη επικύρωση.

Για την ολοκλήρωση της δοκιμαστικής ροής καταχωρίστηκε το EAL2 ως υποχρεωτική τεχνική παράμετρος της πλατφόρμας. Η καταχώριση δεν αποτελεί επιλογή πακέτου διασφάλισης, αξίωση EAL, απονομή επιπέδου EUCC ή αριθμητική σύνδεση με τα αποτελέσματα του MONARC. Η λεπτομερής αυτόματη αλυσίδα που εμφανίστηκε στην πλατφόρμα διατηρήθηκε στο εσωτερικό audit trail και δεν χρησιμοποιείται ως εύρημα ή βάση συμπεράσματος.

Η αποτίμηση γίνεται ανά ζεύγος απαίτησης–asset. Το Compliance συμπληρώνεται από τον κάτοχο και το Verdict από τον αξιολογητή. Ο κάτοχος έχει τρεις επιλογές και ο αξιολογητής τέσσερις, περιλαμβανομένου του Inconclusive, αποτυπώνοντας τη διάκριση ρόλων του ISO/IEC 18045 [17].

Συμπληρώθηκαν δύο δηλώσεις Compliance, με το πεδίο Verdict να παραμένει κενό. Στο ζεύγος του λογισμικού διεπαφής με την FAU_GEN.1 δηλώθηκε Positive, με σημείωση ότι στηρίζεται στην προδιαγραφή του Παραρτήματος ΣΤ' και όχι σε ανεξάρτητη επαλήθευση. Στο

ζεύγος με την FPT_TST_EXT.1 δηλώθηκε Negative, ως διευρυμένη συνιστώσα την οποία η προδιαγραφή δεν αξιώνει και για την οποία δεν υπάρχει τεκμήριο. Η επιλογή να μη δηλωθούν όλα θετικά είναι μέρος της άσκησης: η αποτίμηση ετοιμότητας καταγράφει και τα κενά.

Με βάση τα παραπάνω παρήχθη σύνθετο προφίλ προστασίας (Composite Protection Profile). Η αντιπαραβολή του με τη σκιαγράφηση της §5.4.3 γίνεται στην §5.6.3, ώστε να διατηρηθεί η χρονική σειρά: η σκιαγράφηση διατυπώθηκε πριν από την παρατήρηση.

Ο δείκτης κινδύνου της πλατφόρμας έμεινε 0,0% επειδή δεν καταχωρίστηκαν ευπάθειες. Δεν σχετίζεται με τις τιμές MONARC του Κεφαλαίου 4 και οι δύο δείκτες δεν συγκρίνονται ούτε μετατρέπονται.

Η πλατφόρμα υποστήριξε τη δομημένη καταχώριση απαιτήσεων και την αποτίμηση ανά ζεύγος, όχι την αντιστοίχιση οργανωσιακών δικλίδων. Το πεδίο μέτρων έμεινε κενό, άρα η χαρτογράφηση προς ISO/IEC 27002:2022 του Πίνακα 5.9 παραμένει εκτός πλατφόρμας.

5.6 Συγκριτική αποτίμηση των δύο προσεγγίσεων και των εργαλείων

5.6.1 Δύο ερωτήματα, δύο παραδείγματα — μία σχέση παραλληλίας

Οι δύο άξονες απαντούν σε διαφορετικά ερωτήματα. Η ανάλυση κινδύνου είναι συνεχής και οργανωσιακή, παράγοντας μητρώο κινδύνων και μέτρωπα αντιμετώπισης. Η ετοιμότητα πιστοποίησης είναι οριοθετημένη και αποδεικτική, παράγοντας προσχέδιο ST και μητρώο τεκμηρίων. Δεν είναι διαδοχικά στάδια της ίδιας διεργασίας, αλλά παράλληλες προσεγγίσεις, όπως δείχνουν CYRENE και TVRA [54], [56].

5.6.2 Η συμπληρωματικότητα στην πράξη: τι έδωσε ο ένας άξονας στον άλλον

Η ανάλυση κινδύνου έδωσε στον δεύτερο άξονα επιλογή ΤοΕ, ιεράρχηση απαιτήσεων και μέτρο κρισιμότητας. Ο άξονας ετοιμότητας επέστρεψε σαφές όριο, τυποποιημένη γλώσσα και απαίτηση τεκμηρίων. Το ανθρώπινο/οργανωσιακό εύρημα μετατράπηκε σε ρητές παραδοχές και στόχους περιβάλλοντος. Η συμπληρωματικότητα επιδείχθηκε στο συγκεκριμένο αρχέτυπο, χωρίς αξίωση γενικής επικύρωσης.

5.6.3 Τα εργαλεία: MONARC και πλατφόρμα CUSTODES

Η σύγκριση σε επίπεδο εργαλείων οριοθετείται από την ασυμμετρία ωριμότητας: το MONARC είναι εδραιωμένο εργαλείο ανοικτού κώδικα με σταθερή βάση γνώσης, ενώ η πλατφόρμα του CUSTODES είναι ερευνητικό σύστημα εν εξελίξει — η αντιπαραβολή αφορά συνεπώς τον **προσανατολισμό** τους, όχι βαθμολόγηση. Οι διαστάσεις της σύγκρισης προκύπτουν ήδη από τη μεθοδολογική εργασία και συνοψίζονται στον Πίνακα 5.14.

Τα εμπειρικά ευρήματα προέρχονται από μία πλατφόρμα, δύο συνεδρίες, έναν παρατηρητή και ένα ΤοΕ στη συγκεκριμένη κατάσταση λογισμικού. Χρειάζονται ανεξάρτητη επανάληψη και δεύτερο τύπο αντικειμένου. Δεν γενικεύονται στα Common Criteria ή σε άλλα εργαλεία.

Δηλώνεται επίσης μια διόρθωση της ίδιας της παρατήρησης. Οι πρώτες λήψεις κατέγραψαν επτά κατηγορίες απειλής, επειδή αποτυπώθηκε μόνο η πρώτη οθόνη του καταλόγου, ενώ ο επανέλεγχος έδειξε τριάντα τρεις — το αρχικό συμπέρασμα ήταν μερικό και αντικαταστάθηκε. Η αρχή που προκύπτει εφαρμόζεται στη συνέχεια συστηματικά: πριν καταγραφεί απουσία, επιβεβαιώνεται ότι ο κατάλογος εξαντλήθηκε.

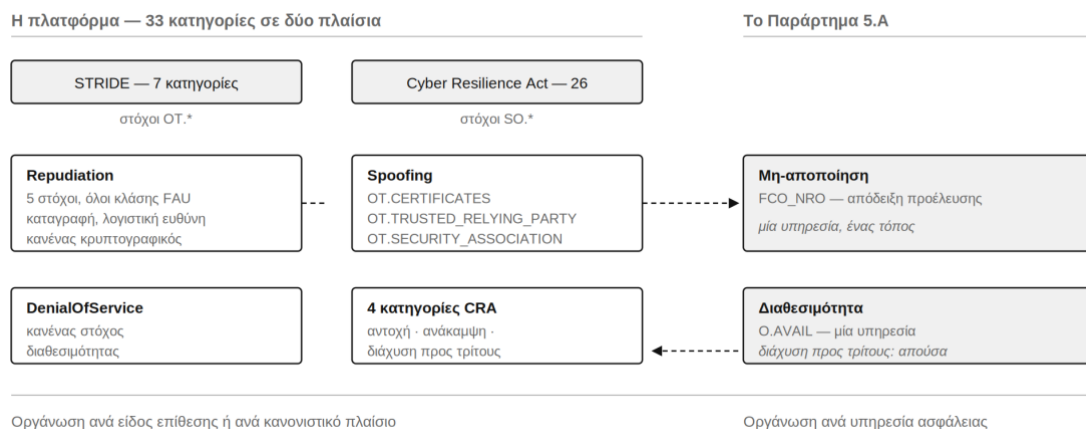
Το κύριο εύρημα αφορά τη δομή του καταλόγου, όπως τη σκιαγράφησε η §5.1.3: δύο πλαίσια συνυπάρχουν, το STRIDE και ο Cyber Resilience Act, με χωριστό λεξιλόγιο στόχων το καθένα. Απέναντί τους το Παράρτημα ΣΤ' έχει μία μόνο οντολογία, οργανωμένη κατά υπηρεσία ασφάλειας όπως ορίζουν τα Common Criteria. Από τη συνάντηση των δύο δομών προέκυψε το ίδιο μοτίβο δύο φορές, ανεξάρτητα.

Η πρώτη εκδήλωση αφορά τη μη-αποποίηση, που είναι ο πυρήνας του συγκεκριμένου αντικειμένου και εκφράζεται στο προσχέδιο με την οικογένεια FCO_NRO. Στην κατηγορία Repudiation η πλατφόρμα προσφέρει πέντε στόχους, όλους της κλάσης FAU: λογιστική ευθύνη,

προστασία ιχνών, παρακολούθηση συστήματος, καταγραφή μέσων και απόκριση σε απώλεια ιχνών. Κανένας δεν είναι κρυπτογραφικός. Το κρυπτογραφικό λεξιλόγιο υπάρχει — OT.CERTIFICATES, OT.TRUSTED_RELIVING_PARTY, OT.SECURITY_ASSOCIATION— αλλά είναι καλωδιωμένο στην κατηγορία Spoofing. Πρόκειται για δρομολόγηση, όχι για έλλειψη, και η διάκριση αυτή είναι ουσιώδης.

Η δρομολόγηση εξηγείται από τον ίδιο τον ορισμό που η πλατφόρμα δίνει στην κατηγορία: δυνατότητα άρνησης ενεργειών λόγω απουσίας λογιστικής ευθύνης. Με αυτόν τον ορισμό η επιλογή στόχων καταγραφής είναι απολύτως συνεπής. Τα Common Criteria όμως αντιμετωπίζουν τη μη-αποποίηση και ως κρυπτογραφική απόδειξη προέλευσης, όχι μόνο ως λογιστική ευθύνη. Η απόκλιση συνεπώς δεν βαρύνει καμία πλευρά: προκύπτει από δύο διαφορετικούς ορισμούς της ίδιας έννοιας.

Η δεύτερη εκδήλωση αφορά τη διαθεσιμότητα. Στην κατηγορία DenialOfService του STRIDE δεν προσφέρεται στόχος διαθεσιμότητας. Στο πλαίσιο του Cyber Resilience Act προσφέρονται τέσσερις, σε χρονική διάρθρωση: αντοχή κατά τη διάρκεια του περιστατικού, ανάκαμψη μετά από αυτό, και δύο που αφορούν τη διάχυση της βλάβης προς τρίτους. Επαναλαμβάνεται δηλαδή το ίδιο σχήμα, με το λεξιλόγιο να υπάρχει αλλά να ανήκει σε άλλο πλαίσιο.



Εικόνα 5.3. Οι δύο οντολογίες σε αντιπαράθεση: το ίδιο λεξιλόγιο, διαφορετική οργάνωση.

Η αντιπαράθεση απέδωσε γνώση και προς την αντίθετη κατεύθυνση. Οι δύο στόχοι που αφορούν τη διάχυση προς τρίτους εκφράζουν μια διάσταση που το προσχέδιο του Παραρτήματος ΣΤ΄ δεν περιλαμβάνει καθόλου: το αντικείμενο ως φορέας βλάβης προς άλλα συστήματα. Για διεπαφή συνδεδεμένη με ΚΕΔ και ΡΕΡΡΟΛ η διάσταση αυτή είναι εύλογη. Η παράλειψη καταγράφεται ως κενό του προσχεδίου και όχι ως αδυναμία του εργαλείου.

Η πλατφόρμα παρήγαγε σύνθετο προφίλ, όπως είχε προβλεφθεί για ΤοΕ από δομικά στοιχεία. Διαφέρει όμως στο περιεχόμενο: οργανώνεται γύρω από τους στόχους των επιλεγμένων κατηγοριών, ενώ η σκιαγράφηση της §5.4.3 γύρω από επτά υπηρεσίες ασφάλειας.

Πίνακας 5.14. Αντιπαράθεση των δύο εργαλείων κατά τις διαστάσεις της §5.6.3.

Διάσταση	MONARC (Κεφ. 4)	Πλατφόρμα CUSTODES (Κεφ. 5)
Μονάδα εργασίας	Μητρώο κινδύνων οργανισμού	Αντικείμενο αξιολόγησης με δομικά στοιχεία
Πρώτη ύλη	Βάση γνώσης απειλών και ευπαθειών	Κατάλογος κατηγοριών απειλής και στόχων
Οργανωτική αρχή	Αγαθό και κίνδυνος	Κατηγορία επίθεσης και κανονιστικό πλαίσιο
Έξοδος	Ιεραρχημένος κίνδυνος και μέτρα	Απαιτήσεις, ζεύγη αποτίμησης, προφίλ προστασίας
Σχέση με τον χρόνο	Περιοδική επανεκτίμηση	Διατήρηση διασφάλισης
Ρόλοι	Ενιαίος αναλυτής	Διακριτοί κάτοχοι και αξιολογητές, με ασύμμετρες κλίμακες

Διάσταση	MONARC (Κεφ. 4)	Πλατφόρμα CUSTODES (Κεφ. 5)
Ποσοτικός δείκτης	$R = I \times T \times V$, τιμές 1 έως 64	Δείκτης επί καταχωρισμένων ευπαθειών

Οι δείκτες MONARC και CUSTODES μετρούν διαφορετικά πράγματα και δεν μετατρέπονται μεταξύ τους. Η ανάλυση κινδύνου επιλέγει και ιεραρχεί το ToE και τις απαιτήσεις, αλλά δεν παράγει επίπεδο διασφάλισης. Τυχόν μελλοντική επιλογή επιπέδου θα απαιτούσε χωριστή αιτιολόγηση στο πλαίσιο εφαρμοστέου σχήματος και ανεξάρτητης αξιολόγησης.

Η διατύπωση που μπορεί να μεταφερθεί πέραν της συγκεκριμένης παρατήρησης είναι η ακόλουθη. Όταν ένα εργαλείο συνθέτει περισσότερες από μία ταξινομίες απειλών, οι υπηρεσίες ασφάλειας κατανέμονται ανά είδος επίθεσης ή ανά κανονιστικό πλαίσιο και όχι ανά υπηρεσία. Ο συντάκτης στόχου ασφάλειας που αναζητά στόχο με βάση την υπηρεσία ενδέχεται να μην τον εντοπίσει, ακόμη και όταν υπάρχει.

