



ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

**Κυβερνοασφάλεια και Κανονιστική Συμμόρφωση στην Ψηφιακή
Εφοδιαστική Αλυσίδα: Σχεδιασμός και Αναλυτική Αξιολόγηση
Ενοποιημένου Πλαισίου**

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Σπυρίδων Γρουζτίδης

Επιβλέπουσα: Βασιλική Διαμαντοπούλου, Μόνιμη Επίκουρη Καθηγήτρια

Μέλη εξεταστικής επιτροπής: Καρύδα Μαρία, Καθηγήτρια

Σπαθούλας Γεώργιος, Αναπληρωτής Καθηγητής

Καρλόβασι, Σάμος, Οκτώβριος 2026

Η σελίδα αυτή είναι σκόπιμα λευκή.

ΠΡΟΛΟΓΟΣ ΚΑΙ ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω θερμά την επιβλέπουσα καθηγήτριά μου, Βασιλική Διαμαντοπούλου, για την επιστημονική καθοδήγηση, τη διαθεσιμότητα και τις ουσιαστικές παρατηρήσεις σε όλα τα στάδια εκπόνησης της παρούσας διπλωματικής εργασίας. Ευχαριστώ επίσης τα μέλη της εξεταστικής επιτροπής για τον χρόνο και την αξιολόγησή τους.

Ιδιαίτερες ευχαριστίες οφείλω στην οικογένειά μου και στους ανθρώπους που με στήριξαν κατά τη διάρκεια των σπουδών και της συγγραφής της συγκεκριμένης εργασίας. Η υπομονή, η ενθάρρυνση και η εμπιστοσύνη τους συνέβαλαν ουσιαστικά στην ολοκλήρωση της εργασίας.

Η σελίδα αυτή είναι σκόπιμα λευκή.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ 1 — Εισαγωγή	1
1.1 Ερευνητικό αντικείμενο και πλαίσιο της εργασίας	1
1.2 Ερευνητικό κενό και συνεισφορά της εργασίας	1
1.3 Σκοπός και επιμέρους στόχοι	2
1.4 Ερευνητικά ερωτήματα	2
1.5 Μεθοδολογική προσέγγιση.....	3
1.5.1 Ερευνητικός σχεδιασμός	3
1.5.2 Σώμα πηγών και χρονική οριοθέτηση	3
1.5.3 Εντοπισμός και κριτήρια επιλογής πηγών	3
1.5.4 Ανάλυση πηγών και σύνθεση του πλαισίου	4
1.5.5 Αναλυτική αξιολόγηση και έλεγχος τεκμηρίωσης	4
1.6 Πεδίο εφαρμογής και περιορισμοί.....	4
1.7 Διάρθρωση της εργασίας.....	5
ΚΕΦΑΛΑΙΟ 2 — Κυβερνοασφάλεια και Εφοδιαστική Αλυσίδα	6
2.1 Ορισμός και χαρακτηριστικά της εφοδιαστικής αλυσίδας	6
2.2 Ψηφιακός μετασχηματισμός και διασυνδεδεμένα συστήματα	6
2.3 Κυβερνοκίνδυνοι και επιχειρησιακές επιπτώσεις.....	7
2.4 Περιστατικά τρίτων και επιθέσεις εφοδιαστικής αλυσίδας	7
2.5 Σύνδεση κυβερνοκινδύνου και κανονιστικών απαιτήσεων	8
2.6 Υφιστάμενες προσεγγίσεις και ερευνητικό κενό.....	9
2.6.1 Τεχνικά πλαίσια και πρότυπα διαχείρισης.....	9
2.6.2 Ερευνητικές προσεγγίσεις και όρια αξιολόγησης	9
2.6.3 Ερευνητικό κενό και συνέπειες για τον σχεδιασμό	11
2.7 Συμπεράσματα κεφαλαίου.....	11
ΚΕΦΑΛΑΙΟ 3 — Κανονιστικό Πλαίσιο Κυβερνοασφάλειας και Προστασίας Δεδομένων	12
3.1 Μεθοδολογία κανονιστικής ανάλυσης	12
3.2 Οδηγία NIS2.....	13
3.2.1 Σκοπός, πεδίο εφαρμογής και ενσωμάτωση στην ελληνική έννομη τάξη.....	13
3.2.2 Προσέγγιση βάσει κινδύνου και μέτρα διαχείρισης κινδύνων κυβερνοασφάλειας.....	14
3.2.3 Ασφάλεια της εφοδιαστικής αλυσίδας και σχέσεις με προμηθευτές.....	15
3.2.4 Σημαντικά περιστατικά και υποχρεώσεις αναφοράς.....	15

3.2.5 Ευθύνη διοίκησης, εποπτεία και κυρώσεις.....	16
3.3 Γενικός Κανονισμός Προστασίας Δεδομένων	17
3.3.1 Πεδίο εφαρμογής και βασικές αρχές επεξεργασίας προσωπικών δεδομένων	17
3.3.2 Προσέγγιση βάσει κινδύνου και ασφάλεια της επεξεργασίας.....	18
3.3.3 Παραβίαση προσωπικών δεδομένων και υποχρεώσεις γνωστοποίησης	19
3.3.4 Λογοδοσία, τεκμηρίωση και εκτίμηση αντικτύπου.....	20
3.4 Κανονισμός DORA	21
3.4.1 Σκοπός, πεδίο εφαρμογής και σχέση με τη NIS2	21
3.4.2 Ψηφιακή επιχειρησιακή ανθεκτικότητα και πλαίσιο διαχείρισης κινδύνων ΤΠΕ.....	22
3.4.3 Κίνδυνοι τρίτων παρόχων ΤΠΕ και συμβατικές απαιτήσεις	23
3.4.4 Διαχείριση, ταξινόμηση και αναφορά περιστατικών ΤΠΕ.....	23
3.4.5 Δοκιμές ψηφιακής επιχειρησιακής ανθεκτικότητας και TLPT	25
3.5 Συμπεράσματα κεφαλαίου.....	25
ΚΕΦΑΛΑΙΟ 4 — Συγκριτική Ανάλυση και Ενοποιημένη Χαρτογράφηση των NIS2, GDPR και DORA .	27
4.1 Μεθοδολογική προσέγγιση και όρια της σύγκρισης	27
4.1.1 Αντικείμενο και πηγές της ανάλυσης	27
4.1.2 Χαρακτήρας των πινάκων και ερευνητικοί περιορισμοί	27
4.2 Πεδίο εφαρμογής και σχέση των τριών πλαισίων	28
4.2.1 NIS2: οριζόντια ασφάλεια δικτύων και πληροφοριακών συστημάτων.....	28
4.2.2 GDPR: προστασία θεμελιωδών δικαιωμάτων κατά την επεξεργασία προσωπικών δεδομένων ..	28
4.2.3 DORA: τομεακή ψηφιακή επιχειρησιακή ανθεκτικότητα και αρχή lex specialis	28
4.3 Η έννοια του περιστατικού και οι υποχρεώσεις αναφοράς	29
4.3.1 NIS2: «σημαντικό περιστατικό»	29
4.3.2 GDPR: «παραβίαση προσωπικών δεδομένων»	30
4.3.3 DORA: συμβάν ΤΠΕ και «μείζον συμβάν που σχετίζεται με ΤΠΕ»	30
4.3.4 Ένα πραγματικό γεγονός, τρεις αυτοτελείς νομικές αξιολογήσεις.....	31
4.4 Συγκριτική ανάλυση με προσανατολισμό στον κίνδυνο	32
4.4.1 Διαφορετικά αντικείμενα κινδύνου, κοινή ανάγκη λογοδοσίας.....	32
4.4.2 Διακυβέρνηση, ασφάλεια και απόδειξη αποτελεσματικότητας	32
4.4.3 Επιχειρησιακή συνέχεια και κίνδυνος τρίτων	32
4.4.4 Τι προσθέτει η ενοποιημένη χαρτογράφηση	33
4.5 Εφαρμογή σε σενάριο παρόχου υπηρεσιών εφοδιαστικής (3PL).....	34
4.5.1 Παραδοχές του σεναρίου	34

4.5.2 Αρχική αξιολόγηση και διαδρομή γνωστοποιήσεων.....	34
4.6 Πρότυπο χαρτογράφησης συμμόρφωσης για τη μελέτη περίπτωσης.....	35
4.7 Προκλήσεις εφαρμογής και προτεινόμενες κατευθύνσεις	36
4.7.1 Κύριες δυσχέρειες	36
4.7.2 Πρακτικές κατευθύνσεις ενοποίησης	36
4.8 Συμπεράσματα κεφαλαίου.....	37
ΚΕΦΑΛΑΙΟ 5 — Σχεδιασμός Ενοποιημένου Πλαισίου Συμμόρφωσης και Πρωτόκολλο Εφαρμογής	38
5.1 Μεθοδολογία και απαιτήσεις σχεδιασμού.....	38
5.1.1 Είσοδοι, όρια και μονάδα ανάλυσης.....	38
5.1.2 Απαιτήσεις σχεδιασμού του πλαισίου	39
5.1.3 Λογική κινδύνου και ιχνηλασιμότητα	41
5.2 Πεντασταδιακή πορεία εφαρμογής.....	42
5.2.1 Στάδιο 1 — οριοθέτηση και χαρτογράφηση.....	42
5.2.2 Στάδιο 2 — αξιολόγηση κινδύνων και αποκλίσεων.....	42
5.2.3 Στάδιο 3 — επιλογή μέτρων και σχέδιο αντιμετώπισης.....	42
5.2.4 Στάδιο 4 — δοκιμή ανθεκτικότητας και ετοιμότητα περιστατικών	43
5.2.5 Στάδιο 5 — μέτρηση, ανασκόπηση και βελτίωση.....	43
5.3 Διαχείριση κινδύνου τρίτων και εφοδιαστικής αλυσίδας.....	44
5.3.1 Κρισιμότητα και δέουσα επιμέλεια	44
5.3.2 Σύμβαση, ένταξη και κατανομή ευθυνών.....	44
5.3.3 Παρακολούθηση, αλλαγή και έξοδος.....	45
5.4 Ενιαία ροή διαχείρισης περιστατικών με χωριστούς νομικούς κλάδους.....	46
5.4.1 Λειτουργικά ερωτήματα ταξινόμησης περιστατικού	46
5.4.2 Κοινό επιχειρησιακό αρχείο και κατανομή ρόλων.....	46
5.4.3 Διακυβέρνηση των προθεσμιών και ποιότητα της απόφασης.....	47
5.5 Πλαίσιο τεκμηρίωσης και διασφάλισης	48
5.6 Δείκτες και διοικητική αναφορά	49
5.6.1 Αρχές επιλογής και ερμηνείας.....	49
5.6.2 Διοικητική ανασκόπηση και κλιμάκωση.....	51
5.7 Πρωτόκολλο εφαρμογής του προτύπου στο Κεφάλαιο 6.....	51
5.8 Συμπεράσματα.....	52
ΚΕΦΑΛΑΙΟ 6 — Εφαρμογή του ενοποιημένου πλαισίου στο υποθετικό σενάριο LogiTrans.....	54
6.1 Πρωτόκολλο αξιολόγησης, προφίλ και όρια εφαρμογής	54

6.1.1 Σχεδιασμός και κριτήρια αξιολόγησης.....	54
6.1.2 Παραδοχές του οργανωτικού σεναρίου	55
6.1.3 Έλεγχος εφαρμογής NIS2, GDPR και DORA.....	56
6.1.4 Δομή διακυβέρνησης και γραμμές ευθύνης	57
6.2 Χαρτογράφηση υπηρεσιών, δεδομένων και ρόλων επεξεργασίας	58
6.2.1 Κρίσιμες επιχειρησιακές υπηρεσίες και πληροφοριακά συστήματα	58
6.2.2 Ρόλοι GDPR ανά δραστηριότητα επεξεργασίας.....	59
6.3 Κρίσιμες εξαρτήσεις και κίνδυνος τρίτων μερών.....	60
6.3.1 Αλυσίδες τεχνικής και λειτουργικής εξάρτησης	60
6.3.2 Το κρίσιμο όριο εμπιστοσύνης της πύλης προμηθευτή.....	61
6.4 Ανάλυση κινδύνου και εξέλιξη του περιστατικού.....	61
6.4.1 Μέθοδος αξιολόγησης κινδύνου	61
6.4.2 Σενάριο επίθεσης μέσω της αλυσίδας εφοδιασμού	62
6.4.3 Χρονολόγιο γεγονότων, επίγνωσης και αποφάσεων	63
6.4.4 Αιτιολόγηση του περιστατικού ανά κανονιστικό πλαίσιο.....	64
6.5 Εφαρμογή του ενοποιημένου πλαισίου	65
6.5.1 Εφαρμογή των πέντε σταδίων	65
6.5.2 Ενιαίο μητρώο αποφάσεων και διατήρηση τεκμηρίων	66
6.5.3 Αποτίμηση χρόνων και επιχειρησιακής επίδοσης	66
6.6 Κενά, αιτίες και προτεραιότητες βελτίωσης.....	67
6.6.1 Διάκριση κενού ελέγχου και νομικής παράβασης.....	67
6.6.2 Λογική ιεράρχησης.....	68
6.7 Πιθανές λύσεις και σχέδιο υλοποίησης	69
6.7.1 Άμεσες λύσεις: 0–30 ημέρες	69
6.7.2 Βραχυπρόθεσμες λύσεις: 1–3 μήνες.....	69
6.7.3 Μεσοπρόθεσμες λύσεις: 3–12 μήνες.....	70
6.7.4 Εφικτότητα, κόστος και υπολειπόμενος κίνδυνος.....	71
6.8 Αξιολόγηση της εφαρμογής, περιορισμοί και συμπεράσματα	71
6.8.1 Αποτελέσματα βάσει των προκαθορισμένων κριτηρίων.....	71
6.8.2 Συγκριτική αποτίμηση έναντι βάσης αναφοράς	72
6.8.3 Περιορισμοί της μελέτης περίπτωσης	73
6.8.4 Συνολικά συμπεράσματα.....	73
ΚΕΦΑΛΑΙΟ 7 — Συμπεράσματα, συμβολή και κατευθύνσεις μελλοντικής έρευνας	75

7.1 Σύνοψη	75
7.2 Απάντηση στο RQ1 — Ψηφιακές εξαρτήσεις.....	75
7.3 Απάντηση στο RQ2 — Κανονιστική σύγκριση	75
7.4 Απάντηση στο RQ3 — Σχεδιασμός του πλαισίου.....	76
7.5 Απάντηση στο RQ4 — Σεναριακή αξιολόγηση	76
7.6 Συμβολή της εργασίας.....	77
7.6.1 Εννοιολογική συμβολή.....	77
7.6.2 Μεθοδολογική συμβολή.....	77
7.6.3 Πρακτική συμβολή	78
7.7 Περιορισμοί της εργασίας	78
7.8 Κατευθύνσεις μελλοντικής έρευνας	79
ΒΙΒΛΙΟΓΡΑΦΙΑ.....	80
ΠΑΡΑΡΤΗΜΑ Α — Πρακτικός οδηγός εφαρμογής	85
Α.1 Σκοπός και τρόπος χρήσης	85
Α.2 Προετοιμασία του φακέλου εφαρμογής	85
Α.3 Στάδιο 1 Οριοθέτηση και χαρτογράφηση.....	85
Α.4 Στάδιο 2 Από τη ροή στον κίνδυνο και στο κενό	86
Α.5 Στάδιο 3 Επιλογή και υλοποίηση μέτρων.....	86
Α.6 Στάδιο 4 Δοκιμές και ετοιμότητα περιστατικών	86
Α.7 Στάδιο 5 Μέτρηση και διοικητική ανασκόπηση.....	86
Α.8 Ολοκλήρωση και επαναχρησιμοποίηση	87
ΠΑΡΑΡΤΗΜΑ Β — Υποδείγματα και επεξήγηση πινάκων	88
Β.1 Επιλογή υποδείγματος ανά ανάγκη	88
Β.2 Ελάχιστη εγγραφή έναρξης εφαρμογής.....	88
Β.3 Σύνδεση ροής κινδύνου κενού ενέργειας και τεκμηρίου.....	89
Β.4 Δελτίο δοκιμής και αποδοχής τεκμηρίου.....	89
Β.5 Επιλογή δεικτών και ελάχιστα δεδομένα.....	90
ΠΑΡΑΡΤΗΜΑ Γ — Χάρτες και παραδείγματα ροών	91
Γ.1 Τρόπος ανάγνωσης των χαρτών.....	91
Γ.2 Αναλυτικός χάρτης ροών και εξαρτήσεων.....	91
Γ.3 Λεξικό ροών.....	92
Γ.4 Αναλυτική καρτέλα ροής	93

ΚΑΤΑΛΟΓΟΣ ΣΧΗΜΑΤΩΝ

Σχήμα 5.1: Από τις απαιτήσεις και τις τεχνικές κατευθύνσεις στην επαλήθευση και επανεξέταση.....	41
Σχήμα Γ.1: Χάρτης περιβάλλοντος υπηρεσίας παραγγελιών	91
Σχήμα Γ.2: Αναλυτικός χάρτης επιλεγμένων ροών και εξαρτήσεων	92

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

Πίνακας 1.1: Ερευνητικά ερωτήματα και διαδρομή τεκμηρίωσης	2
Πίνακας 2.1: Ψηφιακά συστήματα και βασικές εξαρτήσεις.....	6
Πίνακας 2.2: Περιστατικό τρίτου και επίθεση εφοδιαστικής αλυσίδας	8
Πίνακας 2.3: Σύγκριση προσεγγίσεων και σύνδεση με την παρούσα εργασία	10
Πίνακας 3.1: Βήματα κανονιστικής ανάλυσης.....	12
Πίνακας 4.1: Πεδίο εφαρμογής, κανονιστικός σκοπός και σχέση των NIS2, GDPR και DORA	29
Πίνακας 4.2: Συγκριτική αποτύπωση της έννοιας και της αναφοράς περιστατικού	31
Πίνακας 4.3: Ενοποιημένη χαρτογράφηση βασικών περιοχών ελέγχου	33
Πίνακας 4.4: Αφετηρία ενεργειών για το υποθετικό περιστατικό ransomware σε πάροχο 3PL	34
Πίνακας 4.5: Επαναχρησιμοποιήσιμο πρότυπο αξιολόγησης για τη μελέτη περίπτωσης.....	35
Πίνακας 5.1: Αρχιτεκτονική του προτεινόμενου πλαισίου συμμόρφωσης	39
Πίνακας 5.2: Προέλευση των απαιτήσεων σχεδιασμού DR1–DR6	40
Πίνακας 5.3: Πεντασταδιακή πορεία εφαρμογής και σημεία απόφασης	43
Πίνακας 5.4: Κύκλος ζωής ελέγχου κρίσιμων τρίτων.....	45
Πίνακας 5.5: Ενιαία ροή περιστατικού και χωριστές υποχρεώσεις αξιολόγησης/αναφοράς	47
Πίνακας 5.6: Αφετηρία τεκμηρίων και ελέγχου ποιότητας.....	48
Πίνακας 5.7: Λεξικό βασικών δεικτών του πλαισίου.....	50
Πίνακας 5.8: Διαδρομή από το πρότυπο του Κεφαλαίου 4 στη μελέτη περίπτωσης	52
Πίνακας 6.1: Βασικές παραδοχές του υποθετικού οργανισμού LogiTrans.....	55
Πίνακας 6.2: Απόφαση πεδίου εφαρμογής στο σενάριο LogiTrans.....	56
Πίνακας 6.3: Κατανομή ρόλων για την εφαρμογή του σεναρίου.....	57
Πίνακας 6.4: Χαρτογράφηση κρίσιμων υπηρεσιών και εξαρτήσεων.....	58
Πίνακας 6.5: Λειτουργική κατανομή ρόλων GDPR στη LogiTrans	59
Πίνακας 6.6: Αξιολόγηση κρίσιμων τρίτων μερών και εξαρτήσεων	60
Πίνακας 6.7: Μητρώο βασικών κινδύνων του σεναρίου.....	61
Πίνακας 6.8: Χρονολόγιο του υποθετικού περιστατικού και σημεία απόφασης	63
Πίνακας 6.9: Δελτίο αιτιολόγησης κανονιστικής ενεργοποίησης	65
Πίνακας 6.10: Εφαρμογή του πλαισίου του Κεφαλαίου 5 στη LogiTrans	66
Πίνακας 6.11: Ενδεικτικοί δείκτες επίδοσης από το περιστατικό	67
Πίνακας 6.12: Μητρώο κενών και προτεραιοτήτων	68
Πίνακας 6.13: Οδικός χάρτης πιθανών λύσεων για τη LogiTrans	70
Πίνακας 6.14: Σύγκριση χωριστής και ενοποιημένης ανάλυσης στο σενάριο	72

Πίνακας 7.1: Αντιστοίχιση ερευνητικών ερωτημάτων, απαντήσεων και ορίων	77
Πίνακας 7.2: Διαστάσεις, παραδοτέα και όρια της συμβολής.....	78
Πίνακας 7.3: Προτεινόμενα σχέδια μελλοντικής έρευνας	79
Πίνακας Α.1: Πύλες μετάβασης του κύκλου εφαρμογής	87
Πίνακας Β.1: Επιλογέας υποδειγμάτων και παραδοτέων.....	88
Πίνακας Β.2: Ελάχιστη εγγραφή έναρξης εφαρμογής	88
Πίνακας Β.3: Παράδειγμα σύνδεσης $R \rightarrow G \rightarrow A \rightarrow E$	89
Πίνακας Β.4: Δελτίο δοκιμής και αποδοχής τεκμηρίου	90
Πίνακας Β.5: Επιλογή δεικτών και ελάχιστα δεδομένα	90
Πίνακας Γ.1: Λεξικό ροών του διδακτικού χάρτη.....	92
Πίνακας Γ.2: Αναλυτική καρτέλα ροής με παράδειγμα F-02.....	93

ΚΑΤΑΛΟΓΟΣ ΣΥΝΤΟΜΟΓΡΑΦΙΩΝ ΚΑΙ ΑΚΡΩΝΥΜΙΩΝ

Ακρωνύμιο	Αγγλική απόδοση	Ελληνική απόδοση
3PL	Third-Party Logistics	Πάροχος υπηρεσιών εφοδιαστικής τρίτου μέρους
API	Application Programming Interface	Διεπαφή προγραμματισμού εφαρμογών
CISO	Chief Information Security Officer	Υπεύθυνος ασφάλειας πληροφοριών
CRM	Customer Relationship Management	Διαχείριση σχέσεων πελατών
CSF	Cybersecurity Framework	Πλαίσιο κυβερνοασφάλειας
CSIRT	Computer Security Incident Response Team	Ομάδα απόκρισης σε περιστατικά ασφάλειας υπολογιστών
C-SCRM	Cybersecurity Supply Chain Risk Management	Διαχείριση κυβερνοκινδύνου εφοδιαστικής αλυσίδας
DOI	Digital Object Identifier	Ψηφιακό αναγνωριστικό αντικειμένου
DORA	Digital Operational Resilience Act	Κανονισμός για την Ψηφιακή Επιχειρησιακή Ανθεκτικότητα
DPIA	Data Protection Impact Assessment	Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων
DPO	Data Protection Officer	Υπεύθυνος προστασίας δεδομένων
EDPB	European Data Protection Board	Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων
EL-CSIRT	Hellenic Computer Security Incident Response Team	Ομάδα απόκρισης για συμβάντα κυβερνοασφάλειας της ΕΑΚ
EDR	Endpoint Detection and Response	Ανίχνευση και απόκριση σε τερματικά
ENISA	European Union Agency for Cybersecurity	Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια
ERP	Enterprise Resource Planning	Σύστημα διαχείρισης επιχειρησιακών πόρων
GDPR/ΤΚΠΔ	General Data Protection Regulation	Γενικός Κανονισμός για την Προστασία Δεδομένων
ΤΠΕ/ICT	Information and Communication Technology	Τεχνολογίες πληροφοριών και επικοινωνιών
ISO	International Organization for Standardization	Διεθνής Οργανισμός Τυποποίησης
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission	Διεθνείς οργανισμοί τυποποίησης
IT/OT	Information Technology / Operational Technology	Πληροφοριακή / επιχειρησιακή τεχνολογία
ITS	Intelligent Transport Systems	Ευφυή συστήματα μεταφορών
KPI	Key Performance Indicator	Βασικός δείκτης επίδοσης
M365	Microsoft 365	Πλατφόρμα Microsoft 365

Ακρωνύμιο	Αγγλική απόδοση	Ελληνική απόδοση
MFA	Multi-Factor Authentication	Αυθεντικοποίηση πολλαπλών παραγόντων
NIS2	Network and Information Systems Directive 2	Οδηγία (ΕΕ) 2022/2555
NIST	National Institute of Standards and Technology	Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας των ΗΠΑ
RACI	Responsible, Accountable, Consulted, Informed	Εκτελών, υπόλογος, συμβουλευόμενος, ενημερούμενος
RPO	Recovery Point Objective	Στόχος σημείου ανάκτησης
RTO	Recovery Time Objective	Στόχος χρόνου ανάκαμψης
SaaS	Software as a Service	Λογισμικό ως υπηρεσία
SCRM	Supply Chain Risk Management	Διαχείριση κινδύνου εφοδιαστικής αλυσίδας
SIEM	Security Information and Event Management	Διαχείριση πληροφοριών και συμβάντων ασφάλειας
SLA	Service Level Agreement	Συμφωνία επιπέδου υπηρεσιών
SOC	Security Operations Center	Κέντρο επιχειρήσεων ασφάλειας
TLPT	Threat-Led Penetration Testing	Δοκιμές διείσδυσης βάσει απειλών
TMS	Transportation Management System	Σύστημα διαχείρισης μεταφορών
WMS	Warehouse Management System	Σύστημα διαχείρισης αποθήκης
ΑΠΔΠΧ	Hellenic Data Protection Authority	Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
EAK	National Cybersecurity Authority	Εθνική Αρχή Κυβερνοασφάλειας
ΕΕ	European Union	Ευρωπαϊκή Ένωση
ΕΚ	European Community	Ευρωπαϊκή Κοινότητα
ΚΥΑ	Joint Ministerial Decision	Κοινή Υπουργική Απόφαση
ΥΑ	Ministerial Decision	Υπουργική Απόφαση
ΦΕΚ	Government Gazette	Εφημερίδα της Κυβερνήσεως

Κωδικοί του προτεινόμενου πλαισίου

Κωδικός	Σημασία
A	Action – διορθωτική ενέργεια
D	Dependency – καταγεγραμμένη εξάρτηση
DR1–DR6	Απαιτήσεις σχεδιασμού του ενοποιημένου πλαισίου
E	Evidence – απαιτούμενο τεκμήριο
F	Flow – καταγεγραμμένη ροή δεδομένων
G	Gap – κενό ή απόκλιση
R	Risk – κίνδυνος
RQ1–RQ4	Ερευνητικά ερωτήματα της εργασίας
T-	Πρόθεμα διδακτικού ή παραδειγματικού αρχείου
ΑΞ1–ΑΞ8	Κριτήρια αναλυτικής αξιολόγησης του σεναρίου LogiTrans
K1–K8	Δείκτες παρακολούθησης και διοικητικής αναφοράς

ΠΕΡΙΛΗΨΗ

Η ψηφιοποίηση των υπηρεσιών logistics έχει δημιουργήσει σύνθετες τεχνικές, οργανωτικές και συμβατικές εξαρτήσεις μεταξύ πληροφοριακών συστημάτων, υποδομών νέφους, διεπαφών και εξωτερικών παρόχων. Ένα περιστατικό σε έναν κρίσιμο κρίκο μπορεί να επηρεάσει ταυτόχρονα την επιχειρησιακή συνέχεια, την ασφάλεια δικτύων και συστημάτων, την προστασία προσωπικών δεδομένων και τη συμμόρφωση με πολλαπλές κανονιστικές υποχρεώσεις. Σκοπός της εργασίας είναι ο σχεδιασμός και η αναλυτική αξιολόγηση ενός ενοποιημένου πλαισίου διαχείρισης κυβερνοκινδύνου και κανονιστικής συμμόρφωσης για ψηφιακές υπηρεσίες εφοδιαστικής αλυσίδας.

Η έρευνα ακολουθεί ποιοτική, αναλυτική και συνθετική προσέγγιση. Συνδυάζει στοχευμένη επισκόπηση νομοθεσίας, επίσημης καθοδήγησης, τεχνικών προτύπων και επιστημονικής βιβλιογραφίας, συγκριτική χαρτογράφηση της Οδηγίας NIS2, του Γενικού Κανονισμού για την Προστασία Δεδομένων και του Κανονισμού για την Ψηφιακή Επιχειρησιακή Ανθεκτικότητα, καθώς και εφαρμογή σε υποθετικό οργανωτικό σενάριο. Η κανονιστική ανάλυση έχει χρονικό όριο την 31η Αυγούστου 2026 και διατηρεί χωριστές τις νομικές κρίσεις για το πεδίο εφαρμογής, τους ρόλους, τον χαρακτηρισμό περιστατικών και τις αναφορές.

Το προτεινόμενο πλαίσιο οργανώνεται σε πέντε στάδια: οριοθέτηση της υπηρεσίας και χαρτογράφηση εξαρτήσεων, αξιολόγηση κινδύνων και αποκλίσεων, επιλογή μέτρων, δοκιμή ανθεκτικότητας και ετοιμότητας περιστατικών, και μέτρηση με διοικητική ανασκόπηση. Η ιχνηλασιμότητα από τον κίνδυνο στο κενό, στη διορθωτική ενέργεια και στο απαιτούμενο τεκμήριο συνδέει κάθε απόφαση με υπεύθυνο, προθεσμία και κριτήριο αποδοχής. Η αναλυτική εφαρμογή στο υποθετικό σενάριο LogiTrans ανέδειξε τη σημασία της κοινής επιχειρησιακής τεκμηρίωσης, αλλά και την ανάγκη αυτοτελούς αξιολόγησης των υποχρεώσεων NIS2, GDPR και DORA. Εντόπισε επίσης αβεβαιότητες στους χρόνους επίγνωσης, στις σχέσεις με τρίτους, στην αιτιολόγηση αποφάσεων προστασίας δεδομένων και στους στόχους ανάκαμψης.

Η συμβολή της εργασίας συνίσταται στη σύνδεση της κανονιστικής σύγκρισης με ένα εφαρμόσιμο σύστημα τεκμηρίωσης, δεικτών, υποδειγμάτων και χαρτών ροών. Η αξιολόγηση αφορά την πληρότητα του σχεδιασμού και την εσωτερική συνέπεια της αναλυτικής εφαρμογής. Τα προτεινόμενα μέτρα δεν υλοποιήθηκαν σε πραγματικό οργανισμό και δεν πραγματοποιήθηκε ανεξάρτητη εμπειρική επαλήθευση. Επομένως, δεν τεκμηριώνεται πραγματική μείωση κινδύνου, κόστους ή χρόνου απόκρισης. Μελλοντική έρευνα απαιτεί εφαρμογή του πλαισίου σε πραγματικά περιβάλλοντα και συγκριτική αξιολόγηση της πρακτικής του αποτελεσματικότητας.

Λέξεις-κλειδιά: κυβερνοασφάλεια εφοδιαστικής αλυσίδας, logistics, NIS2, GDPR, DORA, κανονιστική συμμόρφωση, ψηφιακή επιχειρησιακή ανθεκτικότητα

ABSTRACT

Cybersecurity and Regulatory Compliance in the Digital Supply Chain: Design and Analytical Evaluation of an Integrated Framework

The digitalisation of logistics services has created complex technical, organisational, and contractual dependencies among information systems, cloud infrastructure, interfaces, and external providers. An incident affecting one critical link may simultaneously disrupt business continuity, network and information system security, personal data protection, and compliance with several regulatory obligations. This thesis designs and analytically evaluates an integrated framework for cyber-risk management and regulatory compliance in digital supply-chain services.

The research follows a qualitative, analytical, and synthetic approach. It combines a targeted review of legislation, official guidance, technical standards, and academic literature with comparative mapping of the NIS2 Directive, the General Data Protection Regulation, and the Digital Operational Resilience Act, followed by application to a constructed organisational scenario. The regulatory analysis has a cut-off date of 31 August 2026 and keeps separate the legal assessments concerning scope, roles, incident classification, and reporting obligations.

The proposed framework comprises five stages: service scoping and dependency mapping; risk and gap assessment; control selection and implementation; resilience testing and incident preparedness; and measurement with management review. Traceability from risk to gap, corrective action, and required evidence links each decision to an owner, a deadline, and an acceptance criterion. Its analytical application to the hypothetical LogiTrans scenario highlighted the value of shared operational evidence while confirming the need for separate assessments under NIS2, GDPR, and DORA. It also identified uncertainty in awareness times, third-party relationships, the reasoning behind data-protection decisions, and recovery objectives.

The thesis contributes by connecting regulatory comparison with a usable system of evidence, indicators, templates, and data-flow maps. The evaluation concerns design completeness and the internal consistency of the analytical application. The proposed measures were not implemented in a real organisation, and no independent empirical validation was conducted. The study therefore does not demonstrate an actual reduction in risk, cost, or response time. Future research should apply the framework in operational settings and comparatively assess its practical effectiveness.

Keywords: *supply chain cybersecurity, logistics, NIS2, GDPR, DORA, regulatory compliance, digital operational resilience*

ΚΕΦΑΛΑΙΟ 1 Εισαγωγή

1.1 Ερευνητικό αντικείμενο και πλαίσιο της εργασίας

Η εργασία εξετάζει τη σύνδεση των απαιτήσεων κυβερνοασφάλειας με τις ψηφιακές εξαρτήσεις της εφοδιαστικής αλυσίδας, με έμφαση στους οργανισμούς logistics. Αντικείμενό της είναι η Οδηγία (ΕΕ) 2022/2555 για υψηλό κοινό επίπεδο κυβερνοασφάλειας στην Ένωση (NIS2), ο Γενικός Κανονισμός για την Προστασία Δεδομένων (General Data Protection Regulation, GDPR) και ο Κανονισμός για την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα (Digital Operational Resilience Act, DORA). Οι τρεις πράξεις εξετάζονται ως προς τις προϋποθέσεις εφαρμογής τους και τις διαφορετικές αποφάσεις που απαιτούν από τις εμπλεκόμενες οντότητες (Ευρωπαϊκή Ένωση, 2016, 2022a, 2022b).

Η εκτέλεση μιας παραγγελίας μπορεί να εξαρτάται από συστήματα διαχείρισης επιχειρησιακών πόρων (Enterprise Resource Planning, ERP), αποθήκης (Warehouse Management System, WMS) και μεταφορών (Transportation Management System, TMS), καθώς και από εξωτερικούς παρόχους. Η επαναφορά μιας εφαρμογής δεν εξασφαλίζει την ολοκλήρωση της υπηρεσίας, εάν παραμένουν μη διαθέσιμα τα αναγκαία δεδομένα ή μια εξωτερική διασύνδεση. Η ανάλυση χρειάζεται επομένως να συνδέει την ασφάλεια των επιμέρους συστημάτων με τη συνέχεια της υπηρεσίας και τις επιπτώσεις στους πελάτες και στα φυσικά πρόσωπα.