Ως προς την πρωτοτυπία τηρείται περιορισμένη διατύπωση: δεν εντοπίστηκε δημοσιευμένη καταγραφή μοντελοποίησης αντικειμένου τύπου υπηρεσίας στη συγκεκριμένη πλατφόρμα, πράγμα που δεν σημαίνει ότι δεν έχει γίνει, παρά μόνο ότι δεν είναι δημοσιευμένη.

Η αποτίμηση του κεφαλαίου τροφοδοτεί ευθέως τα ερευνητικά ερωτήματα της εργασίας: η επίδειξη ετοιμότητας επί οριοθετημένου υποσυστήματος υψηλής κρισιμότητας απαντά στο τρίτο ερευνητικό ερώτημα, ενώ η εμπειρικά τεκμηριωμένη συμπληρωματικότητα των δύο αξόνων συγκροτεί την απάντηση του τετάρτου — αντικείμενο συστηματικής σύνθεσης στο Κεφάλαιο 6.

6. Συμπεράσματα

6.1 Απαντήσεις στα ερευνητικά ερωτήματα

Τα τέσσερα ερευνητικά ερωτήματα απαντώνται με την ίδια δομή: σύντομη απάντηση, τεκμήριο, όριο και πρακτική συνέπεια.

Πρώτο ερώτημα: ποιοι είναι οι κύριοι κίνδυνοι ενός δημόσιου συστήματος οικονομικής διαχείρισης και πώς εντοπίζονται συστηματικά. Οι σοβαρότεροι κίνδυνοι του αρχετύπου συγκεντρώνονται κατά κύριο λόγο στην ταυτότητα, την πρόσβαση και την ανθρώπινη συμπεριφορά, χωρίς αυτό να αναιρεί τη συμβολή της τεχνολογικής υποδομής.

Το μητρώο κινδύνων περιλαμβάνει 16 απειλές, 200 τοποθετήσεις και 90 μοναδικές γραμμές. Με $R = I \times T \times V$ και κατώφλια 8/27, 48 γραμμές ήταν μη αποδεκτές, 42 ενδιάμεσες και καμία πλήρως αποδεκτή. Οι 11 μέγιστες γραμμές αφορούν σταθμούς εργασίας, προσωπικό, διαχειριστές και οργάνωση πληροφορικής, με πλαστοπροσωπία και κακόβουλο λογισμικό. Δύο εξαγωγές και χωριστός επανυπολογισμός έδωσαν μηδενικές αποκλίσεις. Οι κλίμακες ENISA χρησιμοποιήθηκαν ως κοινή αναφορά, όχι ως δεύτερη μέθοδος.

Οι τιμές βασίζονται σε ρητές παραδοχές και μη εγκεκριμένα κατώφλια, άρα αποδίδουν σχετική προτεραιότητα και όχι απόλυτη έκθεση πραγματικού φορέα.

Το εύρημα έχει πρακτική συνέπεια. Ένας φορέας που θα διάβαζε μόνο τον κατάλογο των μηχανημάτων του θα επένδυε σε εξοπλισμό και σε τείχη προστασίας, ενώ το μοντέλο δείχνει ότι η μεγαλύτερη έκθεση βρίσκεται σε πρόσωπα, ρόλους και καθημερινές πρακτικές.

Δεύτερο ερώτημα: πώς αποτιμάται η οργανωτική ετοιμότητα και ποιες παρεμβάσεις υποδεικνύει. Η σύγκριση με έναν διεθνή κατάλογο μέτρων δείχνει τρεις κατηγορίες παρέμβασης, δηλαδή ποιος λογοδοτεί, ποιος γνωρίζει να κάνει τι, και ποιες διαδικασίες υπάρχουν γραμμένες και δοκιμασμένες.

Το φύλλο αποκλίσεων κατανέμει τα 93 μέτρα σε 16 θεσμικά κατοχυρωμένα, 42 κεντρικά παρεχόμενα χωρίς τοπική επαλήθευση και 35 υπό διαμόρφωση. Τα σενάρια ενεργοποίησαν 61 μέτρα, με επτά από τα οκτώ της κατηγορίας «Ανθρώποι». Και τα έξι μέτρα του πρώτου μετώπου ανήκουν στις μη σταθεροποιημένες πρακτικές. Οι 22 εθνικές απαιτήσεις επιβεβαιώνουν τη σημασία πολιτικών πρόσβασης, κατανομής αρμοδιοτήτων και ευθύνης διοίκησης.

Το 61/93 δείχνει εύρος χαρτογράφησης, όχι βαθμό συμμόρφωσης, εφαρμογής ή αποτελεσματικότητας. Η εργασία δεν εκδίδει ετυμηγορία συμμόρφωσης ούτε ταξινομεί νομικά το αρχέτυπο.

Κρίσιμο είναι το είδος της απόστασης που μετράται. Ο δρόμος ενός φορέα προς ένα πιστοποιήσιμο σύστημα διαχείρισης δεν είναι κυρίως τεχνολογικός, αλλά αφορά ρόλους που δεν έχουν οριστεί, διαδικασίες που δεν έχουν γραφτεί και αποδείξεις που δεν έχουν παραχθεί.

Τρίτο ερώτημα: πώς αποτιμάται η ετοιμότητα ενός κρίσιμου υποσυστήματος προς μελλοντική αξιολόγηση. Η ετοιμότητα αποτιμάται όταν παραχθούν δύο πράγματα, ένα κείμενο που περιγράφει τι ακριβώς προστατεύεται και με ποιον τρόπο, και ένας κατάλογος των αποδείξεων που το στηρίζουν.

Η πλατφόρμα δέχθηκε τέσσερα δομικά στοιχεία service-type ToE χωρίς CPE ή SBOM. Δύο κατηγορίες απειλής παρήγαγαν τέσσερις στόχους, επτά SFR και 23 ζεύγη αποτίμησης, με ιχνηλασιμότητα προς τον στόχο. Η διεπαφή διακρίνει τον κάτοχο από τον αξιολογητή και επιτρέπει στον δεύτερο να δηλώσει ανεπαρκή τεκμήρια.

Η «Start Assessment» δεν ενεργοποιήθηκε, δεν απονεμήθηκε επίπεδο και δεν διεκδικήθηκε επιλεξιμότητα EUCC. Πραγματική αξιολόγηση θα απαιτούσε διαπιστευμένο εργαστήριο και φορέα πιστοποίησης. Το Compliance συμπληρώθηκε μόνο από τον κάτοχο, χωρίς ανεξάρτητο Verdict, και μία από τις δύο δηλώσεις ήταν αρνητική λόγω έλλειψης τεκμηρίου.

Έτσι η ετοιμότητα γίνεται απარიθμηση. Παύει να είναι διαβεβαίωση και γίνεται κατάλογος του τι υπάρχει και του τι λείπει, τον οποίο ένας φορέας μπορεί να χρησιμοποιήσει ως σχέδιο εργασίας πριν καν απευθυνθεί σε αξιολογητή.

Τέταρτο ερώτημα: πόσο συμπληρώνονται οι δύο άξονες και πού σταματούν. Οι δύο άξονες λειτουργούν παράλληλα και τροφοδοτεί ο ένας τον άλλον, χωρίς όμως να μοιράζονται κοινή μονάδα μέτρησης.

Η ανάλυση κινδύνου έδωσε επιλογή αντικειμένου, προτεραιότητες και κρισιμότητα. Η ετοιμότητα επέστρεψε σαφές όριο, κοινή γλώσσα απαιτήσεων και απαίτηση αποδείξεων. Ο ανθρώπινος και οργανωτικός παράγοντας μετατράπηκε σε ρητές, ελέγξιμες παραδοχές περιβάλλοντος.

Καμία αριθμητική αντιστοίχιση δεν επιχειρήθηκε μεταξύ βαθμού κινδύνου και επιπέδου ελέγχου, όπως αναπτύσσεται αμέσως παρακάτω. Η συμπληρωματικότητα δείχθηκε σε ένα αρχέτυπο, ένα αντικείμενο και μία χρονική περίοδο, οπότε δεν αποδεικνύεται ότι ισχύει για κάθε συνδυασμό εργαλείων ή για κάθε τύπο συστήματος.

Η ανάλυση κινδύνου και η ετοιμότητα προς πιστοποίηση απαντούν σε διαφορετικά ερωτήματα· το ένα δεν καλύπτει αυτομάτως το άλλο.

6.2 Κύρια ευρήματα και συνεισφορά της εργασίας

Η εργασία παρήγαγε τρία ευρήματα που δεν προϋπήρχαν σε κανένα από τα κεφάλαιά της. Το πρώτο αφορά τη σχέση των δύο αξόνων, το δεύτερο προέκυψε από την παρατήρηση της πλατφόρμας, και το τρίτο στρέφεται προς την ίδια την εργασία.

Η διαδρομή κίνδυνος → ΤοΕ → απειλές → στόχοι → απαιτήσεις → τεκμήρια καταγράφηκε με διατηρημένα ενδιάμεσα προϊόντα, ώστε να μπορεί να ελεγχθεί από τρίτον.

Καμία βαθμολογία κινδύνου δεν μετατράπηκε σε επίπεδο διασφάλισης. Το ίδιο asset μπορεί να έχει υψηλή τιμή MONARC και 0,0% στην πλατφόρμα επειδή οι δείκτες χρησιμοποιούν διαφορετικά δεδομένα. Η σύνδεση αφορά την επιλογή ΤοΕ και την προτεραιότητα απαιτήσεων, όχι τον υπολογισμό assurance level.

Οι υπηρεσίες ασφάλειας βρίσκονται εκεί που τις τοποθετεί το είδος της επίθεσης, όχι εκεί που τις αναζητεί ο συντάκτης. Χρειάζονται δύο διευκρινίσεις πριν από τη διατύπωση. Κατάλογος απειλών είναι μια κλειστή λίστα που ομαδοποιεί τις απειλές κατά κατηγορίες.

Το εύρημα διατυπώνεται ως εξής. Όταν ένα εργαλείο συνθέτει περισσότερους από έναν καταλόγους απειλών, οι υπηρεσίες ασφάλειας κατανέμονται ανά είδος επίθεσης ή ανά κανονιστικό πλαίσιο και όχι ανά υπηρεσία. Ο συντάκτης στόχου ασφάλειας που αναζητά στόχο με βάση την υπηρεσία ενδέχεται να μην τον εντοπίσει, ακόμη και όταν υπάρχει. Το εύρημα προέκυψε από μία πλατφόρμα, σε δύο συνεδρίες, με έναν παρατηρητή και ένα αντικείμενο αξιολόγησης, χωρίς έλεγχο από δεύτερο πρόσωπο και χωρίς δοκιμή σε άλλο εργαλείο, και τα όρια αυτά ισχύουν για κάθε πρόταση της παρούσας παραγράφου.

Το μοτίβο εμφανίστηκε δύο φορές, ανεξάρτητα η μία εκδήλωση από την άλλη. Η πρώτη αφορά την απόδειξη ενεργειών, δηλαδή τη δυνατότητα να τεκμηριωθεί ότι κάποιος έκανε κάτι και να μην μπορεί να το αρνηθεί αργότερα. Οι πέντε στόχοι που βρέθηκαν κάτω από τη σχετική κατηγορία αφορούσαν όλοι την καταγραφή ενεργειών σε αρχεία, ενώ οι στόχοι που στηρίζονται σε κρυπτογραφία ήταν συνδεδεμένοι με άλλη κατηγορία. Η δεύτερη αφορά τη διαθεσιμότητα, όπου κάτω από την κατηγορία της άρνησης υπηρεσίας δεν υπήρχε κανένας σχετικός στόχος, ενώ τέσσερις τέτοιοι στόχοι υπήρχαν σε κατηγορίες του κανονιστικού σκέλους. Και στις δύο περιπτώσεις το λεξιλόγιο υπάρχει μέσα στο εργαλείο και απλώς οδηγεί αλλού.

Η εξήγηση βρίσκεται στον ορισμό που δίνει η ίδια η πλατφόρμα στην κατηγορία, δηλαδή στη δυνατότητα άρνησης μιας ενέργειας λόγω απουσίας λογοδοσίας. Με αυτόν τον ορισμό, η καταγραφή σε αρχείο είναι η φυσική απάντηση και η κρυπτογραφική βεβαίωση ανήκει κάπου αλλού. Το πρότυπο όμως αντιμετωπίζει την ίδια έννοια και ως κρυπτογραφική απόδειξη προέλευσης, όχι μόνο ως λογοδοσία. Η απόκλιση επομένως δεν βαρύνει καμία πλευρά, καθώς προκύπτει από δύο διαφορετικούς ορισμούς της ίδιας έννοιας και συνιστά σχεδιαστική επιλογή με συνέπειες.

Η βιβλιογραφία περιγράφει τα συστατικά του φαινομένου χωριστά. Ο Türrpe [76] δείχνει ότι οι ανάγκες ασφάλειας γεννιούνται από τη συνάντηση τριών διαστάσεων, των απειλών, των στόχων και της σχεδίασης, και ότι όποιος κινείται σε μία μόνο από αυτές βλέπει μερική εικόνα. Οι Scandariato, Wuyts και Joosen [77] μέτρησαν πειραματικά πόσες απειλές διαφεύγουν όταν χρησιμοποιείται αυτή η οικογένεια καταλόγων. Οι Hermann και οι συνεργάτες του [78] έθεσαν το ερώτημα του πού εντοπίζεται ένα χαρακτηριστικό ασφάλειας ως αυτοτελές πρόβλημα. Το πέμπτο κεφάλαιο τηρεί περιορισμένη διατύπωση πρωτοτυπίας, δηλαδή ότι δεν εντοπίστηκε

δημοσιευμένη καταγραφή μοντελοποίησης αντικειμένου τύπου υπηρεσίας στη συγκεκριμένη πλατφόρμα. Μεταγενέστερος και ευρύτερος έλεγχος σε ακαδημαϊκές βάσεις και σε φορείς προτύπων δεν εντόπισε ούτε δημοσίευση που να ενώνει τα τρία παραπάνω ρεύματα στη σύνταξη προδιαγραφής πάνω σε εργαλείο δύο καταλόγων. Η απουσία δημοσίευσης δεν αποδεικνύει προτεραιότητα, και τα όρια του ελέγχου δηλώνονται στην επόμενη ενότητα.

Η αντιπαράβολή έδειξε κενό στην ίδια την εργασία. Το τρίτο εύρημα δεν αφορά την πλατφόρμα αλλά την προδιαγραφή που συντάχθηκε εδώ. Ο κατάλογος του κανονιστικού σκέλους περιέχει μια διάσταση που η προδιαγραφή μας δεν περιλαμβάνει καθόλου, δηλαδή το αντικείμενο ως φορέα βλάβης προς άλλα συστήματα. Για μια διεπαφή που στέλνει δεδομένα σε κεντρικό κόμβο και σε ευρωπαϊκό δίκτυο ανταλλαγής, η διάσταση αυτή είναι εύλογη και η απουσία της συνιστά παράλειψη του συντάκτη.

Η μεθοδολογική συνέπεια είναι ότι η σύγκριση δύο προσεγγίσεων δεν παράγει μόνο κριτική της μίας από την άλλη. Παράγει και διόρθωση προς την κατεύθυνση του συντάκτη, εφόσον εκείνος δεχθεί να την καταγράψει αντί να την αποσιωπήσει.

Η ανάλυση ευαισθησίας έδειξε ότι η ακριβής κορυφή αλλάζει όταν μειώνεται η βασική βαθμίδα ωριμότητας, αλλά η ταυτότητα και η πρόσβαση παραμένουν στην κορυφή. Η θεματική σειρά προτεραιότητας είναι ανθεκτικότερη από την ακριβή βαθμολογία.

Τα πέντε κριτήρια της §1.6 καλύφθηκαν: πραγματική εργαστηριακή εκτέλεση, επανάληψη από ίδιες εισόδους, μηδενικές αριθμητικές αποκλίσεις, ιχνηλασιμότητα επιλογών και δοκιμή ευαισθησίας. Η προγενέστερη πρόβλεψη για τη μορφή της εξόδου συγκρίθηκε με την πραγματική πλατφόρμα. Τα κριτήρια αξιολογούν την εσωτερική ποιότητα της εφαρμογής, όχι μεταφεριμότητα.

6.3 Περιορισμοί της μελέτης

Τα όρια που ακολουθούν οριοθετούν την εμβέλεια όσων δείχθηκαν και αποτελούν μέρος του αποτελέσματος.

Ένα αρχέτυπο, όχι δείγμα. Η μελέτη εξέτασε ένα κατασκευασμένο σύστημα και όχι δείγμα φορέων. Το αρχέτυπο συγκροτήθηκε αποκλειστικά από δημόσια διαθέσιμες πηγές και δεν αντιστοιχεί σε κανέναν συγκεκριμένο οργανισμό, ώστε να αποκλειστεί κάθε δυνατότητα ταύτισης. Το τίμημα της επιλογής είναι ότι τα αριθμητικά αποτελέσματα δεν γενικεύονται στατιστικά σε καμία κατηγορία φορέων. Δείχνουν ότι η μέθοδος εκτελείται από άκρη σε άκρη και τι παράγει όταν εκτελεστεί, όχι πόσο συχνά θα παρήγε το ίδιο αλλού. Η γενίκευση θα απαιτούσε επανάληψη σε περισσότερα αρχέτυπα, με διαφορετικό μέγεθος, διαφορετική τεχνολογική βάση και διαφορετική φάση ωριμότητας.

Κανείς δεν επανέλαβε τη δουλειά ανεξάρτητα. Ο ίδιος άνθρωπος συγκρότησε το μοντέλο, εκτέλεσε τον υπολογισμό, παρατήρησε την πλατφόρμα και συνέταξε το κείμενο, χωρίς δεύτερο πρόσωπο σε κανένα από τα τέσσερα βήματα. Ο περιορισμός βαραίνει περισσότερο το εύρημα των δύο καταλόγων, το οποίο στηρίζεται σε παρατήρηση οθόνης και στην ερμηνεία της. Τρία πράγματα έμειναν χωρίς επιβεβαίωση από τρίτον: η ερμηνεία του τι έδειχνε η οθόνη, η καταμέτρηση των στοιχείων της, και η επιλογή του τι αποτυπώθηκε και τι παραλείφθηκε. Τα στιγμιότυπα που τηρήθηκαν ως εσωτερικό υλικό αποδεικνύουν τι εμφανίστηκε στην οθόνη, όχι ότι ερμηνεύτηκε ορθά. Η πλατφόρμα δεν δηλώνει αριθμό έκδοσης, οπότε ούτε η κατάσταση του λογισμικού κατά την παρατήρηση μπορεί να ανακτηθεί από άλλον για σύγκριση.

Η ωριμότητα δηλώθηκε, δεν μετρήθηκε. Καμία επιτόπια επιθεώρηση δεν έγινε, και δεν θα ήταν άλλωστε δυνατή σε σύστημα που δεν υπάρχει. Η κατάσταση των μέτρων ασφάλειας τέθηκε ως ενιαία παραδοχή τριών κατηγοριών, ανάλογα με το ποιος κρατά την εγγύηση, και εφαρμόστηκε σε ογδόντα πέντε από τις ενενήντα γραμμές του μητρώου. Οι υπόλοιπες πέντε κληρονόμησαν την τιμή των αγαθών στα οποία τοποθετήθηκαν. Προβλέφθηκε ρητά η δυνατότητα τεκμηριωμένης απόκλισης σε μεμονωμένη γραμμή, και δεν χρησιμοποιήθηκε ούτε μία φορά, επειδή καμία δημόσια πηγή δεν τη δικαιολογούσε.

Το βαρύτερο σκέλος του περιορισμού δεν είναι η ίδια η παραδοχή αλλά η εμβελεία της. Η ίδια παραδοχή τροφοδοτεί ταυτόχρονα τρία αποτελέσματα: τους αριθμούς του μητρώου κινδύνων, την ανάλυση αποκλίσεων έναντι των ενενήντα τριών μέτρων, και την οργανωτική ανάγνωση που προκύπτει από αυτήν. Αν η παραδοχή αποδειχθεί εσφαλμένη, μετακινούνται και τα τρία προς την

ίδια κατεύθυνση. Τα αποτελέσματα συμφωνούν επομένως μεταξύ τους, αλλά η συμφωνία τους δεν συνιστά ανεξάρτητη επιβεβαίωση, επειδή πηγάζουν από κοινή ρίζα και όχι από χωριστές μετρήσεις.

Ένα λάθος που έγινε και διορθώθηκε. Η πρώτη καταγραφή του καταλόγου απειλών ανέφερε επτά κατηγορίες, επειδή αποτυπώθηκε μόνο η πρώτη οθόνη του καταλόγου. Ο επανέλεγχος έδειξε τριάντα τρεις. Το αρχικό συμπέρασμα ήταν μερικό και αντικαταστάθηκε, ενώ το επεισόδιο σημειώνεται εδώ επειδή παρήγαγε κανόνα που εφαρμόστηκε στη συνέχεια συστηματικά.

Ο κανόνας διατυπώνεται απλά: πριν καταγραφεί ότι κάτι λείπει, επιβεβαιώνεται ότι ο κατάλογος εξαντλήθηκε. Η δήλωση απουσίας είναι βαρύτερη από τη δήλωση παρουσίας, γιατί απαιτεί έλεγχο ολόκληρου του πεδίου και όχι ενός σημείου του. Ο κανόνας δεσμεύει και τον ισχυρισμό πρωτοτυπίας της παραγράφου των ευρημάτων, ο οποίος είναι επίσης δήλωση απουσίας. Ο σχετικός έλεγχος κάλυψε ακαδημαϊκές βάσεις δεδομένων και φορείς προτύπων, αλλά δεν κάλυψε κείμενα προσβάσιμα μόνο με συνδρομή, μη αγγλόφωνη βιβλιογραφία, ούτε μη δημόσια παραδοτέα ερευνητικών έργων. Το τελευταίο δεν θα μπορούσε άλλωστε να λειτουργήσει ως τεκμήριο απουσίας, επειδή ισχυρισμός στηριγμένος σε υλικό που ο αναγνώστης δεν μπορεί να προσπελάσει δεν είναι ελέγξιμος.

6.4 Προτάσεις για μελλοντική έρευνα

Οι περιορισμοί της προηγούμενης ενότητας ορίζουν το πρώτο ερευνητικό βήμα. Πριν από κάθε νέα κατεύθυνση, χρειάζεται επικύρωση όσων δείχθηκαν εδώ, ώστε τα επόμενα βήματα να στηριχθούν σε επιβεβαιωμένη και όχι σε υποθετική βάση.

Τι θα απαιτούσε η επικύρωση. Το εύρημα των δύο καταλόγων στηρίζεται σε έναν παρατηρητή. Ο έλεγχος θα απαιτούσε να αναζητήσουν τους ίδιους στόχους ασφάλειας δύο συντάκτες χωριστά, χωρίς να επικοινωνήσουν μεταξύ τους. Το κρίσιμο δεν θα ήταν πόσους στόχους εντόπισε ο καθένας, αλλά αν δυσκολεύτηκαν στα ίδια σημεία του καταλόγου. Κοινή δυσκολία θα έδειχνε ότι αιτία είναι η δομή του καταλόγου, ενώ διαφορετική δυσκολία θα έδειχνε ότι αιτία είναι η προσοχή του καθενός. Το σχήμα δεν χρειάζεται να επινοηθεί, καθώς αντίστοιχο πείραμα [77] έχει ήδη εκτελεστεί για την ίδια οικογένεια καταλόγων απειλών.

Η επικύρωση απαιτεί επίσης μεταβολή τριών παραμέτρων που εδώ έμειναν σταθερές. Πρώτη είναι το εργαλείο, ώστε να φανεί αν το μοτίβο ανήκει σε μία υλοποίηση ή σε κάθε εργαλείο που συνθέτει πολλαπλούς καταλόγους. Δεύτερη είναι ο τύπος του αντικειμένου, με δοκιμή σε προϊόν αντί για υπηρεσία. Τρίτη είναι το αρχέτυπο, με επανάληψη σε συστήματα διαφορετικού μεγέθους, τεχνολογικής βάσης και φάσης ωριμότητας. Ο απαιτούμενος αριθμός αρχετύπων εξαρτάται από το ερώτημα: λίγα αρκούν για ναδειχθεί ότι το φαινόμενο εμφανίζεται αλλού, πολλά χρειάζονται για να εκτιμηθεί πόσο συχνά.

Τέλος, η παραδοχή ωριμότητας θα αντικαθίστατο από μέτρηση. Αυτό προϋποθέτει πρόσβαση σε πραγματικό φορέα και τεκμήρια που το αρχέτυπο εξ ορισμού δεν διαθέτει: αρχεία εσωτερικού ελέγχου, πραγματικές παραμετροποιήσεις, ιστορικό περιστατικών και επιτόπια επαλήθευση των διαδικασιών.

6.4.1 Ενσωμάτωση της κλιματικής διάστασης στην αξιολόγηση ετοιμότητας

Η τροποποίηση του ISO/IEC 27001:2022 που δημοσιεύθηκε το 2024 [23] προσθέτει την υποχρέωση να εξεταστεί αν η κλιματική αλλαγή αποτελεί σχετικό ζήτημα για τον οργανισμό, χωρίς να προδικάζει την απάντηση. Η παρούσα εργασία δεν εξέτασε το ερώτημα, επειδή τα φυσικά και περιβαλλοντικά μέτρα αποδόθηκαν στη σφαίρα του παρόχου φιλοξενίας.

Εκεί ακριβώς βρίσκεται το ερευνητικό ενδιαφέρον. Όταν οι περιβαλλοντικές εξαρτήσεις μετατοπίζονται σε τρίτον, η κλιματική έκθεση δεν εξαφανίζεται αλλά αλλάζει κάτοχο, και η ερώτηση γίνεται πώς τεκμηριώνεται μια εξάρτηση που ο φορέας δεν ελέγχει. Η διερεύνηση θα εξέταζε αν οι υφιστάμενες προδιαγραφές ασφάλειας μπορούν να εκφράσουν τέτοιες εξαρτήσεις και με ποια τεκμήρια θα τις υποστήριζαν.

6.4.2 Διερεύνηση των ευρύτερων μακροοικονομικών και θεσμικών επιπτώσεων περιστατικών σε πληροφοριακά συστήματα της δημόσιας διοίκησης

Η εργασία μέτρησε την έκθεση ενός συστήματος και δεν εξέτασε τι συμβαίνει όταν αυτή η έκθεση πραγματοποιηθεί. Το ερώτημα αν και πώς ένα περιστατικό σε σύστημα οικονομικής διαχείρισης μεταφέρεται σε ευρύτερες δημοσιονομικές ή θεσμικές συνέπειες παραμένει ανοικτό και δεν απαντάται από το υλικό της παρούσας μελέτης.

Μια τέτοια έρευνα θα ήταν διεπιστημονική και θα ξεκινούσε από ζητήματα μεθόδου. Θα έπρεπε να οριστεί τι μετριέται, να βρεθούν δεδομένα περιστατικών του δημόσιου τομέα με επαρκή ανάλυση, και να αντιμετωπιστεί η δυσκολία της αιτιώδους σύνδεσης μεταξύ ενός τεχνικού γεγονότος και μεγεθών που επηρεάζονται ταυτόχρονα από πολλούς παράγοντες.

6.4.3 Προσαρμοστική και αυτοματοποιημένη απόκριση σε εξελισσόμενες και μη προβλέψιμες απειλές

Η αντιπαράβολή των δύο εργαλείων ανέδειξε διαφορετική σχέση με τον χρόνο. Η ανάλυση κινδύνου προβλέπει περιοδική επανεκτίμηση, ενώ η πιστοποίηση προϋποθέτει διατήρηση της διασφάλισης ανάμεσα στις αξιολογήσεις.

Το ερευνητικό ερώτημα είναι πότε μια δήλωση ασφάλειας παύει να ισχύει και ποιο γεγονός το σηματοδοτεί. Εξεταστέο είναι αν η ανίχνευση μπορεί να αυτοματοποιηθεί, ώστε η εμφάνιση νέας ευπάθειας σε δομικό στοιχείο να ενεργοποιεί επανεξέταση των σχετικών απαιτήσεων. Η παρούσα εργασία δεν μπορούσε να το εξετάσει, επειδή ο κατάλογος ευπαθειών του αρχετύπου ήταν κενός εξ ορισμού.