Το ερώτημα είναι πώς τα κοινά επιχειρησιακά στοιχεία μπορούν να υποστηρίξουν διαφορετικές κανονιστικές κρίσεις. Μια διακοπή υπηρεσίας μπορεί να συνδέεται με παραβίαση προσωπικών δεδομένων ή να επηρεάζει έναν χρηματοοικονομικό πελάτη, αλλά κάθε υποχρέωση απαιτεί δική της αιτιολόγηση. Η εμπορική περιγραφή «logistics» και η ύπαρξη τραπεζικού πελάτη δεν αρκούν για να συναχθεί υπαγωγή σε όλα τα πλαίσια. Απαιτείται εξέταση της οντότητας, της δραστηριότητας, της επεξεργασίας και της συγκεκριμένης υπηρεσίας, όπως αναλύεται στο Κεφάλαιο 3 (Ευρωπαϊκή Ένωση, 2016, 2022a, 2022b).

1.2 Ερευνητικό κενό και συνεισφορά της εργασίας

Οι υπάρχουσες προσεγγίσεις προσφέρουν διαφορετικές αφετηρίες για το πρόβλημα. Οι Ivanov και Dolgui (2020) εξετάζουν τη βιωσιμότητα αλληλεξαρτώμενων δικτύων εφοδιασμού, αναδεικνύοντας τη σημασία των σχέσεων μεταξύ οργανισμών για τη συνέχεια των υπηρεσιών. Στο πεδίο της κυβερνοασφάλειας, ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (European Union Agency for Cybersecurity, ENISA) συγκεντρώνει πρακτικές για τη διαχείριση της ασφάλειας στην εφοδιαστική αλυσίδα (ENISA, 2023). Το Πλαίσιο Κυβερνοασφάλειας 2.0 (Cybersecurity Framework, CSF) του Εθνικού Ινστιτούτου Προτύπων και Τεχνολογίας των ΗΠΑ (National Institute of Standards and Technology, NIST) οργανώνει επιδιωκόμενα αποτελέσματα διακυβέρνησης, διαχείρισης κινδύνου και συνεργασίας με προμηθευτές, χωρίς να προδιαγράφει μία ενιαία μέθοδο επίτευξής τους (NIST, 2024).

Η ύπαρξη αυτών των προσεγγίσεων θέτει το ζήτημα της εξειδίκευσής τους στο συγκεκριμένο επιχειρησιακό και κανονιστικό περιβάλλον. Για μια υπηρεσία logistics χρειάζεται να αποτυπωθεί πώς μια απαίτηση συνδέεται με την υπηρεσία, τις εξαρτήσεις της, έναν κίνδυνο και μια διορθωτική ενέργεια, καθώς και ποια στοιχεία επαρκούν για την επαλήθευση της ενέργειας. Παράλληλα, πρέπει να διατηρούνται διακριτά ο υπόχρεος, το προστατευόμενο συμφέρον, το γεγονός που ενεργοποιεί την υποχρέωση και η αιτιολόγηση της απόφασης για κάθε πλαίσιο.

Στο εξεταζόμενο σώμα πηγών δεν εντοπίστηκε η συγκεκριμένη σύνθεση μιας διαδικασίας που συνδέει τις ψηφιακές εξαρτήσεις υπηρεσιών logistics με χωριστές αποφάσεις NIS2, GDPR και DORA και με αλυσίδα κινδύνου, κενού, ενέργειας και τεκμηρίου. Η οριοθέτηση του ερευνητικού κενού στηρίζεται στη συγκριτική τεκμηρίωση της §2.6 και του Πίνακα 2.3 και συμπληρώνεται από την κανονιστική ανάλυση των Κεφαλαίων 3–4. Αφορά τις επιλεγμένες πηγές και τη συγκεκριμένη επιχειρησιακή εξειδίκευση, χωρίς ισχυρισμό καθολικής απουσίας συναφών λύσεων.

Η συνεισφορά αναπτύσσεται σε τρεις συνδεδεμένες διαστάσεις. Αρχικά αντιστοιχίζονται οι κανονιστικές διαφορές με τα στοιχεία που χρειάζεται κάθε απόφαση. Η ανάλυση αυτή στηρίζει τον σχεδιασμό του πλαισίου πέντε σταδίων και της διαδρομής από την απαίτηση στον κίνδυνο, στο κενό, στην ενέργεια και στο απαιτούμενο τεκμήριο, με υπευθύνους και κριτήρια αποδοχής. Η εφαρμογή στη LogiTrans εξετάζει αυτές τις συνδέσεις και εντοπίζει αποφάσεις ή διορθώσεις που παραμένουν ανεπαρκώς τεκμηριωμένες.

Το πρωτότυπο στοιχείο της πρότασης εντοπίζεται στη συγκεκριμένη σύνθεση και εξειδίκευση αυτών των παραδοτέων. Ένας κοινός επιχειρησιακός φάκελος μπορεί να αξιοποιείται για περισσότερες αξιολογήσεις, ενώ η κανονιστική απόφαση διατηρεί τη δική της βάση. Τα μητρώα, τα υποδείγματα και ο πρακτικός οδηγός αποτελούν εργαλεία αυτής της σύνθεσης. Η χρησιμότητά τους τεκμηριώνεται στο επίπεδο του σχεδιασμού και της αναλυτικής εφαρμογής· η αποτελεσματικότητα σε πραγματικό οργανισμό απαιτεί περαιτέρω αξιολόγηση.

1.3 Σκοπός και επιμέρους στόχοι

Σκοπός της εργασίας είναι η διαμόρφωση και η αναλυτική αξιολόγηση ενός πλαισίου διαχείρισης κυβερνοκινδύνου και κανονιστικών απαιτήσεων για υπηρεσίες logistics. Η πρόταση επιδιώκει να καταστήσει ελέγξιμη τη μετάβαση από το επιχειρησιακό γεγονός στην αιτιολογημένη απόφαση και στη διορθωτική ενέργεια.

Οι επιμέρους στόχοι είναι η αποτύπωση των κρίσιμων εξαρτήσεων, η σύγκριση των απαιτήσεων των τριών πλαισίων, ο σχεδιασμός συνδεδεμένων εργαλείων τεκμηρίωσης και η εξέτασή τους σε υποθετικό περιστατικό. Η αξιολόγηση αναζητά τόσο τις συνδέσεις που μπορούν να υποστηριχθούν από τα δεδομένα όσο και εκείνες για τις οποίες χρειάζονται πρόσθετα στοιχεία. Οι στόχοι εξειδικεύονται στα τέσσερα ερευνητικά ερωτήματα του Πίνακα 1.1.

1.4 Ερευνητικά ερωτήματα

Ο Πίνακας 1.1 αντιστοιχίζει κάθε ερευνητικό ερώτημα με τα κεφάλαια που παρέχουν την κύρια τεκμηρίωσή του. Η συνολική αποτίμηση και των τεσσάρων ερωτημάτων συγκεντρώνεται στο Κεφάλαιο 7.

Πίνακας 1.1: Ερευνητικά ερωτήματα και διαδρομή τεκμηρίωσης

Κωδικός	Ερευνητικό ερώτημα	Κύρια θέση στην εργασία
RQ1 Ψηφιακές εξαρτήσεις	Πώς οι ψηφιακές και οργανωτικές εξαρτήσεις υπηρεσιών, συστημάτων και τρίτων διαμορφώνουν τον κυβερνοκίνδυνο στην εφοδιαστική αλυσίδα;	Κεφάλαια 2 και 6.
RQ2 Κανονιστική σύγκριση	Ποια στοιχεία των NIS2, GDPR και DORA μπορούν να υποστηριχθούν από κοινή επιχειρησιακή οργάνωση και ποιες κρίσεις πρέπει να παραμένουν διακριτές;	Κεφάλαια 3 και 4. Εξειδίκευση στα Κεφάλαια 5 και 6.

Κωδικός	Ερευνητικό ερώτημα	Κύρια θέση στην εργασία
RQ3 Σχεδιασμός πλαίσιου	Πώς οργανώνεται ένα πλαίσιο που συνδέει απαιτήσεις, υπηρεσίες, κινδύνους, διορθώσεις, υπευθύνους και κριτήρια επαλήθευσης;	Κεφάλαιο 5 και παραδοτέα του Κεφαλαίου 6 και των Παραρτημάτων Α–Γ.
RQ4 Αναλυτική εφαρμογή	Ποιες δυνατότητες και ποια όρια αναδεικνύει η εφαρμογή του πλαισίου σε υποθετικό περιστατικό εταιρείας logistics;	Πρωτόκολλο στη §5.7 και αποτίμηση στη §6.8.

Πηγή: Διατύπωση και αντιστοίχιση του συγγραφέα με τη διάρθρωση της εργασίας.

1.5 Μεθοδολογική προσέγγιση

1.5.1 Ερευνητικός σχεδιασμός

Η εργασία ακολουθεί ποιοτική αναλυτική και συνθετική προσέγγιση. Συνδυάζει στοχευμένη, δομημένη βιβλιογραφική και κανονιστική επισκόπηση, συγκριτική χαρτογράφηση, σχεδιασμό πλαισίου και αξιολόγηση μέσω υποθετικού σεναρίου. Η επισκόπηση είναι στοχευμένη: οργανώνει τις επιλεγμένες πηγές γύρω από τα ερευνητικά ερωτήματα, χωρίς να αξιώνει εξαντλητική κάλυψη της βιβλιογραφίας ή εφαρμογή πλήρους πρωτοκόλλου συστηματικής ανασκόπησης.

1.5.2 Σώμα πηγών και χρονική οριοθέτηση

Το υλικό περιλαμβάνει ενωσιακές και ελληνικές κανονιστικές πράξεις, επίσημη εποπτική καθοδήγηση, τεχνικά πρότυπα και πλαίσια, καθώς και επιλεγμένα επιστημονικά άρθρα. Για τη νομοθεσία, σημεία αναφοράς είναι το EUR-Lex και η Εφημερίδα της Κυβερνήσεως. Για την καθοδήγηση και τα τεχνικά πλαίσια χρησιμοποιούνται οι δημοσιεύσεις των αρμόδιων φορέων, ιδίως της ENISA, του NIST και του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων (European Data Protection Board, EDPB). Τα επιστημονικά άρθρα συνδέονται με τις εκδοτικές εγγραφές τους και με ψηφιακό αναγνωριστικό αντικειμένου (Digital Object Identifier, DOI), όπου διατίθεται.

Χρονικό όριο της κανονιστικής ανάλυσης είναι η 31η Αυγούστου 2026. Οι πράξεις εξετάζονται με βάση την έκδοση και τον χρόνο εφαρμογής που αφορούν την ανάλυση, με διάκριση μεταξύ δημοσίευσης, έναρξης ισχύος και έναρξης εφαρμογής. Δεν τίθεται ενιαίο κατώτερο χρονικό όριο για τη βιβλιογραφία, επειδή παλαιότερες θεμελιώδεις πηγές παραμένουν χρήσιμες για τις έννοιες του κινδύνου και της ανθεκτικότητας.

1.5.3 Εντοπισμός και κριτήρια επιλογής πηγών

Ο εντοπισμός και η επαλήθευση των βασικών πηγών συνδυάζουν την αναζήτηση με ακριβή τίτλο, αριθμό πράξης ή αναγνωριστικό DOI με θεματικούς όρους. Ενδεικτικοί όροι είναι «supply chain cybersecurity», «cybersecurity supply chain risk management», «third-party risk», «supply chain resilience», «incident reporting» και «personal data breach notification», σε συνδυασμό με NIS2, GDPR ή DORA. Οι όροι οργανώνουν τη στοχευμένη αναζήτηση και τον έλεγχο συνάφειας. Η εργασία δεν παρουσιάζει πλήρες ημερολόγιο αναζητήσεων ανά βάση ούτε αριθμητική ροή επιλογής δημοσιεύσεων, γεγονός που περιορίζει την ικανότητα αναπαραγωγής του εντοπισμού του συνόλου των πηγών.

Κριτήρια ένταξης είναι η άμεση συνάφεια με τουλάχιστον ένα ερευνητικό ερώτημα, η αναγνωρίσιμη προέλευση, η δυνατότητα ελέγχου του περιεχομένου που αξιοποιείται και η συμβατότητα με το χρονικό και γεωγραφικό πεδίο της μελέτης. Στις νομικές κρίσεις προτεραιότητα έχουν οι επίσημες πράξεις. Στη

βιβλιογραφική σύνθεση προτιμώνται επιστημονικές δημοσιεύσεις που αναλύουν εξαρτήσεις, κίνδυνο, ανθεκτικότητα ή διαχείριση τρίτων. Οι θεματικές επικαλύψεις αξιοποιούνται για σύγκριση, χωρίς να αντιμετωπίζονται ως ανεξάρτητη επιβεβαίωση του ίδιου ισχυρισμού.

Αποκλείονται από τη θεμελίωση υποχρεώσεων ανυπόγραφα ή ατεκμηρίωτα κείμενα, εμπορικές περιλήψεις χωρίς παραπομπή στην αρχική πηγή και πηγές εκτός αντικειμένου. Παρωχημένες εκδόσεις δεν χρησιμοποιούνται ως ισχύων κανόνας όταν έχει εντοπιστεί η αντικατάστασή τους. Για τεχνικά πρότυπα αξιοποιείται μόνο το περιεχόμενο που μπορεί να ελεγχθεί· η αναφορά σε τίτλο ή περίληψη δεν εξομοιώνεται με πλήρη αξιολόγηση των απαιτήσεων του προτύπου.

1.5.4 Ανάλυση πηγών και σύνθεση του πλαισίου

Η σύγκριση οργανώνεται σε κοινούς άξονες: πεδίο εφαρμογής, προστατευόμενο συμφέρον, υπόχρεο οντότητα, διαχείριση κινδύνου, σχέσεις με τρίτους, περιστατικά, ανάκαμψη και τεκμηρίωση. Για κάθε κανονιστική κρίση εξετάζονται η πηγή, η σχετική διάταξη, οι προϋποθέσεις ενεργοποίησης και τα στοιχεία που απαιτούνται για την αιτιολόγησή της. Οι νομικές απαιτήσεις, οι συμβατικές δεσμεύσεις και οι προτεινόμενες οργανωτικές πρακτικές διακρίνονται, ώστε μια τεχνική σύσταση να μην αποδίδεται ως αυτοτελής νομική υποχρέωση.

Η χαρτογράφηση του Κεφαλαίου 4 τροφοδοτεί τα πέντε στάδια του Κεφαλαίου 5. Μονάδα εφαρμογής είναι η επιχειρησιακή υπηρεσία μαζί με τις εξαρτήσεις της. Η ιχνηλασιμότητα οργανώνεται με τους κωδικούς R για κινδύνους, G για κενά, A για ενέργειες και E για απαιτούμενα τεκμήρια. Η διαδρομή $R \rightarrow G \rightarrow A \rightarrow E$ συνδέεται με την αρχική απαίτηση, τον υπεύθυνο και το κριτήριο επαλήθευσης, επιτρέποντας να ελεγχθεί γιατί προτείνεται κάθε διόρθωση και τι χρειάζεται για το κλείσιμό της.

1.5.5 Αναλυτική αξιολόγηση και έλεγχος τεκμηρίωσης

Η αξιολόγηση χρησιμοποιεί τη LogiTrans ως υποθετικό σενάριο εταιρείας logistics. Το σενάριο συνδυάζει ψηφιακές εξαρτήσεις, διαφορετικούς ρόλους επεξεργασίας δεδομένων και σχέση με χρηματοοικονομικό πελάτη, ώστε να εξεταστούν οι διακρίσεις που απαιτεί το πλαίσιο. Οι τέσσερις άξονες ελέγχου της §5.7 είναι η αιτιολόγηση της εφαρμογής κάθε πλαισίου, η ορθότητα των χρονικών αφετηριών, η σύνδεση ενεργειών με κενά και τεκμήρια και η επάρκεια των δεδομένων για τους υπολογισμούς. Η αποτίμησή τους παρουσιάζεται στη §6.8 και υποστηρίζει κυρίως το RQ4.

Η δυνατότητα ελέγχου στηρίζεται σε ρητές παραδοχές, παραπομπές στις πηγές και σταθερούς κωδικούς μεταξύ πινάκων. Γεγονότα του σεναρίου, ερμηνείες και προτεινόμενες διορθώσεις καταγράφονται χωριστά. Ελλείποντα στοιχεία διατηρούνται ως ανοικτά ζητήματα, ενώ τα E περιγράφουν τεκμήρια που θα απαιτούνταν για μελλοντική επαλήθευση. Οι δοκιμές σχεδιάζονται αλλά δεν εκτελούνται. Επομένως, η αποτίμηση αφορά την εσωτερική συνέπεια και την πληρότητα των συνδέσεων της μεθόδου υπό τις δηλωμένες παραδοχές.

1.6 Πεδίο εφαρμογής και περιορισμοί

Η μελέτη εστιάζει στο ευρωπαϊκό κανονιστικό πλαίσιο με ελληνική εξειδίκευση και στις ψηφιακές εξαρτήσεις υπηρεσιών logistics. Δεν συνιστά πλήρη έλεγχο κάθε εθνικής δικαιοδοσίας, τομεακής απαίτησης ή συμβατικής δέσμευσης που ενδέχεται να αφορά έναν πραγματικό οργανισμό. Η επιλογή ελληνόγλωσσων και αγγλόγλωσσων πηγών και ο στοχευμένος χαρακτήρας της επισκόπησης περιορίζουν το εύρος της βιβλιογραφικής κάλυψης.

Η LogiTrans, τα δεδομένα, οι χρόνοι και οι τεχνικές αδυναμίες της είναι υποθετικά. Η υπαγωγή στη NIS2 βασίζεται στις παραδοχές του σεναρίου, οι ρόλοι GDPR εξετάζονται ανά επεξεργασία και η σχέση με την τράπεζα περιορίζεται στη συμβατική διεπαφή που περιγράφεται. Δεν πραγματοποιείται πλήρης ταξινόμηση συμβάντος DORA για την τράπεζα. Οι ελλείψεις αυτές περιορίζουν τα κανονιστικά συμπεράσματα που μπορούν να εξαχθούν από το περιστατικό.

Η αξιολόγηση περιορίζεται στην εσωτερική συνέπεια του υποθετικού σεναρίου: δεν πραγματοποιήθηκαν συνεντεύξεις, έρευνα πεδίου, ανεξάρτητη εμπειρική αξιολόγηση ή μετρήσεις πριν και μετά την εφαρμογή. Η ανάπτυξη του πλαισίου και του σεναρίου από τον ίδιο συγγραφέα δημιουργεί κίνδυνο ενοϊκής επιλογής παραδοχών. Οι συνέπειες για τη γενίκευση και την αποτίμηση αποτελεσματικότητας αναπτύσσονται συγκεντρωτικά στη §7.7.

1.7 Διάρθρωση της εργασίας

Το Κεφάλαιο 2 παρουσιάζει το θεωρητικό και βιβλιογραφικό υπόβαθρο της κυβερνοασφάλειας στην εφοδιαστική αλυσίδα. Το Κεφάλαιο 3 αναλύει χωριστά NIS2, GDPR και DORA, ενώ το Κεφάλαιο 4 συγκρίνει τις απαιτήσεις και διαμορφώνει τη βάση της χαρτογράφησης.

Το Κεφάλαιο 5 αναπτύσσει το προτεινόμενο πλαίσιο, τα στάδια εφαρμογής, τα εργαλεία τεκμηρίωσης και τα κριτήρια αξιολόγησης. Το Κεφάλαιο 6 το εφαρμόζει αναλυτικά στη LogiTrans και καταγράφει συνδέσεις, αποκλίσεις και ανοικτά ζητήματα. Το Κεφάλαιο 7 συνθέτει τις απαντήσεις στα ερευνητικά ερωτήματα, τη συνεισφορά, τους περιορισμούς και τις κατευθύνσεις μελλοντικής έρευνας.

Ο πρακτικός οδηγός και τα υποδείγματα των Παραρτημάτων Α–Γ συμπληρώνουν την ερευνητική ανάλυση με βήματα αξιοποίησης των πινάκων, χάρτες ροών δεδομένων και παράδειγμα σύνδεσης απαίτησης, κινδύνου, ενέργειας και επαλήθευσης. Το υλικό αποτελεί παραδοτέο εφαρμογής του σχεδιασμού και δεν προσθέτει εμπειρικά αποτελέσματα.

ΚΕΦΑΛΑΙΟ 2 Κυβερνοασφάλεια και Εφοδιαστική Αλυσίδα

2.1 Ορισμός και χαρακτηριστικά της εφοδιαστικής αλυσίδας

Η εφοδιαστική αλυσίδα είναι το δίκτυο οργανισμών και διαδικασιών που συνδέει την προμήθεια, την παραγωγή, την αποθήκευση, τη μεταφορά και την παράδοση αγαθών. Η φυσική διακίνηση συνυπάρχει με ροές πληροφοριών που επιτρέπουν τον συντονισμό των συμμετεχόντων. Στην ψηφιακή εφοδιαστική αλυσίδα, οι τεχνολογίες αυτές μεταβάλλουν τον τρόπο οργάνωσης και εκτέλεσης των διαδικασιών (Büyükkökan & Göçer, 2018).

Η θεώρηση των αλληλεξαρτώμενων δικτύων συνδέει τη συνέχεια μιας επιχείρησης με τη λειτουργία των συνεργατών της (Ivanov & Dolgui, 2020). Η ασφάλεια της τεχνολογικής εφοδιαστικής αλυσίδας εξετάζει επιπλέον την περιορισμένη ορατότητα στην ανάπτυξη, ενσωμάτωση και υποστήριξη των προϊόντων και υπηρεσιών που προμηθεύεται ο οργανισμός (Boyens et al., 2024). Οι οπτικές συμπληρώνονται: η πρώτη εξηγεί τη λειτουργική εξάρτηση, ενώ η δεύτερη εξετάζει πώς προϊόντα, προσβάσεις και σχέσεις εμπιστοσύνης δημιουργούν έκθεση σε κυβερνοκίνδυνο.

Για τις υπηρεσίες logistics, ένας πάροχος λογισμικού ή ταυτοποίησης μπορεί να είναι κρίσιμος για τις παραδόσεις χωρίς να μεταφέρει προϊόντα. Η μονάδα ανάλυσης της εργασίας είναι επομένως η επιχειρησιακή υπηρεσία μαζί με τα συστήματα, τα δεδομένα και τους τρίτους από τους οποίους εξαρτάται.

2.2 Ψηφιακός μετασχηματισμός και διασυνδεδεμένα συστήματα

Η ψηφιοποίηση συνδέει στοιχεία παραγγελιών, αποθεμάτων και μεταφορών. Τα αναμενόμενα οφέλη χρειάζονται ξεχωριστή αξιολόγηση: η μελέτη των Hendricks et al. (2007) καταγράφει μικτά αποτελέσματα ανά κατηγορία επιχειρησιακού συστήματος και δείκτη χρηματοοικονομικής επίδοσης. Η εγκατάσταση μιας εφαρμογής δεν αποτελεί από μόνη της απόδειξη βελτίωσης της λειτουργίας ή της ανθεκτικότητας.

Βασικές εφαρμογές είναι τα συστήματα διαχείρισης επιχειρησιακών πόρων (Enterprise Resource Planning, ERP), αποθήκης (Warehouse Management System, WMS) και μεταφορών (Transportation Management System, TMS). Ο Πίνακας 2.1 συνδέει τις λειτουργίες τους με ενδεικτικά δεδομένα και εξαρτήσεις. Οι περιγραφές κινδύνου αποτελούν αναλυτικά παραδείγματα της εργασίας.

Πίνακας 2.1: Ψηφιακά συστήματα και βασικές εξαρτήσεις

Σύστημα ή υποδομή	Λειτουργία	Ενδεικτικά δεδομένα	Εξαρτήσεις και κίνδυνοι
ERP	Συντονισμός προμηθειών, αποθεμάτων, συναλλαγών και παραγγελιών.	Οικονομικά στοιχεία, προϊόντα, προμηθευτές και πελάτες.	Πάροχος λογισμικού και διασυνδέσεις. Μη εξουσιοδοτημένη πρόσβαση ή διακοπή.
WMS	Παραλαβή, αποθήκευση, συλλογή και διακίνηση προϊόντων.	Αποθέματα, θέσεις αποθήκευσης και παραγγελίες.	ERP, σαρωτές και δίκτυο αποθήκης. Αλλοίωση στοιχείων ή αδυναμία εκτέλεσης παραγγελιών.
TMS	Σχεδιασμός δρομολογίων και παρακολούθηση μεταφορών.	Δρομολόγια, αποστολές, οδηγοί και παραλήπτες.	Μεταφορείς και διεπαφές προγραμματισμού εφαρμογών (Application Programming Interfaces, API). Διακοπή ή ανακριβή δεδομένα.

Σύστημα ή υποδομή	Λειτουργία	Ενδεικτικά δεδομένα	Εξαρτήσεις και κίνδυνοι
Υπηρεσίες νέφους	Φιλοξενία εφαρμογών, αποθήκευση και υπολογιστικοί πόροι.	Ανάλογα με την εφαρμογή που υποστηρίζεται.	Πάροχος, υπεργολάβοι και συνδεσιμότητα. Απώλεια πρόσβασης και συγκέντρωση εξαρτήσεων.

Πηγή: Σύνθεση του συγγραφέα βάσει Büyükozkcan και Göçer (2018), Faber et al. (2013), Mell και Grance (2011) και Boyens et al. (2024).

Μια παραγγελία μπορεί να καταχωρίζεται στο ERP, να μεταφέρεται στο WMS για προετοιμασία και να τροφοδοτεί το TMS για διανομή. Αστοχία στη διασύνδεση εμποδίζει τη διαδικασία ακόμη και όταν οι εφαρμογές λειτουργούν. Κοινός πάροχος υποδομής ή μηχανισμός ταυτοποίησης μπορεί επίσης να επηρεάσει πολλές υπηρεσίες ταυτόχρονα. Γι' αυτό η απογραφή εφαρμογών συμπληρώνεται από χάρτη ροών δεδομένων και κοινών εξαρτήσεων.

Το υπολογιστικό νέφος είναι μοντέλο παροχής υπολογιστικών πόρων και υπηρεσιών, στο οποίο μπορούν να στηρίζονται οι παραπάνω εφαρμογές (Mell & Grance, 2011). Οι εξαρτήσεις από συνδεσιμότητα, πάροχο και δυνατότητες αποκατάστασης εξετάζονται μαζί με τις λειτουργικές ανάγκες. Η ανάλυση της αποθήκης απαιτεί αντίστοιχα κατανόηση των εργασιών και της πολυπλοκότητάς τους, πέρα από την καταγραφή του WMS (Faber et al., 2013).

2.3 Κυβερνοκίνδυνοι και επιχειρησιακές επιπτώσεις

Η περιγραφή ενός κυβερνοκινδύνου συνδέει σενάριο απειλής, αξιοποιήσιμη αδυναμία και συνέπεια για υπηρεσίες ή πληροφορίες (Boyens et al., 2024). Ενδεικτικά, η κακόβουλη χρήση λογαριασμού συνεργάτη μπορεί να αξιοποιήσει υπερβολικά δικαιώματα και να οδηγήσει σε εξαγωγή στοιχείων παραδόσεων. Η ανάλυση προσδιορίζει ποια υπηρεσία και ποια δεδομένα εκτίθενται, καθώς και ποιους επηρεάζει το συμβάν.

Οι επιπτώσεις εξετάζονται ως προς τη διαθεσιμότητα, την ακεραιότητα και την εμπιστευτικότητα. Κακόβουλο λογισμικό εκβίασης (ransomware) ή διακοπή παρόχου μπορεί να αναστείλει την προετοιμασία παραγγελιών. Αλλοιωμένα στοιχεία αποθεμάτων ή δρομολόγησης μπορούν να προκαλέσουν λανθασμένες αποστολές, ενώ μη εξουσιοδοτημένη πρόσβαση μπορεί να εκθέσει εμπορικές πληροφορίες και προσωπικά δεδομένα.

Η διάρκεια, η κρισιμότητα της υπηρεσίας και οι διαθέσιμες εναλλακτικές επηρεάζουν τη σοβαρότητα της διατάραξης. Η επαναφορά της λειτουργίας δεν αναιρεί προηγούμενη διαρροή, ενώ μια διαθέσιμη εφαρμογή μπορεί να εξακολουθεί να χρησιμοποιεί αλλοιωμένα δεδομένα. Συνεπώς, η αποτίμηση χρειάζεται χωριστές διαστάσεις για την επιχειρησιακή συνέχεια και τις επιπτώσεις στις πληροφορίες και στα πρόσωπα.

Στην ανακοίνωση της 5ης Ιουλίου 2025, η Ingram Micro ανέφερε εντοπισμό ransomware σε εσωτερικά συστήματα και προληπτική απόσυρση ορισμένων από τη λειτουργία, με στόχο την αποκατάσταση της επεξεργασίας και αποστολής παραγγελιών (Ingram Micro Holding Corporation, 2025). Η συγκεκριμένη ανακοίνωση τεκμηριώνει λειτουργική διατάραξη σε κόμβο διανομής. Δεν επαρκεί για να συναχθεί ότι ο κόμβος χρησιμοποιήθηκε ως διαδρομή επίθεσης στα συστήματα των πελατών του.

2.4 Περιστατικά τρίτων και επιθέσεις εφοδιαστικής αλυσίδας

Ως περιστατικό τρίτου μέρους νοείται εδώ παραβίαση, τεχνική αστοχία ή διακοπή εξωτερικού παρόχου που επηρεάζει έναν οργανισμό λόγω της μεταξύ τους εξάρτησης. Πρόκειται για ευρεία κατηγορία. Η επίθεση

εφοδιαστικής αλυσίδας αποτελεί ειδικότερη περίπτωση, στην οποία η σχέση εφοδιασμού χρησιμοποιείται ως μηχανισμός προσβολής.

Στον ορισμό του Οργανισμού της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (European Union Agency for Cybersecurity, ENISA), ο επιτιθέμενος προσβάλλει προμηθευτή και τον αξιοποιεί για επίθεση σε πελάτη ή επόμενο προμηθευτή (ENISA, 2021). Κριτήριο διάκρισης είναι η διαδρομή της επίθεσης και όχι ο αριθμός των θυμάτων. Ο Πίνακας 2.2 αποτυπώνει τη σχέση των δύο κατηγοριών.

Πίνακας 2.2: Περιστατικό τρίτου και επίθεση εφοδιαστικής αλυσίδας

Κριτήριο	Περιστατικό τρίτου μέρους Ευρύτερη κατηγορία	Επίθεση εφοδιαστικής αλυσίδας Ειδική περίπτωση
Αρχικό γεγονός	Παραβίαση, τεχνική αστοχία ή διακοπή παρόχου.	Σκόπιμη προσβολή προμηθευτή.
Σχέση με τον πελάτη	Επηρεάζεται λόγω εξάρτησης από υπηρεσία, προϊόν ή δεδομένα τρίτου.	Ο παραβιασμένος προμηθευτής ή το προϊόν του χρησιμοποιείται ως διαδρομή επίθεσης.
Επίθεση στον πελάτη	Δεν απαιτείται επίθεση στα δικά του συστήματα ή δεδομένα.	Ο πελάτης αποτελεί στόχο μέσω της σχέσης εφοδιασμού.
Κριτήριο διάκρισης	Η επίπτωση λόγω εξάρτησης, ανεξάρτητα από την ύπαρξη επίθεσης.	Ο μηχανισμός προμηθευτή-πελάτη, όχι ο αριθμός των θυμάτων.
Παράδειγμα	Διακοπή εξωτερικής υπηρεσίας χωρίς επίθεση στον πελάτη.	SolarWinds/SUNBURST.

Πηγή: Σύνοψη του συγγραφέα του ορισμού της ENISA (2021) και της διάκρισης εξάρτησης και διαδρομής προσβολής στην παρούσα ανάλυση.

Στο περιστατικό SolarWinds, που αποκαλύφθηκε το 2020, ο κώδικας SUNBURST ενσωματώθηκε σε εκδόσεις της πλατφόρμας Orion και διανεμήθηκε με ενημερώσεις λογισμικού. Στην ετήσια έκθεση για το 2020, που υποβλήθηκε το 2021, η εταιρεία εκτίμησε ότι λιγότεροι από 18.000 πελάτες θα μπορούσαν να είχαν εγκαταστήσει επηρεαζόμενη έκδοση. Διευκρίνισε ότι οι οργανισμοί στους οποίους ακολούθησε εκμετάλλευση ήταν σημαντικά λιγότεροι (SolarWinds Corporation, 2021). Η δυνητική εγκατάσταση ευάλωτης έκδοσης διακρίνεται έτσι από την επιβεβαιωμένη περαιτέρω προσβολή.

Για την παρούσα εργασία, η διάκριση καθορίζει ποια στοιχεία χρειάζεται να συλλεχθούν. Σε διακοπή τρίτου εξετάζονται η εξαρτώμενη υπηρεσία και οι εναλλακτικές συνέχειες. Όταν υπάρχουν ενδείξεις επίθεσης μέσω προμηθευτή, εξετάζονται επιπλέον οι προσβάσεις, οι διασυνδέσεις και οι ενημερώσεις που χρησιμοποιήθηκαν. Στο ίδιο συμβάν μπορεί να συνυπάρχουν λειτουργικές επιπτώσεις και διαδρομή κακόβουλης προσβολής.

2.5 Σύνδεση κυβερνοκινδύνου και κανονιστικών απαιτήσεων

Η τεχνική αποτύπωση υποστηρίζει την κανονιστική αξιολόγηση, επειδή προσδιορίζει την επηρεαζόμενη υπηρεσία, τα δεδομένα και τους εμπλεκόμενους. Η Οδηγία NIS2 αφορά την κυβερνοασφάλεια των καλυπτόμενων οντοτήτων, ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR) την προστασία των φυσικών προσώπων κατά την επεξεργασία δεδομένων τους και ο Κανονισμός DORA την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα. Ο τελευταίος περιλαμβάνει ειδικές απαιτήσεις για κινδύνους από τρίτους παρόχους υπηρεσιών τεχνολογίας πληροφοριών και επικοινωνιών (ΤΠΕ) (Ευρωπαϊκή Ένωση, 2016, 2022a, 2022b).

Ένα κοινό τεχνικό γεγονός μπορεί να εξετάζεται σε περισσότερα πλαίσια, αλλά η υπαγωγή και η υποχρέωση κάθε οντότητας αιτιολογούνται αυτοτελώς. Η συνεργασία με τράπεζα, για παράδειγμα, απαιτεί εξέταση της παρεχόμενης υπηρεσίας και της συμβατικής σχέσης. Δεν συνεπάγεται ότι κάθε επιχείρηση logistics υπάγεται αυτομάτως στο σύνολο των υποχρεώσεων DORA. Οι νομικές προϋποθέσεις αναλύονται στο Κεφάλαιο 3 και συγκρίνονται στο Κεφάλαιο 4.

Η διάκριση αυτή καθοδηγεί την αξιοποίηση των τεχνικών πλαισίων που ακολουθεί. Ένα πλαίσιο διαχείρισης κινδύνου οργανώνει ρόλους, διαδικασίες και τεκμηρίωση, ενώ η βάση κάθε νομικής υποχρέωσης αναζητείται στην εφαρμοστέα πράξη. Η αντιστοίχιση πρακτικών και απαιτήσεων χρειάζεται επομένως να δηλώνει τόσο τα κοινά στοιχεία όσο και τις διαφορές τους.

2.6 Υφιστάμενες προσεγγίσεις και ερευνητικό κενό

Η σύγκριση ακολουθεί τη στοχευμένη επισκόπηση του Κεφαλαίου 1 και καλύπτει επιλεγμένες πηγές εντός του χρονικού ορίου της 31ης Αυγούστου 2026. Εξετάζει τη μονάδα ανάλυσης, τη διαχείριση τρίτων, την κανονιστική σύνδεση, την τεκμηρίωση αποφάσεων και το είδος αξιολόγησης. Οι άξονες επιτρέπουν να συσχετιστούν πηγές με διαφορετικό σκοπό, διατηρώντας τη διάκριση μεταξύ επιστημονικής μελέτης, τεχνικής καθοδήγησης και κανονιστικής απαίτησης.

2.6.1 Τεχνικά πλαίσια και πρότυπα διαχείρισης

Το Πλαίσιο Κυβερνοασφάλειας 2.0 (Cybersecurity Framework, CSF) του Εθνικού Ινστιτούτου Προτύπων και Τεχνολογίας των ΗΠΑ (National Institute of Standards and Technology, NIST) παρέχει κοινό λεξιλόγιο επιδιωκόμενων αποτελεσμάτων. Η κατηγορία GV.SC καλύπτει τη διαχείριση κυβερνοκινδύνου στην εφοδιαστική αλυσίδα, ενώ οι κατηγορίες διακυβέρνησης συνδέουν ευθύνες, εξαρτήσεις και νομικές ή συμβατικές απαιτήσεις. Η αξία του είναι η οργάνωση και επικοινωνία των στόχων· ο οργανισμός εξειδικεύει τις διαδικασίες και τα τεκμήρια που θα τους υποστηρίξουν (NIST, 2024).

Η ειδική οδηγία NIST SP 800-161 Rev. 1 εμβαθύνει στη διαχείριση κυβερνοκινδύνου εφοδιαστικής αλυσίδας (Cybersecurity Supply Chain Risk Management, C-SCRM), σε επίπεδο οργανισμού, επιχειρησιακών διαδικασιών και συστημάτων. Περιλαμβάνει στρατηγική, πολιτικές, σχέδια και αξιολόγηση προϊόντων και υπηρεσιών. Εδώ χρησιμοποιείται η έκδοση με ενημερώσεις έως την 1η Νοεμβρίου 2024 (Boyens et al., 2024). Συμπληρώνει το CSF με αναλυτικότερη καθοδήγηση, της οποίας η εφαρμογή προϋποθέτει προσαρμογή στον οργανισμό.

Τα ISO/IEC 27001:2022 και 27005:2022, του Διεθνούς Οργανισμού Τυποποίησης και της Διεθνούς Ηλεκτροτεχνικής Επιτροπής, παρέχουν αντίστοιχα απαιτήσεις συστήματος διαχείρισης ασφάλειας πληροφοριών και καθοδήγηση για τη διαχείριση σχετικών κινδύνων (ISO/IEC, 2022a, 2022b). Η παρούσα σύγκριση αξιοποιεί το επίσημα δημοσιευμένο αντικείμενό τους, χωρίς να συνιστά πλήρη αντιστοίχιση ρητρών ή έλεγχο πιστοποίησης. Η ENISA (2023) εξειδικεύει πρακτικές για στρατηγική, διαχείριση κινδύνου και σχέσεων με προμηθευτές, ευπάθειες και ποιότητα προϊόντων. Η καθοδήγηση αυτή συνδέεται με τη NIS2, ενώ οι δεσμευτικές απαιτήσεις αντλούνται από τη νομοθεσία.

2.6.2 Ερευνητικές προσεγγίσεις και όρια αξιολόγησης

Η επιστημονική βιβλιογραφία προσθέτει εξηγήσεις για τον τρόπο με τον οποίο συνδέονται οι τεχνολογικές και οργανωτικές εξαρτήσεις. Οι Ghadge et al. (2020) συνθέτουν μελέτες κυβερνοκινδύνου και αναδεικνύουν τη σημασία ανθρώπινων και οργανωτικών παραγόντων, πέρα από τα τεχνικά μέτρα. Η οπτική αυτή

συμπληρώνει τη θεώρηση αλληλεξαρτώμενων δικτύων των Ivanov και Dolgui (2020). Για την παρούσα εργασία προκύπτει ότι η ανάλυση υπηρεσιών χρειάζεται να συνδέεται με την κατανομή ευθύνης και τη συνεργασία μεταξύ οργανισμών.

Νεότερες εργασίες εξετάζουν ήδη τη σύνθεση πλαισίων. Οι Seid et al. (2025) συγκρίνουν ISO, NIST και NIS2 με στοιχεία από ειδικούς της ασφάλειας πληροφοριών, εστιάζοντας στην εφαρμογή και στις δυσκολίες διαχείρισης κινδύνου τρίτων. Οι Latsiou και Lambrinouidakis (2026) χαρτογραφούν μεθόδους και πρότυπα ανά τύπο προμηθευτή, διακρίνοντας κατασκευαστές, ολοκληρωτές συστημάτων, παρόχους διαχείρισης ΤΠΕ και ψηφιακών υπηρεσιών. Οι πρώτοι προσφέρουν εμπειρική οπτική υιοθέτησης, ενώ οι δεύτεροι βοηθούν στην επιλογή καθοδήγησης ανά σχέση προμήθειας.

Συναφής είναι και η διακανονιστική προσέγγιση των Yu et al. (2026), η οποία μεταφράζει απαιτήσεις δεδομένων και τεχνητής νοημοσύνης σε οργανωτικές αρμοδιότητες και επίπεδα αποφάσεων. Η μελέτη δείχνει ότι η ενοποίηση υποχρεώσεων και ρόλων αποτελεί ήδη αντικείμενο έρευνας. Η εξειδίκευση σε υπηρεσίες logistics και στη σύνδεση NIS2, GDPR και DORA αποτελεί το πεδίο της παρούσας εργασίας.

Η σύγκριση διακρίνει την τεχνική καθοδήγηση και τη βιβλιογραφική σύνθεση από την εμπειρική αξιολόγηση. Η υποθετική εφαρμογή της εργασίας ελέγχει την εσωτερική συνέπεια του πλαισίου, όχι τη μετρημένη αποτελεσματικότητά του σε οργανισμούς. Ο Πίνακας 2.3 συνοψίζει τα ευρήματα.

Πίνακας 2.3: Σύγκριση προσεγγίσεων και σύνδεση με την παρούσα εργασία

Προσέγγιση	Κύρια εστίαση	Τι αξιοποιείται	Πεδίο εξειδίκευσης ή όριο
NIST CSF 2.0 (NIST, 2024)	Αποτελέσματα κυβερνοασφάλειας και διακυβέρνηση.	Εξαρτήσεις, ευθύνες και στόχοι διαχείρισης τρίτων.	Επιλογή διαδικασιών και τεκμηρίων για τη συγκεκριμένη υπηρεσία.
NIST SP 800-161 Rev. 1 (Boyens et al., 2024)	Διαχείριση κυβερνοκινδύνου εφοδιασμού σε πολλαπλά επίπεδα.	Στρατηγική, σχέδια και αξιολόγηση προϊόντων και παρόχων.	Προσαρμογή των πρακτικών στο ευρωπαϊκό πεδίο και στους ρόλους κάθε οντότητας.
ISO/IEC 27001 και 27005 (2022a, 2022b)	Σύστημα διαχείρισης ασφάλειας και κύκλος διαχείρισης κινδύνου.	Σύνδεση αξιολόγησης, αντιμετώπισης και ανασκόπησης κινδύνων.	Σύγκριση βάσει δημοσιευμένου αντικειμένου. Δεν ελέγχονται όλες οι ρήτρες.
ENISA (2023)	Πρακτικές κυβερνοασφάλειας στην εφοδιαστική αλυσίδα.	Διαχείριση προμηθευτών και ευπαθειών με σύνδεση στη NIS2.	Αυτοτελής εξέταση των πρόσθετων απαιτήσεων GDPR και DORA.
Latsiou και Lambrinouidakis (2026)	Χαρτογράφηση μεθόδων και προτύπων ανά τύπο προμηθευτή.	Διαφοροποίηση αξιολόγησης ανά παρεχόμενο προϊόν ή υπηρεσία.	Επισκόπηση πηγών. Δεν αποτελεί εμπειρική εφαρμογή της παρούσας διαδρομής τεκμηρίωσης.
Seid et al. (2025)	Σύγκριση ISO, NIST και NIS2 με στοιχεία από ειδικούς.	Εμπειρική οπτική στις δυσκολίες εφαρμογής και διαχείρισης τρίτων.	Διαφορετικό σύνολο πλαισίων και διαφορετική μέθοδος αξιολόγησης από τη LogiTrans.
Yu et al. (2026)	Διακανονιστική οργάνωση απαιτήσεων δεδομένων και τεχνητής νοημοσύνης.	Σύνδεση υποχρεώσεων με αρμοδιότητες και επίπεδα αποφάσεων.	Εξειδίκευση στο περιστατικό logistics και στις τρεις εξεταζόμενες κανονιστικές κρίσεις.

Προσέγγιση	Κύρια εστίαση	Τι αξιολογείται	Πεδίο εξειδίκευσης ή όριο
Προτεινόμενο πλαίσιο Κεφάλαια 4–6	Υπηρεσίες logistics και αποφάσεις NIS2, GDPR και DORA.	Κοινά στοιχεία, χωριστή αιτιολόγηση και σύνδεση κινδύνου, κενού, ενέργειας και τεκμηρίου.	Υποθετικό σενάριο. Απουσιάζουν ανεξάρτητη επικύρωση και μετρημένη αποτελεσματικότητα.

Πηγή: Συγκριτική σύνθεση του συγγραφέα των πηγών που αναφέρονται ανά γραμμή. Οι εκτιμήσεις εξειδίκευσης εκφράζουν την ανάλυση της παρούσας εργασίας· δεν αποτελούν βαθμολόγηση ή μέτρηση αποτελεσματικότητας.

2.6.3 Ερευνητικό κενό και συνέπειες για τον σχεδιασμό

Η σύγκριση αναδεικνύει ένα συγκεκριμένο πρόβλημα εφαρμογής. Η διαθέσιμη γνώση υποστηρίζει τη διαχείριση τρίτων, τη διακυβέρνηση και τη σύνθεση υποχρεώσεων, αλλά ο οργανισμός χρειάζεται να προσδιορίσει πώς αυτά συνδέονται σε μια ελέγξιμη ακολουθία εργασίας. Στην παρούσα μελέτη, η ακολουθία ξεκινά από την υπηρεσία και την εφαρμοστέα απαίτηση και καταλήγει στον κίνδυνο, στο κενό, στην ενέργεια και στο τεκμήριο επαλήθευσης. Στο ίδιο επιχειρησιακό γεγονός πρέπει επίσης να διατηρούνται διακριτοί οι υπόχρεοι και οι προϋποθέσεις κάθε κανονιστικής απόφασης.

Το ερευνητικό κενό οριοθετείται συνεπώς ως ανάγκη εξειδίκευσης και αναλυτικού ελέγχου αυτής της σύνδεσης για υπηρεσίες logistics. Η παρούσα επισκόπηση δεν τεκμηριώνει καθολική απουσία ενοποιημένων μεθόδων ούτε συγκριτική υπεροχή της πρότασης. Η πρωτοτυπία της εργασίας εξετάζεται στη συγκεκριμένη διάταξη των παραδοτέων και στον τρόπο με τον οποίο η εφαρμογή τους καθιστά ορατές τις ανεπαρκώς αιτιολογημένες αποφάσεις. Οι προγενέστερες μελέτες αξιολογούνται με βάση το δικό τους αντικείμενο και όχι ως ελλειπείς επειδή δεν καλύπτουν μεταγενέστερη νομοθεσία.

Για τον σχεδιασμό του Κεφαλαίου 5 προκύπτουν τέσσερις κατευθύνσεις: μονάδα ανάλυσης η υπηρεσία με τις εξαρτήσεις της, αυτοτελής κανονιστική αιτιολόγηση, σύνδεση κάθε ενέργειας με υπεύθυνο και κριτήριο επαλήθευσης, και ρητή καταγραφή των στοιχείων που λείπουν. Η διαδρομή $R \rightarrow G \rightarrow A \rightarrow E$ αντιστοιχεί σε κίνδυνο, κενό, ενέργεια και απαιτούμενο τεκμήριο. Η ύπαρξη μιας συμπληρωμένης εγγραφής ελέγχεται χωριστά από την απόδειξη ότι η προβλεπόμενη ενέργεια υλοποιήθηκε επιτυχώς.

2.7 Συμπεράσματα κεφαλαίου

Ως προς το RQ1, οι ψηφιακές και οργανωτικές εξαρτήσεις διαμορφώνουν τον κυβερνοκίνδυνο επειδή συνδέουν τη λειτουργία μιας υπηρεσίας με πόρους, δεδομένα και αποφάσεις εκτός των άμεσων ορίων του οργανισμού. Η κρίσιμη πληροφορία είναι ποια υπηρεσία επηρεάζεται, μέσω ποιας εξάρτησης και με ποιες συνέπειες. Η διάκριση περιστατικού τρίτου και επίθεσης εφοδιαστικής αλυσίδας βοηθά να καθοριστεί το αντικείμενο της τεχνικής διερεύνησης.

Οι εξεταζόμενες προσεγγίσεις παρέχουν βάση για διαχείριση κινδύνου, ευθύνη και συνεργασία. Η εργασία αξιοποιεί αυτή τη βάση για να συνδέσει την επιχειρησιακή εικόνα με τις διαφορετικές κανονιστικές αποφάσεις και τα απαιτούμενα τεκμήρια. Το Κεφάλαιο 3 προσδιορίζει τις προϋποθέσεις εφαρμογής των τριών πράξεων, ώστε η συγκριτική χαρτογράφηση του Κεφαλαίου 4 και ο σχεδιασμός που ακολουθεί να στηρίζονται σε σαφή νομική και επιχειρησιακή οριοθέτηση.

ΚΕΦΑΛΑΙΟ 3 Κανονιστικό Πλαίσιο Κυβερνοασφάλειας και Προστασίας Δεδομένων

Οι ψηφιακές εξαρτήσεις που παρουσιάστηκαν στο Κεφάλαιο 2 δημιουργούν υποχρεώσεις ασφάλειας, διαχείρισης περιστατικών και προστασίας δεδομένων. Το παρόν κεφάλαιο εξετάζει τη νομική βάση των υποχρεώσεων αυτών μέσα από την Οδηγία NIS2, τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR) και τον Κανονισμό DORA. Προϋπόθεση της εφαρμογής τους είναι ο προσδιορισμός της δραστηριότητας, της υπηρεσίας και του ρόλου κάθε εμπλεκόμενου οργανισμού.

Η NIS2 ρυθμίζει την κυβερνοασφάλεια των οντοτήτων που υπάγονται στο πεδίο της, ο GDPR την προστασία των φυσικών προσώπων κατά την επεξεργασία προσωπικών δεδομένων και ο DORA την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα. Η προσέγγιση βάσει κινδύνου συνδέει και τα τρία πλαίσια με τις επιχειρησιακές εξαρτήσεις, αλλά το προστατευόμενο συμφέρον και ο υπόχρεος διαφέρουν. Η συμμετοχή σε εφοδιαστική αλυσίδα δεν συνεπάγεται αυτομάτως υπαγωγή και στα τρία.

Η ανάλυση επικεντρώνεται στο πεδίο εφαρμογής, στα μέτρα ασφάλειας, στις σχέσεις με τρίτους και στις υποχρεώσεις αναφοράς. Οι κοινές έννοιες χρησιμοποιούνται μόνο ως σημεία σύγκρισης· κάθε νομική κρίση παραμένει αυτοτελής και συνδέεται με τη δική της βάση, τον υπόχρεο και τις προϋποθέσεις ενεργοποίησης.

3.1 Μεθοδολογία κανονιστικής ανάλυσης

Η ανάλυση ακολουθεί ιεραρχία πηγών. Οι κανονισμοί της Ευρωπαϊκής Ένωσης και οι κατ' εξουσιοδότηση ή εκτελεστικές πράξεις τους εξετάζονται ως δεσμευτικό ενωσιακό δίκαιο. Η NIS2, ως οδηγία, αναλύεται μαζί με τον Ν. 5160/2024 και τις εφαρμοστικές ελληνικές πράξεις. Οι κατευθυντήριες γραμμές του EDPB, οι εγκύκλιοι των εθνικών αρχών και τα τεχνικά πρότυπα χρησιμοποιούνται για ερμηνεία ή εφαρμογή. Δεν δημιουργούν από μόνα τους νέα υποχρέωση, εκτός εάν δεσμευτική διάταξη τα ενσωματώνει ή παραπέμπει σε αυτά.

Για κάθε πλαίσιο εφαρμόζονται τέσσερα διαδοχικά βήματα. Πρώτα προσδιορίζεται το πεδίο εφαρμογής και ο ρόλος της οντότητας. Έπειτα εντοπίζονται η συγκεκριμένη υποχρέωση και το γεγονός που την ενεργοποιεί. Ακολουθούν ο υπόχρεος, ο αποδέκτης και η προθεσμία. Τέλος, καταγράφεται το τεκμήριο που αποδεικνύει τόσο την απόφαση όσο και την εφαρμογή της. Ο Πίνακας 3.1 συνοψίζει τη διαδικασία.

Το χρονικό όριο της έρευνας είναι η 31η Αυγούστου 2026. Προτιμώνται οι επίσημες και, όπου υπάρχουν, οι ενοποιημένες εκδόσεις των πράξεων. Οι νομικές θέσεις συνδέονται με συγκεκριμένο άρθρο, ενώ οι πρακτικές εφαρμογής δηλώνονται ως αναλυτική εξειδίκευση. Μεταγενέστερες πράξεις δεν λαμβάνονται υπόψη στο παρόν κεφάλαιο.

Πίνακας 3.1: Βήματα κανονιστικής ανάλυσης

Βήμα	Ερώτημα ελέγχου	Παραγόμενο τεκμήριο
1. Πεδίο και ρόλος	Υπάγεται η οντότητα, η υπηρεσία ή η επεξεργασία και με ποια ιδιότητα;	Αιτιολόγηση υπαγωγής ή μη υπαγωγής.
2. Υποχρέωση και ενεργοποίηση	Ποια διάταξη εφαρμόζεται και ποιο γεγονός ενεργοποιεί την υποχρέωση;	Κανονιστική απόφαση με συγκεκριμένη νομική βάση.
3. Διαδικασία και χρόνος	Ποιος αποφασίζει ή αναφέρει, σε ποιον και έως πότε;	Χρονογραμμή, ρόλοι και αποδέκτες.

Βήμα	Ερώτημα ελέγχου	Παραγόμενο τεκμήριο
4. Απόδειξη	Ποια στοιχεία αποδεικνύουν την κρίση και την εφαρμογή του μέτρου;	Αρχείο απόφασης, ενέργεια και απαιτούμενο τεκμήριο.

Πηγή: Μεθοδολογική σύνθεση του συγγραφέα βάσει της ιεραρχίας και των κριτηρίων ανάλυσης του παρόντος κεφαλαίου.

3.2 Οδηγία NIS2

3.2.1 Σκοπός, πεδίο εφαρμογής και ενσωμάτωση στην ελληνική έννομη τάξη

Η [Οδηγία \(ΕΕ\) 2022/2555](#), γνωστή ως NIS2, αντικατέστησε την Οδηγία NIS και διεύρυνε τους καλυπτόμενους τομείς, με σκοπό υψηλό κοινό επίπεδο κυβερνοασφάλειας στην Ένωση. Αντικείμενό της είναι η ασφάλεια των συστημάτων δικτύου και πληροφοριών και ο περιορισμός των επιπτώσεων των περιστατικών στις υπηρεσίες των καλυπτόμενων οντοτήτων (άρθρα 1–3).

Κατά τον γενικό κανόνα, υπάγονται δημόσιες ή ιδιωτικές οντότητες των τύπων που απαριθμούνται στα Παραρτήματα I και II, οι οποίες είναι μεσαίες επιχειρήσεις ή υπερβαίνουν τα αντίστοιχα όρια και παρέχουν υπηρεσίες ή ασκούν δραστηριότητες στην Ένωση. Το μέγεθος προσδιορίζεται με τη Σύσταση 2003/361/ΕΚ (Ευρωπαϊκή Επιτροπή, 2003), συνεκτιμώντας εργαζομένους, οικονομικά μεγέθη και στοιχεία συνεργαζόμενων ή συνδεδεμένων επιχειρήσεων. Επομένως, ούτε ο αριθμός εργαζομένων ούτε ο χαρακτηρισμός «logistics» αρκεί μόνος του για την υπαγωγή. Τα παραρτήματα καλύπτουν, μεταξύ άλλων, συγκεκριμένες υπηρεσίες μεταφορών, ψηφιακές υποδομές, διαχείριση υπηρεσιών τεχνολογιών πληροφοριών και επικοινωνιών (ΤΠΕ, ΤΠΕ), καθώς και ταχυδρομικές και ταχυμεταφορικές υπηρεσίες.

Το άρθρο 2 προβλέπει και υπαγωγή ανεξάρτητα από το μέγεθος, μεταξύ άλλων για ορισμένους παρόχους ηλεκτρονικών επικοινωνιών, υπηρεσιών εμπιστοσύνης και συστήματος ονομάτων τομέα. Περιλαμβάνει επίσης περιπτώσεις μοναδικού παρόχου ουσιώδους υπηρεσίας, σοβαρών συνεπειών για τη δημόσια ασφάλεια ή υγεία, συστημικού κινδύνου και ιδιαίτερης εθνικής ή περιφερειακής σημασίας. Η αξιολόγηση χρειάζεται συνεπώς έλεγχο τόσο του γενικού κανόνα όσο και των ειδικών περιπτώσεων και των σχετικών εθνικών πράξεων.

Η διάκριση σε βασικές και σημαντικές οντότητες γίνεται με το άρθρο 3. Κατά κανόνα, οι οντότητες του Παραρτήματος I που υπερβαίνουν τα όρια της μεσαίας επιχείρησης είναι βασικές, ενώ οι λοιπές καλυπτόμενες οντότητες των Παραρτημάτων I και II είναι σημαντικές, με τις ειδικές εξαιρέσεις και τους χαρακτηρισμούς του ίδιου άρθρου. Δεν ταυτίζεται επομένως κάθε οντότητα του Παραρτήματος I με βασική οντότητα. Και οι δύο κατηγορίες υπέχουν υποχρεώσεις διαχείρισης κινδύνων και αναφοράς, αλλά διαφοροποιούνται η εποπτεία και τα ανώτατα επίπεδα προστίμων.

Στον κλάδο της εφοδιαστικής, η υπαγωγή απαιτεί αντιστοίχιση της πραγματικής υπηρεσίας με συγκεκριμένο τύπο οντότητας. Ενδεικτικά, οι οδικές μεταφορές του Παραρτήματος I αφορούν αρμόδιες οδικές αρχές και φορείς εκμετάλλευσης ευφών συστημάτων μεταφορών· δεν καλύπτουν αδιακρίτως κάθε οδικό μεταφορέα ή αποθήκη. Οι ταχυδρομικές και ταχυμεταφορικές υπηρεσίες εξετάζονται στο Παράρτημα II. Η διάκριση αυτή προηγείται της αξιολόγησης μεγέθους και αποτρέπει την αυτόματη υπαγωγή μιας επιχείρησης μόνο λόγω της συμμετοχής της σε εφοδιαστική αλυσίδα.

Στην Ελλάδα, η NIS2 ενσωματώθηκε με τον Ν. 5160/2024 (Ελληνική Δημοκρατία, 2024· ΦΕΚ Α' 195/27.11.2024). Η ΚΥΑ 1689/2025 (Ελληνική Δημοκρατία, 2025b) (ΦΕΚ Β' 2186/06.05.2025) θεσπίζει το Εθνικό Πλαίσιο Απαιτήσεων Κυβερνοασφάλειας με είκοσι δύο απαιτήσεις και τεχνικά, οργανωτικά και

επιχειρησιακά μέτρα. Η ΚΥΑ 1381/2025 (Ελληνική Δημοκρατία, 2025a), όπως τροποποιήθηκε, ρυθμίζει την πλατφόρμα εγγραφής βασικών και σημαντικών οντοτήτων, ενώ η ΥΑ 1899/2025 (Ελληνική Δημοκρατία, 2025c) εξειδικεύει τον ρόλο του Υπεύθυνου Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών. Η ελληνική αξιολόγηση στηρίζεται συνεπώς στον νόμο και στις κανονιστικές πράξεις που αντιστοιχούν στη συγκεκριμένη υποχρέωση.

Η εγκύκλιος 28427/30.07.2026 της Εθνικής Αρχής Κυβερνοασφάλειας (2026) παρέχει ειδική καθοδήγηση για τη διαχείριση ευπαθειών από βασικές οντότητες. Χρησιμοποιείται εντός του πεδίου της ως διοικητική καθοδήγηση και δεν διευρύνει αυτοτελώς τις κατηγορίες οντοτήτων που υπάγονται στον Ν. 5160/2024.

3.2.2 Προσέγγιση βάσει κινδύνου και μέτρα διαχείρισης κινδύνων κυβερνοασφάλειας

Το άρθρο 21 επιβάλλει κατάλληλα και αναλογικά τεχνικά, επιχειρησιακά και οργανωτικά μέτρα για τη διαχείριση κινδύνων των συστημάτων δικτύου και πληροφοριών και για την πρόληψη ή τον περιορισμό των επιπτώσεων στους αποδέκτες και σε άλλες υπηρεσίες. Η υποχρέωση αφορά τόσο την πρόληψη όσο και την ικανότητα απόκρισης και ανάκαμψης.

Η αναλογικότητα εκτιμάται με βάση το σύγχρονο επίπεδο της τεχνολογίας, τα σχετικά πρότυπα, το κόστος εφαρμογής, το μέγεθος και την έκθεση της οντότητας, καθώς και την πιθανότητα και σοβαρότητα των επιπτώσεων. Η διάταξη απαιτεί αιτιολογημένη επιλογή μέτρων, χωρίς να επιβάλλει μία μοναδική αριθμητική μέθοδο βαθμολόγησης κινδύνου.

Σε πρακτικό επίπεδο, η απαίτηση μπορεί να οργανωθεί σε χαρτογράφηση κρίσιμων υπηρεσιών, συστημάτων και εξαρτήσεων, αναγνώριση απειλών και ευπαθειών και αξιολόγηση πιθανότητας και επίπτωσης. Η επίπτωση περιλαμβάνει τη διακοπή υπηρεσιών, τη βλάβη δεδομένων και τις συνέπειες για τρίτους. Πρόκειται για τρόπο επιχειρησιακής υλοποίησης της υποχρέωσης, τον οποίο το Κεφάλαιο 5 εξειδικεύει σε προτεινόμενη μεθοδολογία.

Η αντιμετώπιση μπορεί να περιλαμβάνει μείωση ή αποφυγή του κινδύνου, συμβατική ή ασφαλιστική κάλυψη μέρους των συνεπειών και τεκμηριωμένη αποδοχή υπολειπόμενου κινδύνου. Η μεταφορά οικονομικών συνεπειών δεν μεταφέρει την κανονιστική ευθύνη, ενώ η αποδοχή κινδύνου δεν επιτρέπει παράκαμψη υποχρεωτικών μέτρων. Οι σχετικές αποφάσεις χρειάζονται διοικητική εποπτεία και επανεξέταση.

Η προσέγγιση έναντι κάθε είδους κινδύνου (all-hazards approach) καλύπτει και το φυσικό περιβάλλον των συστημάτων. Τα ελάχιστα πεδία του άρθρου 21 παράγραφος 2 περιλαμβάνουν πολιτικές ανάλυσης κινδύνων, χειρισμό περιστατικών, επιχειρησιακή συνέχεια και ανάκαμψη, ασφάλεια εφοδιαστικής αλυσίδας, ασφαλή απόκτηση και συντήρηση συστημάτων, διαχείριση ευπαθειών, αξιολόγηση αποτελεσματικότητας, κυβερνοϋγιεινή και εκπαίδευση. Περιλαμβάνουν επίσης κρυπτογραφία, ασφάλεια ανθρώπινου δυναμικού, έλεγχο πρόσβασης, διαχείριση περιουσιακών στοιχείων και, όπου ενδείκνυται, πολυπαραγοντική ή συνεχή αυθεντικοποίηση και ασφαλείς επικοινωνίες.

Ο Εκτελεστικός Κανονισμός (ΕΕ) 2024/2690 (Ευρωπαϊκή Επιτροπή, 2024a) εξειδικεύει τεχνικές και μεθοδολογικές απαιτήσεις και περιπτώσεις σημαντικών περιστατικών για τις συγκεκριμένες κατηγορίες ψηφιακών παρόχων του πεδίου του. Δεν αποτελεί αυτομάτως δεσμευτικό κατάλογο για κάθε οντότητα NIS2. Η χρήση του ως τεχνικού σημείου αναφοράς για άλλον οργανισμό πρέπει να διακρίνεται από την άμεση εφαρμογή του.

Η αξιολόγηση και τα μέτρα επανεξετάζονται σε συνάρτηση με αλλαγές, περιστατικά και αποτελέσματα ελέγχων. Η τεκμηρίωση συνδέει τον αναγνωρισμένο κίνδυνο με το επιλεγμένο μέτρο και με τα στοιχεία αποτελεσματικότητάς του, ώστε η διοίκηση και η αρμόδια αρχή να μπορούν να ελέγξουν τη σχετική απόφαση.

3.2.3 Ασφάλεια της εφοδιαστικής αλυσίδας και σχέσεις με προμηθευτές

Το άρθρο 21 παράγραφος 2 στοιχείο δ' εντάσσει ρητά στα μέτρα την ασφάλεια των σχέσεων με άμεσους προμηθευτές και παρόχους υπηρεσιών. Η παράγραφος 3 απαιτεί να λαμβάνονται υπόψη οι ειδικές ευπάθειες κάθε προμηθευτή, η συνολική ποιότητα των προϊόντων και οι πρακτικές κυβερνοασφάλειάς του, περιλαμβανομένης της ασφαλούς ανάπτυξης. Η χαρτογράφηση εξαρτήσεων του Κεφαλαίου 2 αποκτά έτσι συγκεκριμένο κανονιστικό αντικείμενο.

Η απαίτηση μπορεί να εφαρμοστεί με ελέγχους κατά την επιλογή, τη σύναψη σύμβασης, τη λειτουργία και τη λήξη της συνεργασίας. Η έκταση των ελέγχων προσαρμόζεται στην υπηρεσία και στις εφαρμοστέες ενωσιακές και εθνικές απαιτήσεις. Η παρακάτω οργάνωση του κύκλου ζωής αποτελεί πρακτική εξειδίκευση και όχι αυτούσια απαρίθμηση του άρθρου 21.

Για την αξιολόγηση προμηθευτή είναι χρήσιμα η κρισιμότητα της υπηρεσίας, τα δικαιώματα πρόσβασης, τα επεξεργαζόμενα δεδομένα, η υπεργολαβία, η τοποθεσία των υποδομών και η δυνατότητα αντικατάστασης. Η συγκέντρωση κρίσιμων υπηρεσιών σε έναν πάροχο μπορεί να ενισχύσει τις συνέπειες κοινής αστοχίας, ακόμη και αν κάθε επιμέρους υπηρεσία φαίνεται επαρκώς προστατευμένη.

Οι συμβατικοί όροι μπορούν να περιλαμβάνουν απαιτήσεις ασφάλειας πρόσβασης, ενημερώσεων, ειδοποίησης περιστατικών, επιχειρησιακής συνέχειας, ελέγχου, υπεργολαβίας και επιστροφής ή διαγραφής δεδομένων. Η συγκεκριμένη επιλογή και αυστηρότητά τους προκύπτει από τον κίνδυνο και το εφαρμοστέο πλαίσιο· δεν συνιστά ενιαίο συμβατικό υπόδειγμα που επιβάλλει η ίδια η Οδηγία σε κάθε σχέση.

Η ανάθεση δεν απαλλάσσει την καλυπτόμενη οντότητα από τις υποχρεώσεις της. Η παρακολούθηση μπορεί να τεκμηριώνεται με συμφωνημένους δείκτες, αποτελέσματα ελέγχων, αναφορές αποκλίσεων και διορθωτικές ενέργειες. Μια πιστοποίηση του παρόχου αποτελεί στοιχείο αξιολόγησης, χωρίς να υποκαθιστά τον έλεγχο της συγκεκριμένης υπηρεσίας και των εξαρτήσεών της.

Το άρθρο 22 προβλέπει συντονισμένες ενωσιακές αξιολογήσεις κινδύνων ασφάλειας κρίσιμων αλυσίδων εφοδιασμού. Οι οντότητες λαμβάνουν υπόψη τα σχετικά αποτελέσματα κατά το άρθρο 21 παράγραφος 3. Η πρόβλεψη συνδέει την αξιολόγηση μιας διμερούς σχέσης με κινδύνους που μπορεί να επηρεάζουν ολόκληρο κλάδο.

3.2.4 Σημαντικά περιστατικά και υποχρεώσεις αναφοράς

Κατά το άρθρο 6 σημείο 6, περιστατικό είναι γεγονός που θέτει σε κίνδυνο τη διαθεσιμότητα, αυθεντικότητα, ακεραιότητα ή εμπιστευτικότητα δεδομένων ή υπηρεσιών μέσω συστημάτων δικτύου και πληροφοριών. Ο ορισμός καλύπτει κακόβουλες επιθέσεις, αλλά και ανθρώπινα σφάλματα, τεχνικές αστοχίες ή φυσικά συμβάντα.

Δεν γνωστοποιείται υποχρεωτικά κάθε τεχνικό συμβάν. Η υποχρέωση του άρθρου 23 ενεργοποιείται όταν το περιστατικό έχει σημαντικό αντίκτυπο στην παροχή των υπηρεσιών. Ένα περιστατικό θεωρείται σημαντικό όταν έχει προκαλέσει ή μπορεί να προκαλέσει σοβαρή λειτουργική διαταραχή ή οικονομική ζημία

στην οντότητα ή όταν έχει επηρεάσει ή μπορεί να επηρεάσει άλλα φυσικά ή νομικά πρόσωπα προκαλώντας σημαντική υλική ή μη υλική ζημία.