Βιβλιογραφία

- [1] Υπουργείο Ψηφιακής Διακυβέρνησης, «Βίβλος Ψηφιακού Μετασχηματισμού 2020–2025», Ιούνιος 2021. [Online]. Available: <https://digitalstrategy.gov.gr/>
- [2] ISO/IEC, «ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements», 3η έκδ., Γενεύη: Διεθνής Οργανισμός Τυποποίησης, 2022. [Online]. Available: <https://www.iso.org/standard/82875.html>
- [3] ISO/IEC, «ISO/IEC 27002:2022 — Information security, cybersecurity and privacy protection — Information security controls», 3rd ed., Feb. 2022. [Online]. Available: <https://www.iso.org/standard/75652.html>
- [4] European Parliament and Council of the European Union, «Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive)», Official Journal of the European Union, OJ L 333, pp. 80–152, 27 Dec. 2022. [Online]. Available: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>
- [5] Ελληνική Δημοκρατία, «Νόμος υπ’ αριθμ. 5160/2024 — Ενσωμάτωση της Οδηγίας (ΕΕ) 2022/2555 (NIS 2) και άλλες διατάξεις», Εφημερίδα της Κυβερνήσεως, ΦΕΚ Α’ 195/27-11-2024. [Online]. Available: <https://search.et.gr/el/fek/?fekId=777144>
- [6] Κοινή Υπουργική Απόφαση 1689/2025, «Εθνικό Πλαίσιο Απαιτήσεων Κυβερνοασφάλειας Βασικών και Σημαντικών Οντοτήτων», Εφημερίδα της Κυβερνήσεως, ΦΕΚ Β’ 2186/06-05-2025. [Online]. Available: <https://cyber.gov.gr/wp-content/uploads/2025/05/20250202186.pdf>
- [7] European Parliament and Council of the European Union, «Directive (EU) 2022/2557 of 14 December 2022 on the resilience of critical entities», Official Journal of the European Union, OJ L 333, pp. 164–198, 27 Dec. 2022. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2557>
- [8] Υπουργείο Ψηφιακής Διακυβέρνησης, «Σε στάδιο υλοποίησης περνά το Gov-ERP για την αναβάθμιση του συστήματος χρηματοοικονομικής και δημοσιονομικής διαχείρισης του Ελληνικού Δημοσίου», Κοινό Δελτίο Τύπου, 6 Μαΐου 2022. [Online]. Available: <https://www.mindigital.gr/archives/3148>
- [9] Ελλάδα 2.0, «Μεταρρύθμιση του Δημοσιονομικού Συστήματος στην Κεντρική Διοίκηση και τη λοιπή Γενική Κυβέρνηση (gov-ERP)» — Δράση 4.2.8 (16705), Κωδ. ΟΠΣ ΤΑ 5136212. [Online]. Available: <https://greece20.gov.gr/?projects=psifiakos-metastichatismos-dimosionomikis-diacheirisis-kai-epopteias-sti-geniki-kyvernisi-amp-ilektroniki-timologisi-16705>
- [10] Ελλάδα 2.0 / ΕΥΣΤΑ, «Τροποποίηση απόφασης ένταξης του Έργου ‘SUB1. Μεταρρύθμιση του Δημοσιονομικού Συστήματος στην Κεντρική Διοίκηση και τη λοιπή Γενική Κυβέρνηση (gov-ERP)’ (Κωδικός ΟΠΣ ΤΑ 5136212)», 2025. [Online]. Available: https://greece20.gov.gr/wp-content/uploads/2025/05/1841.Tropopoiisi_Sub1_Metarrithmisi_Dimosionomikou_Sistimat os_Kentrikis_Dioikisis_k_loipis_Gen.Kivernisi_gov-ERP_5136212.pdf
- [11] ISO/IEC, «ISO/IEC 27005:2022 — Information security, cybersecurity and privacy protection — Guidance on managing information security risks», Oct. 2022. [Online]. Available: <https://www.iso.org/standard/80585.html>
- [12] ENISA, «Interoperable EU Risk Management Toolbox», Feb. 2023. [Online]. Available: <https://doi.org/10.2824/68948>
- [13] Luxembourg House of Cybersecurity, «MONARC — Method for an Optimised aNalysis of Risks», τεκμηρίωση μεθόδου και δημοσιεύσεις. [Online]. Available: <https://www.monarc.lu/>
- [14] CUSTODES project, «A Certification approach for dynamic, agile and reUSable assessment fOr composite systems of ICT proDucts, servicEs, and processeS (CUSTODES)», Horizon Europe, Grant Agreement No. 101120684, 2023–2026. [Online]. Available: <https://doi.org/10.3030/101120684>
- [15] CUSTODES Consortium, «Product Owner’s Tutorial», project training document, n.d., Horizon Europe Grant Agreement No. 101120684.

- [16] ISO/IEC, «ISO/IEC 15408:2022 — Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Parts 1–5», 2022. [Online]. Available (Μέρος 1): <https://www.iso.org/standard/72891.html>
- [17] ISO/IEC, «ISO/IEC 18045:2022 — Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Methodology for IT security evaluation», 3rd ed., 2022. [Online]. Available: <https://www.iso.org/standard/72889.html>
- [18] ISO/IEC, «ISO/IEC 17000:2020 — Conformity assessment — Vocabulary and general principles», 2nd ed., 2020. [Online]. Available: <https://www.iso.org/standard/73029.html>
- [19] European Parliament and Council of the European Union, «Regulation (EU) 2019/881 on ENISA and on information and communications technology cybersecurity certification (Cybersecurity Act)», OJ L 151, pp. 15–69, 7 Jun. 2019, όπως τροποποιήθηκε από τον Κανονισμό (ΕΕ) 2025/37 (διαχειριζόμενες υπηρεσίες ασφάλειας). [Online]. Available: <https://eur-lex.europa.eu/eli/reg/2019/881/oj>
- [20] European Commission, «Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC)», OJ L, 2024/482, 7 Feb. 2024, όπως τροποποιήθηκε από τους Εκτελεστικούς Κανονισμούς (ΕΕ) 2024/3144 και (ΕΕ) 2025/2462. [Online]. Available: https://eur-lex.europa.eu/eli/reg_impl/2024/482/oj
- [21] ISO, «ISO 31000:2018 — Risk management — Guidelines», 2nd ed., 2018. [Online]. Available: <https://www.iso.org/standard/65694.html>
- [22] ISO, «ISO 31073:2022 — Risk management — Vocabulary», 1st ed., 2022. [Online]. Available: <https://www.iso.org/standard/79637.html>
- [23] ISO/IEC, «ISO/IEC 27001:2022/Amd 1:2024 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements — Amendment 1: Climate action changes», 3rd ed., Feb. 2024. [Online]. Available: <https://www.iso.org/standard/88435.html>
- [24] ISO/IEC, «ISO/IEC TS 27110:2021 — Information technology, cybersecurity and privacy protection — Cybersecurity framework development guidelines», 2021. [Online]. Available: <https://www.iso.org/standard/72435.html>
- [25] ISO/IEC, «ISO/IEC 27017:2015 — Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services», 1st ed. Geneva: ISO/IEC, 2015. [Online]. Available: <https://www.iso.org/standard/43757.html>
- [26] ISO/IEC, «ISO/IEC 27017:2026 — Information security, cybersecurity and privacy protection — Information security controls based on ISO/IEC 27002 for cloud services», 2nd ed. Geneva: ISO/IEC, 2026. [Online]. Available: <https://www.iso.org/standard/82878.html>
- [27] National Institute of Standards and Technology, «Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy», NIST SP 800-37 Rev. 2, Dec. 2018. [Online]. Available: <https://doi.org/10.6028/NIST.SP.800-37r2>
- [28] National Institute of Standards and Technology, «Guide for Conducting Risk Assessments», NIST SP 800-30 Rev. 1, Sep. 2012. [Online]. Available: <https://doi.org/10.6028/NIST.SP.800-30r1>
- [29] National Institute of Standards and Technology, «The NIST Cybersecurity Framework (CSF) 2.0», NIST CSWP 29, Feb. 2024. [Online]. Available: <https://doi.org/10.6028/NIST.CSWP.29>
- [30] Agence nationale de la sécurité des systèmes d'information (ANSSI), «EBIOS Risk Manager — The method», Version 1.0, Nov. 2019, ANSSI-PA-048-EN. [Online]. Available: <https://messervices.cyber.gouv.fr/guides/en-ebios-risk-manager-method>
- [31] R. A. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson, «Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process», Software Engineering Institute, Carnegie Mellon University, CMU/SEI-2007-TR-012, May 2007. [Online]. Available: <https://doi.org/10.1184/R1/6574790.v1>

- [32] CLUSIF, «MEHARI — Méthode Harmonisée d'Analyse de Risques.» [Online]. Available: <https://clusif.fr/services/management-des-risques/>
- [33] K. Kioskli, E. Seralidou, and N. Polemi, «A Practical Human-Centric Risk Management (HRM) Methodology», *Electronics*, vol. 14, no. 3, art. 486, Jan. 2025. [Online]. Available: <https://doi.org/10.3390/electronics14030486>
- [34] S. Schauer, N. Polemi, and H. Mouratidis, «MITIGATE: a dynamic supply chain cyber risk assessment methodology», *Journal of Transportation Security*, vol. 12, no. 1–2, pp. 1–35, 2019. [Online]. Available: <https://doi.org/10.1007/s12198-018-0195-z>
- [35] European Commission, «Multidimensional, IntegraTed, risk assessment framework and dynamic, collaborative Risk ManaGement tools for critical information infrastructures (MITIGATE)», Horizon 2020, Grant Agreement No. 653212, CORDIS. [Online]. Available: <https://cordis.europa.eu/project/id/653212>
- [36] ENISA, «Compendium of Risk Management Frameworks with Potential Interoperability», Jan. 2022. [Online]. Available: <https://www.enisa.europa.eu/publications/compendium-of-risk-management-frameworks>
- [37] Luxembourg House of Cybersecurity, «Risk Assessment Optimisation with MONARC», MONARC Publications, 2018. [Online]. Available: <https://www.monarc.lu/publications/risk-assessment-optimisation-with-monarc/>
- [38] intuitem, «CISO Assistant — Open-source GRC.» [Online]. Available: <https://github.com/intuitem/ciso-assistant-community>
- [39] intuitem, «Mappings — CISO Assistant Documentation.» [Online]. Available: <https://intuitem.gitbook.io/ciso-assistant/features/mappings>
- [40] SerNet GmbH, «verinice — the ISMS tool.» [Online]. Available: <https://verinice.com/en/>
- [41] Eramba, «eramba — GRC software.» [Online]. Available: <https://www.eramba.org/>
- [42] European Parliament and Council of the European Union, «Regulation (EC) No 765/2008 setting out the requirements for accreditation and repealing Regulation (EEC) No 339/93», OJ L 218, pp. 30–47, 13 Aug. 2008. [Online]. Available: <https://eur-lex.europa.eu/eli/reg/2008/765/oj>
- [43] ISO/IEC, «ISO/IEC 17011:2017 — Conformity assessment — Requirements for accreditation bodies accrediting conformity assessment bodies», 2nd ed., 2017. [Online]. Available: <https://www.iso.org/standard/67198.html>
- [44] ISO/IEC, «ISO/IEC 17025:2017 — General requirements for the competence of testing and calibration laboratories», 3rd ed., 2017. [Online]. Available: <https://www.iso.org/standard/66912.html>
- [45] ISO/IEC, «ISO/IEC 17065:2012 — Conformity assessment — Requirements for bodies certifying products, processes and services», 1st ed., 2012. [Online]. Available: <https://www.iso.org/standard/46568.html>
- [46] Common Criteria, «Common Criteria for Information Technology Security Evaluation, CC:2022 Release 1 — Part 1: Introduction and general model», Nov. 2022. [Online]. Available: <https://www.commoncriteriaportal.org/files/ccfiles/CC2022PART1R1.pdf>
- [47] CCRA Participants, «Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security», 2 Jul. 2014, ratified 8 Sep. 2014. [Online]. Available: <https://www.commoncriteriaportal.org/files/CCRA%20-%20July%202%2C%202014%20-%20Ratified%20September%208%202014.pdf>
- [48] Common Criteria, «Common Methodology for Information Technology Security Evaluation (CEM), CEM:2022 Release 1», Nov. 2022. [Online]. Available: <https://www.commoncriteriaportal.org/files/ccfiles/CEM2022R1.pdf>
- [49] ENISA, «Cybersecurity Certification: EUCC — A candidate cybersecurity certification scheme to serve as a successor to the existing SOG-IS», v1.1.1, May 2021. [Online]. Available: <https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme-v1-1.1>
- [50] ISO/IEC, «ISO/IEC TS 23532-1:2021 — Information security, cybersecurity and privacy protection — Requirements for the competence of IT security testing and evaluation laboratories — Part 1: Evaluation for ISO/IEC 15408», 1st ed., 2021. [Online]. Available: <https://www.iso.org/standard/77199.html>