Η οντότητα χρειάζεται κριτήρια αξιολόγησης που συνδέονται με τη διάρκεια, την έκταση, τις υπηρεσίες, τους επηρεαζόμενους αποδέκτες και τις πιθανές ζημιές. Όπου εφαρμόζεται ο Κανονισμός 2024/2690, χρησιμοποιούνται και τα ειδικά κριτήριά του. Η εσωτερική βαθμολόγηση ενός συμβάντος δεν υποκαθιστά τον έλεγχο των νομικών προϋποθέσεων του άρθρου 23.

Η διαδικασία χειρισμού πρέπει να επιτρέπει έγκαιρη ανίχνευση, αξιολόγηση και κλιμάκωση, με σαφή αρμοδιότητα για την υποβολή αναφοράς. Καταγράφονται χωριστά ο εντοπισμός του συμβάντος, η γνώση του σημαντικού περιστατικού και οι μεταγενέστερες ενημερώσεις. Έτσι τεκμηριώνεται η αφετηρία της προθεσμίας, χωρίς αναμονή για πλήρη τεχνική διερεύνηση.

Για σημαντικό περιστατικό, το άρθρο 23 παράγραφος 4 προβλέπει προς την αρμόδια ομάδα απόκρισης σε περιστατικά ασφάλειας υπολογιστών (CSIRT) ή την αρμόδια εθνική αρχή:

1. Έγκαιρη προειδοποίηση χωρίς αδικαιολόγητη καθυστέρηση και πάντως εντός 24 ωρών από τη στιγμή κατά την οποία έλαβε γνώση του σημαντικού περιστατικού.
2. Γνωστοποίηση χωρίς αδικαιολόγητη καθυστέρηση και πάντως εντός 72 ωρών από τη γνώση του σημαντικού περιστατικού, με αρχική αξιολόγηση σοβαρότητας και επιπτώσεων και διαθέσιμους δείκτες παραβίασης. Για παρόχους υπηρεσιών εμπιστοσύνης ισχύει η ειδική προθεσμία των 24 ωρών για σημαντικά περιστατικά που επηρεάζουν τις υπηρεσίες αυτές.
3. Ενδιάμεση έκθεση, όταν αυτή ζητηθεί από το CSIRT ή την αρμόδια αρχή.
4. Τελική έκθεση το αργότερο μέσα σε έναν μήνα από τη γνωστοποίηση του περιστατικού. Εάν η διαχείρισή του συνεχίζεται κατά τον χρόνο υποβολής, παρέχεται έκθεση προόδου και η τελική έκθεση ακολουθεί μέσα σε έναν μήνα από την ολοκλήρωση της διαχείρισης.

Η έγκαιρη προειδοποίηση περιλαμβάνει, όπου συντρέχει περίπτωση, την πιθανή κακόβουλη προέλευση και τις διασυννοριακές επιπτώσεις. Οι επόμενες αναφορές συμπληρώνουν την αρχική εικόνα. Οι 24 και 72 ώρες έχουν την ίδια αφετηρία γνώσης του σημαντικού περιστατικού· η δεύτερη προθεσμία δεν αρχίζει από την υποβολή της προειδοποίησης.

Οι αναφορές δεν υποβάλλονται απευθείας στην ENISA. Κατά το άρθρο 23 παράγραφοι 1–2, ενημέρωση αποδεκτών υπηρεσιών απαιτείται, κατά περίπτωση, για σημαντικά περιστατικά που είναι πιθανό να επηρεάσουν αρνητικά την παροχή τους και για μέτρα αντιμετώπισης σημαντικών κυβερνοαπειλών. Η ενημέρωση αυτή διακρίνεται από την αναφορά στην αρμόδια αρχή.

3.2.5 Ευθύνη διοίκησης, εποπτεία και κυρώσεις

Η NIS2 μεταφέρει την κυβερνοασφάλεια από το επίπεδο της τεχνικής λειτουργίας στο επίπεδο της εταιρικής διοίκησης. Σύμφωνα με το άρθρο 20, τα διοικητικά όργανα των βασικών και σημαντικών οντοτήτων εγκρίνουν τα μέτρα διαχείρισης κινδύνων κυβερνοασφάλειας, εποπτεύουν την εφαρμογή τους και μπορούν να υπέχουν ευθύνη για παραβάσεις των σχετικών υποχρεώσεων. Παράλληλα, τα μέλη των διοικητικών οργάνων πρέπει να λαμβάνουν κατάλληλη εκπαίδευση, ώστε να μπορούν να κατανοούν τους κινδύνους και να αξιολογούν τις πρακτικές διαχείρισής τους.

Η διοίκηση χρειάζεται επαρκή πληροφόρηση για να εγκρίνει μέτρα, να διαθέτει πόρους και να παρακολουθεί διορθωτικές ενέργειες. Η τεχνική εκτέλεση μπορεί να ανατεθεί σε ειδικούς, αλλά η έγκριση και η εποπτεία που προβλέπει το άρθρο 20 δεν εξαντλούνται στην ανάθεση στο τμήμα πληροφορικής.

Η εποπτεία των βασικών οντοτήτων μπορεί να ασκείται τόσο προληπτικά όσο και μετά την ύπαρξη ενδείξεων παράβασης. Οι αρμόδιες αρχές μπορούν να πραγματοποιούν επιτόπιες επιθεωρήσεις, απομακρυσμένη εποπτεία, τακτικούς ή στοχευμένους ελέγχους, σαρώσεις ασφάλειας και αιτήματα παροχής πληροφοριών ή αποδεικτικών στοιχείων. Για τις σημαντικές οντότητες η εποπτεία έχει κατά βάση εκ των υστέρων χαρακτήρα, όταν υπάρχουν ενδείξεις ή πληροφορίες ότι δεν τηρούνται οι υποχρεώσεις.

Οι αρχές διαθέτουν εξουσίες προειδοποίησης, δεσμευτικών εντολών, απαίτησης διορθωτικών ενεργειών και επιβολής κυρώσεων. Για παραβάσεις των άρθρων 21 και 23, το άρθρο 34 απαιτεί τα εθνικά ανώτατα όρια προστίμων να είναι τουλάχιστον ίσα με το υψηλότερο από 10 εκατομμύρια ευρώ ή 2% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών της προηγούμενης οικονομικής χρήσης για τις βασικές οντότητες, και 7 εκατομμύρια ευρώ ή 1,4% αντίστοιχα για τις σημαντικές. Τα ποσά αυτά αφορούν τα απαιτούμενα ανώτατα όρια και όχι ελάχιστο πρόστιμο για κάθε παράβαση. Η συγκεκριμένη επιβολή εξαρτάται από τις περιστάσεις και το εφαρμοστέο εθνικό δίκαιο.

Η τεκμηρίωση μπορεί να περιλαμβάνει εγκεκριμένες πολιτικές και αξιολογήσεις κινδύνων, κατανομή ρόλων, αποφάσεις διοίκησης, αρχεία εκπαίδευσης, ελέγχων, προμηθευτών και περιστατικών. Η αξία της έγκειται στη δυνατότητα σύνδεσης της απόφασης με την πραγματική εφαρμογή του μέτρου, όχι απλώς στην ύπαρξη εγγράφων.

3.3 Γενικός Κανονισμός Προστασίας Δεδομένων

3.3.1 Πεδίο εφαρμογής και βασικές αρχές επεξεργασίας προσωπικών δεδομένων

Ο [Κανονισμός \(ΕΕ\) 2016/679](#) προστατεύει τα φυσικά πρόσωπα κατά την επεξεργασία προσωπικών δεδομένων και ρυθμίζει την ελεύθερη κυκλοφορία τους. Καλύπτει αυτοματοποιημένη επεξεργασία και μη αυτοματοποιημένη επεξεργασία δεδομένων που περιλαμβάνονται ή πρόκειται να περιληφθούν σε σύστημα αρχειοθέτησης, με τις εξαιρέσεις του άρθρου 2. Το εδαφικό πεδίο του άρθρου 3 περιλαμβάνει επεξεργασία στο πλαίσιο εγκατάστασης στην Ένωση και, υπό προϋποθέσεις, προσφορά αγαθών ή υπηρεσιών και παρακολούθηση συμπεριφοράς προσώπων που βρίσκονται στην Ένωση από οργανισμούς εκτός αυτής.

Προσωπικό δεδομένο είναι πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο. Η επεξεργασία περιλαμβάνει όλο τον κύκλο ζωής της πληροφορίας, από τη συλλογή και χρήση μέχρι τη διαβίβαση και διαγραφή, και δεν ταυτίζεται με την αποθήκευση (άρθρο 4). Υπεύθυνος επεξεργασίας είναι εκείνος που καθορίζει τους σκοπούς και τα μέσα· εκτελών την επεξεργασία είναι εκείνος που επεξεργάζεται δεδομένα για λογαριασμό του. Ο ρόλος κρίνεται ανά δραστηριότητα, με βάση τα πραγματικά καθήκοντα, όχι μόνο τον τίτλο της σύμβασης.

Στον τομέα των logistics, προσωπικά δεδομένα μπορεί να αποτελούν τα στοιχεία αποστολέων και παραληπτών, οι διευθύνσεις παράδοσης, οι αριθμοί τηλεφώνου, οι ηλεκτρονικές υπογραφές, τα στοιχεία εργαζομένων και οδηγών, οι καταγραφές καμερών και τα δεδομένα γεωγραφικής θέσης ή τηλεματικής, εφόσον συνδέονται με συγκεκριμένο φυσικό πρόσωπο. Αντίθετα, πληροφορίες που αφορούν αποκλειστικά νομικά πρόσωπα δεν αποτελούν κατ' ανάγκη προσωπικά δεδομένα, εκτός εάν συνδέονται συγχρόνως με ταυτοποιήσιμο φυσικό πρόσωπο.

Το άρθρο 5 του GDPR καθιερώνει τις βασικές αρχές επεξεργασίας. Πρώτη είναι η αρχή της νομιμότητας, αντικειμενικότητας και διαφάνειας. Κάθε επεξεργασία πρέπει να στηρίζεται σε νόμιμη βάση και να πραγματοποιείται με τρόπο κατανοητό και προβλέψιμο για τα υποκείμενα των δεδομένων. Οι νόμιμες βάσεις του άρθρου 6 περιλαμβάνουν τη συγκατάθεση, την εκτέλεση σύμβασης, τη συμμόρφωση με έννομη υποχρέωση, την προστασία ζωτικών συμφερόντων, την εκτέλεση καθήκοντος προς το δημόσιο συμφέρον και το έννομο συμφέρον. Η συγκατάθεση δεν αποτελεί τη μοναδική ούτε πάντοτε την καταλληλότερη νομική βάση.

Η αρχή του περιορισμού του σκοπού απαιτεί τα δεδομένα να συλλέγονται για καθορισμένους, σαφείς και νόμιμους σκοπούς και να μην υποβάλλονται σε περαιτέρω επεξεργασία ασύμβατη με αυτούς. Η αρχή της ελαχιστοποίησης επιβάλλει τη συλλογή μόνο των δεδομένων που είναι κατάλληλα, συναφή και αναγκαία για τον συγκεκριμένο σκοπό. Η αρχή της ακρίβειας απαιτεί τη λήψη εύλογων μέτρων για τη διόρθωση ή διαγραφή ανακριβών δεδομένων.

Ο περιορισμός της περιόδου αποθήκευσης σημαίνει ότι τα προσωπικά δεδομένα δεν πρέπει να διατηρούνται σε μορφή που επιτρέπει την ταυτοποίηση για μεγαλύτερο διάστημα από αυτό που απαιτεί ο σκοπός. Η αρχή δεν επιβάλλει μία ενιαία περίοδο διατήρησης για όλα τα δεδομένα. Ο οργανισμός πρέπει να καθορίζει και να αιτιολογεί διαφορετικές περιόδους ανά κατηγορία δεδομένων, σκοπό επεξεργασίας και εφαρμοζόμενη νομική υποχρέωση.

Η αρχή της ακεραιότητας και εμπιστευτικότητας απαιτεί κατάλληλη ασφάλεια έναντι παράνομης επεξεργασίας και τυχαίας απώλειας ή βλάβης. Η λογοδοσία του άρθρου 5 παράγραφος 2 αναθέτει στον υπεύθυνο επεξεργασίας την ευθύνη τήρησης και απόδειξης των αρχών. Οι αρχές συνδέονται λειτουργικά: η περιττή διατήρηση δεδομένων, για παράδειγμα, αυξάνει και την πιθανή έκθεση σε παραβίαση.

3.3.2 Προσέγγιση βάσει κινδύνου και ασφάλεια της επεξεργασίας

Το άρθρο 32 επιβάλλει τόσο στον υπεύθυνο όσο και στον εκτελούντα την επεξεργασία κατάλληλα τεχνικά και οργανωτικά μέτρα. Συνεκτιμώνται το σύγχρονο επίπεδο της τεχνολογίας, το κόστος εφαρμογής, η φύση, το πεδίο, το πλαίσιο και οι σκοποί της επεξεργασίας και, κυρίως, η πιθανότητα και σοβαρότητα των κινδύνων για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων.

Στον GDPR ο κίνδυνος δεν αφορά πρωτίστως τη ζημία της επιχείρησης, αλλά τις πιθανές επιπτώσεις στα φυσικά πρόσωπα. Τέτοιες επιπτώσεις μπορεί να είναι η απώλεια ελέγχου των δεδομένων, η κλοπή ταυτότητας, η οικονομική απώλεια, η διάκριση, η βλάβη στη φήμη, η αποκάλυψη εμπιστευτικών πληροφοριών, η παρακολούθηση της συμπεριφοράς ή η αδυναμία άσκησης δικαιωμάτων. Η οργανωτική ή οικονομική ζημία της επιχείρησης μπορεί να συνεκτιμάται στο συνολικό σύστημα διαχείρισης κινδύνων, αλλά δεν αντικαθιστά την αξιολόγηση των κινδύνων για τα υποκείμενα.

Η αποτίμηση συνδέει κάθε δραστηριότητα με τα δεδομένα, τους σκοπούς, τους αποδέκτες, τις προσβάσεις και τον χρόνο διατήρησης. Πάνω σε αυτή τη χαρτογράφηση εξετάζονται σενάρια απώλειας εμπιστευτικότητας, ακεραιότητας ή διαθεσιμότητας και οι συνέπειές τους στα πρόσωπα. Η κοινή τεχνική απογραφή μπορεί συνεπώς να υποστηρίξει την ανάλυση, αλλά χρειάζεται ειδική αξιολόγηση των επιπτώσεων στα υποκείμενα.

Το άρθρο 32 αναφέρει ενδεικτικά ψευδωνυμοποίηση και κρυπτογράφηση, συνεχή εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα και ανθεκτικότητα, έγκαιρη αποκατάσταση πρόσβασης μετά από περιστατικό και τακτική δοκιμή των μέτρων. Η εφαρμογή μπορεί να περιλαμβάνει έλεγχο πρόσβασης, πολυπαραγοντική

αυθεντικοποίηση, καταγραφή ενεργειών, αντίγραφα ασφαλείας και εκπαίδευση. Αυτές οι τεχνικές επιλογές αιτιολογούνται από τον κίνδυνο· δεν επιβάλλονται όλες αδιακρίτως σε κάθε επεξεργασία.

Η επιλογή των μέτρων πρέπει να συνδέεται με συγκεκριμένα σενάρια κινδύνου. Για παράδειγμα, η κρυπτογράφηση μπορεί να μειώσει τον κίνδυνο από την απώλεια φορητής συσκευής, δεν αντιμετωπίζει όμως από μόνη της την κατάχρηση δεδομένων από νόμιμα εξουσιοδοτημένο χρήστη. Αντίστοιχα, τα αντίγραφα ασφαλείας ενισχύουν τη διαθεσιμότητα, αλλά δεν εμποδίζουν κατ' ανάγκη την εξαγωγή δεδομένων. Απαιτείται επομένως συνδυασμός προληπτικών, ανιχνευτικών και διορθωτικών μέτρων.

Η προστασία δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού, σύμφωνα με το άρθρο 25, απαιτεί την ενσωμάτωση των αρχών προστασίας δεδομένων κατά τον καθορισμό των μέσων της επεξεργασίας και κατά την ίδια την επεξεργασία. Εξ ορισμού πρέπει να υποβάλλονται σε επεξεργασία μόνο τα προσωπικά δεδομένα που είναι αναγκαία για κάθε συγκεκριμένο σκοπό, ως προς την ποσότητα, την έκταση επεξεργασίας, την περίοδο διατήρησης και την προσβασιμότητα. Η απαίτηση αφορά τόσο νέα πληροφοριακά συστήματα όσο και σημαντικές αλλαγές σε υφιστάμενες διαδικασίες ([EDPB, 2020](#)).

Όταν πάροχος ενεργεί ως εκτελών την επεξεργασία, το άρθρο 28 απαιτεί επαρκείς εγγυήσεις και δεσμευτική σύμβαση ή άλλη νομική πράξη, σε έγγραφη και ενδεχομένως ηλεκτρονική μορφή. Ρυθμίζονται ιδίως οι τεκμηριωμένες εντολές, η εμπιστευτικότητα, η ασφάλεια, η συνδρομή, οι υπεργολάβοι και η επιστροφή ή διαγραφή δεδομένων. Δεν είναι κάθε εμπορικός συνεργάτης εκτελών: μπορεί να ενεργεί ως αυτοτελής υπεύθυνος ή, εάν συντρέχουν οι όροι του άρθρου 26, ως από κοινού υπεύθυνος. Για διαβίβαση σε τρίτη χώρα ελέγχονται επιπλέον οι προϋποθέσεις του Κεφαλαίου V· η σύμβαση του άρθρου 28 δεν αρκεί μόνη της.

3.3.3 Παραβίαση προσωπικών δεδομένων και υποχρεώσεις γνωστοποίησης

Ο GDPR χρησιμοποιεί τον ειδικό όρο «παραβίαση δεδομένων προσωπικού χαρακτήρα». Σύμφωνα με το άρθρο 4 σημείο 12, πρόκειται για παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, μη εξουσιοδοτημένη γνωστοποίηση ή πρόσβαση σε προσωπικά δεδομένα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν με οποιονδήποτε άλλο τρόπο σε επεξεργασία.

Η παραβίαση μπορεί να αφορά μη εξουσιοδοτημένη αποκάλυψη ή πρόσβαση, αλλοίωση ή απώλεια διαθεσιμότητας. Μια επίθεση ransomware που καθιστά προσωπικά δεδομένα προσωρινά μη προσβάσιμα μπορεί συνεπώς να αποτελεί παραβίαση ακόμη και χωρίς εξαγωγή τους. Η ύπαρξη αντιγράφων και η ταχύτητα αποκατάστασης επηρεάζουν την αξιολόγηση κινδύνου και την ανάγκη γνωστοποίησης· δεν αναιρούν αυτομάτως την παραβίαση. Αντίθετα, η προγραμματισμένη συντήρηση δεν αποτελεί από μόνη της παραβίαση ασφάλειας (EDPB, [Κατευθυντήριες γραμμές 9/2022, έκδοση 2.0, 2023](#), παρ. 18–24).

Δεν αποτελεί κάθε περιστατικό κυβερνοασφάλειας παραβίαση προσωπικών δεδομένων. Εάν ένα περιστατικό επηρεάζει μόνο εταιρικά συστήματα ή δεδομένα που δεν αφορούν φυσικά πρόσωπα, δεν ενεργοποιεί από μόνο του τις διατάξεις των άρθρων 33 και 34. Αντίθετα, ένα ανθρώπινο σφάλμα, όπως η αποστολή αρχείου πελατών σε λανθασμένο παραλήπτη, μπορεί να αποτελεί παραβίαση προσωπικών δεδομένων ακόμη και χωρίς κακόβουλη κυβερνοεπίθεση.

Μετά την αναγνώριση μιας παραβίασης απαιτείται αξιολόγηση του κινδύνου για τα δικαιώματα και τις ελευθερίες των επηρεαζόμενων προσώπων. Εξετάζονται το είδος και η ευαισθησία των δεδομένων, ο αριθμός των προσώπων και των εγγράφων, η ευκολία ταυτοποίησης, οι πιθανές συνέπειες, τα χαρακτηριστικά των υποκειμένων, η διάρκεια της έκθεσης και τα μέτρα προστασίας που ήταν ενεργά. Η

κρυπτογράφηση, για παράδειγμα, μπορεί να μειώσει ουσιαστικά τον κίνδυνο, εφόσον το κλειδί δεν έχει παραβιαστεί και ο αλγόριθμος παραμένει κατάλληλος.

Κατά το άρθρο 33, ο υπεύθυνος επεξεργασίας γνωστοποιεί την παραβίαση στην αρμόδια εποπτική αρχή χωρίς αδικαιολόγητη καθυστέρηση και, εφόσον είναι εφικτό, εντός 72 ωρών από τη γνώση της, εκτός εάν είναι απίθανο να προκύψει κίνδυνος για τα πρόσωπα. Η καθυστέρηση αιτιολογείται. Ως γνώση νοείται η εύλογη βεβαιότητα ότι συνέβη περιστατικό ασφάλειας που έθεσε σε κίνδυνο προσωπικά δεδομένα, χωρίς να απαιτείται ολοκλήρωση όλης της διερεύνησης (EDPB, [Κατευθυντήριες γραμμές 9/2022, έκδοση 2.0, 2023](#), παρ. 31–34).

Η γνωστοποίηση πρέπει να περιγράφει τη φύση της παραβίασης και, όπου είναι δυνατόν, τις κατηγορίες και τον κατά προσέγγιση αριθμό των επηρεαζόμενων προσώπων και εγγραφών. Πρέπει επίσης να περιλαμβάνει στοιχεία επικοινωνίας, περιγραφή των πιθανών συνεπειών και τα μέτρα που έχουν ληφθεί ή προτείνονται για την αντιμετώπιση και τον περιορισμό των επιπτώσεων. Όταν οι πληροφορίες δεν είναι όλες διαθέσιμες μέσα στην αρχική προθεσμία, μπορούν να παρέχονται σταδιακά χωρίς περαιτέρω αδικαιολόγητη καθυστέρηση ([Κανονισμός \(ΕΕ\) 2016/679, άρθρο 33](#)).

Όταν είναι πιθανός υψηλός κίνδυνος, ο υπεύθυνος επεξεργασίας ανακοινώνει την παραβίαση στα υποκείμενα χωρίς αδικαιολόγητη καθυστέρηση και με σαφή γλώσσα (άρθρο 34). Δεν προβλέπεται ενιαία προθεσμία 72 ωρών για αυτή την ανακοίνωση. Οι εξαιρέσεις αφορούν αποτελεσματική προστασία που καθιστά τα δεδομένα ακατανόητα σε μη εξουσιοδοτημένους, μεταγενέστερα μέτρα που αποτρέπουν την επέλευση υψηλού κινδύνου ή δυσανάλογη προσπάθεια ατομικής επικοινωνίας, οπότε απαιτείται εξίσου αποτελεσματική δημόσια ανακοίνωση ή παρόμοιο μέτρο.

Ο εκτελών ενημερώνει τον υπεύθυνο επεξεργασίας χωρίς αδικαιολόγητη καθυστέρηση μόλις λάβει γνώση παραβίασης (άρθρο 33 παράγραφος 2). Δεν διαθέτει αυτοτελή προθεσμία 72 ωρών για να αναμείνει πριν ενημερώσει, ούτε αποφασίζει αντί του υπευθύνου εάν θα γίνει γνωστοποίηση στην αρχή. Οργανισμός που έχει διαφορετικούς ρόλους σε διαφορετικές επεξεργασίες εξετάζει χωριστά τις αντίστοιχες υποχρεώσεις.

Όλες οι παραβιάσεις πρέπει να τεκμηριώνονται, ακόμη και όταν κρίνεται ότι δεν απαιτείται γνωστοποίηση. Το αρχείο πρέπει να περιλαμβάνει τα πραγματικά περιστατικά, τις συνέπειες, την αξιολόγηση κινδύνου, την απόφαση γνωστοποίησης ή μη και τις διορθωτικές ενέργειες. Οι κατευθυντήριες γραμμές του EDPB παρέχουν πρακτικά παραδείγματα για ransomware, εξαγωγή δεδομένων, απώλεια συσκευών, αποστολή δεδομένων σε λανθασμένο παραλήπτη και επιθέσεις κοινωνικής μηχανικής (EDPB, 2022).

3.3.4 Λογοδοσία, τεκμηρίωση και εκτίμηση αντικτύπου

Το άρθρο 30 προβλέπει διαφορετικό περιεχόμενο αρχείου δραστηριοτήτων για υπεύθυνο και εκτελούντα την επεξεργασία. Στο αρχείο του υπευθύνου περιλαμβάνονται σκοποί, κατηγορίες προσώπων και δεδομένων, αποδέκτες, διαβιβάσεις και, όπου είναι δυνατόν, χρόνοι διαγραφής και γενική περιγραφή μέτρων ασφάλειας. Η εξαίρεση για οργανισμούς με λιγότερους από 250 εργαζομένους είναι περιορισμένη: δεν καλύπτει, μεταξύ άλλων, μη περιστασιακή επεξεργασία ή επεξεργασία που ενδέχεται να δημιουργήσει κίνδυνο. Η συστηματική διαχείριση στοιχείων πελατών και εργαζομένων δεν εξαιρείται απλώς λόγω μικρού μεγέθους.

Η τεκμηρίωση συμπληρώνεται από ενημερώσεις προς τα υποκείμενα, διαδικασίες άσκησης δικαιωμάτων, κανόνες διατήρησης, συμβάσεις και μητρώο παραβιάσεων. Όπου συντρέχουν οι προϋποθέσεις του άρθρου 37, ορίζεται Υπεύθυνος Προστασίας Δεδομένων (DPO), ο οποίος συμβουλεύει και παρακολουθεί τη

συμμόρφωση με την ανεξαρτησία των άρθρων 38–39. Η ύπαρξή του δεν μεταφέρει σε αυτόν τις ευθύνες του υπευθύνου ή του εκτελούντος.

Η Εκτίμηση Αντικτύπου σχετικά με την Προστασία Δεδομένων, γνωστή ως DPIA, αποτελεί ειδικό εργαλείο λογοδοσίας. Σύμφωνα με το άρθρο 35, απαιτείται πριν από μία επεξεργασία η οποία, λόγω της φύσης, της έκτασης, του πλαισίου ή των σκοπών της και ιδίως όταν χρησιμοποιεί νέες τεχνολογίες, είναι πιθανό να δημιουργήσει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων.

Οι ρητές περιπτώσεις του άρθρου 35 παράγραφος 3 περιλαμβάνουν συστηματική και εκτενή αυτοματοποιημένη αξιολόγηση στην οποία βασίζονται αποφάσεις με έννομα ή παρόμοια σημαντικά αποτελέσματα, επεξεργασία ειδικών κατηγοριών ή ποινικών δεδομένων σε μεγάλη κλίμακα και συστηματική παρακολούθηση δημόσια προσβάσιμου χώρου σε μεγάλη κλίμακα. Στα logistics, εκτεταμένη παρακολούθηση οδών, βιομετρικός έλεγχος ή αυτοματοποιημένη αξιολόγηση εργαζομένων χρειάζονται έλεγχο με βάση τα πραγματικά χαρακτηριστικά τους και τον κατάλογο της αρμόδιας εποπτικής αρχής (ΑΠΔΠΧ, Απόφαση 65/2018).

Η DPIA περιλαμβάνει περιγραφή πράξεων και σκοπών, έλεγχο αναγκαιότητας και αναλογικότητας, αξιολόγηση κινδύνων και μέτρα αντιμετώπισης. Όταν η εκτίμηση δείχνει υψηλό υπολειπόμενο κίνδυνο που ο υπεύθυνος δεν μπορεί να μετριάσει επαρκώς, απαιτείται διαβούλευση με την εποπτική αρχή πριν αρχίσει η επεξεργασία (άρθρο 36).

Η αξιολόγηση ασφάλειας του άρθρου 32 και η DPIA έχουν διαφορετική λειτουργία. Η πρώτη στηρίζει την επιλογή μέτρων για κάθε επεξεργασία, ενώ η δεύτερη εξετάζει ευρύτερα την αναγκαιότητα, την αναλογικότητα και τις επιπτώσεις επεξεργασιών πιθανού υψηλού κινδύνου. Η απουσία υποχρέωσης DPIA δεν αίρει την υποχρέωση ασφάλειας. Στην Ελλάδα, το πλαίσιο συμπληρώνεται από τον [Ν. 4624/2019](#) και η εποπτεία ασκείται από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, με την επιφύλαξη των ενωσιακών κανόνων αρμοδιότητας για διασυνοριακή επεξεργασία.

3.4 Κανονισμός DORA

3.4.1 Σκοπός, πεδίο εφαρμογής και σχέση με τη NIS2

Ο Κανονισμός (ΕΕ) 2022/2554 για την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα, γνωστός ως DORA, θεσπίζει ενιαίες απαιτήσεις για τη διαχείριση κινδύνων τεχνολογιών πληροφοριών και επικοινωνιών. Εφαρμόζεται από τις 17 Ιανουαρίου 2025 και είναι άμεσα δεσμευτικός σε όλα τα κράτη μέλη (Κανονισμός (ΕΕ) 2022/2554).

Το άρθρο 2 καλύπτει, μεταξύ άλλων, πιστωτικά ιδρύματα, ιδρύματα πληρωμών και ηλεκτρονικού χρήματος, επιχειρήσεις επενδύσεων, παρόχους υπηρεσιών κρυπτοστοιχείων, υποδομές χρηματοπιστωτικών αγορών, ασφαλιστικές επιχειρήσεις και διαχειριστές κεφαλαίων. Η υπαγωγή ελέγχεται με τις εξαιρέσεις του ίδιου άρθρου. Η αναλογικότητα και το απλουστευμένο πλαίσιο του άρθρου 16 διαφοροποιούν επιμέρους απαιτήσεις και δεν πρέπει να συγχέονται με πλήρη εξαίρεση από τον Κανονισμό.

Οι τρίτοι πάροχοι υπηρεσιών ΤΠΕ περιλαμβάνονται επίσης στο ρυθμιστικό σύστημα, χωρίς να υπέχουν όλοι τις ίδιες υποχρεώσεις με χρηματοοικονομική οντότητα. Οι απαιτήσεις διαχείρισης κινδύνων, αναφοράς και δοκιμών βαρύνουν τις χρηματοοικονομικές οντότητες κατά τις εφαρμοστέες διατάξεις, ενώ οι σχέσεις τους με παρόχους ρυθμίζονται στα άρθρα 28–30. Άμεσο ενωσιακό πλαίσιο εποπτείας προβλέπεται ειδικά για παρόχους που χαρακτηρίζονται κρίσιμοι κατά το άρθρο 31.

Μια επιχείρηση μεταφορών ή αποθήκευσης δεν γίνεται πάροχος ΤΠΕ μόνο επειδή συνεργάζεται με τράπεζα ή χρησιμοποιεί λογισμικό. Ελέγχεται το αντικείμενο της υπηρεσίας που παρέχει στον πελάτη της, με βάση τον ορισμό των υπηρεσιών ΤΠΕ του άρθρου 3 σημείο 21. Εάν προσφέρει, για παράδειγμα, συνεχή υπηρεσία δεδομένων μέσω ψηφιακής πλατφόρμας, εξετάζεται χωριστά αυτή η υπηρεσία. Συμβατικές απαιτήσεις ασφάλειας μπορεί να υφίστανται και σε άλλες εμπορικές σχέσεις, χωρίς να αποδεικνύουν από μόνες τους υπαγωγή στον DORA.

Για χρηματοοικονομικές οντότητες που προσδιορίζονται ως βασικές ή σημαντικές κατά τη NIS2, ο DORA αποτελεί ειδική τομεακή ενωσιακή πράξη για τους σκοπούς του άρθρου 4 της NIS2 (DORA, άρθρο 1 παράγραφος 2). Οι αντίστοιχες απαιτήσεις και η συναφής εποπτεία εφαρμόζονται βάσει του ειδικού πλαισίου, ώστε να αποφεύγεται η διπλή ρύθμιση των ίδιων υποχρεώσεων. Αυτό δεν συνιστά γενική κατάργηση της NIS2 για κάθε τεχνολογικό πάροχο χρηματοοικονομικών πελατών ούτε επηρεάζει τον GDPR.

3.4.2 Ψηφιακή επιχειρησιακή ανθεκτικότητα και πλαίσιο διαχείρισης κινδύνων ΤΠΕ

Η ψηφιακή επιχειρησιακή ανθεκτικότητα αφορά την ικανότητα της χρηματοοικονομικής οντότητας να διατηρεί την επιχειρησιακή ακεραιότητα και αξιοπιστία της μέσω κατάλληλων δυνατοτήτων ΤΠΕ, ακόμη και σε διαταραχές (άρθρο 3). Περιλαμβάνει προστασία, ανίχνευση, απόκριση και ανάκαμψη και δεν περιορίζεται στην αποτροπή επιθέσεων.

Το άρθρο 5 αποδίδει στο διοικητικό όργανο την τελική ευθύνη για τη διαχείριση των κινδύνων ΤΠΕ. Η διοίκηση πρέπει να καθορίζει και να εγκρίνει το πλαίσιο διαχείρισης, το επίπεδο ανοχής κινδύνου, τη στρατηγική ψηφιακής επιχειρησιακής ανθεκτικότητας, την πολιτική επιχειρησιακής συνέχειας, τα σχέδια απόκρισης και αποκατάστασης και την πολιτική χρήσης υπηρεσιών τρίτων παρόχων. Πρέπει επίσης να εξασφαλίζει επαρκή προϋπολογισμό, κατάλληλες δεξιότητες και τακτική εκπαίδευση των μελών της.

Το άρθρο 6 προβλέπει τεκμηριωμένο πλαίσιο διαχείρισης κινδύνων ΤΠΕ, ενταγμένο στο συνολικό σύστημα κινδύνων. Επανεξετάζεται τουλάχιστον ετησίως, ή περιοδικά για τις πολύ μικρές επιχειρήσεις, και μετά από μείζονα περιστατικά, εποπτικές οδηγίες ή σχετικά συμπεράσματα ελέγχων και δοκιμών. Οι οντότητες που απαριθμούνται στο άρθρο 16 ακολουθούν το ειδικό απλουστευμένο πλαίσιο αντί των άρθρων 5–15.

Στο γενικό πλαίσιο του άρθρου 8, αναγνωρίζονται και ταξινομούνται οι λειτουργίες, τα πληροφοριακά και τεχνολογικά περιουσιακά στοιχεία και οι εξαρτήσεις από τρίτους. Η επάρκεια της ταξινόμησης επανεξετάζεται τουλάχιστον ετησίως. Οι πηγές κινδύνου και οι ευπάθειες παρακολουθούνται διαρκώς, ενώ για οντότητες εκτός πολύ μικρών επιχειρήσεων προβλέπονται ειδικές αξιολογήσεις μετά από σημαντικές αλλαγές και για παλαιά συστήματα.