- [51] ISO/IEC, «ISO/IEC 17020:2026 — Conformity assessment — Requirements for bodies performing inspection», 3rd ed., 2026. [Online]. Available: <https://www.iso.org/standard/86292.html>
- [52] ISO/IEC, «ISO/IEC 17021-1:2015 — Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements», 2015. [Online]. Available: <https://www.iso.org/standard/61651.html>
- [53] ISO/IEC, «ISO/IEC 27006-1:2024 — Information security, cybersecurity and privacy protection — Requirements for bodies providing audit and certification of information security management systems — Part 1: General», 1st ed., 2024. [Online]. Available: <https://www.iso.org/standard/82908.html>
- [54] CYRENE Consortium, «D2.1 — Supply Chain Analysis and Requirements», Horizon 2020, Grant Agreement No. 952690, v1.0, 31 May 2021. Deliverable Security Class: Public. [Online]. Available: <https://doi.org/10.5281/zenodo.6786171>
- [55] CYRENE Consortium, «D3.1 — Conformity Evaluation Process & Multi-Level Evidence-Driven Supply Chain Risk Assessment», Horizon 2020, Grant Agreement No. 952690, v1.0, 30 Sep. 2021. Deliverable Security Class: Public. [Online]. Available: <https://doi.org/10.5281/zenodo.6786244>
- [56] ETSI, «ETSI TS 102 165-1 — CYBER; Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)», V5.3.1, Feb. 2025. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/102100_102199/10216501/05.03.01_60/ts_10216501v050301p.pdf
- [57] Υπουργείο Ψηφιακής Διακυβέρνησης — Βίβλος Ψηφιακού Μετασχηματισμού 2020–2025, «Κεντρικό και Ενιαίο Σύστημα Δημοσιονομικής Πολιτικής (Government ERP)». [Online]. Available: https://digitalstrategy.gov.gr/project/government_erp
- [58] Υπουργείο Ψηφιακής Διακυβέρνησης, «Gov-ERP: Προς υλοποίηση το νέο e-εργαλείο συνολικής Δημοσιονομικής Διαχείρισης του κράτους», 11/06/2021. [Online]. Available: <https://www.mindigital.gr/archives/2433>
- [59] InfoCom, «Σε δημόσια διαβούλευση ο διαγωνισμός για το gov-ERP», 23/02/2021. [Online]. Available: <https://www.infocom.gr/2021/02/23/dimosia-diavoulefsi-diagonismos-gia-gov-erp/53561/>
- [60] Υπουργείο Εθνικής Οικονομίας και Οικονομικών, «GOV ERP, ένα καινοτόμο πληροφοριακό σύστημα στην υπηρεσία της Δημόσιας Διοίκησης», 15/12/2023. [Online]. Available: <https://minfin.gov.gr/gov-erp-ena-kainotomo-pliroforiako-systima-stin-ypiresia-tis-dimosias-dioikisis/>
- [61] Κοινωνία της Πληροφορίας Μ.Α.Ε., «Gov-ERP: Μεταρρύθμιση του Δημοσιονομικού Συστήματος στην Κεντρική Διοίκηση και τη λοιπή Γενική Κυβέρνηση». [Online]. Available: <https://www.ktpae.gr/erga/gov-erp/>
- [62] Οικονομικός Ταχυδρόμος (ot.gr), «GOV ERP: Στην τελική ευθεία το έργο που 'βλέπει' το Δημόσιο σε πραγματικό χρόνο», 28/05/2026. [Online]. Available: <https://www.ot.gr/2026/05/28/epikairothta/gov-erp-stin-teliki-eytheia-to-ergo-pou-vlepei-to-dimosio-se-pragmatiko-xrono/>
- [63] Υπουργεία Εθνικής Οικονομίας και Οικονομικών & Ψηφιακής Διακυβέρνησης, ΑΑΔΕ, «Νέα εφαρμογή για Ηλεκτρονικά Τιμολόγια σε συμβάσεις με το Δημόσιο (B2G)», 16/09/2025. [Online]. Available: <https://minfin.gov.gr/nea-efarmogi-gia-ilektronika-timologia-se-symvaseis-me-to-dimosio-b2g/>
- [64] ΓΓΠΣΨΔ, «Συχνές Ερωτήσεις — Ηλεκτρονική Τιμολόγηση στις συναλλαγές B2G». [Online]. Available: <https://www.gsis.gr/polites-epiheiriseis/pliromes-kai-eispraxeis/e-invoice/syhnes>
- [65] ICT Plus, «Η ΚτΠ με το νέο govERP αλλάζει την δημοσιονομική διαχείριση της χώρας», 09/01/2026. [Online]. Available: <https://www.ictplus.gr/i-ktp-me-to-neo-goverp-allazei-tin-dimosionomiki-diacheirisi-tis-choras/>
- [66] Ν. 4270/2014, «Αρχές δημοσιονομικής διαχείρισης και εποπτείας (ενσωμάτωση της Οδηγίας 2011/85/ΕΕ) — δημόσιο λογιστικό και άλλες διατάξεις» (ΦΕΚ Α' 143/28-06-2014), όπως ισχύει.

- [67] Ν. 4622/2019, «Επιτελικό Κράτος: οργάνωση, λειτουργία και διαφάνεια της Κυβέρνησης, των κυβερνητικών οργάνων και της κεντρικής δημόσιας διοίκησης» (ΦΕΚ Α' 133/07-08-2019), όπως ισχύει.
- [68] Υπουργείο Εθνικής Οικονομίας και Οικονομικών, Γενικό Λογιστήριο του Κράτους, Εγκύκλιος Α.Π. 14044/27-01-2026, «Οδηγίες για την αναμόρφωση της επιχειρησιακής λειτουργίας των Γενικών Διευθύνσεων Οικονομικών Υπηρεσιών των Φορέων της Κεντρικής Διοίκησης ενόψει της μεταρρύθμισης του Δημοσιονομικού Συστήματος (gov-ERP)» (ΑΔΑ: 6ΖΔΠΗ-ΚΘ3). [Online]. Available: <https://diavgeia.gov.gr/decision/view/6ΖΔΠΗ-ΚΘ3>
- [69] ΓΓΠΣΨΔ, «Τα Έργα της Γ.Γ.Π.Σ.» (περιγραφές ΟΠΣΔΠ — τήρηση Θησαυροφυλακίου/Ταμειακού Προγραμματισμού· ΟΠΣ Ενιαίας Αρχής Πληρωμής). [Online]. Available: <https://www.gsis.gr/ggps/ta-erga-tis-ggps>
- [70] monarc-project, «MonarcAppFO — MONARC (Method for an Optimised aNalysis of Risks)», επίσημο αποθετήριο πηγαίου κώδικα και οδηγίες εγκατάστασης (INSTALL), GitHub. [Online]. Available: <https://github.com/monarc-project/MonarcAppFO> (ελεύθερο λογισμικό υπό GNU AGPL· δεδομένα βάσης γνώσης υπό CC0 1.0)
- [71] ENISA, «ENISA Threat Landscape 2025», v1.2, Οκτ. 2025, ISBN 978-92-9204-723-8, DOI 10.2824/1946374. [Online]. Available: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025>
- [72] Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (Γενικός Κανονισμός για την Προστασία Δεδομένων — ΓΚΠΔ), ΕΕ L 119, 4.5.2016.
- [73] Ν. 4624/2019, «Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 και ενσωμάτωση της Οδηγίας (ΕΕ) 2016/680» (ΦΕΚ Α' 137/29-08-2019).
- [74] Υπουργική Απόφαση 1899/2025, «Καθορισμός προσόντων, καθηκόντων, ασυμβιβάστων και υποχρεώσεων των Υπεύθυνων Ασφαλείας Συστημάτων Πληροφορικής και Επικοινωνιών», Εφημερίδα της Κυβερνήσεως, ΦΕΚ Β' 4250/05-08-2025. [Online]. Available: https://cyber.gov.gr/wp-content/uploads/2025/08/%CE%91%CE%A0%CE%9F%CE%A6%CE%91%CE%A3%CE%97_%CE%A5%CE%A0%CE%9F%CE%A5%CE%A1%CE%93%CE%9F%CE%A5_1899_20250204250.pdf
- [75] Common Criteria, «Common Criteria for Information Technology Security Evaluation, CC:2022 Release 1 — Part 5: Pre-defined packages of security requirements», CCMB-2022-11-005, Nov. 2022. [Online]. Available: <https://www.commoncriteriaportal.org/files/ccfiles/CC2022PART5R1.pdf>
- [76] S. Türpe, «The Trouble with Security Requirements», in *Proc. IEEE 25th Int. Requirements Engineering Conf. (RE)*, Lisbon, Portugal, 2017, pp. 122–133. [Online]. Available: <https://doi.org/10.1109/RE.2017.13>
- [77] R. Scandariato, K. Wuyts and W. Joosen, «A descriptive study of Microsoft's threat modeling technique», *Requirements Engineering*, vol. 20, no. 2, pp. 163–180, 2015. [Online]. Available: <https://doi.org/10.1007/s00766-013-0195-2>
- [78] K. Hermann et al., «A taxonomy of functional security features and how they can be located», *Empirical Software Engineering*, vol. 30, no. 5, art. 117, 2025. [Online]. Available: <https://doi.org/10.1007/s10664-025-10649-7>

Παράρτημα Α' — Αναλογική μετάφραση των κλιμάκων συνεπειών ROLFP σε δημόσιο πλαίσιο

Οι κλίμακες ROLFP της βάσης γνώσης χρησιμοποιούν ιδιωτικοοικονομικό λεξιλόγιο. Η παρούσα εργασία διατηρεί τις τιμές 0–4 και μεταφράζει αναλογικά τις περιγραφές σε δημόσιο πλαίσιο, όπως ορίστηκε στην §4.4.2. Η μετάφραση εφαρμόζεται ομοιόμορφα σε όλα τα αγαθά. Οι οικονομικές τάξεις μεγέθους εκφράζονται ως ποσοστά των διαχειριζόμενων πιστώσεων. Η μετάφραση αποδίδεται στον Πίνακα Α'.1.

Πίνακας Α'.1. Αναλογική μετάφραση των κλιμάκων συνεπειών ROLFP της βάσης γνώσης MONARC σε δημόσιο πλαίσιο.

Επίπεδο	Reputation	Operational	Legal	Financial	Personal
0	Καμία συνέπεια	Καμία συνέπεια	Καμία συνέπεια	Καμία συνέπεια	Καμία συνέπεια
1	Περιστασιακή αρνητική δημοσιότητα	Μεμονωμένα περιστατικά χωρίς επίπτωση σε πολίτες/συναλλασσόμενους	Αμελητέα πιθανότητα πειθαρχικής/διοικητικής συνέπειας	Οριακή δημοσιονομική επιβάρυνση (τάξης ~1%)	Ήπια όχληση, αναστρέψιμη χωρίς δυσκολία
2	Προσωρινή υποβάθμιση εμπιστοσύνης πολιτών/θεσμού	Μεμονωμένα περιστατικά με διαχειρίσιμη επίπτωση σε πολίτες/συναλλασσόμενους	Πιθανή πειθαρχική/διοικητική κύρωση οργάνου ή υπαλλήλου	Μη οριακή επιβάρυνση (τάξης ~5%)	Σημαντική όχληση, αναστρέψιμη με κάποια δυσκολία
3	Έντονη υποβάθμιση εμπιστοσύνης, σοβαρή/επαναλαμβανόμενη αρνητική δημοσιότητα	Διακοπή λειτουργίας ολόκληρης οργανικής μονάδας/Διεύθυνσης	Πειθαρχική/ποινική δίωξη οργάνου ή υπαλλήλου	Σοβαρή επιβάρυνση (τάξης ~10%)	Σοβαρές συνέπειες, αναστρέψιμες με δυσκολία
4	Οριστική πλήξη εμπιστοσύνης, εθνική/διεθνής δημοσιότητα	Πλήρης αδυναμία εκτέλεσης της δημοσιονομικής λειτουργίας	Σοβαρή πειθαρχική/ποινική ευθύνη, ακυρότητα πράξης	Σημαντική επιβάρυνση (τάξης ~20% ή μη αναστρέψιμη)	Σοβαρές, μη αναστρέψιμες συνέπειες σε πρόσωπο

Στο επίπεδο 4 της στήλης Reputation η προεπιλεγμένη περιγραφή αναφέρει «θάνατο προσώπου». Η διατύπωση είναι εννοιολογικά συναφέστερη με τη στήλη Personal και πιθανόν προέρχεται από άλλο πεδίο εφαρμογής. Δεν επηρέασε την ανάλυση, επειδή η τιμή Reputation=4 δεν χρησιμοποιήθηκε.

Παράρτημα Β' — Συγκεντρωτικές αποτιμήσεις επιπτώσεων των πέντε πρωτευόντων αγαθών

Ο Πίνακας Β'.1 συνοψίζει τις τιμές C/I/A και την κύρια αιτιολόγηση της μέγιστης τιμής για κάθε πρωτεύον αγαθό. Η §4.4.2 παραθέτει ως παράδειγμα τον πλήρη πίνακα ROLFP του P1. Οι πλήρεις καταχωρίσεις και των πέντε αγαθών περιέχονται στην εξαγωγή JSON v2· το ενδεικτικό στιγμιότυπο «Edit impacts» του P1 στο Παράρτημα Δ' τεκμηριώνει τη διαδικασία καταχώρισης, η οποία είναι πανομοιότυπη και για τα πέντε αγαθά.

Πίνακας Β'.1. Συγκεντρωτικές αποτιμήσεις C/I/A των πέντε πρωτευόντων αγαθών και η κύρια σγκύρωση της μέγιστης τιμής.

Αγαθό	C	I	A	Κύρια αγκύρωση της μέγιστης τιμής
P1 — Ροή δημοσιονομικής εκκαθάρισης (Service)	2	4	3	I: Legal — αλλοίωση της ροής εγκρίσεων παραβιάζει ευθέως το θεσμικό κύκλωμα του άρθρου 65 ν. 4270/2014 (ασυμβίβαστο διατάκτη/ΠΟΥ)
P2 — Δημοσιονομικές/λογιστικές εγγραφές και στοιχεία προμηθευτών-δικαιούχων (Information)	3	4	3	C: Legal/Personal — ρητό παράδειγμα κλίμακας «τραπεζικό απόρρητο / ευαίσθητα προσωπικά δεδομένα» (IBAN, στοιχεία δικαιούχων)· I: Legal — πλαστογραφία/αχρεώστητη καταβολή
P3a — Διεργασία παραλαβής/επικύρωσης ηλεκτρονικού τιμολογίου (Service)	2	3	3	A: Operational — η πτώση αφορά ένα κανάλι, όχι το σύνολο των υπηρεσιών· η υψηλή πιθανοφάνεια DDoS εκφράζεται στην πιθανοφάνεια της §4.6, όχι ως διογκωμένη επίπτωση
P3b — Περιεχόμενο ηλεκτρονικού τιμολογίου (Information)	3	4	2	I: Legal — πλαστογράφηση περιεχομένου που τροφοδοτεί δημόσια πληρωμή· η ιδιότητα που «σηκώνεται» στον στόχο αξιολόγησης του Κεφαλαίου 5
P4 — Ίχνη ελέγχου και τεκμήρια (Information)	2	4	2	I: Legal — αλλοίωση ιχνών ισοδυναμεί με συγκάλυψη/παραποίηση αποδεικτικού υλικού και καταστρέφει τη λογοδοσία

Παράρτημα Γ' — Πλήρες μητρώο των 90 μοναδικών αξιολογήσεων κινδύνου

Πηγή του Πίνακα Γ'.1 είναι η εξαγωγή CSV v2 της 05/07/2026, η οποία συμφωνεί με την εξαγωγή JSON v2 (§4.6.2). Τ είναι η πιθανοφάνεια απειλής, V η βαθμίδα ευπάθειας και C/I/A ο τρέχων κίνδυνος ανά κριτήριο, με $R=I \times T \times V$. Το σύμβολο «—» δηλώνει μη πληττόμενο κριτήριο και Max τη μέγιστη τιμή γραμμής. Η στήλη «Μέτρα 27002» περιέχει την προ-χαρτογράφηση της βάσης γνώσης και τη χειροκίνητη αντιστοίχιση E1–E3 της §4.7.3.

Πίνακας Γ'.1. Πλήρες μητρώο των 90 μοναδικών αξιολογήσεων κινδύνου, από την εξαγωγή CSV v2 της 05/07/2026.

Υποστηρικτικό αγαθό	Απειλή	T	Ευπάθεια	V	C	I	A	Max	Μέτρα 27002
Employees	Forging of rights	4	No protection of confidential authentication information	4	32	64	48	64	5.17, 6.3
Employees	Forging of rights	4	Lack of teleworking rules	4	32	64	48	64	6.7
IT organization	Forging of rights	4	Logical access authorisations are not checked regularly	4	32	64	48	64	5.18
System administrator	Forging of rights	4	No protection of confidential authentication information	4	48	64	48	64	5.17, 6.3
System administrator	Forging of rights	4	Lack of teleworking rules	4	48	64	48	64	6.7
User workstations	Forging of rights	4	Authorisation management is flawed	4	32	64	48	64	8.1, 8.2, 5.18, 5.16
User workstations	Forging of rights	4	User authentication is not ensured	4	32	64	48	64	8.1, 5.17
User workstations	Forging of rights	4	The user workstation is not monitored	4	32	64	48	64	7.7, 8.1, 7.8, 6.3
User workstations	Malware infection	4	Programs can be downloaded and installed without monitoring	4	32	64	48	64	8.1, 8.19, 6.3, 8.7
User workstations	Malware infection	4	Update management (patches) is flawed	4	32	64	48	64	8.1, 8.8, 8.7
User workstations	Malware infection	4	No detection system of malicious programs	4	32	64	48	64	8.7
Employees	Error in use	3	Users are not made aware of information security	4	24	48	36	48	5.4, 6.4, 6.3
Employees	Error in use	3	No IT charter specifying the rules of use	4	24	48	36	48	5.4, 5.10

Υποστηρικτικό αγαθό	Απειλή	T	Ευπάθεια	V	C	I	A	Max	Μέτρα 27002
Employees	Error in use	3	No training on the equipment or software used	4	24	48	36	48	6.1, 6.3
IT organization	Error in use	3	No document base for rules and procedures	4	24	48	36	48	5.37
N1 — Κανάλι ΚΕΔ/ΡΕΡΡΟΛ, πιστοποιητικά & κλειδιά υπογραφής	Forging of rights	4	Flaws in the management of administrator accounts	3	36	48	24	48	8.21, 5.17, 8.18
N2 — Διεπαφές ΔΙΑΥΓΕΙΑ/ΚΗΜΔΗΣ/ΕΣΗΔΗΣ & ταμειακού κυκλώματος	Forging of rights	4	Flaws in the management of administrator accounts	3	24	48	36	48	8.21, 5.17, 8.18
Network and Telecom	Forging of rights	4	Flaws in the management of administrator accounts	3	36	48	36	48	8.21, 5.17, 8.18
S1 — Εφαρμογή ERP (ενότητες)	Forging of rights	4	Authorisation management is flawed	3	24	48	36	48	5.17, 5.18, 5.16, 5.15
S1 — Εφαρμογή ERP (ενότητες)	Forging of rights	4	User authentication is not ensured	3	24	48	36	48	8.5, 5.17, 5.16
S2 — ΣΔΒΔ/Βάση δεδομένων	Forging of rights	4	Authorisation management is flawed	3	36	48	36	48	5.17, 5.18, 5.16, 5.15
S2 — ΣΔΒΔ/Βάση δεδομένων	Forging of rights	4	User authentication is not ensured	3	36	48	36	48	8.5, 5.17, 5.16
S3 — Λογισμικό διεπαφής e-invoicing & επικύρωση	Forging of rights	4	Authorisation management is flawed	3	36	48	24	48	5.17, 5.18, 5.16, 5.15
S3 — Λογισμικό διεπαφής e-invoicing & επικύρωση	Forging of rights	4	User authentication is not ensured	3	36	48	24	48	8.5, 5.17, 5.16
S4 — Μηχανισμός ταυτότητας & ρόλων (IAM)	Forging of rights	4	Authorisation management is flawed	3	36	48	36	48	5.17, 5.18, 5.16, 5.15
S4 — Μηχανισμός ταυτότητας & ρόλων (IAM)	Forging of rights	4	User authentication is not ensured	3	36	48	36	48	8.5, 5.17, 5.16

Υποστηρικτικό αγαθό	Απειλή	T	Ευπάθεια	V	C	I	A	Max	Μέτρα 27002
S5 — Μηχανισμός καταγραφής (logging)	Forging of rights	4	Authorisation management is flawed	3	24	48	24	48	5.17, 5.18, 5.16, 5.15
S5 — Μηχανισμός καταγραφής (logging)	Forging of rights	4	User authentication is not ensured	3	24	48	24	48	8.5, 5.17, 5.16
Server management	Forging of rights	4	Possibility of remote system administration	3	36	48	36	48	6.7
Server management	Forging of rights	4	Flaws in the management or use of accounts with privileges	3	36	48	36	48	8.2, 5.18, 5.15
Server management	Malware infection	4	Update management (patches) is flawed	3	36	48	36	48	8.8, 8.7
Server management	Malware infection	4	Lack of a system hardening policy	3	36	48	36	48	8.19, 8.9, 8.8
System administrator	Error in use	3	Users are not made aware of information security	4	36	48	36	48	5.4, 6.4, 6.3
System administrator	Error in use	3	No IT charter specifying the rules of use	4	36	48	36	48	5.4, 5.10
System administrator	Error in use	3	No training on the equipment or software used	4	36	48	36	48	6.1, 6.3
N1 — Κανάλι ΚΕΔ/PEPPOL, πιστοποιητικά & κλειδιά υπογραφής	Equipment malfunction or failure	3	No service level management	3		36	18	36	7.13, 5.20, 8.21
N1 — Κανάλι ΚΕΔ/PEPPOL, πιστοποιητικά & κλειδιά υπογραφής	Saturation of the information system	4	Possibility of subjecting the relays to an excessive number of requests or intense interference (e.g. denial of service attacks such as smurfing, SYN flood etc.)	3			36	36	— (χειροκίνητη §4.7.3)
N2 — Διεπαφές ΔΙΑΥΓΕΙΑ/ΚΗΜΔΗΣ/ΕΣΗΔΗΣ & ταμειακού κυκλώματος	Equipment malfunction or failure	3	No service level management	3		36	27	36	7.13, 5.20, 8.21
N2 — Διεπαφές ΔΙΑΥΓΕΙΑ/ΚΗΜΔΗΣ/ΕΣΗΔΗΣ & ταμειακού κυκλώματος	Saturation of the information system	4	Possibility of subjecting the relays to an excessive number of requests or intense interference (e.g. denial of service attacks such as smurfing, SYN flood etc.)	3			36	36	— (χειροκίνητη §4.7.3)

Υποστηρικτικό αγαθό	Απειλή	T	Ευπάθεια	V	C	I	A	Max	Μέτρα 27002
Network and Telecom	Equipment malfunction or failure	3	No service level management	3		36	27	36	7.13, 5.20, 8.21
S3 — Λογισμικό διεπαφής e-invoicing & επικύρωση	Data from untrustworthy sources	3	Protocol not allowing safe authentication of the sender of a communication	3		36		36	— (χειροκίνητη §4.7.3)
Server management	Equipment malfunction or failure	3	No service level management	3		36	27	36	7.13, 5.20, 8.6
Specific software maintenance	Error in use	3	Tools or programs are not adapted for use or are not ergonomic	3	27	36	27	36	5.37, 8.6
Specific software maintenance	Software malfunction	3	Update management (patches) is flawed	3		36	27	36	8.32, 8.8, 8.16
Specific software maintenance	Software malfunction	3	Problems in change management or software maintenance	3		36	27	36	5.8, 5.37, 8.32, 8.29
IT organization	Denial of actions	2	No definition of responsibilities	4		32		32	5.3, 6.2, 5.2
IT organization	Abuse of rights	2	No coordination between the departments concerned before hiring staff and when contracts are modified	4	16	32	24	32	6.5, 5.11
User workstations	Abuse of rights	2	No procedures for system install and configuration	4	16	32	24	32	8.1, 8.19, 8.3
S1 — Εφαρμογή ERP (ενότητες)	Disclosure	3	The need-to-know principle is not respected	3	27			27	8.2, 5.18, 5.15
S1 — Εφαρμογή ERP (ενότητες)	Disclosure	3	User rights allow information to be exported	3	27			27	5.12, 8.3, 8.12
S2 — ΣΔΒΔ/Βάση δεδομένων	Disclosure	3	The need-to-know principle is not respected	3	27			27	8.2, 5.18, 5.15

Υποστηρικτικό αγαθό	Απειλή	T	Ευπάθεια	V	C	I	A	Max	Μέτρα 27002
S2 — ΣΔΒΔ/Βάση δεδομένων	Disclosure	3	User rights allow information to be exported	3	27			27	5.12, 8.3, 8.12
S3 — Λογισμικό διεπαφής e-invoicing & επικύρωση	Disclosure	3	The need-to-know principle is not respected	3	27			27	8.2, 5.18, 5.15
S3 — Λογισμικό διεπαφής e-invoicing & επικύρωση	Disclosure	3	User rights allow information to be exported	3	27			27	5.12, 8.3, 8.12
S4 — Μηχανισμός ταυτότητας & ρόλων (IAM)	Disclosure	3	The need-to-know principle is not respected	3	27			27	8.2, 5.18, 5.15
S4 — Μηχανισμός ταυτότητας & ρόλων (IAM)	Disclosure	3	User rights allow information to be exported	3	27			27	5.12, 8.3, 8.12
Backup management	Equipment malfunction or failure	3	Backups are not carried out in accordance with the state of the art	2		24	18	24	5.30, 8.14, 8.13
Employees	Breach of personnel availability	2	No substitutes for strategic personnel	4			24	24	5.37, 8.14, 8.6
IT organization	Theft or destruction of media, documents or equipment	2	Physical access authorisations are not checked regularly	4	16		24	24	7.2, 7.8, 5.18
IT organization	Disclosure	3	No rules for checking equipment entering/leaving the organisation	4	24			24	7.10, 5.9, 7.9
IT organization	Breach of information system maintainability	2	No recovery plan	4			24	24	5.30, 5.29
IT organization	Breach of information system maintainability	2	No organisation for management of security incidents	4			24	24	5.24, 5.26, 6.8

Υποστηρικτικό αγαθό	Απειλή	T	Ευπάθεια	V	C	I	A	Max	Μέτρα 27002
S1 — Εφαρμογή ERP (ενότητες)	Denial of actions	2	No storage of activity tracks	3		24		24	5.28, 8.15, 8.16
S2 — ΣΔΒΔ/Βάση δεδομένων	Corruption of data	2	No means of protecting and monitoring data integrity	3		24		24	— (χειροκίνητη §4.7.3)
S2 — ΣΔΒΔ/Βάση δεδομένων	Denial of actions	2	No storage of activity tracks	3		24		24	5.28, 8.15, 8.16
S3 — Λογισμικό διεπαφής e-invoicing & επικύρωση	Corruption of data	2	No means of protecting and monitoring data integrity	3		24		24	— (χειροκίνητη §4.7.3)
S3 — Λογισμικό διεπαφής e-invoicing & επικύρωση	Denial of actions	2	No storage of activity tracks	3		24		24	5.28, 8.15, 8.16
S4 — Μηχανισμός ταυτότητας & ρόλων (IAM)	Denial of actions	2	No storage of activity tracks	3		24		24	5.28, 8.15, 8.16
S5 — Μηχανισμός καταγραφής (logging)	Denial of actions	2	No storage of activity tracks	3		24		24	5.28, 8.15, 8.16
Server management	Denial of actions	2	No storage of activity tracks	3		24		24	8.15, 8.16
Server management	Abuse of rights	2	The principle of least privilege is not applied	3	18	24	18	24	8.2, 5.15
Specific software maintenance	Software malfunction	3	No SLAs with third parties (internal or external)	2		24	18	24	5.20, 5.19, 5.22
Specific software maintenance	Abuse of rights	2	The supplier does not manage remote maintenance properly	3	18	24	18	24	5.19, 8.21, 8.15, 8.2
System administrator	Breach of personnel availability	2	No substitutes for strategic personnel	4			24	24	5.37, 8.14, 8.6
N1 — Κανάλι ΚΕΔ/PEPPOL, πιστοποιητικά & κλειδιά υπογραφής	Eavesdropping	2	No partitioning of communication networks	3	18			18	8.22, 5.15

Υποστηρικτικό αγαθό	Απειλή	T	Ευπάθεια	V	C	I	A	Max	Μέτρα 27002
N1 — Κανάλι ΚΕΔ/PEPPOL, πιστοποιητικά & κλειδιά υπογραφής	Eavesdropping	2	Wireless network connections are poorly managed	3	18			18	8.24, 5.14, 8.22, 8.12, 5.15
Network and Telecom	Eavesdropping	2	No partitioning of communication networks	3	18			18	8.22, 5.15
Network and Telecom	Eavesdropping	2	Wireless network connections are poorly managed	3	18			18	8.24, 5.14, 8.22, 8.12, 5.15
S1 — Εφαρμογή ERP (ενότητες)	Eavesdropping	2	Use of an unsecured method of communication	3	18			18	8.24, 5.14, 8.26
S2 — ΣΔΒΔ/Βάση δεδομένων	Eavesdropping	2	Use of an unsecured method of communication	3	18			18	8.24, 5.14, 8.26
S3 — Λογισμικό διεπαφής e-invoicing & επικύρωση	Eavesdropping	2	Use of an unsecured method of communication	3	18			18	8.24, 5.14, 8.26
S4 — Μηχανισμός ταυτότητας & ρόλων (IAM)	Eavesdropping	2	Use of an unsecured method of communication	3	18			18	8.24, 5.14, 8.26
S5 — Μηχανισμός καταγραφής (logging)	Disclosure	3	The need-to-know principle is not respected	3	18			18	8.2, 5.18, 5.15
S5 — Μηχανισμός καταγραφής (logging)	Disclosure	3	User rights allow information to be exported	3	18			18	5.12, 8.3, 8.12
Server management	Retrieval of recycled or discarded media	2	Presence of residual data unknown to the user of reallocated or discarded equipment	3	18			18	7.14
User workstations	Retrieval of recycled or discarded media	2	Presence of residual data unknown to the user of reallocated or discarded equipment	4	16			16	8.1, 7.14, 8.10
Backup management	Theft or destruction of media, documents or equipment	2	Backup media are not stored in a suitable place	2	12		12	12	7.10, 8.24, 7.1, 7.4

Υποστηρικτικό αγαθό	Απειλή	T	Ευπάθεια	V	C	I	A	Max	Μέτρα 27002
N2 — Διεπαφές ΔΙΑΥΓΕΙΑ/ΚΗΜΔΗΣ/ΕΣΗΔΗΣ & ταμειακού κυκλώματος	Eavesdropping	2	No partitioning of communication networks	3	12			12	8.22, 5.15
N2 — Διεπαφές ΔΙΑΥΓΕΙΑ/ΚΗΜΔΗΣ/ΕΣΗΔΗΣ & ταμειακού κυκλώματος	Eavesdropping	2	Wireless network connections are poorly managed	3	12			12	8.24, 5.14, 8.22, 8.12, 5.15
S5 — Μηχανισμός καταγραφής (logging)	Eavesdropping	2	Use of an unsecured method of communication	3	12			12	8.24, 5.14, 8.26

Παράρτημα Δ' — Τεκμήρια αναπαραγωγιμότητας και αρχεία τεκμηρίωσης

Τα αρχεία του Πίνακα Δ'.1 αποτελούν τα τεκμήρια αναπαραγωγιμότητας του μοντέλου. Η πλήρης ανασύσταση προϋποθέτει τη διάθεσή τους μαζί με το ηλεκτρονικό παράρτημα. Η εξαγωγή JSON είναι η αυθεντική πηγή των δεδομένων ανά τοποθέτηση. Επειδή τα αναγνωριστικά της διεπαφής μεταβάλλονται μεταξύ φορτώσεων, κάθε γραμμή αγκυρώνεται στο ζεύγος αγαθού και κειμένου ευπάθειας.