Τα άρθρα 9–14 καλύπτουν πρόληψη και προστασία, ανίχνευση, επιχειρησιακή συνέχεια, απόκριση και αποκατάσταση, αντίγραφα ασφαλείας, μάθηση και επικοινωνία. Ο Κατ' εξουσιοδότηση Κανονισμός (ΕΕ) 2024/1774 (Ευρωπαϊκή Επιτροπή, 2024d) εξειδικεύει τις πολιτικές, μεθόδους και διαδικασίες τόσο του γενικού όσο και του απλουστευμένου πλαισίου. Η αξία της εξειδίκευσης είναι ότι συνδέει τη διοικητική ευθύνη με συγκεκριμένες λειτουργικές διαδικασίες.

Η αναλογικότητα του άρθρου 4 συνδέει την εφαρμογή με το μέγεθος, το προφίλ κινδύνου και τη φύση, κλίμακα και πολυπλοκότητα των υπηρεσιών. Δεν επιτρέπει αυθαίρετη παράλειψη ρητών υποχρεώσεων. Οι ειδικές εξαιρέσεις για πολύ μικρές επιχειρήσεις και οι διατάξεις του άρθρου 16 εξετάζονται αυτοτελώς, αντί να θεωρείται ότι όλες οι μικρές οντότητες έχουν το ίδιο καθεστώς.

3.4.3 Κίνδυνοι τρίτων παρόχων ΤΠΕ και συμβατικές απαιτήσεις

Κατά το άρθρο 28, η χρηματοοικονομική οντότητα παραμένει πλήρως υπεύθυνη για τη συμμόρφωσή της όταν χρησιμοποιεί υπηρεσίες τρίτων παρόχων ΤΠΕ. Η απαίτηση αυτή καλύπτει γενικά τις συμβατικές ρυθμίσεις χρήσης ΤΠΕ, με ενισχυμένους κανόνες όταν υποστηρίζονται κρίσιμες ή σημαντικές λειτουργίες.

Με εξαίρεση τις πολύ μικρές επιχειρήσεις και τις οντότητες του άρθρου 16 παράγραφος 1, απαιτούνται στρατηγική κινδύνων τρίτων και πολιτική για υπηρεσίες που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες. Το μητρώο πληροφοριών του άρθρου 28 παράγραφος 3 καλύπτει όλες τις συμβατικές ρυθμίσεις χρήσης υπηρεσιών ΤΠΕ και διακρίνει όσες υποστηρίζουν τέτοιες λειτουργίες. Τα τυποποιημένα υποδείγματα καθορίζονται στον Εκτελεστικό Κανονισμό (ΕΕ) 2024/2956 (Ευρωπαϊκή Επιτροπή, 2024ε).

Πριν από τη σύναψη σύμβασης, η οντότητα πρέπει να εξετάζει εάν η υπηρεσία υποστηρίζει κρίσιμη ή σημαντική λειτουργία, να αξιολογεί όλους τους σχετικούς κινδύνους, να πραγματοποιεί δέουσα επιμέλεια και να εξετάζει πιθανές συγκρούσεις συμφερόντων. Η αξιολόγηση πρέπει να καλύπτει την καταλληλότητα και την ασφάλεια του παρόχου, την οικονομική και λειτουργική του σταθερότητα, τη χρήση υπεργολάβων, τη γεωγραφική θέση, την προστασία δεδομένων, τη δυνατότητα ελέγχου και τη δυνατότητα ασφαλούς διακοπής της συνεργασίας.

Το άρθρο 29 απαιτεί εκτίμηση του κινδύνου συγκέντρωσης, ιδίως όταν ο πάροχος δεν αντικαθίσταται εύκολα ή συγκεντρώνει πολλαπλές κρίσιμες ή σημαντικές υπηρεσίες. Η εξέταση εναλλακτικών λαμβάνει υπόψη και τους κινδύνους της ίδιας της μετάβασης, όχι μόνο το κόστος της.

Το άρθρο 30 απαιτεί σαφή έγγραφη κατανομή δικαιωμάτων και υποχρεώσεων. Οι συμβάσεις πρέπει να περιλαμβάνουν πλήρη περιγραφή των υπηρεσιών και των επιτρεπόμενων υπεργολαβιών, τις τοποθεσίες παροχής των υπηρεσιών και επεξεργασίας δεδομένων, όρους για τη διαθεσιμότητα, αυθεντικότητα, ακεραιότητα και εμπιστευτικότητα, κανόνες πρόσβασης, ανάκτησης και επιστροφής δεδομένων, επίπεδα υπηρεσιών, υποστήριξη κατά τη διάρκεια περιστατικών, συνεργασία με τις αρμόδιες αρχές και δικαιώματα καταγγελίας ([Κανονισμός \(ΕΕ\) 2022/2554, άρθρα 28–30](#)).

Για υπηρεσίες που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες απαιτούνται επιπρόσθετα ακριβείς ποσοτικοί και ποιοτικοί στόχοι υπηρεσίας, υποχρεώσεις γνωστοποίησης εξελίξεων με ουσιώδη επίδραση, σχέδια επιχειρησιακής συνέχειας του παρόχου, συμμετοχή σε TLPT όταν απαιτείται, απεριόριστα δικαιώματα πρόσβασης, επιθεώρησης και ελέγχου και επαρκείς στρατηγικές εξόδου. Η στρατηγική εξόδου πρέπει να προβλέπει μεταβατική περίοδο που επιτρέπει τη συνέχιση της υπηρεσίας και την ασφαλή μεταφορά σε άλλον πάροχο ή σε εσωτερική λύση.

Ο Κατ' εξουσιοδότηση Κανονισμός (ΕΕ) 2024/1773 (Ευρωπαϊκή Επιτροπή, 2024ε) εξειδικεύει την πολιτική συμβατικών ρυθμίσεων για ΤΠΕ που υποστηρίζει κρίσιμες ή σημαντικές λειτουργίες. Ο Κατ' εξουσιοδότηση Κανονισμός (ΕΕ) 2025/532 (Ευρωπαϊκή Επιτροπή, 2025ε) συμπληρώνει τις απαιτήσεις αξιολόγησης και συμβατικής ρύθμισης της υπεργολαβίας τέτοιων υπηρεσιών. Έτσι, ο έλεγχος εκτείνεται και στην αλυσίδα υπεργολάβων που μπορεί να επηρεάσει την παρεχόμενη υπηρεσία.

3.4.4 Διαχείριση, ταξινόμηση και αναφορά περιστατικών ΤΠΕ

Κατά το άρθρο 3, περιστατικό σχετιζόμενο με ΤΠΕ είναι μη προγραμματισμένο γεγονός ή σειρά συνδεδεμένων γεγονότων που θέτει σε κίνδυνο την ασφάλεια συστημάτων και επηρεάζει αρνητικά δεδομένα ή υπηρεσίες. Μείζον είναι το περιστατικό με υψηλό αρνητικό αντίκτυπο στα συστήματα που υποστηρίζουν

κρίσιμες ή σημαντικές λειτουργίες. Ο νομικός χαρακτηρισμός στηρίζεται και στα ειδικά κριτήρια και όρια των κανονιστικών τεχνικών προτύπων.

Το άρθρο 17 απαιτεί διαδικασία ανίχνευσης, διαχείρισης και γνωστοποίησης, καταγραφή περιστατικών ΤΠΕ και σημαντικών κυβερνοαπειλών, τεκμηρίωση αιτίων, δείκτες έγκαιρης προειδοποίησης και ταξινόμηση. Η διαδικασία κατανέμει ρόλους, προβλέπει εσωτερική κλιμάκωση και ενημέρωση της διοίκησης τουλάχιστον για τα μείζονα περιστατικά και τις ενέργειες απόκρισης.

Η ταξινόμηση του άρθρου 18 εξετάζει πελάτες, αντισυμβαλλομένους και συναλλαγές, φήμη, διάρκεια και χρόνο διακοπής, γεωγραφική έκταση, απώλειες δεδομένων, κρισιμότητα και οικονομικό αντίκτυπο. Ο Κατ' εξουσιοδότηση Κανονισμός (ΕΕ) 2024/1772 (Ευρωπαϊκή Επιτροπή, 2024b) εξειδικεύει τα όρια. Κατά το άρθρο 8 του, απαιτείται επηρεασμός κρίσιμων υπηρεσιών και είτε το ειδικό κατώφλι του άρθρου 9 παράγραφος 5 στοιχείο β' είτε συνδυασμός τουλάχιστον δύο από τα λοιπά όρια. Προβλέπεται και συγκεντρωτική αξιολόγηση επαναλαμβανόμενων περιστατικών με την ίδια εμφανή βασική αιτία. Συνεπώς, ένα μεμονωμένο ποσοτικό στοιχείο δεν αρκεί πάντοτε για την ταξινόμηση.

Τα μείζονα περιστατικά ΤΠΕ γνωστοποιούνται στην αρμόδια χρηματοοικονομική εποπτική αρχή κατά το άρθρο 19. Το άρθρο 5 του Κατ' εξουσιοδότηση Κανονισμού (ΕΕ) 2025/301 (Ευρωπαϊκή Επιτροπή, 2025a) διακρίνει τη γνώση του περιστατικού από την ταξινόμησή του ως μείζονος και ορίζει:

1. Η αρχική γνωστοποίηση υποβάλλεται το συντομότερο δυνατόν και πάντως εντός τεσσάρων ωρών από την ταξινόμηση του περιστατικού ως μείζονος και όχι αργότερα από 24 ώρες από τη στιγμή κατά την οποία η οντότητα έλαβε γνώση του περιστατικού. Εάν η ταξινόμηση ως μείζονος γίνει μετά το πρώτο 24ωρο από τη γνώση του περιστατικού, η αρχική γνωστοποίηση υποβάλλεται εντός τεσσάρων ωρών από την ταξινόμηση.
2. Ενδιάμεση έκθεση εντός 72 ωρών από την αρχική γνωστοποίηση, ακόμη και εάν δεν έχει αλλάξει η κατάσταση ή ο χειρισμός. Επικαιροποιημένη ενδιάμεση έκθεση υποβάλλεται χωρίς αδικαιολόγητη καθυστέρηση και, σε κάθε περίπτωση, όταν αποκατασταθούν οι συνθήκες δραστηριότητες.
3. Η τελική έκθεση υποβάλλεται το αργότερο μέσα σε έναν μήνα από την ενδιάμεση ή την τελευταία επικαιροποιημένη ενδιάμεση έκθεση (Κατ' εξουσιοδότηση Κανονισμός (ΕΕ) 2025/301, άρθρο 5).

Εάν δεν είναι δυνατή η τήρηση προθεσμίας, η οντότητα ενημερώνει την αρχή έως τη λήξη της και εξηγεί την καθυστέρηση. Οι παράγραφοι 4–6 προβλέπουν περιορισμένη δυνατότητα υποβολής έως το μεσημέρι της επόμενης εργάσιμης όταν η προθεσμία λήγει σε Σαββατοκύριακο ή αργία. Η δυνατότητα δεν ισχύει για αρχική ή ενδιάμεση αναφορά πιστωτικών ιδρυμάτων, κεντρικών αντισυμβαλλομένων, διαχειριστών τόπων διαπραγμάτευσης και λοιπών χρηματοοικονομικών οντοτήτων που έχουν προσδιοριστεί ως βασικές ή σημαντικές κατά NIS2· μπορεί επίσης να αποκλειστεί από την αρμόδια αρχή για άλλες σημαντικές ή συστημικές οντότητες.

Η τελική έκθεση τεκμηριώνει την αιτία, την επίλυση και τις επιπτώσεις, με τα υποδείγματα του Εκτελεστικού Κανονισμού (ΕΕ) 2025/302 (Ευρωπαϊκή Επιτροπή, 2025b). Αν θίγονται οικονομικά συμφέροντα πελατών από μείζον περιστατικό, ενημερώνονται χωρίς αδικαιολόγητη καθυστέρηση. Η υποβολή αναφορών μπορεί να ανατεθεί σε τρίτο, αλλά η χρηματοοικονομική οντότητα παραμένει υπεύθυνη (DORA, άρθρο 19).

3.4.5 Δοκιμές ψηφιακής επιχειρησιακής ανθεκτικότητας και TLPT

Το άρθρο 24 απαιτεί από τις χρηματοοικονομικές οντότητες, εκτός πολύ μικρών επιχειρήσεων, ολοκληρωμένο πρόγραμμα δοκιμών βάσει κινδύνου. Η παράγραφος 6 προβλέπει για αυτές κατάλληλες δοκιμές τουλάχιστον ετησίως στα συστήματα και στις εφαρμογές που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες. Για τις πολύ μικρές επιχειρήσεις, το άρθρο 25 παράγραφος 3 προβλέπει δοκιμές με ειδική στάθμιση πόρων, χρόνου και κινδύνου· η εξαίρεσή τους από το ολοκληρωμένο πρόγραμμα δεν ισοδυναμεί με πλήρη απαλλαγή από δοκιμές.

Το άρθρο 25 περιλαμβάνει ενδεικτικά σαρώσεις ευπαθειών, αξιολογήσεις ασφάλειας δικτύων, αναλύσεις αποκλίσεων, ελέγχους φυσικής ασφάλειας και πηγαίου κώδικα, δοκιμές βάσει σεναρίων, συμβατότητας, απόδοσης και διείσδυσης. Η επιλογή και το βάθος τους προσαρμόζονται στην κρισιμότητα και στον κίνδυνο.

Οι προηγμένες δοκιμές διείσδυσης βάσει απειλών (Threat-Led Penetration Testing, TLPT) επιβάλλονται στις οντότητες που προσδιορίζονται από τις αρμόδιες αρχές, με τις εξαιρέσεις του άρθρου 26 παράγραφος 1. Δεν αποτελούν γενική υποχρέωση κάθε οντότητας DORA. Διενεργούνται τουλάχιστον ανά τρία έτη, με δυνατότητα προσαρμογής της συχνότητας από την αρχή βάσει κινδύνου και επιχειρησιακών συνθηκών.

Το TLPT μιμείται τις τακτικές, τεχνικές και διαδικασίες πραγματικών παραγόντων απειλής και πραγματοποιείται σε ζωντανά συστήματα παραγωγής που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες. Το πεδίο δοκιμής καθορίζεται βάσει αξιολόγησης της οντότητας και εγκρίνεται από την αρμόδια αρχή. Όταν κρίσιμες λειτουργίες υποστηρίζονται από τρίτους παρόχους ΤΠΕ, οι πάροχοι μπορεί να πρέπει να συμμετάσχουν στη δοκιμή, χωρίς να μεταφέρεται σε αυτούς η ευθύνη της χρηματοοικονομικής οντότητας (Κανονισμός (ΕΕ) 2022/2554, άρθρο 26).

Οι γενικές δοκιμές απαιτούν ανεξαρτησία και διαχείριση συγκρούσεων συμφερόντων. Για TLPT ισχύουν οι ειδικοί όροι των άρθρων 26–27: όταν χρησιμοποιούνται εσωτερικοί δοκιμαστές, ανατίθεται δοκιμή σε εξωτερικούς τουλάχιστον κάθε τρεις δοκιμές, ενώ τα σημαντικά πιστωτικά ιδρύματα του άρθρου 6 παράγραφος 4 του Κανονισμού (ΕΕ) 1024/2013 (Συμβούλιο της Ευρωπαϊκής Ένωσης, 2013) χρησιμοποιούν μόνο εξωτερικούς. Ο Κατ' εξουσιοδότηση Κανονισμός (ΕΕ) 2025/1190 (Ευρωπαϊκή Επιτροπή, 2025d) εξειδικεύει την επιλογή οντοτήτων, τις φάσεις, τους δοκιμαστές και τη συνεργασία με τις αρχές.

Τα ευρήματα ιεραρχούνται, ανατίθενται για αποκατάσταση και επανελέγχονται. Η σύνδεση των αποτελεσμάτων με το πλαίσιο κινδύνων και τα σχέδια συνέχειας μετατρέπει τη δοκιμή σε στοιχείο επαλήθευσης της πραγματικής ανθεκτικότητας.

3.5 Συμπεράσματα κεφαλαίου

Ως προς το RQ2, η εφαρμογή των κανόνων αρχίζει από τον έλεγχο υπαγωγής και την κατανομή ευθύνης. Για μια επιχείρηση logistics εξετάζονται χωριστά ο τύπος υπηρεσίας και το μέγεθος κατά NIS2, ο ρόλος ανά επεξεργασία κατά GDPR και το αντικείμενο τυχόν υπηρεσίας ΤΠΕ προς χρηματοοικονομικό πελάτη κατά DORA. Οι σχέσεις προμηθευτών μπορεί να δημιουργούν συμβατικές ή λειτουργικές υποχρεώσεις χωρίς να αποδεικνύουν από μόνες τους άμεση εποπτική υπαγωγή.

Κοινή επιχειρησιακή οργάνωση μπορεί να υποστηρίξει την απογραφή υπηρεσιών, συστημάτων, δεδομένων, τρίτων και περιστατικών. Δεν συγχωνεύει όμως τα διαφορετικά κατώφλια κινδύνου, τους υπόχρεους, τους αποδέκτες των αναφορών ή τις αφετηρίες των προθεσμιών. Το κοινό τεκμήριο επαναχρησιμοποιείται μόνο όταν η καταλληλότητά του αιτιολογείται χωριστά για κάθε πλαίσιο.

Το Κεφάλαιο 4 αξιοποιεί αυτή τη νομική βάση για τη συγκριτική χαρτογράφηση των απαιτήσεων. Η χαρτογράφηση προσδιορίζει ποια πραγματικά στοιχεία, διαδικασίες και αποδεικτικά μέσα μπορούν να είναι κοινά και ποιες αποφάσεις χρειάζονται αυτοτελή κανονιστική αξιολόγηση πριν από τον σχεδιασμό του πλαισίου στο Κεφάλαιο 5.

ΚΕΦΑΛΑΙΟ 4 Συγκριτική Ανάλυση και Ενοποιημένη Χαρτογράφηση των NIS2, GDPR και DORA

Το Κεφάλαιο 3 προσδιόρισε τις υποχρεώσεις των NIS2, GDPR και DORA. Το παρόν κεφάλαιο εξετάζει ποιες διαδικασίες και ποια αποδεικτικά στοιχεία μπορούν να χρησιμοποιηθούν από κοινού και ποιες αποφάσεις απαιτούν χωριστή νομική αξιολόγηση. Η συγκριτική σύνθεση στηρίζεται στη διάκριση ανάμεσα στο πεδίο εφαρμογής, στο προστατευόμενο συμφέρον και στην ευθύνη κάθε εμπλεκόμενης οντότητας.

Μια επίθεση ransomware μπορεί να διακόψει υπηρεσίες, να καταστήσει προσωπικά δεδομένα μη διαθέσιμα ή να επηρεάσει χρηματοοικονομικές λειτουργίες. Οι συνέπειες αυτές δεν ενεργοποιούν αυτομάτως και τα τρία καθεστώτα αναφοράς. Το κεφάλαιο δείχνει πώς μια κοινή καταγραφή γεγονότων μπορεί να υποστηρίξει διαφορετικές αποφάσεις για τον υπόχρεο, το κατώφλι αναφοράς, τον αποδέκτη και την προθεσμία.

Η χαρτογράφηση οργανώνεται σε κοινή καταγραφή επιχειρησιακών στοιχείων και σε χωριστές κανονιστικές αποφάσεις. Η §4.4.4 εξηγεί τις προϋποθέσεις επαναχρησιμοποίησης της πληροφορίας και των τεκμηρίων.

Η σύγκριση ακολουθεί τη σειρά NIS2–GDPR–DORA και διατηρεί ως χρονικό όριο την 31η Αυγούστου 2026. Καταλήγει σε πρότυπο χαρτογράφησης απαιτήσεων, το οποίο αξιοποιείται στον σχεδιασμό του Κεφαλαίου 5 και εφαρμόζεται στο υποθετικό σενάριο του Κεφαλαίου 6.

4.1 Μεθοδολογική προσέγγιση και όρια της σύγκρισης

4.1.1 Αντικείμενο και πηγές της ανάλυσης

Η ανάλυση ακολουθεί δογματική και συγκριτική προσέγγιση. Βασικές πηγές είναι η Οδηγία (ΕΕ) 2022/2555, ο Κανονισμός (ΕΕ) 2016/679 και ο Κανονισμός (ΕΕ) 2022/2554, μαζί με τις εφαρμοστικές πράξεις που παραπέμπονται ανά θέμα. Για τη NIS2 στην Ελλάδα συνεκτιμώνται ο Ν. 5160/2024 και η ΚΥΑ 1689/2025. Οι κατευθυντήριες γραμμές του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων (EDPB) υποστηρίζουν την ερμηνεία του GDPR. Το NIST CSF 2.0 και οι καλές πρακτικές του ENISA χρησιμοποιούνται ως τεχνικά σημεία αναφοράς και δεν εξομοιώνονται με δεσμευτικές νομικές απαιτήσεις.

Μονάδα ανάλυσης είναι η συγκεκριμένη υποχρέωση σε σχέση με μια λειτουργία του οργανισμού. Για κάθε αντιστοίχιση ελέγχονται ο υπόχρεος και το πεδίο εφαρμογής, το γεγονός ενεργοποίησης, η απαιτούμενη ενέργεια και το στοιχείο τεκμηρίωσής της. Στις αναφορές περιστατικών προστίθενται ο αποδέκτης και η αφετηρία της προθεσμίας. Η διαδικασία επιτρέπει να διακρίνονται η κοινή επιχειρησιακή λειτουργία και οι διαφορετικοί νομικοί όροι της.

Η σύγκριση οργανώνεται σε εννέα διαστάσεις: πεδίο εφαρμογής, προστατευόμενο συμφέρον, υπεύθυνη οντότητα, διαχείριση κινδύνου, χειρισμός περιστατικού, κίνδυνος τρίτων, συνέχεια και ανάκαμψη, αναφορά και αποδεικτικά στοιχεία. Για κάθε διάσταση εξετάζονται η νομική βάση, το γεγονός ενεργοποίησης, ο υπεύθυνος, η απαιτούμενη ενέργεια και το τεκμήριο που μπορεί να υποστηρίξει την αξιολόγηση.

4.1.2 Χαρακτήρας των πινάκων και ερευνητικοί περιορισμοί

Οι πίνακες αποτελούν συγκριτική σύνθεση του συγγραφέα. Κάθε αντιστοίχιση στηρίζεται στις διατάξεις που αναγράφονται στον πίνακα ή στην πηγή του. Τα προτεινόμενα αποδεικτικά στοιχεία είναι παραδείγματα εφαρμογής και όχι υποχρεωτικά υποδείγματα των νομοθετών. Η σύνθεση δεν βασίζεται σε εμπειρικά δεδομένα οργανισμού ούτε έχει επικυρωθεί με ανεξάρτητη κωδικοποίηση ή δοκιμή πεδίου.

Επιλέγονται περιοχές που συνδέονται με τις εξαρτήσεις της εφοδιαστικής αλυσίδας του Κεφαλαίου 2: διακυβέρνηση, κίνδυνος, περιστατικά, συνέχεια, τρίτοι και αποτελεσματικότητα μέτρων. Δεν καλύπτεται το σύνολο των υποχρεώσεων κάθε πράξης· ενδεικτικά, οι νόμιμες βάσεις επεξεργασίας και τα δικαιώματα των υποκειμένων κατά GDPR υπερβαίνουν αυτή τη χαρτογράφηση ασφάλειας. Επομένως, η κάλυψη των πινάκων δεν ισοδυναμεί με πλήρη συμμόρφωση.

Στον Πίνακα 4.3 το ● δηλώνει ρητή πρόβλεψη για τη συγκεκριμένη περιοχή και το ○ σύνδεση που προκύπτει από γενικότερη απαίτηση ή καλύπτει μέρος της περιοχής. Οι ενδείξεις είναι ποιοτικές: δεν αθροίζονται και δεν κατατάσσουν τα πλαίσια ως προς αυστηρότητα ή αποτελεσματικότητα. Το ● δεν σημαίνει εφαρμογή του ίδιου μέτρου σε κάθε οντότητα· οι ειδικές προϋποθέσεις, η αναλογικότητα και οι εξαιρέσεις εξακολουθούν να ελέγχονται. Το μητρώο κινδύνων, για παράδειγμα, προτείνεται ως τεκμήριο και δεν επιβάλλεται με ενιαίο τύπο από όλες τις πράξεις.

4.2 Πεδίο εφαρμογής και σχέση των τριών πλαισίων

4.2.1 NIS2: οριζόντια ασφάλεια δικτύων και πληροφοριακών συστημάτων

Στη σύγκριση, η NIS2 ενεργοποιείται από τον συνδυασμό τομέα, παρεχόμενης υπηρεσίας, μεγέθους και ειδικών περιπτώσεων ένταξης ανεξαρτήτως μεγέθους (άρθρα 2–3). Η χρήση πληροφοριακού συστήματος ή η συμμετοχή σε αλυσίδα εφοδιασμού δεν αρκεί. Η μονάδα ελέγχου είναι η καλυπτόμενη οντότητα και οι υπηρεσίες της, ενώ τα μέτρα του άρθρου 21 αφορούν την ασφάλεια και συνέχεια αυτών των υπηρεσιών.

4.2.2 GDPR: προστασία θεμελιωδών δικαιωμάτων κατά την επεξεργασία προσωπικών δεδομένων

Αντίθετα, ο GDPR ακολουθεί την επεξεργασία προσωπικών δεδομένων και τον ρόλο κάθε μέρους ως υπευθύνου ή εκτελούντος, υπό τις προϋποθέσεις των άρθρων 2–3. Ένας οργανισμός μπορεί να υπάγεται στον GDPR χωρίς να καλύπτεται από NIS2 ή DORA· το ίδιο τεχνικό συμβάν εξετάζεται κατά GDPR μόνο εφόσον επηρεάζει προσωπικά δεδομένα. Το κρίσιμο αντικείμενο κινδύνου είναι τα δικαιώματα και οι ελευθερίες φυσικών προσώπων.

4.2.3 DORA: τομεακή ψηφιακή επιχειρησιακή ανθεκτικότητα και αρχή *lex specialis*

Ο DORA αφορά τις χρηματοοικονομικές οντότητες του άρθρου 2 και τις σχέσεις τους με τρίτους παρόχους υπηρεσιών τεχνολογιών πληροφοριών και επικοινωνιών (ΤΠΕ), με ειδική άμεση εποπτεία για παρόχους που χαρακτηρίζονται κρίσιμοι. Η παροχή φυσικής υπηρεσίας *logistics* σε τράπεζα δεν αρκεί για υπαγωγή του προμηθευτή στο καθεστώς παρόχων ΤΠΕ. Ελέγχεται αν το αντικείμενο της υπηρεσίας πληροί τον ορισμό του άρθρου 3 σημείο 21, όπως αναλύθηκε στο Κεφάλαιο 3.

Κατά το άρθρο 1 παράγραφος 2 DORA και το άρθρο 4 NIS2, ο DORA αποτελεί τομεακή πράξη για τις χρηματοοικονομικές οντότητες που προσδιορίζονται ως βασικές ή σημαντικές κατά NIS2. Οι ισοδύναμες απαιτήσεις διαχείρισης κινδύνων ΤΠΕ και αναφοράς περιστατικών, μαζί με τη συναφή εποπτεία και επιβολή, αντιμετωπίζονται μέσω του ειδικού καθεστώτος. Η σχέση αυτή δεν απαλλάσσει γενικά κάθε προμηθευτή της τράπεζας από τη NIS2. Ο GDPR διατηρεί αυτοτελή εφαρμογή στις καλυπτόμενες επεξεργασίες προσωπικών δεδομένων.

Η συγκριτική χαρτογράφηση διατηρεί και τη διάκριση των αρχών. Στη NIS2 οι εθνικές αρμόδιες αρχές ασκούν εποπτεία, ενώ τα CSIRT έχουν λειτουργίες αντιμετώπισης περιστατικών και ο ENISA υποστηρικτικό ρόλο. Στον GDPR αρμόδιες είναι οι αρχές προστασίας δεδομένων. Στον DORA οι εποπτικές

αρμοδιότητες κατανέμονται κατά το άρθρο 46, με χωριστό ενωσιακό μηχανισμό για κρίσιμους τρίτους παρόχους ΤΠΕ. Ο Πίνακας 4.1 συνοψίζει τις διαφορές ως προς το αντικείμενο, το πεδίο, τη διάσταση κινδύνου, τη λογοδοσία, την εποπτεία και τη σχέση μεταξύ των πλαισίων.

Πίνακας 4.1: Πεδίο εφαρμογής, κανονιστικός σκοπός και σχέση των NIS2, GDPR και DORA

Κριτήριο	NIS2	GDPR	DORA
Νομική πράξη	Οδηγία 2022/2555· στην Ελλάδα Ν. 5160/2024 και εφαρμοστικές πράξεις.	Κανονισμός 2016/679· άμεσα εφαρμοστέος.	Κανονισμός 2022/2554· εφαρμόζεται από 17.1.2025.
Αντικείμενο	Ασφάλεια δικτύων, συστημάτων και υπηρεσιών.	Προστασία φυσικών προσώπων κατά την επεξεργασία δεδομένων.	Ψηφιακή επιχειρησιακή ανθεκτικότητα χρηματοοικονομικών οντοτήτων.
Πεδίο	Τύπος οντότητας, μέγεθος και ειδικές περιπτώσεις των άρθρων 2–3.	Επεξεργασία και εδαφικό πεδίο των άρθρων 2–3· ρόλος ανά δραστηριότητα.	Οντότητες του άρθρου 2· ειδικό καθεστώς τρίτων παρόχων ΤΠΕ.
Διάσταση κινδύνου	Συνέπειες για συστήματα, υπηρεσίες και επηρεαζόμενα πρόσωπα.	Συνέπειες για δικαιώματα και ελευθερίες φυσικών προσώπων.	Συνέπειες κινδύνων ΤΠΕ στις χρηματοοικονομικές υπηρεσίες.
Λογοδοσία	Έγκριση και εποπτεία μέτρων από το διοικητικό όργανο (άρθρο 20).	Υπεύθυνος επεξεργασίας (άρθρα 5(2), 24)· ειδικές υποχρεώσεις εκτελούντος.	Τελική ευθύνη διοικητικού οργάνου για κίνδυνο ΤΠΕ (άρθρο 5).
Εποπτεία	Εθνικές αρμόδιες αρχές· τα CSIRT υποστηρίζουν την αντιμετώπιση περιστατικών.	Ανεξάρτητες αρχές προστασίας δεδομένων.	Αρχές του άρθρου 46· χωριστή εποπτεία κρίσιμων τρίτων παρόχων.
Σχέση πλαισίων	Το άρθρο 4 αναγνωρίζει ισοδύναμες τομεακές απαιτήσεις.	Παράλληλη εφαρμογή στις καλυπτόμενες επεξεργασίες.	Τομεακή πράξη έναντι NIS2 για τις σχετικές χρηματοοικονομικές οντότητες (άρθρο 1(2)).

Πηγή: Συγκριτική σύνθεση του συγγραφέα βάσει της Οδηγίας (ΕΕ) 2022/2555, του Κανονισμού (ΕΕ) 2016/679 και του Κανονισμού (ΕΕ) 2022/2554.

4.3 Η έννοια του περιστατικού και οι υποχρεώσεις αναφοράς

Η σύγκριση διακρίνει τον ορισμό του περιστατικού από το κατώφλι εξωτερικής αναφοράς. Ένα συμβάν μπορεί να απαιτεί εσωτερική καταγραφή και αντιμετώπιση χωρίς να είναι ανακοινώσιμο στην αρχή. Αντίστροφα, η υποχρέωση αναφοράς μπορεί να ενεργοποιείται πριν ολοκληρωθεί η τεχνική διερεύνηση. Οι επόμενες ενότητες εστιάζουν στις διαφορές που αλλάζουν την απόφαση.

4.3.1 NIS2: «σημαντικό περιστατικό»

Στη NIS2 η αξιολόγηση αφορά την ασφάλεια δεδομένων και υπηρεσιών της καλυπτόμενης οντότητας. Το άρθρο 23 παράγραφος 3 θέτει ως κατώφλι την πρόκληση ή δυνατότητα πρόκλησης σοβαρής λειτουργικής διατάραξης ή οικονομικής ζημίας για την οντότητα, ή σημαντικής υλικής ή μη υλικής ζημίας σε άλλα πρόσωπα. Η δυνητική επίπτωση έχει συνεπώς σημασία και δεν απαιτείται να έχει ήδη οριστικοποιηθεί η ζημία. Για τις ειδικές κατηγορίες ψηφιακών παρόχων του πεδίου του εφαρμόζονται και τα κριτήρια του Κανονισμού (ΕΕ) 2024/2690.

Οι 24 ώρες της έγκαιρης προειδοποίησης και οι 72 ώρες της γνωστοποίησης αρχίζουν και οι δύο από τη γνώση του σημαντικού περιστατικού, όχι διαδοχικά. Η ειδική γνωστοποίηση για παρόχους υπηρεσιών εμπιστοσύνης γίνεται εντός 24 ωρών για σημαντικά περιστατικά που επηρεάζουν τις υπηρεσίες τους. Η τελική έκθεση υποβάλλεται μέσα σε έναν μήνα από τη γνωστοποίηση· αν η διαχείριση συνεχίζεται, υποβάλλεται έκθεση προόδου και τελική έκθεση μέσα σε έναν μήνα από την ολοκλήρωση της διαχείρισης (άρθρο 23 παράγραφος 4).

4.3.2 GDPR: «παραβίαση προσωπικών δεδομένων»

Στον GDPR εξετάζεται αν παραβιάστηκε η ασφάλεια προσωπικών δεδομένων και ποια συνέπεια προκύπτει για τα φυσικά πρόσωπα. Η παραβίαση μπορεί να αφορά εμπιστευτικότητα, ακεραιότητα ή διαθεσιμότητα χωρίς κακόβουλη ενέργεια. Ακόμη και προσωρινή απώλεια διαθεσιμότητας λόγω συμβάντος ασφάλειας μπορεί να αποτελεί παραβίαση· η γρήγορη αποκατάσταση επηρεάζει την αξιολόγηση κινδύνου, χωρίς να αναιρεί αυτομάτως τον χαρακτηρισμό (EDPB, 2023, παράγραφοι 18–24). Κάθε παραβίαση τεκμηριώνεται κατά το άρθρο 33 παράγραφος 5.

Ο υπεύθυνος επεξεργασίας γνωστοποιεί στην αρμόδια αρχή χωρίς αδικαιολόγητη καθυστέρηση και, εφόσον είναι δυνατό, εντός 72 ωρών από τη γνώση, εκτός αν δεν είναι πιθανό να προκύψει κίνδυνος για τα δικαιώματα και τις ελευθερίες φυσικών προσώπων. Για υψηλό κίνδυνο ενημερώνει και τα υποκείμενα χωρίς αδικαιολόγητη καθυστέρηση, με τις εξαιρέσεις του άρθρου 34 παράγραφος 3. Ο εκτελών ενημερώνει τον υπεύθυνο χωρίς αδικαιολόγητη καθυστέρηση (άρθρο 33 παράγραφος 2)· δεν διαθέτει αυτοτελές περιθώριο 72 ωρών. Η ευθύνη γνωστοποίησης στην αρχή παραμένει στον υπεύθυνο επεξεργασίας.