Πίνακας Δ'.1. Τεκμήρια αναπαραγωγιμότητας και αρχεία τεκμηρίωσης του μοντέλου.

Τεκμήριο	Περιγραφή
govERP_analysis_2026-07-04.json (v1)	Πλήρης εξαγωγή προ Φάσης 3 — 190 τοποθετήσεις / 85 μοναδικές, όλα τα T/V κενά· το «πριν»
govERP_analysis_2026-07-05_v2.json (v2)	Πλήρης εξαγωγή τελικού μοντέλου — 200/90, μηδέν κενά, μηδέν αριθμητικά σφάλματα στον ανεξάρτητο επανυπολογισμό
govERP_analysis_risks_2026-07-05_v2.csv	Προβολή μητρώου 90 γραμμών — ταύτιση 100% με JSON· πηγή του Παραρτήματος Γ'
Κεφ4_Φύλλο_Αποκλίσεων_ISO27001.xlsx	Ηλεκτρονικό παράρτημα ανάλυσης αποκλίσεων (βλ. Παράρτημα Ε')
Στιγμιότυπα kef4_*	kef4_mitroo_kindynon_01–06 · kef4_prasinos_kindynos_P4_01/02 · kef4_n1_ypo_p3a / kef4_n1_ypo_p3b · kef4_risk_sheet_referentials · kef4_edit_impacts_p1 (ενδεικτικό, ένα για τη διαδικασία) · kef4_monarc_version_verified_setup / _live · kef4_operational_keno · kef4_dialogos_specific_risk · kef4_S3_opsi_E2_E3 / kef4_S2_opsi_E3
Στιγμιότυπο υποδομής (πάροχος)	Εικόνα συστήματος «govERP-MONARC-2.13.4-final» για ταχεία επαναφορά του περιβάλλοντος· φορητό αντίγραφο ασφαλείας = JSON v1/v2 + CSV

Η σύμβαση ονοματοδοσίας των στιγμιότυπων χρησιμοποιεί λατινικούς χαρακτήρες ASCII με πρόθεμα kef4_ και πεζά με κάτω παύλες· η απόδοση «kindynon» αποτελεί συνειδητή απλοποίηση της μεταγραφής ΕΛΟΤ 743 για λόγους φορητότητας ονομάτων αρχείων.

Παράρτημα Ε΄ — Ηλεκτρονικό παράρτημα: υπολογιστικό φύλλο ανάλυσης αποκλίσεων

Το υπολογιστικό φύλλο «Κεφ4_Φύλλο_Αποκλίσεων_ISO27001.xlsx» αποτελεί το ηλεκτρονικό παράρτημα της §4.8. Περιλαμβάνει τα φύλλα Μεθοδολογία, Ρήτρες_4_10, Παράρτημα_A και ΚΥΑ_1689. Το πρώτο καταγράφει τις πηγές, τις τρεις βαθμίδες και την αυτόματη σύνοψη. Το δεύτερο περιέχει τις 25 απαιτήσεις των ρητρών 4–10. Το τρίτο περιέχει τα 93 μέτρα με βαθμίδα, ένταση χαρτογράφησης, κατάσταση, απόκλιση και προτεραιότητα. Το τέταρτο αντιστοιχίζει τις 22 απαιτήσεις της ΚΥΑ 1689/2025 με τα ISO/IEC 27001 και 27002. Οι τύποι επανυπολογίζονται χωρίς σφάλματα και το φύλλο μπορεί να χρησιμοποιηθεί για παρακολούθηση της ωρίμανσης καθώς προστίθενται τεκμήρια.

Παράρτημα ΣΤ' — Προσχέδιο Στόχου Ασφάλειας (Security Target) για τη διεπαφή ηλεκτρονικής τιμολόγησης και εκκαθάρισης του αρχετύπου govERP

ST.1 Εισαγωγή του στόχου ασφάλειας

ST.1.1 Αναφορά του στόχου ασφάλειας

Πίνακας ΣΤ'.1. Στοιχεία αναφοράς του προσχεδίου Στόχου Ασφάλειας.

Πεδίο	Τιμή
Τίτλος	Προσχέδιο Στόχου Ασφάλειας — Διεπαφή ηλεκτρονικής τιμολόγησης και εκκαθάρισης govERP
Αναγνωριστικό	ST-govERP-EINV — v0.1 (προσχέδιο ετοιμότητας)
Ημερομηνία	12/07/2026
Πλαίσιο αναφοράς	ISO/IEC 15408:2022 (Common Criteria, CC:2022) [16], [75]
Συντάκτης	Γεώργιος Καπέρδας — στο πλαίσιο της παρούσας διπλωματικής εργασίας

ST.1.2 Αναφορά του στόχου αξιολόγησης

Πίνακας ΣΤ'.2. Στοιχεία αναφοράς του στόχου αξιολόγησης.

Πεδίο	Τιμή
Στόχος αξιολόγησης (ToE)	Διεπαφή ηλεκτρονικής τιμολόγησης και εκκαθάρισης του αρχετύπου govERP — συστατικό #6 του πίνακα συστατικών της §4.1.5
Τύπος	Υποσύστημα τύπου υπηρεσίας/διεπαφής (όχι προϊόν) — βλ. ST.2
Έκδοση	Άνευ έκδοσης προϊόντος: ο ToE είναι συνθετικό αρχέτυπο, μοντελοποιημένο αποκλειστικά από δημόσιες πηγές (§4.1, §5.2.1) — όριο ετοιμότητας : σε πραγματική προετοιμασία, η αναφορά δεσμεύει συγκεκριμένη έκδοση/διαμόρφωση

ST.1.3 Επισκόπηση του στόχου αξιολόγησης

(Πηγή: §5.2.1)

Ο ToE είναι το υποσύστημα του govERP που παραλαμβάνει τα ηλεκτρονικά τιμολόγια των προμηθευτών — εκδιδόμενα κατά το ευρωπαϊκό πρότυπο EN 16931 και δρομολογούμενα μέσω του δικτύου PEPPOL και του Κέντρου Διαλειτουργικότητας — τα επικυρώνει έναντι επιχειρησιακών και φορολογικών κανόνων αποδοχής και τροφοδοτεί τη ροή εκκαθάρισης [63], [64]. Κύρια χρήση: κανάλι εισόδου των δημοσιονομικών υποχρεώσεων του φορέα. Κεντρικές ιδιότητες ασφάλειας: ακεραιότητα, αυθεντικότητα και μη-αποποίηση των παραστατικών· ακολουθούν εμπιστευτικότητα, διαθεσιμότητα του καναλιού εισροής και λογοδοσία (§5.2.3).

ST.1.4 Περιγραφή του στόχου αξιολόγησης

(Πηγή: §5.2.2–§5.2.3)

Φυσικό/λογικό όριο — εντός: πέντε λειτουργικά στοιχεία: (i) μονάδα παραλαβής τιμολογίου· (ii) μηχανή επικύρωσης (επιχειρησιακοί και φορολογικοί κανόνες αποδοχής)· (iii) σύνδεσμος μετάδοσης προς/από το εξωτερικό κανάλι διασύνδεσης· (iv) συστατικό εκκαθάρισης και Αξιολόγηση Κινδύνων Ασφάλειας Πληροφοριών και Οργανωτικής Ετοιμότητας Κρίσιμων Υποδομών Πληροφορικής 99

κατάστασης (εγγραφές και εξέλιξη συναλλαγών)· (ν) τοπικό ίχνος καταγραφής (logging) των ενεργειών της διεπαφής.

Εκτός ορίου (περιβάλλον λειτουργίας): ο πυρήνας του ERP με το αποθετήριο δεδομένων του, το γενικό υποσύστημα διαχείρισης ταυτότητας και πρόσβασης, η δικτυακή υποδομή και η περίμετρος, οι σταθμοί εργασίας των χειριστών, και η εξωτερική υποδομή διαλειτουργικότητας της Πολιτείας (Κέντρο Διαλειτουργικότητας) ως εξωτερική οντότητα.

Διεπαφές: (α) διεπαφή χειριστή· (β) εσωτερική διεπαφή προς τον πυρήνα του ERP (master data, ενημέρωση καθολικού)· (γ) εξωτερική διεπαφή προς το κανάλι διασύνδεσης ΚΕΔ/PEPPOL — το κέντρο βάρους του μοντέλου· (δ) διεπαφή ελέγχου/καταγραφής.

Περιουσιακά στοιχεία (Πίνακας 5.1 του κεφαλαίου — αντιστοιχία με το μοντέλο MONARC του Κεφ. 4): πρωτεύοντα — περιεχόμενο τιμολογίου (P3b), διεργασία παραλαβής/επικύρωσης/εκκαθάρισης (P3a), κανόνες επικύρωσης (ενσωματωμένοι στα P3a/S3)· υποστηρικτικά — λογισμικό διεπαφής (S3), κανάλι διασύνδεσης με πιστοποιητικά και κλειδιά υπογραφής (N1), ίχνη ελέγχου της διεπαφής (S5 — με τη διευκρίνιση ιχνηλασιμότητας της §5.2.3: αντιστοίχιση σε επίπεδο ταυτότητας αγαθού, όχι θέσης στο δέντρο του Κεφ. 4).

ST.2 Δηλώσεις συμμόρφωσης

(Πηγή: §5.2.1 — δεύτερη διευκρίνιση· §5.3.3–§5.3.4)

Πίνακας ΣΤ΄.3. Δηλώσεις συμμόρφωσης του προσχεδίου προς τα Common Criteria, προς προφίλ προστασίας και προς πακέτο διασφάλισης.

Δήλωση	Περιεχόμενο
Συμμόρφωση CC	Το προσχέδιο συντάσσεται κατά τη δομή και την ορολογία του ISO/IEC 15408:2022 / CC:2022 [16], [75]· οι λειτουργικές απαιτήσεις δηλώνονται σε επίπεδο οικογένειας του Μέρους 2 (βλ. ST.5.1 — όριο ετοιμότητας)
Συμμόρφωση προς PP	Καμία αξίωση συμμόρφωσης προς υφιστάμενο προφίλ προστασίας· η §5.4.3 σκιαγραφεί (μόνο) τη δυνατότητα μελλοντικού PP για την κατηγορία «διεπαφή ηλεκτρονικής τιμολόγησης/εκκαθάρισης δημόσιου ERP»
Πακέτο διασφάλισης	Καμία αξίωση πακέτου SAR, EAL ή επιπέδου EUCC. Η εργασία αποτιμά μόνο τη διαθεσιμότητα τεκμηρίων ανά κλάση διασφάλισης. Τυχόν μελλοντική επιλογή θα απαιτούσε εφαρμοστέο σχήμα, οριστικοποιημένο ΤοΕ, πραγματικά τεκμήρια και ανεξάρτητη αξιολόγηση (§5.3.4).
Τύπος ΤοΕ	Υπηρεσία/διεπαφή: το EUCC αφορά προϊόντα ΤΠΕ [20]· η μεθοδολογική κάλυψη για ΤοΕ τύπου υπηρεσίας τεκμηριώνεται δημόσια από το CYRENE [54], με την προσέγγιση σύνθετων αντικειμένων του CUSTODES στην ίδια κατεύθυνση [14] (§3.5, §3.6, §5.2.1)

ST.3 Ορισμός του προβλήματος ασφάλειας

(Πηγή: §5.3.1)

ST.3.1 Απειλές

Πίνακας ΣΤ΄.4. Απειλές κατά του στόχου αξιολόγησης — αναπαραγωγή του Πίνακα 5.3.

Κωδικός	Περιγραφή	Θεμελίωση στο Κεφάλαιο 4
T.TAMPER	Αλλοίωση δεδομένων τιμολογίου ή εγγραφών εκκαθάρισης, εν	E3: I = 24 υπό P3b, I = 18 υπό P3a· συνεργεί με το E2

Κωδικός	Περιγραφή	Θεμελίωση στο Κεφάλαιο 4
	κινήσει ή εν ηρεμία, με συνέπεια νόθευση της δημοσιονομικής ροής	
T.FORGE	Υποβολή πλαστού ή παραποιημένου τιμολογίου από μη γνήσια πηγή	E2: I = 36 υπό P3b — η βαρύτερη τιμή του κλάδου
T.REPUDIATE	Άρνηση της προέλευσης ή της υποβολής παραστατικού/συναλλαγής εκ των υστέρων	Η ευπάθεια του E2 (αδυναμία ασφαλούς αυθεντικοποίησης αποστολέα)
T.DOS	Διακοπή ή υποβάθμιση της υπηρεσίας παραλαβής/εκκαθάρισης μέσω εξάντλησης πόρων του καναλιού	E1: A = 36 υπό P3a — η μη αποδεκτή διαθεσιμότητα εμφανίζεται στο μοντέλο αποκλειστικά μέσω του E1 (εκτός ορίου: N2 υπό P1)
T.DISCLOSE	Μη εξουσιοδοτημένη αποκάλυψη οικονομικών στοιχείων και δεδομένων προμηθευτών	Κίνδυνοι εμπιστευτικότητας πρώτης επανάληψης (S3/N1): θεσμική διάσταση §4.6.3
T.INTERCEPT	Υποκλοπή ή παρεμβολή στο κανάλι διασύνδεσης (επίθεση ενδιάμεσου)	Κίνδυνοι καναλιού πρώτης επανάληψης (N1): προϋπόθεση των T.FORGE/T.DISCLOSE στο σημείο διασύνδεσης
T.LOG	Αλλοίωση, απώλεια ή καταστολή των ιχνών ελέγχου της διεπαφής	Θεσμική ανάγνωση §4.6.3· σκέλος «παρακολούθησης» της ευπάθειας του E3

ST.3.2 Παραδοχές για το περιβάλλον λειτουργίας

Πίνακας ΣΤ΄.5. Παραδοχές για το περιβάλλον λειτουργίας — αναπαραγωγή του Πίνακα 5.4.