Το κατώφλι του GDPR δεν είναι η διακοπή μιας υπηρεσίας ούτε το ύψος της οικονομικής ζημίας. Η αξιολόγηση λαμβάνει υπόψη τη φύση, ευαισθησία και έκταση των δεδομένων, τον αριθμό και τα χαρακτηριστικά των υποκειμένων, τη δυνατότητα ταυτοποίησης και τις πιθανές συνέπειες. Κατά συνέπεια, ένα περιορισμένο σε διάρκεια συμβάν μπορεί να απαιτεί γνωστοποίηση, εάν εκθέτει δεδομένα υψηλής ευαισθησίας, ενώ μια τεχνικά σοβαρή διακοπή χωρίς προσωπικά δεδομένα δεν ενεργοποιεί τα άρθρα 33–34.

4.3.3 DORA: συμβάν ΤΠΕ και «μείζον συμβάν που σχετίζεται με ΤΠΕ»

Στον DORA η χρηματοοικονομική οντότητα εξετάζει την επίπτωση συμβάντος ΤΠΕ στις δικές της υπηρεσίες, ακόμη και όταν η προέλευση βρίσκεται σε τρίτο. Υποχρεωτική αναφορά απαιτείται εφόσον το συμβάν ταξινομείται ως μείζον κατά το άρθρο 18 και τον Κανονισμό (ΕΕ) 2024/1772. Η σοβαρότητα που αποδίδει ο προμηθευτής στο δικό του περιστατικό δεν υποκαθιστά αυτή την ταξινόμηση.

Η ταξινόμηση συνδυάζει την κρισιμότητα των επηρεαζόμενων υπηρεσιών με τα ειδικά όρια του Κανονισμού 2024/1772. Κατά το άρθρο 8, απαιτείται επηρεασμός κρίσιμων υπηρεσιών και είτε το ειδικό κατώφλι του άρθρου 9 παράγραφος 5 στοιχείο β' είτε τουλάχιστον δύο από τα λοιπά κατώφλια. Συνεκτιμώνται επίσης επαναλαμβανόμενα περιστατικά υπό τις προβλεπόμενες προϋποθέσεις. Επομένως, η απλή απαρίθμηση διάρκειας, ζημίας ή αριθμού πελατών δεν αρκεί χωρίς τον κανόνα συνδυασμού τους.

Ο Κανονισμός (ΕΕ) 2025/301 διακρίνει τη γνώση του συμβάντος από την ταξινόμησή του ως μείζονος. Η αρχική αναφορά γίνεται το συντομότερο δυνατό, εντός τεσσάρων ωρών από την ταξινόμηση και έως 24 ώρες από τη γνώση. Αν η ταξινόμηση γίνει μετά το πρώτο 24ωρο, ισχύουν τέσσερις ώρες από την ταξινόμηση. Η ενδιάμεση αναφορά υποβάλλεται εντός 72 ωρών από την αρχική, ακόμη και χωρίς αλλαγή κατάστασης, και η τελική μέσα σε έναν μήνα από την ενδιάμεση ή την τελευταία επικαιροποίησή της. Οι

ειδικές ρυθμίσεις ενημέρωσης, καθυστέρησης και περιορισμένης παράτασης λόγω αργιών του άρθρου 5 αναλύθηκαν στο Κεφάλαιο 3.

4.3.4 Ένα πραγματικό γεγονός, τρεις αυτοτελείς νομικές αξιολογήσεις

Η κοινή τεχνική βάση μπορεί να περιλαμβάνει χρόνο ανίχνευσης, συστήματα, δεδομένα, λειτουργίες, επηρεαζόμενους αποδέκτες και ενέργειες περιορισμού. Κάθε οντότητα τηρεί τον δικό της φάκελο και τις αποφάσεις για τα πλαίσια που την αφορούν. Η ανταλλαγή στοιχείων με προμηθευτή ή πελάτη δεν συνεπάγεται κοινή νομική ευθύνη ούτε έναν ενιαίο χρόνο γνώσης για όλους.

Η καταγραφή διακρίνει τουλάχιστον τη γνώση σημαντικού περιστατικού κατά NIS2, τη γνώση παραβίασης από τον υπεύθυνο επεξεργασίας κατά GDPR και τη γνώση συμβάντος και μεταγενέστερη ταξινόμηση κατά DORA. Κατά το EDPB (2023, παράγραφοι 31–34), η γνώση παραβίασης προϋποθέτει εύλογη βεβαιότητα ότι επηρεάστηκαν προσωπικά δεδομένα. Η αρχική τεχνική ειδοποίηση δεν ταυτίζεται αναγκαστικά με κάθε νομική αφετηρία, αλλά η διερεύνηση δεν δικαιολογεί τεχνητή μετάθεσή της. Ο Πίνακας 4.2 συγκεντρώνει τις διαφορές των βασικών κανόνων.

Πίνακας 4.2: Συγκριτική αποτύπωση της έννοιας και της αναφοράς περιστατικού

Στοιχείο	NIS2	GDPR	DORA
Αντικείμενο αναφοράς	Σημαντικό περιστατικό στην καλυπτόμενη οντότητα.	Παραβίαση προσωπικών δεδομένων με το κατώφλι των άρθρων 33–34.	Μείζον συμβάν ΤΠΕ στην καλυπτόμενη χρηματοοικονομική οντότητα.
Κατώφλι	Πραγματική ή δυνητική σοβαρή διατάραξη ή οικονομική ζημία στην οντότητα, ή σημαντική ζημία σε άλλα πρόσωπα.	Γνωστοποίηση στην αρχή, εκτός αν δεν είναι πιθανός κίνδυνος· ενημέρωση υποκειμένων σε υψηλό κίνδυνο.	Κρίσιμες υπηρεσίες και συνδυασμός κριτηρίων του άρθρου 8 του Κανονισμού 2024/1772.
Υπόχρεος	Βασική ή σημαντική οντότητα.	Υπεύθυνος προς αρχή/υποκείμενα· εκτελών προς υπεύθυνο.	Χρηματοοικονομική οντότητα, ακόμη και αν αναθέτει την υποβολή σε τρίτο.
Αποδέκτης	CSIRT ή αρμόδια αρχή· αποδέκτες υπηρεσιών όπου απαιτείται.	Εποπτική αρχή και υποκείμενα κατά τα αντίστοιχα κατώφλια.	Αρχή του άρθρου 46· πελάτες όταν μείζον συμβάν θίγει τα οικονομικά συμφέροντά τους.
Πρώτη αναφορά	Χωρίς αδικαιολόγητη καθυστέρηση, έως 24 ώρες από τη γνώση σημαντικού περιστατικού.	Προς αρχή: χωρίς αδικαιολόγητη καθυστέρηση, ει δυνατόν εντός 72 ωρών από τη γνώση παραβίασης.	Το συντομότερο δυνατό: 4 ώρες από ταξινόμηση και έως 24 από γνώση. Αν ταξινομηθεί μετά το 24ωρο: 4 ώρες από ταξινόμηση.
Επόμενα στάδια	Γνωστοποίηση έως 72 ώρες από την ίδια γνώση· τελική μέσα σε μήνα από γνωστοποίηση, με ειδική ρύθμιση αν συνεχίζεται η διαχείριση.	Σταδιακή συμπλήρωση πληροφοριών· τεκμηρίωση κάθε παραβίασης. Η ενημέρωση εκτελούντος και υποκειμένων δεν έχει όριο 72 ωρών.	Ενδιάμεση εντός 72 ωρών από αρχική· τελική μέσα σε μήνα από ενδιάμεση ή τελευταία επικαιροποίησή της.
Όριο της σύγκρισης	Δεν αναφέρεται κάθε τεχνικό συμβάν· ισχύουν και ειδικοί κανόνες, π.χ. για υπηρεσίες εμπιστοσύνης.	Μη γνωστοποιήσιμη παραβίαση εξακολουθεί να χρειάζεται καταγραφή και αντιμετώπιση.	Μη μείζον συμβάν εξακολουθεί να χρειάζεται διαχείριση· δεν ταυτίζεται με απλή διακοπή φυσικής προμήθειας.

Πηγή: Συγκριτική σύνθεση του συγγραφέα βάσει NIS2, άρθρα 6 και 23· GDPR, άρθρα 4(12), 33–34· DORA, άρθρα 3 και 17–20· Κανονισμοί (ΕΕ) 2024/1772 και 2025/301. Οι ειδικές προϋποθέσεις των §§4.3.1–4.3.3 συμπληρώνουν τον πίνακα.

4.4 Συγκριτική ανάλυση με προσανατολισμό στον κίνδυνο

4.4.1 Διαφορετικά αντικείμενα κινδύνου, κοινή ανάγκη λογοδοσίας

Κοινός παρονομαστής των τριών πλαισίων είναι ότι απομακρύνονται από μια τυπική αντίληψη συμμόρφωσης, στην οποία αρκεί η ύπαρξη πολιτικών. Ζητούν αναλογικά μέτρα, σύνδεση με τεκμηριωμένο κίνδυνο και δυνατότητα απόδειξης ότι τα μέτρα λειτουργούν. Η ομοιότητα αυτή δεν εξαλείφει τη διαφορά του αντικειμένου: η NIS2 προσανατολίζεται στη συνέχεια και ασφάλεια υπηρεσιών και συστημάτων, ο GDPR στις συνέπειες για το άτομο και ο DORA στην ανθεκτικότητα χρηματοοικονομικών λειτουργιών απέναντι σε διαταραχές ΤΠΕ.

Μια κοινή μεθοδολογία μπορεί να χρησιμοποιεί την ίδια κλίμακα πιθανότητας, διατηρώντας χωριστές διαστάσεις επίπτωσης: συνέχεια υπηρεσίας, δικαιώματα φυσικών προσώπων και χρηματοοικονομικές λειτουργίες. Η συγχώνευσή τους σε έναν μέσο βαθμό θα μπορούσε να αποκρύψει υψηλό κίνδυνο για άτομα μέσα σε χαμηλή επιχειρησιακή ζημία. Η αποδοχή υπολειπόμενου κινδύνου χρειάζεται αιτιολόγηση και αρμόδια έγκριση, αλλά δεν αίρει δεσμευτικό μέτρο ή υποχρέωση αναφοράς.

4.4.2 Διακυβέρνηση, ασφάλεια και απόδειξη αποτελεσματικότητας

Στη NIS2 και στον DORA η διοικητική ευθύνη είναι ιδιαίτερα εμφανής. Η διοίκηση δεν περιορίζεται στην έγκριση προϋπολογισμού, αλλά οφείλει να κατανοεί το προφίλ κινδύνου, να εγκρίνει το σχετικό πλαίσιο και να παρακολουθεί την εφαρμογή του. Στον GDPR η λογοδοσία οργανώνεται γύρω από τον υπεύθυνο επεξεργασίας, ενώ ο Υπεύθυνος Προστασίας Δεδομένων, όπου έχει οριστεί, συμβουλεύει και παρακολουθεί ανεξάρτητα τη συμμόρφωση. Το άρθρο 39 περιλαμβάνει την παρακολούθηση της ευαισθητοποίησης και της κατάρτισης του προσωπικού· δεν μετατρέπει τον DPO σε αποκλειστικό φορέα όλης της εκπαίδευσης.

Η NIS2 προβλέπει αξιολόγηση αποτελεσματικότητας των μέτρων (άρθρο 21 παράγραφος 2 στοιχείο στ'), ενώ ο GDPR τακτικές δοκιμές και αξιολόγηση κατά το άρθρο 32 παράγραφος 1 στοιχείο δ', ανάλογα με τον κίνδυνο. Ο DORA εξειδικεύει περισσότερο το πρόγραμμα και τις δοκιμές: το ολοκληρωμένο πρόγραμμα του άρθρου 24 εξαιρεί τις πολύ μικρές επιχειρήσεις, οι οποίες υπάγονται στη στάθμιση του άρθρου 25 παράγραφος 3. Οι δοκιμές διεύθυνσης βάσει απειλών (TLPT) αφορούν μόνο τις οντότητες που προσδιορίζονται κατά το άρθρο 26 και τον Κανονισμό 2025/1190. Η μεγαλύτερη κανονιστική λεπτομέρεια δεν αποδεικνύει από μόνη της μεγαλύτερη επιχειρησιακή αποτελεσματικότητα.

4.4.3 Επιχειρησιακή συνέχεια και κίνδυνος τρίτων

Η επιχειρησιακή συνέχεια δεν είναι αποκλειστικό θέμα του DORA. Η NIS2 την περιλαμβάνει ρητά στο άρθρο 21 παρ. 2 στοιχ. γ', μαζί με διαχείριση αντιγράφων ασφαλείας, αποκατάσταση μετά από καταστροφή και διαχείριση κρίσεων. Ο GDPR απαιτεί δυνατότητα έγκαιρης αποκατάστασης της διαθεσιμότητας και της πρόσβασης σε προσωπικά δεδομένα μετά από φυσικό ή τεχνικό συμβάν. Ο DORA αναπτύσσει το θέμα με μεγαλύτερη τομεακή λεπτομέρεια, συνδέοντάς το με πολιτικές επιχειρησιακής συνέχειας ΤΠΕ, σχέδια απόκρισης και ανάκαμψης, δοκιμές και διαχείριση κρίσεων.

Στον κίνδυνο τρίτων, το αντικείμενο της σχέσης καθορίζει τον έλεγχο. Η NIS2 καλύπτει την ασφάλεια άμεσων προμηθευτών και παρόχων. Το άρθρο 28 GDPR εφαρμόζεται όταν υπάρχει επεξεργασία για λογαριασμό υπευθύνου, όχι σε κάθε εμπορικό προμηθευτή. Ο DORA αφορά συμβατικές ρυθμίσεις

υπηρεσιών ΤΠΕ, με πρόσθετες απαιτήσεις για κρίσιμες ή σημαντικές λειτουργίες. Το μητρώο του άρθρου 28 DORA δεν ταυτίζεται με κατάλογο περιουσιακών στοιχείων ή με αρχείο δραστηριοτήτων επεξεργασίας GDPR. Οι καλές πρακτικές του ENISA (2023) υποστηρίζουν την εξέταση των σχέσεων προμήθειας, χωρίς να εξισώνουν αυτές τις νομικές κατηγορίες.

Η επαναχρησιμοποίηση τεκμηρίων απαιτεί αντιστοίχιση της υπηρεσίας, του ελέγχου και της περιόδου που καλύπτουν. Για παράδειγμα, μια δοκιμή ανάκτησης μπορεί να στηρίξει τη συνέχεια υπηρεσίας κατά NIS2, την αποκατάσταση πρόσβασης σε προσωπικά δεδομένα κατά GDPR και την ανάκαμψη χρηματοοικονομικής λειτουργίας κατά DORA, εφόσον εξετάζει πράγματι τα αντίστοιχα αντικείμενα. Επιτυχής ανάκτηση δεν αποδεικνύει από μόνη της νόμιμη επεξεργασία, έγκαιρη γνωστοποίηση ή επάρκεια συμβατικών ρητρών.

Πίνακας 4.3: Ενοποιημένη χαρτογράφηση βασικών περιοχών ελέγχου

Περιοχή ελέγχου	NIS2	GDPR	DORA	Ενδεικτικό τεκμήριο
Διοικητική έγκριση και εποπτεία	● 20	● 5(2), 24	● 5–6	Αποφάσεις έγκρισης, πρακτικά διοίκησης
Αξιολόγηση κινδύνου	● 21(2)(α)	● 24, 32· 35 όπου απαιτείται	● 6, 8	Αξιολόγηση και προτεινόμενο μητρώο κινδύνων
Διαχείριση περιστατικών	● 21(2)(β), 23	● 32–34	● 17–20	Αρχείο συμβάντος και αιτιολογημένες αποφάσεις
Συνέχεια και ανάκαμψη	● 21(2)(γ)	● 32(1)(β–γ) για προσωπικά δεδομένα	● 11–12	Σχέδια και αποτελέσματα δοκιμών ανάκτησης
Ασφάλεια σχέσεων με τρίτους	● 21(2)(δ), 21(3)	● 28 για εκτελούντες	● 28–30 για υπηρεσίες ΤΠΕ	Αξιολόγηση παρόχου, σύμβαση και έλεγχοι
Κρυπτογραφία	● 21(2)(η)	● 32(1)(α), κατά περίπτωση	● 9(2), 9(4)(δ)	Πολιτική και τεκμήρια διαχείρισης κλειδιών
Πρόσβαση και ταυτοποίηση	● 21(2)(θ–ι)	● 32, βάσει κινδύνου	● 9(4)(γ–δ)	Δικαιώματα, επανέλεγχοι πρόσβασης και ρυθμίσεις
Αξιολόγηση μέτρων	● 21(2)(στ)	● 32(1)(δ)	● 24–27, με ειδικές προϋποθέσεις	Δοκιμές, ευρήματα και επαλήθευση διορθώσεων
Εκπαίδευση και κυβερνοϋγιεινή	● 20(2), 21(2)(ζ)	● 32, 39(1)(β)	● 5(4), 13(6)	Εκπαίδευση, συμμετοχή και ασκήσεις
Ενημέρωση επηρεαζόμενων προσώπων	● 23(1)–(2), κατά περίπτωση	● 34, σε υψηλό κίνδυνο	● 19(3), υπό προϋποθέσεις	Απόφαση ενημέρωσης, κείμενο και αποδεικτικό αποστολής

Πηγή: Σύνθεση του συγγραφέα: οι αριθμοί ανά κελί παραπέμπουν σε άρθρα της αντίστοιχης πράξης. Η επιλογή περιοχών έχει εννοιολογική αναφορά στις λειτουργίες Govern, Identify, Protect, Detect, Respond και Recover του NIST CSF 2.0 (NIST, 2024), χωρίς να αποτελεί επίσημη αντιστοίχιση του NIST. Τα τεκμήρια είναι ενδεικτικά. Για DORA ελέγχεται και τυχόν εφαρμογή του απλουστευμένου πλαισίου του άρθρου 16.

4.4.4 Τι προσθέτει η ενοποιημένη χαρτογράφηση

Η ενοποιημένη χαρτογράφηση δεν προτείνει μία ενιαία δήλωση συμμόρφωσης. Διαχωρίζει το κοινό επιχειρησιακό επίπεδο από το επίπεδο της κανονιστικής απόφασης. Στο πρώτο καταγράφονται το γεγονός, η υπηρεσία, οι εξαρτήσεις, τα δεδομένα, η χρονογραμμή, το μέτρο και το διαθέσιμο τεκμήριο. Στο δεύτερο

αξιολογούνται χωριστά, για κάθε πράξη, το πεδίο εφαρμογής, ο υπόχρεος, το προστατευόμενο συμφέρον, το κατώφλι, η προθεσμία, ο αποδέκτης και το αιτιολογημένο συμπέρασμα.

Η επαναχρησιμοποίηση ενός τεκμηρίου επιτρέπεται μόνο όταν ταυτίζονται το πραγματικό αντικείμενο, η υπηρεσία, η περίοδος και το μέτρο που εξετάζονται. Ένα αποτέλεσμα δοκιμής ανάκαμψης ή ένα αρχείο περιστατικού μπορεί συνεπώς να συνδέεται με περισσότερες απαιτήσεις, αλλά κάθε σύνδεση χρειάζεται αυτοτελή αιτιολόγηση. Με αυτόν τον τρόπο αποφεύγονται τόσο η άσκοπη διπλή καταγραφή όσο και η εσφαλμένη παραδοχή ότι μία απόδειξη συμμόρφωσης καλύπτει αυτομάτως όλα τα πλαίσια.

Όπως αποτυπώνεται στον Πίνακα 4.3, οι κοινές περιοχές ελέγχου λειτουργούν ως σημεία σύνδεσης, ενώ οι χωριστές στήλες NIS2, GDPR και DORA διατηρούν τη νομική αυτοτέλεια. Η προστιθέμενη αξία της χαρτογράφησης είναι επομένως η ελεγχόμενη επαναχρησιμοποίηση τεκμηρίων με πλήρη ιχνηλασιμότητα προς τη συγκεκριμένη απαίτηση. Η λογική αυτή αποτελεί σχεδιαστική αφετηρία του πλαισίου στο Κεφάλαιο 5.

4.5 Εφαρμογή σε σενάριο παρόχου υπηρεσιών εφοδιαστικής (3PL)

4.5.1 Παραδοχές του σεναρίου

Χρησιμοποιείται συνοπτικά η LogiTrans Europe του Κεφαλαίου 6, υποθετικός πάροχος υπηρεσιών εφοδιαστικής τρίτου μέρους (3PL). Για τη συνεπή εφαρμογή του παραδείγματος υιοθετείται η ίδια παραδοχή: μεγάλη επιχείρηση με αυτοτελή υπηρεσία ευφών συστημάτων μεταφορών (ITS) του Παραρτήματος I NIS2, η οποία έχει καταχωριστεί ως βασική οντότητα. Η παραδοχή δεν αποδεικνύει υπαγωγή οποιασδήποτε επιχείρησης logistics. Το ransomware επηρεάζει αποθήκη και τη συνδεδεμένη υπηρεσία ITS και δημιουργεί ενδείξεις διαρροής δεδομένων παραληπτών. Ο τραπεζικός πελάτης λαμβάνει φυσική υπηρεσία διανομής, με βοηθητική ψηφιακή διασύνδεση· δεν θεωρείται δεδομένη αυτοτελής υπηρεσία ΤΠΕ προς αυτόν.

4.5.2 Αρχική αξιολόγηση και διαδρομή γνωστοποιήσεων

Ο Πίνακας 4.4 διακρίνει τις ενέργειες των δύο οργανισμών. Η LogiTrans ελέγχει τη σημαντικότητα κατά NIS2 και τον ρόλο της ανά επεξεργασία κατά GDPR. Η τράπεζα εξετάζει αν υπάρχει συμβάν ΤΠΕ που επηρεάζει τις δικές της υπηρεσίες και, στη συνέχεια, αν είναι μείζον. Η καθυστέρηση φυσικής διανομής δεν αρκεί μόνη της για αυτόν τον χαρακτηρισμό. Τα στοιχεία που παρέχει η LogiTrans στηρίζουν την αξιολόγηση της τράπεζας βάσει της σύμβασής τους. Η πλήρης χρονογραμμή και οι αποφάσεις αναπτύσσονται στο Κεφάλαιο 6.

Πίνακας 4.4: Αφετηρία ενεργειών για το υποθετικό περιστατικό ransomware σε πάροχο 3PL

Ενέργεια	LogiTrans ως 3PL	Τραπεζικός πελάτης	Τεκμηρίωση
Εντοπισμός	Περιορισμός συμβάντος, διατήρηση στοιχείων και ενεργοποίηση συνέχειας.	Εξετάζει εξάρτηση από τη διακοπή και κλιμακώνει εσωτερικά.	Χρόνοι εντοπισμού, συστήματα, δεδομένα και αποφάσεις.
Έλεγχος NIS2	Με τη ρητή παραδοχή υπαγωγής, ελέγχει σημαντικότητα· αν συντρέχει, προειδοποίηση έως 24 ώρες από τη γνώση της.	Αξιοποιεί τα στοιχεία για τη δική του αξιολόγηση· δεν υποβάλλει αντί της LogiTrans.	Αιτιολογία σημαντικότητας και χρόνος γνώσης.

Ενέργεια	LogiTrans ως 3PL	Τραπεζικός πελάτης	Τεκμηρίωση
Έλεγχος GDPR	Ως εκτελούσα ενημερώνει χωρίς αδικαιολόγητη καθυστέρηση· ως υπεύθυνη αξιολογεί άρθρα 33–34.	Ελέγχει αν επηρεάστηκαν δεδομένα για τα οποία είναι υπεύθυνος.	Ρόλοι, δεδομένα, κίνδυνος για άτομα και απόφαση.
Έλεγχος DORA	Παρέχει τα συμβατικά απαιτούμενα στοιχεία· δεν αποκτά ιδιότητα υπόχρεου αναφοράς DORA ως 3PL.	Ελέγχει πρώτα αν υπάρχει δικό του συμβάν ΤΠΕ και έπειτα αν είναι μείζον.	Στοιχεία επίπτωσης, ταξινόμηση και συμβατικές ειδοποιήσεις.
Ενημερώσεις	Συμπληρώνει τις δικές της αναφορές και πληροφορίες προς πελάτες.	Ενημερώνει αρχή και πελάτες εφόσον ενεργοποιούνται οι αντίστοιχες υποχρεώσεις.	Εκδόσεις, αποδέκτες και χρόνοι υποβολής.
Αποκατάσταση	Διερευνά αίτια, επανελέγχει ανάκτηση και αναθέτει διορθώσεις.	Αξιολογεί συνέχεια φυσικής προμήθειας και συμβατικές εναλλακτικές.	Αποτελέσματα αποκατάστασης, ενέργειες και υπεύθυνοι.

Πηγή: Εφαρμογή του συγγραφέα της συγκριτικής μεθόδου βάσει NIS2, άρθρο 23· GDPR, άρθρα 28 και 33–34· DORA, άρθρα 3 και 17–19. Οι συμβατικές ενέργειες είναι παραδοχές του σεναρίου. Τα άρθρα 28–30 DORA θα εξετάζονταν επιπλέον εάν η υπηρεσία του 3PL πληρούσε τον ορισμό υπηρεσίας ΤΠΕ.

4.6 Πρότυπο χαρτογράφησης συμμόρφωσης για τη μελέτη περίπτωσης

Ο Πίνακας 4.5 συνδέει τη νομική απαίτηση με το πεδίο εφαρμογής, την υπεύθυνη λειτουργία, το τεκμήριο και την αξιολόγηση. Λειτουργεί ως ευρετήριο ελέγχου και δεν αντικαθιστά τα ειδικά μητρώα των επιμέρους πράξεων. Οι ενδεικτικές γραμμές του περιγράφουν τι θα εξεταζόταν σε έναν έλεγχο· δεν αποτελούν ευρήματα για τη LogiTrans.

Κάθε εγγραφή χρειάζεται συγκεκριμένη διάταξη, αιτιολογία εφαρμογής και ελέγξιμο κριτήριο ολοκλήρωσης. Στο τεκμήριο καταγράφονται έκδοση, ημερομηνία, υπηρεσία και περίοδος που καλύπτει, μαζί με τον τρόπο ελέγχου του. Η ύπαρξη εγκεκριμένης διαδικασίας τεκμηριώνει τον σχεδιασμό της· η λειτουργία της χρειάζεται στοιχεία όπως δοκιμή, άσκηση ή καταγραφή εκτέλεσης. Το ίδιο αρχείο μπορεί να συνδέεται με περισσότερες απαιτήσεις, με χωριστή αιτιολόγηση ανά αντιστοίχιση.

Μετά τον έλεγχο χρησιμοποιούνται τέσσερις καταστάσεις: «Συμμορφώνεται» όταν τεκμηριώνεται η εξεταζόμενη απαίτηση, «Μερικώς συμμορφώνεται» όταν τεκμηριώνεται μόνο μέρος της, «Δεν συμμορφώνεται» όταν διαπιστώνεται μη εκπλήρωση και «Δεν εφαρμόζεται» με ειδική αιτιολογία. Όταν λείπουν στοιχεία, σημειώνεται προσωρινά «Εκκρεμεί αξιολόγηση» και προσδιορίζεται τι πρέπει να αναζητηθεί. Η απουσία τεκμηρίου δεν συγχέεται αυτομάτως με απουσία μέτρου· αν όμως η ίδια η διάταξη απαιτεί συγκεκριμένο αρχείο, η έλλειψή του αποτελεί ξεχωριστό εύρημα. Η προτεραιότητα αποκατάστασης εκτιμάται χωριστά βάσει επίπτωσης, πιθανότητας και προθεσμίας.

Πίνακας 4.5: Επαναχρησιμοποιήσιμο πρότυπο αξιολόγησης για τη μελέτη περίπτωσης

Απαίτηση και νομική βάση	Πεδίο και ενεργοποίηση	Υπεύθυνος και τεκμήρια προς έλεγχο	Αξιολόγηση και ενέργεια
Στοιχεία κάθε εγγραφής	Οντότητα, χώρα, υπηρεσία ή επεξεργασία· αιτιολογία εφαρμογής.	Λειτουργία, κωδικός/έκδοση τεκμηρίου, ημερομηνία, εύρος και τρόπος ελέγχου.	Κατάσταση, κενό, προτεραιότητα, ενέργεια, υπεύθυνος και προθεσμία.

Απαίτηση και νομική βάση	Πεδίο και ενεργοποίηση	Υπεύθυνος και τεκμήρια προς έλεγχο	Αξιολόγηση και ενέργεια
Παράδειγμα NIS2, άρθρο 23	Υπαγόμενη οντότητα και γνώση σημαντικού περιστατικού.	Αρμόδια λειτουργία ασφάλειας· χρονογραμμή, απόφαση σημαντικότητας, αποδεικτικό υποβολής.	Εκκρεμεί αξιολόγηση. Ελέγχεται αν η κλιμάκωση και υποβολή τήρησαν την προθεσμία.
Παράδειγμα GDPR, άρθρο 33	Υπεύθυνος επεξεργασίας που έλαβε γνώση παραβίασης· έλεγχος κινδύνου για άτομα.	Υπεύθυνος επεξεργασίας, με συμβουλή DPO όπου έχει οριστεί· αρχείο παραβίασης και αιτιολογία γνωστοποίησης ή μη.	Εκκρεμεί αξιολόγηση. Ελέγχονται καταγραφή, κίνδυνος, χρόνος γνώσης και απόφαση.
Παράδειγμα DORA, άρθρο 30	Χρηματοοικονομική οντότητα με σύμβαση υπηρεσίας ΤΠΕ· έλεγχος αν υποστηρίζει κρίσιμη ή σημαντική λειτουργία.	Αρμόδια λειτουργία συμβάσεων/κινδύνου τρίτων· σύμβαση και αντιστοίχιση με τις εφαρμοστέες ρήτρες.	Εκκρεμεί αξιολόγηση. Ελέγχονται οι απαιτήσεις της παρ. 2 και, όπου εφαρμόζεται, οι πρόσθετες της παρ. 3.

Πηγή: Σύνθεση του συγγραφέα. Οι γραμμές αποτελούν υποδείγματα και η αξιολόγησή τους παραμένει εκκρεμής έως την εξέταση τεκμηρίων. Στο Κεφάλαιο 6 συμπληρώνονται μόνο με τις ρητές παραδοχές του υποθετικού σεναρίου.

4.7 Προκλήσεις εφαρμογής και προτεινόμενες κατευθύνσεις

4.7.1 Κύριες δυσχέρειες

Η κατανομή εργασιών σε ασφάλεια πληροφοριών, προστασία δεδομένων, νομική υπηρεσία και προμήθειες μπορεί να δημιουργήσει διαφορετικές εκδοχές του ίδιου περιστατικού. Η δυσχέρεια αφορά ιδίως τις μεταβιβάσεις πληροφορίας: ποιος επιβεβαιώνει τα γεγονότα, ποιος αποφασίζει για κάθε νομικό κατώφλι και πώς ενημερώνει τους υπόλοιπους. Η κοινή καταγραφή χρειάζεται επομένως διακριτές αρμοδιότητες και ελεγχόμενες εκδόσεις.

Η δεύτερη δυσχέρεια είναι η αβεβαιότητα των πρώτων ωρών. Άγνωστη ροή δεδομένων ή μη καταγεγραμμένη εξάρτηση από τρίτο μπορεί να αλλάξει τον νομικό χαρακτηρισμό αφού έχει αρχίσει μια προθεσμία. Η χαρτογράφηση υπηρεσιών και επεξεργασιών, η ανάλυση επιχειρησιακών επιπτώσεων και οι δοκιμές ανάκαμψης μειώνουν αυτή την αβεβαιότητα, χωρίς να την εξαλείφουν.

Η τρίτη δυσχέρεια είναι η απόδειξη αναλογικότητας. Η απόφαση για ένα μέτρο χρειάζεται σύνδεση με συγκεκριμένο κίνδυνο, εύρος εφαρμογής και αποτέλεσμα ελέγχου. Το κόστος μπορεί να συνεκτιμάται όπου το επιτρέπει η διάταξη, αλλά δεν αρκεί για παράκαμψη υποχρεωτικού μέτρου. Οι εναλλακτικές λύσεις και η αποδοχή υπολειπόμενου κινδύνου πρέπει να παραμένουν εντός των νομικών ορίων.

Η διασυνοριακή εφαρμογή απαιτεί παρακολούθηση του εθνικού δικαίου. Η παραπομπή τεσσάρων κρατών στο Δικαστήριο για μη κοινοποίηση πλήρους μεταφοράς της NIS2, την οποία ανακοίνωσε η Ευρωπαϊκή Επιτροπή στις 8 Ιουλίου 2026, δείχνει ανομοιομορφία κατά τον συγκεκριμένο χρόνο. Δεν αποδεικνύει απουσία κάθε εθνικής υποχρέωσης. Η χαρτογράφηση χρειάζεται συνεπώς χώρα και έκδοση εφαρμοστέου κανόνα (Ευρωπαϊκή Επιτροπή, 2026).

4.7.2 Πρακτικές κατευθύνσεις ενοποίησης

Η σύγκριση οδηγεί σε τρεις κατευθύνσεις σχεδιασμού: καταγραφή του πεδίου εφαρμογής ανά οντότητα και υπηρεσία· κοινή διαχείριση γεγονότων και τεκμηρίων με χωριστές νομικές αποφάσεις· επαλήθευση της

λειτουργίας των μέτρων και παρακολούθηση των κενών. Πρόκειται για προτάσεις οργάνωσης της παρούσας εργασίας. Το Κεφάλαιο 5 τις μετατρέπει σε διαδικασίες, έντυπα, ρόλους και στάδια εφαρμογής.

4.8 Συμπεράσματα κεφαλαίου

Η σύγκριση εντοπίζει δυνατότητα ενοποίησης κυρίως στη συλλογή στοιχείων, στη διαχείριση κινδύνων και στον έλεγχο μέτρων. Τα όρια της ενοποίησης βρίσκονται στο πεδίο εφαρμογής, στο προστατευόμενο συμφέρον και στην κατανομή ευθύνης. Οι διαφορές αυτές εξηγούν γιατί ένα κοινό τεκμήριο μπορεί να υποστηρίξει περισσότερες υποχρεώσεις, χωρίς η συμμόρφωση με μία να αποδεικνύει τις υπόλοιπες.

Στα περιστατικά, το κρίσιμο εύρημα είναι η ανάγκη χωριστών αποφάσεων και χρονικών αφετηριών. Στις σχέσεις προμηθευτών, είναι η διάκριση μεταξύ άμεσης κανονιστικής υπαγωγής και συμβατικής δέσμευσης. Το παράδειγμα της LogiTrans δείχνει πώς οι δύο διακρίσεις εφαρμόζονται σε κοινό γεγονός, υπό ρητές παραδοχές.