Κωδικός	Περιεχόμενο
A.IAM	Το περιβάλλον παρέχει αξιόπιστη ταυτοποίηση/αυθεντικοποίηση εσωτερικών χρηστών και διαχείριση ρόλων (S4 εκτός ορίου)
A.NETWORK	Η δικτυακή υποδομή και η περίμετρος παρέχουν βασική προστασία και διαχωρισμό
A.PHYSICAL	Η φυσική/περιβαλλοντική προστασία της υποδομής φιλοξενίας εξασφαλίζεται (μεταφορά στον πάροχο — §4.5.1)
A.ADMIN	Οι διαχειριστές είναι έμπιστοι και επαρκώς καταρτισμένοι
A.TIME	Διατίθεται αξιόπιστη πηγή χρόνου για τη χρονοσήμανση

ST.3.3 Οργανωσιακές πολιτικές ασφάλειας

Πίνακας ΣΤ΄.6. Οργανωσιακές πολιτικές ασφάλειας — αναπαραγωγή του Πίνακα 5.5.

Κωδικός	Περιεχόμενο
P.AUDIT	Κάθε ενέργεια παραλαβής, επικύρωσης, αποδοχής/απόρριψης και εκκαθάρισης καταγράφεται με ιχνηλασιμότητα ενεργούντος και χρόνου
P.CRYPTO	Χρησιμοποιούνται εγκεκριμένοι κρυπτογραφικοί μηχανισμοί υπογραφής/προστασίας των παραστατικών, κατά το πλαίσιο B2G [63], [64]
P.RETENTION	Παραστατικά και ίχνη τηρούνται κατά το ισχύον πλαίσιο τήρησης δημοσίων οικονομικών αρχείων
P.COMPLIANCE	Η λειτουργία συμμορφώνεται με το θεσμικό πλαίσιο ηλεκτρονικής τιμολόγησης B2G [63], [64]· NIS2 [4] και ν. 5160/2024 [5] αποκλειστικά ως πλαίσιο αναφοράς (§3.7) — το αρχέτυπο δεν ταξινομείται νομικά ως βασική ή σημαντική οντότητα

ST.4 Στόχοι ασφάλειας

(Πηγή: §5.3.2)

ST.4.1 Στόχοι για τον στόχο αξιολόγησης

Πίνακας ΣΤ΄.7. Στόχοι ασφάλειας για τον στόχο αξιολόγησης — το σκέλος O.* του Πίνακα 5.6.

Κωδικός	Περιεχόμενο
O.INTEGRITY	Ακεραιότητα τιμολογίων και εγγραφών, εν κινήσει και εν ηρεμία
O.NONREP	Μη-αποποίηση προέλευσης και υποβολής, μέσω ψηφιακών υπογραφών
O.AUTH	Αυθεντικοποίηση πηγής παραστατικών και άκρων καναλιού
O.CONFID	Εμπιστευτικότητα δεδομένων
O.AUDIT	Παραγωγή και προστασία πλήρων εγγραφών ελέγχου
O.AVAIL	Διαθεσιμότητα υπηρεσίας παραλαβής, ανάκαμψη ροής εκκαθάρισης
O.ACCESS	Εξουσιοδότηση πρόσβασης κατά ρόλο

ST.4.2 Στόχοι για το περιβάλλον λειτουργίας

Πίνακας ΣΤ΄.8. Στόχοι ασφάλειας για το περιβάλλον λειτουργίας — το σκέλος OE.* του Πίνακα 5.6, με τις παραδοχές που καλύπτει καθένας.

Κωδικός	Περιεχόμενο	Καλύπτει
OE.IAM	Αξιόπιστη ταυτοποίηση και εξουσιοδότηση	A.IAM
OE.NETWORK	Προστασία δικτυακής υποδομής	A.NETWORK
OE.PHYSICAL	Φυσική και περιβαλλοντική προστασία της υποδομής φιλοξενίας	A.PHYSICAL
OE.TIME	Αξιόπιστη πηγή χρόνου	A.TIME
OE.ADMIN	Έμπιστη, καταρτισμένη διαχείριση	A.ADMIN

Στους ΟΕ.IAM και ΟΕ.ADMIN μεταφράζεται το πρώτο μέτωπο του Κεφαλαίου 4 — το σύμπλεγμα ταυτότητας–πρόσβασης–ανθρώπινου παράγοντα — ως ελέγξιμη προσδοκία από το περιβάλλον.

ST.4.3 Τεκμηρίωση στόχων (rationale)

(Πηγή: §5.3.2 — αμφίδρομος έλεγχος πληρότητας)

Πίνακας ΣΤ΄.9. Τεκμηρίωση στόχων: αντιστοίχιση κάθε απειλής, παραδοχής και πολιτικής του ορισμού του προβλήματος ασφάλειας προς τους στόχους που την καλύπτουν.

Στοιχείο SPD	Καλύπτεται από
T.TAMPER	O.INTEGRITY
T.FORGE	O.AUTH, O.NONREP, O.INTEGRITY
T.REPUDIATE	O.NONREP
T.DOS	O.AVAIL
T.DISCLOSE	O.CONFID
T.INTERCEPT	O.AUTH, O.CONFID
T.LOG	O.AUDIT
P.AUDIT	O.AUDIT
P.CRYPTO	O.NONREP, O.CONFID
P.RETENTION	O.AUDIT, O.INTEGRITY
P.COMPLIANCE	εγκάρσια, μέσω του συνόλου των στόχων
A.IAM / A.NETWORK / A.TIME / A.ADMIN	OE.IAM / OE.NETWORK / OE.TIME / OE.ADMIN
A.PHYSICAL	OE.PHYSICAL — διά της συμβατικής μεταφοράς στον πάροχο φιλοξενίας (§4.5.1)

Κάθε απειλή αντικρίζεται από τουλάχιστον έναν στόχο, κάθε πολιτική υλοποιείται από στόχο, κάθε παραδοχή καλύπτεται — ο σκελετός τεκμηρίωσης κατά την §3.3.

ST.5 Απαιτήσεις ασφάλειας

(Πηγή: §5.3.3–§5.3.4)

ST.5.1 Λειτουργικές απαιτήσεις (SFR) — επίπεδο οικογένειας

Όριο ετοιμότητας (δηλωμένο στην §5.3.3): η επιλογή τεκμηριώνεται σε επίπεδο οικογένειας του ISO/IEC 15408-2:2022· η στοιχειοθέτηση σε συνιστώσες, με τις πράξεις παραμετροποίησης (assignment/selection/refinement), αποτελεί αντικείμενο πλήρους σύνταξης σε πραγματική προετοιμασία αξιολόγησης.

Πίνακας ΣΤ΄.10. Λειτουργικές απαιτήσεις ασφάλειας ανά οικογένεια και ο στόχος που υπηρετεί καθεμία — συνοπτική προβολή του Πίνακα 5.7 σε δύο στήλες.

Οικογένεια	Στόχος
FCO_NRO — μη-αποποίηση προέλευσης (πυρήνας)	O.NONREP
FDP_DAU — αυθεντικοποίηση δεδομένων	O.INTEGRITY, O.NONREP
FDP_SDI — ακεραιότητα αποθηκευμένων δεδομένων	O.INTEGRITY
FDP_UIT / FDP_UCT — ακεραιότητα/εμπιστευτικότητα διακινούμενων δεδομένων	O.INTEGRITY, O.CONFID
FCS_COP / FCS_CKM — κρυπτογραφικές πράξεις / διαχείριση κλειδιών	O.NONREP, O.CONFID, O.AUTH
FTP_ITC — έμπιστο κανάλι	O.AUTH, O.CONFID
FIA_UID / FIA_UAU — ταυτοποίηση / αυθεντικοποίηση	O.AUTH, O.ACCESS
Κλάση FMT (ενδεικτικά FMT_SMF, FMT_SMR) — διαχείριση ασφάλειας	O.ACCESS

Οικογένεια	Στόχος
FAU_GEN / FAU_STG — παραγωγή / αποθήκευση εγγραφών ελέγχου	O.AUDIT
FPT_STM — αξιόπιστες χρονοσφραγίδες	O.AUDIT, O.NONREP
FRU_RSA / FPT_RCV — κατανομή πόρων / έμπιστη ανάκαμψη	O.AVAIL

Κέντρο βάρους (§5.3.3): FCO_NRO / FCS_COP–FCS_CKM / FTP_ITC αντικρίζουν τη βαρύτερη τιμή του προφίλ (E2, I = 36) και την κεντρική ιδιότητα του αντικειμένου· FAU_GEN/FAU_STG με FPT_STM θωρακίζουν τη λογοδοσία (θεσμικό επίπεδο §4.6.3).

ST.5.2 Απαιτήσεις διασφάλισης (SAR) — διαθεσιμότητα υλικού

Όριο ετοιμότητας (δηλωμένο στην §5.3.4): δεν επιλέγεται πακέτο SAR προς αξιολόγηση· τεκμηριώνεται η διαθεσιμότητα του υλικού ανά κλάση, με το μητρώο τεκμηρίων της §5.4.2 (Πίνακας 5.10) ως αναλυτική αποτύπωση:

Πίνακας ΣΤ΄.11. Απαιτήσεις διασφάλισης και διαθέσιμο υλικό ανά κλάση — αναπαραγωγή του Πίνακα 5.8.

Κλάση	Διαθέσιμο υλικό (πηγή)
ADV	Περιγραφή σχεδίασης και ορίου — §5.2 / ST.1.4
AGD	Ροές χειριστή, κανόνες αποδοχής — μοντελοποιημένες· πλήρης λειτουργική τεκμηρίωση: εκκρεμότητα ετοιμότητας
ALC	Εξάρτηση αναδόχου/ τρίτου μέρους (συστατικό #8) με τη συμβατική της διάσταση· κατάσταση μέτρων §4.8
ATE	Μοντελοποιημένες ροές επικύρωσης· σημειώσεις επικύρωσης — συμπληρώνονται με την §5.5.2
AVA	Μητρώο 90 μοναδικών γραμμών, τριάδες εμπλουτισμού, προγραμματιστικά επαληθευμένες εξαγωγές (Κεφ. 4)

Δεν επιλέγεται ούτε αξιώνεται επίπεδο διασφάλισης EUCC, πακέτο SAR ή EAL. Οι βαθμολογίες κινδύνου του MONARC χρησιμοποιούνται αποκλειστικά για προτεραιοποίηση και δεν αντιστοιχίζονται σε επίπεδα διασφάλισης. Τυχόν μελλοντική επιλογή επιπέδου θα προϋπέθετε εφαρμοστέο σχήμα, οριστικοποιημένο ΤοΕ, πραγματικά τεκμήρια και ανεξάρτητη αξιολόγηση.

ST.5.3 Τεκμηρίωση απαιτήσεων (rationale)

Η κάλυψη στόχων → οικογενειών προκύπτει από τον πίνακα του ST.5.1 (κάθε O.* καλύπτεται από τουλάχιστον μία οικογένεια· ο O.AVAIL καλύπτεται εντός ορίου από τις FRU_RSA/FPT_RCV, ενώ το ογκομετρικό του σκέλος υπηρετείται σε επίπεδο μέτρων λειτουργικής συνέχειας — δέσμη E1 της §5.4.1 — με τον επιμερισμό προς τον πάροχο που τεκμηρίωσε η §4.7.3). Η συνέχεια απαιτήσεων → μέτρων ISO/IEC 27002:2022 [3] αποτυπώνεται στον Πίνακα 5.9 (§5.4.1) και δεν επαναλαμβάνεται εδώ.

ST.6 Συνοπτική προδιαγραφή του στόχου αξιολόγησης

(Προβολή: λειτουργικά στοιχεία του ST.1.4 × οικογένειες του ST.5.1 — παράγωγο 1:1, χωρίς νέους ισχυρισμούς)

Πίνακας ΣΤ΄.12. Συνοπτική προδιαγραφή: ποιο λειτουργικό στοιχείο του στόχου αξιολόγησης υλοποιεί κατά κύριο λόγο κάθε οικογένεια απαιτήσεων.

Λειτουργικό στοιχείο (εντός ορίου)	Υλοποιεί κατά κύριο λόγο
Μονάδα παραλαβής τιμολογίου	FCO_NRO, FDP_DAU, FIA_UID/UAU (σε συνεργασία με OE.IAM)
Μηχανή επικύρωσης	FDP_DAU (γνησιότητα/εγκυρότητα εισερχομένων)· FMT_SMF/SMR (διαχείριση κανόνων αποδοχής)
Σύνδεσμος μετάδοσης προς/από το κανάλι διασύνδεσης	FTP_ITC, FDP_UIT/UCT, FCS_COP/CKM (πιστοποιητικά και κλειδιά του N1)
Συστατικό εκκαθάρισης και κατάστασης	FDP_SDI (ακεραιότητα εγγραφών εν ηρεμία), FDP_DAU
Τοπικό ίχνος καταγραφής	FAU_GEN/FAU_STG, FPT_STM (με στήριξη OE.TIME)

ST.7 Ιχνηλασιμότητα προσχεδίου

Πίνακας ΣΤ΄.13. Ιχνηλασιμότητα του προσχεδίου: κάθε τμήμα του Στόχου Ασφάλειας προς την πηγή του στο Κεφάλαιο 5 και την άγκυρά του στο Κεφάλαιο 4.

Τμήμα ST	Πηγή στο Κεφάλαιο 5	Άγκυρα στο Κεφάλαιο 4
ST.1.3–ST.1.4	§5.2.1–§5.2.3 (Πίνακας 5.1)	§4.1.4–§4.1.5 (συστατικό #6), §4.4.1 (P3a/P3b/S3/N1)
ST.2	§5.2.1, §5.3.3–§5.3.4	—
ST.3	§5.3.1 (Πίνακας 5.3)	§4.5–§4.6: E1–E3 (Πίνακας 5.2), §4.6.3
ST.4	§5.3.2	§4.7.4 (πρώτο μέτωπο → OE)
ST.5	§5.3.3–§5.3.4 (Πίνακας 5.4), §5.4.2 (Πίνακας 5.6)	§4.6 (τιμές), §4.7.3, §4.8
ST.6	§5.2.2 × §5.3.3	—