Ως προς το RQ2, η κοινή επιχειρησιακή οργάνωση υποστηρίζει τη συλλογή και τον έλεγχο στοιχείων, ενώ η αιτιολόγηση της υπαγωγής, των ρόλων και των αποφάσεων αναφοράς παραμένει αυτοτελής ανά κανονιστικό πλαίσιο.

Το πρότυπο του Πίνακα 4.5 μεταφέρει τη συγκριτική ανάλυση στον σχεδιασμό του επόμενου κεφαλαίου. Η συμβολή του είναι μια ελέγξιμη σύνδεση διάταξης, πεδίου, υπευθύνου και τεκμηρίου. Η αποτελεσματικότητά του παραμένει προς εμπειρική διερεύνηση· η εφαρμογή του στο Κεφάλαιο 6 αποτελεί αναλυτική επίδειξη σε υποθετικό σενάριο.

ΚΕΦΑΛΑΙΟ 5 Σχεδιασμός Ενοποιημένου Πλαισίου Συμμόρφωσης και Πρωτόκολλο Εφαρμογής

Το παρόν κεφάλαιο μετατρέπει τη συγκριτική χαρτογράφηση του Κεφαλαίου 4 σε διαδικασία εφαρμογής για οργανισμούς της εφοδιαστικής αλυσίδας. Προσδιορίζει εισόδους, ενέργειες, ρόλους, παραδοτέα και κριτήρια ελέγχου. Η συλλογή στοιχείων και η επιχειρησιακή απόκριση οργανώνονται από κοινού, ενώ οι αποφάσεις NIS2, GDPR και DORA παραμένουν διακριτές.

Αφετηρία είναι ο έλεγχος εφαρμογής ανά οντότητα και δραστηριότητα. Η συμβατική δέσμευση προς χρηματοοικονομικό πελάτη δεν ταυτίζεται με άμεση υπαγωγή στον DORA, ούτε κάθε φυσική υπηρεσία logistics αποτελεί υπηρεσία ΤΠΕ. Χρησιμοποιείται η κανονιστική βάση των Κεφαλαίων 3–4, με χρονικό όριο την 31η Αυγούστου 2026.

Το πλαίσιο είναι πρόταση του συγγραφέα, στηριγμένη σε νομικές πηγές, τεχνικές κατευθύνσεις και βιβλιογραφία διαχείρισης κινδύνου. Η εφαρμογή του Κεφαλαίου 6 εξετάζει τη συνέπεια των αποφάσεων υπό τις υποθετικές παραδοχές της LogiTrans. Τα όρια αυτής της αναλυτικής αξιολόγησης συγκεντρώνονται στη §7.7.

Η σχεδιαστική ακολουθία του κεφαλαίου είναι ρητή: τα προβλήματα που αναδείχθηκαν στα Κεφάλαια 2–4 μετατρέπονται στις έξι απαιτήσεις σχεδιασμού DR1–DR6, οι οποίες καθορίζουν την αρχιτεκτονική και την πεντασταδιακή εφαρμογή του πλαισίου. Το Σχήμα 5.1 συνοψίζει τη μετάβαση από τις κανονιστικές πηγές και την επιχειρησιακή υπηρεσία προς τις εξαρτήσεις, την αλυσίδα $R \rightarrow G \rightarrow A \rightarrow E$, την επαλήθευση και τη διοικητική επανεξέταση. Οι επτά συνιστώσες του Πίνακα 5.1 περιγράφουν το περιεχόμενο, τα πέντε στάδια του Πίνακα 5.3 οργανώνουν την εφαρμογή και οι έξι ενότητες του Πίνακα 5.8 ορίζουν πού θα τεκμηριωθεί η εφαρμογή στη LogiTrans. Πρόκειται για διαφορετικές όψεις της ίδιας μεθόδου, χωρίς αριθμητική αντιστοιχία μία προς μία.

5.1 Μεθοδολογία και απαιτήσεις σχεδιασμού

5.1.1 Είσοδοι, όρια και μονάδα ανάλυσης

Οι εισοδοι οργανώνονται σε τέσσερις κατηγορίες: δεσμευτικές νομικές απαιτήσεις, συμβατικές υποχρεώσεις, στοιχεία επιχειρησιακής λειτουργίας και τεχνικές κατευθύνσεις. Στην πρώτη εντάσσονται η NIS2 με τον Ν. 5160/2024 και την ΚΥΑ 1689/2025, ο GDPR και ο DORA με τις σχετικές εφαρμοστικές πράξεις. Το NIST CSF 2.0 οργανώνει επιδιωκόμενα αποτελέσματα κυβερνοασφάλειας, ενώ τα ISO 31000:2018, ISO/IEC 27005:2022 και ISO/IEC 27001:2022 παρέχουν εννοιολογική βάση για κίνδυνο και σύστημα διαχείρισης. Η αναφορά στα πρότυπα δεν συνιστά πλήρη αντιστοίχιση των απαιτήσεών τους ή ισχυρισμό πιστοποίησης του προτεινόμενου πλαισίου.

Το προτεινόμενο μητρώο εφαρμογής καταγράφει, για κάθε πηγή, την υπόχρεη οντότητα, τη χώρα, την υπηρεσία ή επεξεργασία, τη διάταξη ή συμβατική ρήτρα, την έκδοση του κανόνα και την αιτιολογία υπαγωγής. Ορίζονται υπεύθυνος παρακολούθησης και ημερομηνία επανεξέτασης. Η άμεση νομική υποχρέωση, η συμβατική δέσμευση και η εσωτερική επιλογή σημειώνονται χωριστά. Το μητρώο είναι εργαλείο του παρόντος σχεδιασμού, χωρίς να υποκαθιστά τα ειδικά αρχεία που επιβάλλει κάθε πράξη.

Μονάδα εφαρμογής είναι η επιχειρησιακή υπηρεσία και οι εξαρτήσεις της. Καταγράφονται ιδιοκτήτης, εφαρμογές, συσκευές, εγκαταστάσεις, πάροχοι, ροές δεδομένων και διασυνδέσεις. Η ανάλυση επιχειρησιακών επιπτώσεων προσδιορίζει τον στόχο χρόνου ανάκαμψης (RTO) και τον στόχο σημείου

ανάκτησης (RPO), δηλαδή την αποδεκτή απώλεια δεδομένων εκφρασμένη ως χρονικό διάστημα. Οι στόχοι συνδέονται με ελάχιστη αποδεκτή λειτουργία και επιβεβαιώνονται με δοκιμές· δεν αποτελούν αυτομάτως νομοθετικά όρια.

Το πεδίο περιλαμβάνει οντότητες, χώρες, υπηρεσίες, δεδομένα, πληροφοριακή και επιχειρησιακή τεχνολογία (IT/OT) και τρίτους. Οι εξαρτήσεις εκτός των οργανωτικών ορίων παραμένουν ορατές. Για την κατανομή εργασιών χρησιμοποιείται πίνακας RACI: εκτελών την ενέργεια (Responsible), εσωτερικά υπόλογος για την απόφαση (Accountable), συμβουλευόμενος (Consulted) και ενημερούμενος (Informed). Ο εσωτερικός αυτός διαχωρισμός δεν μεταβιβάζει τη νομική ευθύνη της οντότητας ή του υπευθύνου επεξεργασίας.

Ο Πίνακας 5.1 συνοψίζει τα συστατικά, τις ενέργειες και τα παραδοτέα του πλαισίου.

Πίνακας 5.1: Αρχιτεκτονική του προτεινόμενου πλαισίου συμμόρφωσης

Συστατικό	Σκοπός	Κύριες ενέργειες	Παραδοτέο / τεκμήριο
Πεδίο εφαρμογής	Αιτιολόγηση υπαγωγής.	Καταγραφή πηγών· διάκριση άμεσων νομικών και συμβατικών υποχρεώσεων.	Μητρώο εφαρμογής με αιτιολογία.
Υπηρεσίες και εξαρτήσεις	Σύνδεση με τη λειτουργία.	Χαρτογράφηση υπηρεσιών, IT/OT, δεδομένων, εγκαταστάσεων και τρίτων.	Κατάλογος κρίσιμων υπηρεσιών και χάρτης εξαρτήσεων.
Κίνδυνοι και κενά	Ιεράρχηση παρεμβάσεων.	Εκτίμηση πιθανότητας και διακριτών επιπτώσεων· έλεγχος μέτρων και ελλείψεων.	Μητρώο κινδύνων και ανάλυση αποκλίσεων.
Μέτρα και διακυβέρνηση	Υλοποίηση με σαφείς ευθύνες.	Επιλογή, χρηματοδότηση, εγκατάσταση, έλεγχος αλλαγών και κατανομή RACI.	Σχέδιο, τεκμήρια υλοποίησης και κριτήρια δοκιμής.
Περιστατικά και συνέχεια	Έγκαιρες και αιτιολογημένες αποφάσεις.	Κοινά γεγονότα, χωριστή νομική ταξινόμηση, επικοινωνία και ανάκαμψη.	Φάκελος περιστατικού, αναφορές και ανασκόπηση.
Τρίτα μέρη	Έλεγχος εξωτερικών εξαρτήσεων.	Κρισιμότητα, δέουσα επιμέλεια, συμβάσεις, παρακολούθηση και έξοδος.	Φάκελος προμηθευτή και σχέδιο εξόδου.
Τεκμηρίωση και μέτρηση	Αξιολόγηση και διορθώσεις.	Έλεγχος τεκμηρίων, δείκτες, ανασκόπηση και επανέλεγχος.	Μητρώο τεκμηρίων, τιμές με πηγές και αποφάσεις.

Πηγή: Σύνθεση του συγγραφέα βάσει της Οδηγίας (ΕΕ) 2022/2555, του Κανονισμού (ΕΕ) 2016/679, του Κανονισμού (ΕΕ) 2022/2554, του NIST CSF 2.0 και των ISO/IEC 27001:2022 και ISO 31000:2018. Ο πίνακας δεν προέρχεται αυτούσιος από δημοσιευμένο μοντέλο.

5.1.2 Απαιτήσεις σχεδιασμού του πλαισίου

Οι απαιτήσεις σχεδιασμού δεν αποτελούν νέες κανονιστικές υποχρεώσεις. Είναι λειτουργικοί περιορισμοί που προκύπτουν από τη σύνθεση των προβλημάτων των Κεφαλαίων 2–4: κατακερματισμένη κανονιστική κρίση, αποσύνδεση των καταλόγων περιουσιακών στοιχείων από τις υπηρεσίες, περιορισμένη ορατότητα εξαρτήσεων, ασθενής σύνδεση μεταξύ ευρημάτων και διορθώσεων, ασαφής ιδιοκτησία και κλείσιμο ενεργειών χωρίς επαρκή απόδειξη. Οι έξι απαιτήσεις χρησιμοποιούνται ως κριτήρια με τα οποία αιτιολογούνται η αρχιτεκτονική και τα στάδια εφαρμογής.

DR1: Κανονιστικός διαχωρισμός. Κάθε απόφαση υπαγωγής, εφαρμογής, αναφοράς ή αποδοχής τεκμηρίου λαμβάνεται χωριστά για NIS2, GDPR και DORA και συνοδεύεται από τη δική της νομική βάση και αιτιολόγηση.

DR2: Ανάλυση με επίκεντρο την υπηρεσία. Η βασική μονάδα ανάλυσης είναι η επιχειρησιακή υπηρεσία και όχι ο κανονισμός ή ένα μεμονωμένο περιουσιακό στοιχείο, ώστε η τεχνική αξιολόγηση να συνδέεται με επιχειρησιακή επίπτωση.

DR3: Ορατότητα εξαρτήσεων. Κάθε υπηρεσία συνδέεται με συστήματα, δεδομένα, εγκαταστάσεις, διασυνδέσεις και τρίτους, συμπεριλαμβανομένων εξαρτήσεων εκτός των οργανωτικών ορίων.

DR4: Ιχνηλασιμότητα. Κάθε κίνδυνος R συνδέεται με κενό G, διορθωτική ενέργεια A και τεκμήριο E. Οι συνδέσεις διατηρούν υπεύθυνο, ημερομηνία, έκδοση και αιτιολόγηση ώστε να είναι ιχνηλατήσιμη η πορεία από την απαίτηση έως το αποτέλεσμα.

DR5: Ιδιοκτησία και λογοδοσία. Κάθε ανοικτό ζήτημα έχει τουλάχιστον έναν Responsible και έναν Accountable. Η εσωτερική κατανομή RACI οργανώνει την εργασία, αλλά δεν μεταβιβάζει τη νομική ευθύνη της οντότητας ή του υπευθύνου επεξεργασίας.

DR6: Επαλήθευσιμότητα. Καμία ενέργεια δεν θεωρείται ολοκληρωμένη χωρίς προκαθορισμένο κριτήριο αποδοχής και κατάλληλο τεκμήριο. Η ύπαρξη πολιτικής ή διαδικασίας από μόνη της δεν αποδεικνύει λειτουργική αποτελεσματικότητα.

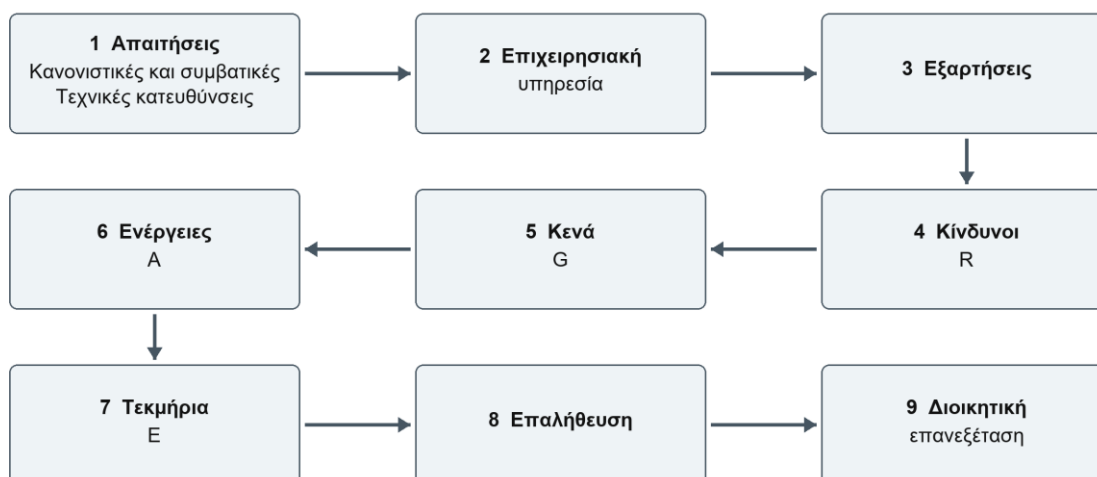
Πίνακας 5.2: Προέλευση των απαιτήσεων σχεδιασμού DR1–DR6

Εύρημα των Κεφαλαίων 2–4	Κύρια τεκμηρίωση	Απαίτηση σχεδιασμού
Διαφορετικά πεδία εφαρμογής, υπόχρεοι, κατώφλια και αφετηρίες αναφοράς.	§§3.2–3.4, 4.2–4.4· Πίνακες 4.1–4.2.	DR1 — Κανονιστικός διαχωρισμός.
Η τεχνική αστοχία αποκτά σημασία μέσω της επίπτωσης στην υπηρεσία.	§§2.2–2.4 και 4.4.1· Πίνακας 2.1.	DR2 — Ανάλυση με επίκεντρο την υπηρεσία.
Κοινές υποδομές και τρίτοι δημιουργούν εξαρτήσεις πέρα από τα οργανωτικά όρια.	§§2.3–2.6 και 4.4.3· Πίνακες 2.2–2.3.	DR3 — Ορατότητα εξαρτήσεων.
Η αντιστοίχιση απαίτησης και μέτρου χρειάζεται συνέχεια μέχρι τη διόρθωση και το τεκμήριο.	§§4.4 και 4.6· Πίνακες 4.3 και 4.5.	DR4 — Ιχνηλασιμότητα R→G→A→E.
Η κοινή πληροφορία δεν αναιρεί τις διακριτές ευθύνες και εξουσιοδοτήσεις.	§§3.2–3.4, 4.4.2 και 4.7.1· Πίνακας 4.1.	DR5 — Ιδιοκτησία και λογοδοσία.
Η ύπαρξη πολιτικής δεν αρκεί για τον έλεγχο λειτουργίας και ολοκλήρωσης.	§§4.4.2 και 4.6· Πίνακας 4.5.	DR6 — Κριτήριο αποδοχής και επαλήθευση.

Πηγή: Σύνθεση του συγγραφέα από τα ευρήματα των Κεφαλαίων 2–4. Οι DR αποτελούν απαιτήσεις του προτεινόμενου σχεδιασμού και δεν εισάγουν νέες νομικές υποχρεώσεις.

Ο Πίνακας 5.2 συνδέει τις απαιτήσεις DR1–DR6 με τα ευρήματα των Κεφαλαίων 2–4. Η σχέση τους με τη ροή εργασίας αποτυπώνεται στο Σχήμα 5.1: οι κανονιστικές και συμβατικές απαιτήσεις και οι τεχνικές κατευθύνσεις συνδέονται με συγκεκριμένη υπηρεσία και τις εξαρτήσεις της, μεταφράζονται σε ελέγξιμη αλυσίδα R→G→A→E και οδηγούν σε επαλήθευση και διοικητική επανεξέταση.

Σχήμα 5.1: Από τις απαιτήσεις και τις τεχνικές κατευθύνσεις στην επαλήθευση και επανεξέταση



Πηγή: Σύνθεση του συγγραφέα βάσει των απαιτήσεων DR1–DR6 και της λογικής $R \rightarrow G \rightarrow A \rightarrow E$ του προτεινόμενου πλαισίου.

5.1.3 Λογική κινδύνου και ιχνηλασιμότητα

Κάθε εγγραφή κινδύνου περιγράφει απειλή ή αστοχία, αδυναμία, επηρεαζόμενη υπηρεσία και πιθανές συνέπειες. Οι επιπτώσεις αποτιμώνται χωριστά για υπηρεσίες και δεδομένα, δικαιώματα φυσικών προσώπων, ασφάλεια προσωπικού ή φορτίου, πελάτες και κανονιστικές ή συμβατικές υποχρεώσεις. Δεν χρησιμοποιείται μέσος όρος που θα μπορούσε να αποκρύψει σοβαρή βλάβη σε μία διάσταση μέσα σε χαμηλή επίπτωση στις υπόλοιπες.

Για την υποθετική εφαρμογή χρησιμοποιείται ποιοτική πιθανότητα: χαμηλή, μέτρια ή υψηλή. Η αιτιολόγηση εξετάζει έκθεση διεπαφών, δικαιώματα πρόσβασης, γνωστές αδυναμίες και αποτελέσματα ελέγχων. Υψηλή πιθανότητα υποστηρίζεται από προσβάσιμη διαδρομή απειλής και ανεπαρκείς δικλίδες· χαμηλή από περιορισμένη έκθεση και ελεγμένα εμπόδια. Οι ενδιαμέσες περιπτώσεις κατατάσσονται ως μέτριες με ρητές παραδοχές. Ελλιπή στοιχεία δηλώνονται ως αβεβαιότητα, όχι ως ένδειξη χαμηλού κινδύνου. Η κλίμακα δεν αποδίδει αριθμητική πιθανότητα.

Η ιχνηλασιμότητα συνδέει απαίτηση, κίνδυνο, κενό, ενέργεια και τεκμήριο με σταθερούς κωδικούς και ελεγχόμενες εκδόσεις. Οι κωδικοί R, G, A και E του Κεφαλαίου 6 χρησιμοποιούνται αντίστοιχα για κινδύνους, κενά, ενέργειες και τεκμήρια. Μια ενέργεια μπορεί να καλύπτει περισσότερα κενά και ένα τεκμήριο περισσότερες απαιτήσεις, με χωριστή αιτιολόγηση. Για κάθε σύνδεση δηλώνονται υπεύθυνος, υπηρεσία, περίοδος κάλυψης, δοκιμή και κριτήριο αποδοχής.

Η εκτίμηση αντικτύπου για την προστασία δεδομένων (DPIA) παραμένει χωριστό, συνδεδεμένο παραδοτέο όταν η επεξεργασία ενδέχεται να επιφέρει υψηλό κίνδυνο κατά το άρθρο 35 GDPR. Εξετάζει και αναγκαιότητα, αναλογικότητα και συνέπειες για τα πρόσωπα, πέρα από την τεχνική ασφάλεια. Η ανάλυση του Gellert (2018) αναδεικνύει τη σημασία της μεθόδου και του είδους κινδύνου που αυτή αξιολογεί. Στον παρόντα σχεδιασμό ο υπεύθυνος επεξεργασίας διατηρεί την απόφαση και ζητά τη συμβουλή του DPO, όπου έχει οριστεί· η εταιρική αποδοχή κινδύνου δεν παρακάμπτει τυχόν υποχρέωση προηγούμενης διαβούλευσης του άρθρου 36.

Η προτεραιότητα τεκμηριώνεται με βάση την πιο σοβαρή εύλογη επίπτωση, την πιθανότητα, την έκταση και τον χρόνο έκθεσης. Ενδείξεις ενεργού εκμετάλλευσης, δυνατότητα διακοπής πολλών κρίσιμων υπηρεσιών ή σοβαρής βλάβης σε πρόσωπα δικαιολογούν άμεση κλιμάκωση. Ακόμη και χαμηλή πιθανότητα μπορεί να απαιτεί υψηλή προτεραιότητα λόγω καταστροφικής συνέπειας. Εσωτερικά όρια και προθεσμίες εγκρίνονται πριν από την εφαρμογή, με αιτιολόγηση κάθε απόκλισης. Δεσμευτικές νομικές απαιτήσεις δεν μετατρέπονται σε προαιρετικές μέσω βαθμολόγησης ή αποδοχής κινδύνου.

5.2 Πεντασταδιακή πορεία εφαρμογής

Η εφαρμογή οργανώνεται σε πέντε στάδια με συγκεκριμένα παραδοτέα και σημεία απόφασης. Η διάρθρωση αποτελεί σύνθεση του συγγραφέα, με αναφορά στη συνεχή διαχείριση κινδύνου του NIST CSF 2.0 και των ISO, και στις πρακτικές εφοδιαστικής αλυσίδας του ENISA (2023). Η απόκριση σε ενεργό περιστατικό δεν περιμένει την ολοκλήρωση των σταδίων. Τα ευρήματά της επιστρέφουν στη χαρτογράφηση, στα μέτρα και στις δοκιμές, όπως συνδέει τη διαχείριση περιστατικών με τη διαχείριση κινδύνου το NIST SP 800-61 Rev. 3 (Nelson et al., 2025).

5.2.1 Στάδιο 1 οριοθέτηση και χαρτογράφηση

Η ομάδα έργου συντάσσει το πεδίο και η αρμόδια διοίκηση το εγκρίνει με εισήγηση των επιχειρησιακών και κανονιστικών λειτουργιών. Για κάθε υπηρεσία αποτυπώνονται ιδιοκτήτης, στόχοι συνέχειας, συστήματα, ροές δεδομένων και τρίτοι. Οι ρόλοι GDPR ελέγχονται ανά επεξεργασία, σύμφωνα με το ποιος καθορίζει σκοπούς και ουσιώδη μέσα. Παραδοτέα είναι το μητρώο εφαρμογής, ο κατάλογος υπηρεσιών και ο χάρτης εξαρτήσεων. Άγνωστα στοιχεία καταχωρίζονται με υπεύθυνο και προθεσμία και δεν αποκλείονται σιωπηρά από το πεδίο.

5.2.2 Στάδιο 2 αξιολόγηση κινδύνων και αποκλίσεων

Με βάση τον χάρτη εξαρτήσεων αναπτύσσονται σενάρια όπως κατάχρηση λογαριασμού συνεργάτη, ransomware σε σύστημα αποθήκης, αλλοίωση δρομολόγησης ή διακοπή cloud. Καταγράφονται η αρχική έκθεση, οι υφιστάμενες δικλίδες και ο υπολειπόμενος κίνδυνος που αυτές τεκμηριωμένα περιορίζουν. Η αναμενόμενη μείωση από μελλοντικό μέτρο καταχωρίζεται χωριστά· δεν παρουσιάζεται ως ήδη επιτευχθείσα.

Η αξιολόγηση κάθε απαίτησης ακολουθεί τις καταστάσεις της §4.6: συμμόρφωση, μερική συμμόρφωση, μη συμμόρφωση ή αιτιολογημένη μη εφαρμογή. Όταν τα στοιχεία δεν επαρκούν, παραμένει «Εκκρεμεί αξιολόγηση». Η ομάδα συνδέει κάθε κενό με συγκεκριμένο κριτήριο και τεκμήριο που λείπει ή αποτυγχάνει. Η διοίκηση εγκρίνει την προτεραιοποίηση και, όπου επιτρέπεται, τεκμηριωμένη προσωρινή αποδοχή υπολειπόμενου κινδύνου με ημερομηνία επανεξέτασης. Η έγκριση δεν νομιμοποιεί παράβαση ή εκπρόθεσμη γνωστοποίηση.

5.2.3 Στάδιο 3 επιλογή μέτρων και σχέδιο αντιμετώπισης

Το τρίτο στάδιο περιλαμβάνει επιλογή και υλοποίηση μέτρων. Κάθε ενέργεια συνδέεται με απαίτηση και κίνδυνο και ορίζει υπεύθυνο, πόρους, εξαρτήσεις, προθεσμία και αναμενόμενο αποτέλεσμα. Οι τεχνικές αλλαγές εγκαθίστανται μέσω ελεγχόμενης διαδικασίας με δυνατότητα επαναφοράς, οι οργανωτικές διαδικασίες τίθενται σε ισχύ και οι συμβατικές δεσμεύσεις επιβεβαιώνονται. Η ολοκλήρωση υλοποίησης τεκμηριώνεται πριν από τον έλεγχο αποτελεσματικότητας του επόμενου σταδίου.

Τα μέτρα μπορεί να περιλαμβάνουν διαχωρισμό καθηκόντων, εκπαίδευση, διαχείριση προσβάσεων, καταγραφή, αντίγραφα, ασφαλείς αλλαγές, τμηματοποίηση δικτύων και συμβατικές ρήτρες. Η προθεσμία εξαρτάται από την έκθεση, την επίπτωση και τα προσωρινά μέτρα. Ενδεικτικός στόχος «κρίσιμες ενημερώσεις εντός 72 ωρών» θα ήταν εσωτερική επιλογή για ορισμένο πεδίο, όχι καθολική απαίτηση των τριών πλαισίων. Το σχέδιο διακρίνει εγκατάσταση, επιτυχή δοκιμή και τελικό κλείσιμο της ενέργειας.

5.2.4 Στάδιο 4 δοκιμή ανθεκτικότητας και ετοιμότητα περιστατικών

Το τέταρτο στάδιο επαληθεύει όσα υλοποιήθηκαν με τεχνικές δοκιμές, ασκήσεις επί χάρτου, ανάκτηση αντιγράφων και επικοινωνία με τρίτους. Η συνέχεια εξετάζεται στο επίπεδο της υπηρεσίας, με αναφορά και στο ISO 22301:2019. Καταγράφονται σενάριο, αναμενόμενο αποτέλεσμα, πραγματικός χρόνος, αποκλίσεις και υπεύθυνος διόρθωσης. Η επιτυχής ανάκτηση ενός αρχείου δεν αρκεί για να αποδειχθεί πλήρης επαναφορά αποθήκης. Αποτυχημένος έλεγχος επιστρέφει στο στάδιο 3 και το κλείσιμο απαιτεί επανέλεγχο.

Το εύρος των δοκιμών προκύπτει από τον κίνδυνο και το εφαρμοστέο δίκαιο. Για DORA διακρίνονται το πρόγραμμα του άρθρου 24, η ειδική στάθμιση πολύ μικρών επιχειρήσεων του άρθρου 25 παράγραφος 3 και οι δοκιμές διείσδυσης βάσει απειλών (TLPT) των επιλεγμένων οντοτήτων του άρθρου 26 και του Κανονισμού 2025/1190. Ένας πάροχος μπορεί να συμμετέχει στο σχετικό μέρος δοκιμής, υπό τους εφαρμοστέους όρους, χωρίς να μετατρέπεται σε χρηματοοικονομική οντότητα. Η ασφαλής εκτέλεση και η διαχείριση επιπτώσεων σε υπηρεσίες προηγούνται της δοκιμής.

5.2.5 Στάδιο 5 μέτρηση, ανασκόπηση και βελτίωση

Στο πέμπτο στάδιο η διοίκηση εξετάζει δείκτες, επαναλαμβανόμενα αίτια, εκκρεμείς διορθώσεις, αστοχίες δοκιμών και αλλαγές εξαρτήσεων. Αποφασίζει για πόρους, επανεξέταση κινδύνων και προσαρμογή μέτρων. Η ανασκόπηση γίνεται στον εγκεκριμένο κύκλο και εκτάκτως μετά από σοβαρό περιστατικό, ουσιώδη αλλαγή, νέο κρίσιμο προμηθευτή ή μεταβολή υποχρεώσεων. Στην υποθετική εφαρμογή αξιολογείται η λογική των αποφάσεων, χωρίς να δηλώνεται αποδεδειγμένη μείωση πραγματικού κινδύνου.

Η απόφαση ανασκόπησης ορίζει ποιο προηγούμενο στάδιο επανεκτελείται και ποιος επιβεβαιώνει το αποτέλεσμα. Νέα υπηρεσία επιστρέφει στην οριοθέτηση, νέα απειλή στην αξιολόγηση και αποτυχημένη δοκιμή στην υλοποίηση. Έτσι η ανασκόπηση παράγει ενέργεια με υπεύθυνο και προθεσμία.

Πίνακας 5.3: Πεντασταδιακή πορεία εφαρμογής και σημεία απόφασης

Στάδιο	Είσοδοι	Εργασία και υπεύθυνοι	Κριτήριο μετάβασης
1. Οριοθέτηση και χαρτογράφηση	Πηγές, συμβάσεις, υπηρεσίες, συστήματα και δεδομένα.	Η ομάδα συντάσσει πεδίο και εξαρτήσεις· η διοίκηση εγκρίνει με αρμόδιες εισηγήσεις.	Εγκεκριμένο πεδίο, ρόλοι και κατάλογος υπηρεσιών· άγνωστα στοιχεία με υπεύθυνο.
2. Κίνδυνοι και αποκλίσεις	Χάρτης εξαρτήσεων, σενάρια και τεκμήρια υφιστάμενων μέτρων.	Ιδιοκτήτες κινδύνου και ασφάλεια εκτιμούν συνέπειες, πιθανότητα, κενά και αβεβαιότητα.	Αιτιολογημένη προτεραιοποίηση· διάκριση πραγματικού και αναμενόμενου υπολειπόμενου κινδύνου.
3. Μέτρα και αντιμετώπιση	Κενά, απαιτήσεις, πόροι και περιορισμοί.	Εξουσιοδοτημένοι ιδιοκτήτες εγκρίνουν σχέδιο· οι ομάδες υλοποιούν αλλαγές και διαδικασίες.	Διαθέσιμα τεκμήρια υλοποίησης, υπεύθυνος και κριτήριο δοκιμής για κάθε ενέργεια.

Στάδιο	Είσοδοι	Εργασία και υπεύθυνοι	Κριτήριο μετάβασης
4. Δοκιμή και ετοιμότητα	Υλοποιημένα μέτρα, σενάρια, σχέδια και επαφές.	Ομάδα δοκιμής επαληθεύει λειτουργία και αποτέλεσμα· ιδιοκτήτης υπηρεσίας αξιολογεί αποκλίσεις.	Επιτυχής έλεγχος ή επιστροφή στο στάδιο 3. Τυχόν αποδοχή κινδύνου εντός νομικών ορίων.
5. Μέτρηση και βελτίωση	Δείκτες, ευρήματα, περιστατικά και αλλαγές.	Η διοίκηση αποφασίζει για πόρους, προτεραιότητες και επανεξέταση.	Απόφαση με υπεύθυνο, προθεσμία και συγκεκριμένο στάδιο επανεκτέλεσης.

Πηγή: Σύνθεση του συγγραφέα, με εννοιολογική αναφορά στο NIST CSF 2.0, στο ISO/IEC 27001:2022, στο ISO/IEC 27005:2022 και στις καλές πρακτικές της ENISA (2023). Η ακολουθία δεν αποτελεί επίσημο μοντέλο ωριμότητας ούτε έχει εμπειρικά επικυρωθεί.

5.3 Διαχείριση κινδύνου τρίτων και εφοδιαστικής αλυσίδας

5.3.1 Κρισιμότητα και δέουσα επιμέλεια

Η ενιαία εξέταση τεχνικών κινδύνων και σχέσεων προμήθειας ακολουθεί τη διεπιστημονική θεώρηση του Boyson (2014), η οποία συνδέει κυβερνοασφάλεια, εφοδιαστική και εταιρική διαχείριση κινδύνου. Για κάθε τρίτο εξετάζονται η υποστηριζόμενη υπηρεσία, η πρόσβαση, τα δεδομένα, οι υπεργολάβοι, η δυνατότητα αντικατάστασης και η συγκέντρωση σε κοινή υποδομή. Η πιστοποίηση αποτελεί στοιχείο αξιολόγησης με συγκεκριμένο εύρος, όχι γενική εγγύηση ασφάλειας.

Ως κρίσιμος προμηθευτής στο προτεινόμενο πλαίσιο χαρακτηρίζεται εκείνος του οποίου η αστοχία ή παραβίαση μπορεί να επιφέρει σοβαρή επίπτωση σε κρίσιμη υπηρεσία ή δεδομένα, ιδίως χωρίς έγκαιρη εναλλακτική. Πρόκειται για εσωτερική κατηγορία κινδύνου, διαφορετική από τον επίσημο χαρακτηρισμό κρίσιμου παρόχου ΤΠΕ κατά DORA. Η αρχική διαβάθμιση καθορίζει το βάθος δέουσας επιμέλειας και αναθεωρείται με τα ευρήματα. Για κρίσιμους τρίτους εξετάζονται έλεγχοι ασφάλειας, συνέχεια, περιστατικά, υπεργολάβοι, τοποθεσία δεδομένων, βιωσιμότητα και έξοδος.

Η εισήγηση καταγράφει ελλείψεις, εναλλακτικά τεκμήρια, προσωρινά μέτρα και υπολειπόμενο κίνδυνο. Ο εξουσιοδοτημένος ιδιοκτήτης αποφασίζει για αποδοχή, απόρριψη ή όρους συνεργασίας, με κανονιστικό έλεγχο όπου απαιτείται. Έκθεση ανεξάρτητου ελέγχου ή περιορισμένη επίδειξη μπορεί να υποκαθιστά μη διαθέσιμη πληροφορία μόνο εφόσον καλύπτει το ζητούμενο αντικείμενο. Απλή βεβαίωση προμηθευτή δεν εξομοιώνεται με ανεξάρτητη επαλήθευση· η υπολειπόμενη αβεβαιότητα καταγράφεται.

5.3.2 Σύμβαση, ένταξη και κατανομή ευθυνών

Οι συμβατικοί όροι επιλέγονται ανά υπηρεσία, ρόλο και εφαρμοστέα απαίτηση. Μπορούν να καλύπτουν επίπεδα υπηρεσίας (SLA), πρόσβαση, αλλαγές, ειδοποίηση περιστατικών, στοιχεία διερεύνησης, συνέχεια, έλεγχο, υπεργολαβία και έξοδο. Ο προτεινόμενος κατάλογος δεν αποτελεί ενιαίο νομικά υποχρεωτικό υπόδειγμα για όλους τους προμηθευτές. Ο χρόνος συμβατικής ενημέρωσης σχεδιάζεται ώστε να αφήνει χρόνο αξιολόγησης στον πελάτη και δεν επιτρέπει αναμονή όταν το εφαρμοστέο δίκαιο απαιτεί ενημέρωση χωρίς αδικαιολόγητη καθυστέρηση.

Οι ρόλοι GDPR προκύπτουν από τον πραγματικό καθορισμό σκοπών και ουσιωδών μέσων ανά επεξεργασία. Για εκτελούντα εφαρμόζεται το άρθρο 28 και, σε παραβίαση, η ενημέρωση του υπευθύνου κατά το άρθρο 33 παράγραφος 2. Αυτοτελείς υπεύθυνοι διατηρούν τις δικές τους υποχρεώσεις, ενώ για από κοινού καθορισμό σκοπών και μέσων εξετάζεται το άρθρο 26. Τυχόν διαβίβαση σε τρίτη χώρα αξιολογείται επιπλέον κατά το Κεφάλαιο V. Η γενική ρήτρα ασφάλειας δεν υποκαθιστά αυτές τις ειδικές απαιτήσεις.

Για χρηματοοικονομικό πελάτη προηγείται έλεγχος αν παρέχεται υπηρεσία ΤΠΕ κατά το άρθρο 3 σημείο 21 DORA. Τότε εξετάζονται οι απαιτήσεις των άρθρων 28–30 και οι πρόσθετοι όροι για κρίσιμες ή σημαντικές λειτουργίες. Σε αμιγώς φυσική υπηρεσία logistics, τυχόν αυστηρές απαιτήσεις ασφάλειας ή ενημέρωσης παραμένουν συμβατικές, χωρίς αυτόματη εφαρμογή του καθεστώτος συμβάσεων ΤΠΕ. Το μητρώο πληροφοριών DORA τηρείται από τη χρηματοοικονομική οντότητα για τις σχετικές συμβατικές ρυθμίσεις· η δική της ευθύνη δεν μεταβιβάζεται στον προμηθευτή.

5.3.3 Παρακολούθηση, αλλαγή και έξοδος

Μετά την ένταξη, η παρακολούθηση βασίζεται στην κρισιμότητα και στα γεγονότα. Περιλαμβάνει συμφωνημένους δείκτες υπηρεσίας και ασφάλειας, λήξη πιστοποιήσεων ή εκθέσεων, ευρήματα, περιστατικά, αλλαγές ιδιοκτησίας ή υποκατασκευαστών και αποκλίσεις από τα σχέδια αποκατάστασης. Μια ετήσια επαναξιολόγηση μπορεί να είναι κατάλληλη για συγκεκριμένη κατηγορία, αλλά δεν αρκεί όταν ενδιάμεσα έχει αλλάξει ουσιωδώς η υπηρεσία ή το προφίλ απειλής.

Το σχέδιο εξόδου ορίζει εναλλακτική υπηρεσία ή προσωρινή λειτουργία, επιστροφή δεδομένων, ανάκληση προσβάσεων και επιβεβαίωση μετάβασης. Η διαγραφή συνδέεται με τις εφαρμοστέες υποχρεώσεις διατήρησης και με ελεγχόμενη διαχείριση αντιγράφων ασφαλείας. Η τεχνική δυνατότητα εξαγωγής δεδομένων δοκιμάζεται όπου δικαιολογείται από την κρισιμότητα. Η συμβατική δυνατότητα καταγγελίας από μόνη της δεν αποδεικνύει ότι η υπηρεσία μπορεί να αντικατασταθεί έγκαιρα.

Ο Πίνακας 5.4 οργανώνει τους ελέγχους, τις αποφάσεις και τα τεκμήρια ανά φάση συνεργασίας με κρίσιμο τρίτο.

Πίνακας 5.4: Κύκλος ζωής ελέγχου κρίσιμων τρίτων

Φάση	Προτεινόμενοι έλεγχοι	Υπεύθυνος / απόφαση	Κύριο τεκμήριο
Σχεδιασμός ανάγκης	Υπηρεσία που υποστηρίζεται, δεδομένα, πρόσβαση, εναλλακτικές, ανοχή διακοπής και συγκέντρωση.	Επιχειρησιακός ιδιοκτήτης με ασφάλεια, προμήθειες και προστασία δεδομένων.	Δελτίο κρισιμότητας και απαιτήσεων προμήθειας.
Δέουσα επιμέλεια	Διακυβέρνηση, ανεξάρτητα τεκμήρια, ευπάθειες, πρόσβαση, συνέχεια, περιστατικά, υπεργολάβοι και τοποθεσία δεδομένων.	Ασφάλεια εισηγείται· εξουσιοδοτημένος ιδιοκτήτης εγκρίνει ή απορρίπτει εντός νομικών ορίων.	Έκθεση αξιολόγησης, ελλείψεις και αποδοχή υπολειπόμενου κινδύνου.
Σύμβαση	SLA, ασφάλεια, ενημέρωση, έλεγχοι, υπεργολάβοι και έξοδος, ανά υπηρεσία και νομικό ρόλο.	Νομική υπηρεσία και προμήθειες, με έγκριση των αρμόδιων ιδιοκτητών.	Υπογεγραμμένη σύμβαση και πίνακας αντιστοίχισης όρων.
Ένταξη	Ελάχιστα δικαιώματα, κατάλληλη ταυτοποίηση, ασφαλής διασύνδεση, καταγραφή και δοκιμή επαφών.	Τεχνικός ιδιοκτήτης και υπεύθυνος υπηρεσίας.	Πρωτόκολλο ένταξης και αποδοχής παραγωγικής λειτουργίας.
Έλεγχος και αλλαγές	Δείκτες, τεκμήρια, ευρήματα, περιστατικά, ουσιώδεις αλλαγές και λήξη πιστοποιήσεων.	Ιδιοκτήτης υπηρεσίας· κλιμάκωση στο εξουσιοδοτημένο όργανο όταν υπερβαίνεται η ανοχή.	Περιοδική κάρτα προμηθευτή και σχέδιο διορθώσεων.

Φάση	Προτεινόμενοι έλεγχοι	Υπεύθυνος / απόφαση	Κύριο τεκμήριο
Περιστατικό	Άμεση επαφή, κοινά πραγματικά στοιχεία, διατήρηση τεκμηρίων, ανάκαμψη και υποστήριξη γνωστοποίησης.	Διαχειριστής περιστατικού· οι νομικές αποφάσεις παραμένουν στον αρμόδιο φορέα.	Χρονολόγιο, ανταλλαγές ενημέρωσης και φάκελος περιστατικού.
Έξοδος	Δοκιμή μετάβασης, επιστροφή δεδομένων, νόμιμη διαγραφή/διατήρηση, ανάκληση πρόσβασης και επαλήθευση.	Ιδιοκτήτης υπηρεσίας με IT, ασφάλεια, νομική υπηρεσία και προμήθειες.	Πρακτικό εξόδου και αποδεικτικό ολοκλήρωσης.

Πηγή: Πρόταση του συγγραφέα κύκλου ζωής βάσει NIS2, άρθρο 21(2)(δ-ε) και 21(3)· GDPR, άρθρο 28· DORA, άρθρα 28–30· ENISA (2023) και NIST SP 800-161 Rev. 1, Update 1 (Boyens et al., 2024). Το εύρος των ελέγχων προσαρμόζεται στη σχέση και στο πεδίο εφαρμογής.

5.4 Ενιαία ροή διαχείρισης περιστατικών με χωριστούς νομικούς κλάδους

5.4.1 Λειτουργικά ερωτήματα ταξινόμησης περιστατικού

Για κάθε περιστατικό εφαρμόζονται τα κριτήρια της §4.3 και καταγράφονται τρεις αποφάσεις, όπου τα αντίστοιχα πλαίσια αφορούν την οντότητα: υπαγωγή και πραγματική ή δυνητική σημαντικότητα κατά NIS2· παραβίαση προσωπικών δεδομένων, ρόλος και κίνδυνος για άτομα κατά GDPR· ύπαρξη και ταξινόμηση συμβάντος ΤΠΕ στη χρηματοοικονομική οντότητα κατά DORA. Η μη εφαρμογή κλάδου αιτιολογείται. Η τεχνική αντιμετώπιση αρχίζει παράλληλα, ανεξάρτητα από την απόφαση εξωτερικής αναφοράς.

5.4.2 Κοινό επιχειρησιακό αρχείο και κατανομή ρόλων

Το κοινό αρχείο συγκεντρώνει γεγονότα για κάθε οντότητα: πρώτο σήμα, επηρεαζόμενες υπηρεσίες και δεδομένα, διάρκεια, έκταση, επιπτώσεις, τρίτους και μέτρα περιορισμού. Κάθε εγγραφή έχει ώρα, ζώνη ώρας, πηγή και χαρακτηρισμό ως επιβεβαιωμένο στοιχείο, εκτίμηση ή άγνωστο. Οι νομικές αφετηρίες γνώσης καταγράφονται χωριστά ανά κλάδο. Το κοινό χρονολόγιο δεν επιβάλλει ίδιο χρόνο γνώσης σε προμηθευτή και πελάτη· κάθε μέρος τεκμηριώνει τη δική του απόφαση.

Ο διαχειριστής περιστατικού συντονίζει την απόκριση, ενώ οι τεχνικές ομάδες καταγράφουν γεγονότα και περιορίζουν τη βλάβη. Ο επιχειρησιακός ιδιοκτήτης εγκρίνει τις προτεραιότητες ανάκαμψης εντός της εξουσιοδότησής του. Η ασφάλεια και η νομική λειτουργία εισηγούνται για τη NIS2, ο υπεύθυνος επεξεργασίας αποφασίζει για GDPR με ανεξάρτητη συμβουλή DPO όπου έχει οριστεί, και η αρμόδια λειτουργία της χρηματοοικονομικής οντότητας αποφασίζει για DORA. Ο προμηθευτής παρέχει στοιχεία και εκπληρώνει τις δικές του υποχρεώσεις.

Η κατανομή RACI εξειδικεύεται πριν από περιστατικό: η τεχνική ομάδα είναι εκτελούσα για περιορισμό, ο ιδιοκτήτης υπηρεσίας υπόλογος για την επιχειρησιακή επαναφορά και ο εξουσιοδοτημένος κανονιστικός αποφασίζων υπόλογος για κάθε αναφορά. Ο DPO συμβουλεύει και η διοίκηση ενημερώνεται βάσει κριτηρίων κλιμάκωσης. Ορίζονται χωριστά υποβάλλον, αναπληρωτής και εναλλακτικό κανάλι επικοινωνίας, με δοκιμασμένη πρόσβαση στην πλατφόρμα υποβολής. Η απουσία στελέχους ή η αναμονή συνεδρίασης δεν αναστέλλει προθεσμία. Για κρίσιμες υπηρεσίες προβλέπεται κάλυψη επικοινωνίας εκτός ωραρίου.

Η κοινή απόκριση και οι χωριστές υποχρεώσεις αξιολόγησης και αναφοράς συνοψίζονται στον Πίνακα 5.5.

Πίνακας 5.5: Ενιαία ροή περιστατικού και χωριστές υποχρεώσεις αξιολόγησης/αναφοράς

Βήμα και υπόχρεος	Απόφαση ή ενέργεια	Χρονικός κανόνας	Τεκμήριο και επανεξέταση
Κοινή απόκριση ανά οντότητα	Διαχειριστής και τεχνικές ομάδες περιορίζουν το συμβάν και συλλέγουν γεγονότα.	Άμεση έναρξη· δεν αναμένει νομική ταξινόμηση.	Αναγνωριστικό, χρονολόγιο, πηγές και αβεβαιότητες.
NIS2· υπαγόμενη οντότητα	Εξουσιοδοτημένος ρόλος αποφασίζει για σημαντικότητα και αναφορά σε CSIRT ή αρχή.	Χωρίς αδικαιολόγητη καθυστέρηση· όρια 24/72 ωρών από γνώση σημαντικού περιστατικού. Ειδικό 24ωρο γνωστοποίησης για υπηρεσίες εμπιστοσύνης.	Κριτήρια, ώρα γνώσης, αποφασίζων και αποδεικτικά υποβολής· νέες επιπτώσεις επανεξετάζονται.
GDPR· εκτελών	Ενημερώνει τον υπεύθυνο όταν λάβει γνώση παραβίασης.	Χωρίς αδικαιολόγητη καθυστέρηση· δεν διαθέτει δικό του περιθώριο 72 ωρών.	Ωρα γνώσης και ενημέρωσης, διαθέσιμα στοιχεία και συμπληρώσεις.
GDPR· υπεύθυνος	Αποφασίζει για γνωστοποίηση στην αρχή με αξιολόγηση κινδύνου για άτομα.	Χωρίς αδικαιολόγητη καθυστέρηση, ει δυνατόν εντός 72 ωρών από γνώση παραβίασης.	Κίνδυνος, αιτιολογία γνωστοποίησης ή μη· υποβολή και εξήγηση τυχόν καθυστέρησης.
DORA· χρηματοοικ. οντότητα	Η αρμόδια λειτουργία ταξινομεί το συμβάν ΤΠΕ και αναφέρει αν είναι μείζον.	Αρχική: το συντομότερο, έως 4 ώρες από ταξινόμηση και 24 από γνώση. Αν ταξινομηθεί μετά το 24ωρο: έως 4 ώρες από ταξινόμηση.	Χωριστές ώρες γνώσης και ταξινόμησης· κριτήρια, υποβολή και πληροφορίες από πάροχο.
Ενημέρωση προσώπων και πελατών	Χωριστός έλεγχος NIS2, άρθρου 23, GDPR, άρθρου 34 και DORA, άρθρου 19(3).	Κατά περίπτωση, χωρίς αδικαιολόγητη καθυστέρηση· χωρίς αναμονή της προθεσμίας προς αρχή.	Αποδέκτες, εφαρμοστέο κατώφλι, εξαιρέσεις, εγκρίσεις και αποστολή.
Συμπληρώσεις και τελικές αναφορές	Ο υπόχρεος κάθε κλάδου επικαιροποιεί στοιχεία και παρακολουθεί εκκρεμότητες.	NIS2: τελική σε μήνα από γνωστοποίηση ή, αν συνεχίζεται η διαχείριση, σε μήνα από ολοκλήρωσή της. DORA: ενδιάμεση σε 72 ώρες από αρχική· τελική σε μήνα από ενδιάμεση ή τελευταία επικαιροποίηση.	NIS2: έκθεση προόδου αν συνεχίζεται η διαχείριση. DORA: ενδιάμεση και χωρίς μεταβολή· ενημέρωση κατά την αποκατάσταση. GDPR: σταδιακή συμπλήρωση και αρχείο παραβίασης.
Μετά την αποκατάσταση	Ιδιοκτήτες υπηρεσίας, ασφάλεια και αρμόδιες λειτουργίες αναθεωρούν μέτρα και σχέδια.	Κύκλος ανασκόπησης και εφαρμοστέες προθεσμίες παραμένουν χωριστά.	Αίτια, διορθώσεις, υπεύθυνοι και δοκιμή κλεισίματος.

Πηγή: Οργάνωση από τον συγγραφέα της ροής βάσει NIS2, άρθρο 23· GDPR, άρθρα 4(12), 33–34· DORA, άρθρα 3 και 17–20· Κανονισμοί 2024/1772, 2025/301 και 2025/302· EDPB (2023). Ο πίνακας αποτελεί οδηγό ενεργειών· οι ειδικοί όροι και εξαιρέσεις αναπτύσσονται στα Κεφάλαια 3–4.

5.4.3 Διακυβέρνηση των προθεσμιών και ποιότητα της απόφασης

Το αρχείο προθεσμιών αποθηκεύει οντότητα, κλάδο, νομική βάση, γεγονός έναρξης, ώρα γνώσης, τυχόν ώρα ταξινόμησης, καταληκτική ώρα και υποβολή. Για NIS2 οι 24 και 72 ώρες έχουν την ίδια αφετηρία γνώσης σημαντικού περιστατικού. Για GDPR η αφετηρία αφορά τη γνώση παραβίασης από τον υπεύθυνο. Για DORA διακρίνονται γνώση συμβάντος, ταξινόμηση ως μείζονος και χρόνοι προηγούμενων αναφορών.

Ο υπολογισμός αυτοματοποιείται μόνο μετά την επιβεβαίωση του σωστού κλάδου και των ειδικών κανόνων· οι εξαιρέσεις αργιών δεν εφαρμόζονται γενικά σε όλες τις οντότητες ή αναφορές.

Αρχική αναφορά μπορεί να περιλαμβάνει διαθέσιμα στοιχεία και να συμπληρώνεται όπως προβλέπει το αντίστοιχο καθεστώς. Το αρχείο διατηρεί την αρχική εκτίμηση και κάθε αναθεώρηση, χωρίς αντικατάσταση της προηγούμενης ώρας γνώσης. Απόφαση μη γνωστοποίησης αναφέρει κριτήρια, στοιχεία, αποφασίζοντας και χρόνο, μαζί με συγκεκριμένο έναυσμα επανεξέτασης, όπως νέα κατηγορία δεδομένων ή μεγαλύτερη έκταση. Το αριθμητικό υπόλοιπο μιας προθεσμίας δεν αποτελεί άδεια αναμονής όταν απαιτείται ενέργεια χωρίς αδικαιολόγητη καθυστέρηση.

Η επικοινωνία οργανώνεται ανά αποδέκτη και νομική βάση. Η γνωστοποίηση στην αρχή, η υποχρεωτική ενημέρωση υποκειμένων ή αποδεκτών υπηρεσιών και η συμβατική ενημέρωση πελάτη έχουν διαφορετικό περιεχόμενο και χρόνο. Οι ενημερώσεις υψηλού κινδύνου GDPR μπορούν να απαιτούνται πριν από οποιοδήποτε όριο 72 ωρών. Για κάθε μήνυμα ορίζονται εγκρίνων, κανάλι, αναγκαίο περιεχόμενο και τρόπος συμπλήρωσης, με περιορισμό πρόσβασης σε προσωπικά δεδομένα και στοιχεία διερεύνησης.

5.5 Πλαίσιο τεκμηρίωσης και διασφάλισης

Για κάθε μέτρο ορίζονται από τον σχεδιασμό το τεκμήριο, η περίοδος κάλυψης και το κριτήριο αποδοχής. Η πολιτική αποτυπώνει τον σχεδιασμό, τα αρχεία εκτέλεσης τη λειτουργία και η δοκιμή το αποτέλεσμα σε καθορισμένο σενάριο. Παλαιά έγκριση ή μεμονωμένο στιγμιότυπο δεν αποδεικνύει συνεχή εφαρμογή. Ο έλεγχος εξετάζει επίσης πληρότητα συστημάτων, συγχρονισμό ώρας και δυνατότητα σύνδεσης του ευρήματος με την εξεταζόμενη απαίτηση.

Το μητρώο τεκμηρίων περιλαμβάνει κωδικούς απαίτησης και ελέγχου, ιδιοκτήτη, αποθετήριο, περίοδο, έκδοση, έγκριση, εμπιστευτικότητα και επόμενη επανεξέταση. Ορίζονται δικαιώματα πρόσβασης και τρόπος προστασίας της ακεραιότητας. Για στοιχεία περιστατικού καταγράφονται προέλευση, συλλογή, μεταβιβάσεις και, όπου ενδείκνυται, ψηφιακό αποτύπωμα. Η διάρκεια διατήρησης συνδέεται με συγκεκριμένο σκοπό, νομική ή συμβατική υποχρέωση και ανάγκη διερεύνησης, συνεκτιμώντας τον περιορισμό αποθήκευσης GDPR. Δεν επιβάλλεται αυθαίρετος ενιαίος χρόνος για όλα τα αρχεία.

Η διασφάλιση ελέγχει σχεδιασμό, λειτουργία και αποτέλεσμα. Όταν χρησιμοποιείται δείγμα, δηλώνονται πληθυσμός, περίοδος, μέθοδος επιλογής και όρια του συμπεράσματος· λίγες επιτυχείς περιπτώσεις δεν αποδεικνύουν πλήρη κάλυψη. Ο επανέλεγχος γίνεται, όπου είναι εφικτό, από πρόσωπο διαφορετικό από τον υλοποιητή, με τήρηση ειδικών απαιτήσεων ανεξαρτησίας. Το εύρημα κλείνει μόνο όταν το τεκμήριο ικανοποιεί το κριτήριο, διαφορετικά παραμένει ανοικτό ή κλιμακώνεται.

Ο Πίνακας 5.6 συνδέει κάθε περιοχή ελέγχου με υπεύθυνο, τεκμήρια και κριτήριο ποιότητας.

Πίνακας 5.6: Αφετηρία τεκμηρίων και ελέγχου ποιότητας

Περιοχή	Υπεύθυνος	Τεκμήρια	Έναυσμα ελέγχου	Κριτήριο ποιότητας
Πεδίο και υπηρεσίες	Διοίκηση και επιχειρησιακοί ιδιοκτήτες	Μητρώο εφαρμογής, κατάλογος υπηρεσιών, RTO/RPO, χάρτης εξαρτήσεων.	Προτεινόμενος ετήσιος έλεγχος και σε ουσιαστική αλλαγή· έλεγχος ειδικών υποχρεώσεων.	Συμφωνία με πραγματικές ροές και συμβάσεις· δειγματοληπτική επιβεβαίωση ιδιοκτητών.

Περιοχή	Υπεύθυνος	Τεκμήρια	Έναυσμα ελέγχου	Κριτήριο ποιότητας
Κίνδυνοι και μέτρα	Ιδιοκτήτες κινδύνου και ασφάλεια	Σενάρια, αιτιολογημένη κατάταξη, αποδοχές, υλοποίηση και αποτελέσματα δοκιμών.	Αλλαγή απειλής ή υπηρεσίας, περιστατικό ή ανασκόπηση διοίκησης.	Ιχνηλασιμότητα απαίτησης–κινδύνου–μέτρου–αποτελέσματος.
Ταυτότητες και πρόσβαση	IT και ιδιοκτήτες εφαρμογών	Εγκρίσεις, κατάλογοι δικαιωμάτων, logs, περιοδικές επανεξετάσεις, ανακλήσεις.	Με βάση την κρισιμότητα και σε πρόσληψη, μετακίνηση ή αποχώρηση.	Δείγμα χρηστών, ορφανά/υπερβολικά δικαιώματα, έγκαιρη ανάκληση και κάλυψη συστημάτων.
Αντίγραφα και ανάκαμψη	IT και ιδιοκτήτης υπηρεσίας	Αναφορές αντιγράφων, δοκιμές επαναφοράς, χρόνοι ανάκαμψης, σφάλματα και διορθώσεις.	Σύμφωνα με το σχέδιο δοκιμών και μετά από σημαντική αλλαγή.	Ανάκτηση υπηρεσίας/δεδομένων στο συμφωνημένο εύρος: χρόνος, RPO και ακεραιότητα.
Τρίτα μέρη	Προμήθειες και ιδιοκτήτης υπηρεσίας	Δέουσα επιμέλεια, σύμβαση, εκθέσεις ελέγχου, KPI/SLA, αλλαγές και σχέδιο εξόδου.	Με βάση τη διαβάθμιση, σε λήξη τεκμηρίου, συμβάν ή ουσιώδη αλλαγή.	Επικαιρότητα, κάλυψη κρίσιμων υπηρεσιών, κλείσιμο ευρημάτων και δυνατότητα εξόδου.
Περιστατικά	Διαχειριστής περιστατικού και αρμόδιοι νομικοί ρόλοι	Χρονολόγιο, αποφάσεις ταξινόμησης, γνωστοποιήσεις, επικοινωνίες, τεχνικά ευρήματα και διδάγματα.	Σε κάθε περιστατικό και άσκηση· ανασκόπηση μετά την αποκατάσταση.	Χρόνοι ανά κλάδο, πηγές, αποφασίζων, υποβολή και επανεξέταση μη αναφοράς.
Διοίκηση	Διοίκηση και λειτουργίες ελέγχου	Πρακτικά, εγκρίσεις κινδύνου, προϋπολογισμός, δείκτες, ευρήματα και αποφάσεις.	Προκαθορισμένη ανασκόπηση και έκτακτη κλιμάκωση.	Οι αποφάσεις έχουν ιδιοκτήτη, προθεσμία, πόρους και επιβεβαιωμένη ολοκλήρωση.

Πηγή: Σύνθεση του συγγραφέα βάσει της αρχής λογοδοσίας του GDPR, των απαιτήσεων διαχείρισης κινδύνου και εποπτείας της NIS2 και του DORA, καθώς και των ISO/IEC 27001:2022 και NIST CSF 2.0. Οι συχνότητες αποτελούν πλαίσιο απόφασης και όχι ενιαίες νομοθετικές προθεσμίες.

5.6 Δείκτες και διοικητική αναφορά

5.6.1 Αρχές επιλογής και ερμηνείας

Οι δείκτες έχουν αξία όταν οδηγούν σε απόφαση. Το πλήθος των συμβάντων, για παράδειγμα, μπορεί να αυξηθεί επειδή βελτιώθηκε η ανίχνευση και όχι επειδή μειώθηκε η ασφάλεια. Αντίστοιχα, ένα υψηλό ποσοστό ολοκλήρωσης εκπαίδευσης δεν αποδεικνύει από μόνο του ότι το προσωπικό αναγνωρίζει μια ύποπτη ενέργεια. Για τον λόγο αυτό το πλαίσιο συνδυάζει δείκτες κάλυψης, χρόνου, ποιότητας και αποτελέσματος και συνοδεύει κάθε τιμή με ερμηνευτικό σχόλιο.

Κάθε δείκτης έχει ιδιοκτήτη, τύπο, μονάδα, πηγή, πληθυσμό, περίοδο και κανόνες εξαιρέσεων. Στα ποσοστά εμφανίζονται αριθμητής και παρονομαστής μαζί με την τιμή. Μηδενικός παρονομαστής δηλώνεται «Δεν εφαρμόζεται για την περίοδο», ενώ ελλιπή δεδομένα «Δεν υπολογίζεται», με περιγραφή του κενού. Καμία

από τις δύο περιπτώσεις δεν μετατρέπεται σε 0% ή 100%. Οι αλλαγές πεδίου και προθεσμιών διατηρούν ιστορικό, ώστε η βελτίωση του δείκτη να μην προκύπτει από αφαίρεση δύσκολων περιπτώσεων.

Οι χρόνοι παρουσιάζονται ανά υπηρεσία, σοβαρότητα και νομικό κλάδο, με σαφές αρχικό και τελικό γεγονός. Για επαρκές δείγμα αναφέρονται διάμεσος και 90ό εκατοστημόριο, μαζί με πλήθος παρατηρήσεων και σταθερή μέθοδο υπολογισμού· σε μικρό δείγμα εμφανίζονται οι επιμέρους χρόνοι και το μέγιστο. Οι μη ολοκληρωμένες υποθέσεις καταγράφονται χωριστά με την τρέχουσα ηλικία τους, ώστε να μην εξαφανίζονται από τη μέτρηση. Οι εσωτερικοί στόχοι εγκρίνονται βάσει κινδύνου και αρχικής γραμμής βάσης· τα νομικά όρια αντλούνται από το εφαρμοστέο καθεστώς.

Οι ορισμοί, οι πηγές και οι περιορισμοί των K1–K8 συγκεντρώνονται στον Πίνακα 5.7.

Πίνακας 5.7: Λεξικό βασικών δεικτών του πλαισίου

Δείκτης	Ορισμός και τύπος	Πηγή, υπεύθυνος και κύκλος	Ερμηνεία και περιορισμός
K1 Κάλυψη κρίσιμων υπηρεσιών	Υπηρεσίες με ιδιοκτήτη, RTO/RPO και ελεγμένο χάρτη εξαρτήσεων ÷ σύνολο κρίσιμων υπηρεσιών × 100.	Κατάλογος υπηρεσιών· ιδιοκτήτες υπηρεσιών· μηνιαία στην αρχική χαρτογράφηση, έπειτα τριμηνιαία.	Στιγμιότυπο στο τέλος περιόδου. Δεν αποδεικνύει εφικτότητα RTO/RPO.
K2 Εμπρόθεσμο κλείσιμο ενεργειών υψηλής προτεραιότητας	Ενέργειες με αρχική προθεσμία μέσα στην περίοδο που έκλεισαν με επαλήθευση έως αυτήν ÷ όλες τις ενέργειες υψηλής προτεραιότητας με αρχική προθεσμία στην ίδια περίοδο × 100.	Μητρώο ενεργειών· ιδιοκτήτης σχεδίου αντιμετώπισης· μηνιαία.	Οι παρατάσεις δεν αλλάζουν την αρχική προθεσμία. Προβάλλονται χωριστά ληξιπρόθεσμα προηγούμενων περιόδων και ηλικία τους.
K3 Κάλυψη κρίσιμων τρίτων	Κρίσιμοι τρίτοι με επίκαιρο και αποδεκτό σύνολο τεκμηρίων ÷ σύνολο κρίσιμων τρίτων × 100.	Φάκελοι προμηθευτών· προμήθειες με ασφάλεια· μηνιαία ή τριμηνιαία.	Αποδοχή με κριτήριο υπηρεσίας, εύρους και περιόδου. Δεν μετρά απόλυτη ασφάλεια.
K4 Χρόνος πρώτης απόφασης	Χρόνος πρώτης τεκμηριωμένης απόφασης ανά νομικό κλάδο μείον πρώτο καταγεγραμμένο σήμα του συμβάντος στην οντότητα.	Αρχείο περιστατικών· διαχειριστής και κανονιστική λειτουργία· ανά περιστατικό και τρίμηνο.	Εσωτερικός χρόνος, όχι νομική αφετηρία γνώσης. Οι μεταγενέστερες αναθεωρήσεις διατηρούνται χωριστά.
K5 Περιθώριο γνωστοποίησης	Καταληκτική ημερομηνία/ώρα μείον ημερομηνία/ώρα υποβολής, σε ώρες, ανά υπόχρεο, κλάδο και στάδιο.	Αρχείο προθεσμιών και αποδεικτικό υποβολής· αρμόδιος υποβάλλων· ανά αναφορά.	Αρνητικό: υπέρβαση αριθμητικού ορίου. Θετικό: δεν αποδεικνύει απουσία αδικαιολόγητης καθυστέρησης. Χωρίς αριθμητικό όριο δεν υπολογίζεται.
K6 Επιτυχία δοκιμών ανάκαμψης	Δοκιμές που πέτυχαν όλα τα προεγκεκριμένα κριτήρια ÷ ολοκληρωμένες δοκιμές × 100.	Αναφορές δοκιμών· ιδιοκτήτης συνέχειας/υπηρεσίας· ανά κύκλο.	Δίπλα εμφανίζονται προγραμματισμένες, ολοκληρωμένες και ακυρωμένες δοκιμές. RTO, RPO και ακεραιότητα ελέγχονται χωριστά.

Δείκτης	Ορισμός και τύπος	Πηγή, υπεύθυνος και κύκλος	Ερμηνεία και περιορισμός
K7 Επίκαιρα τεκμήρια	Εφαρμοζόμενοι έλεγχοι με πλήρες και αποδεκτό τεκμήριο εντός κύκλου ÷ σύνολο εφαρμοζόμενων ελέγχων × 100.	Μητρώο τεκμηρίων· λειτουργία ελέγχου· μηνιαία ή τριμηνιαία.	Άγνωστα ή μη ελεγμένα στοιχεία δεν λογίζονται ως αποδεκτά. Απαιτείται έλεγχος εύρους και γνησιότητας.
K8 Επανάληψη αιτιών	Αναλυμένα περιστατικά περιόδου με τεκμηριωμένα επαναλαμβανόμενη βασική αιτία ÷ όλα τα περιστατικά περιόδου με ολοκληρωμένη ανάλυση αιτίας × 100.	Ανασκοπήσεις· υπεύθυνος διαχείρισης περιστατικών· εξαμηνιαία.	Προκαθορισμένο διάστημα σύγκρισης και κοινή ταξινόμηση αιτιών. Οι εκκρεμείς αναλύσεις εμφανίζονται χωριστά· η επανάληψη δεν αποδεικνύει μόνη της αποτυχία διοίκησης.

Πηγή: Πρόταση του συγγραφέα δεικτών με αναφορά στο NIST CSF 2.0 και στο NIST SP 800-61 Rev. 3 (Nelson et al., 2025). Οι τύποι, οι κωδικοί και οι συχνότητες σχεδιάστηκαν για την παρούσα εργασία. Δεν αποτελούν επίσημο λεξικό των πηγών ή καθολικά κανονιστικά όρια.

Ο Πίνακας 6.11 περιέχει μεμονωμένες τιμές του υποθετικού περιστατικού. Οι χρόνοι NIS2 και GDPR μπορούν να τροφοδοτήσουν τον K5, με τις αντίστοιχες αφετηρίες. Η πρώτη ένδειξη έως την εσωτερική κήρυξη αποτελεί διαφορετικό γεγονός λήξης από την πρώτη κανονιστική απόφαση του K4. Η μερική επαναφορά αποθήκης συγκρίνεται με τον στόχο RTO, αλλά δεν ισοδυναμεί με επιτυχή δοκιμή του K6 ή με πλήρη ανάκαμψη όλων των υπηρεσιών. Τα ποσοστά κάλυψης και οι τάσεις απαιτούν καθορισμένο πληθυσμό και περίοδο και δεν εξάγονται από ένα υποθετικό συμβάν.

5.6.2 Διοικητική ανασκόπηση και κλιμάκωση

Η αναφορά προς τη διοίκηση πρέπει να είναι σύντομη αλλά ελέγξιμη. Για κάθε κρίσιμη υπηρεσία παρουσιάζονται η τάση κινδύνου, οι ληξιπρόθεσμες ενέργειες, οι σημαντικές εξαρτήσεις, οι αποτυχίες δοκιμών, τα σοβαρά περιστατικά και οι αποφάσεις που απαιτούν πόρους ή αποδοχή κινδύνου. Η χρήση χρωματικής ένδειξης συνοδεύεται από αριθμό, περίοδο και αιτιολογία. Διαφορετικά, μια «πράσινη» κατάσταση μπορεί να συγκαλύπτει άγνωστα στοιχεία ή μη ελεγχθείσες εξαιρέσεις.

Η κλιμάκωση ενεργοποιείται όταν απειλείται ανάκαμψη κρίσιμης υπηρεσίας, δεν υπάρχει επαρκές τεκμήριο κρίσιμου τρίτου, καθυστερεί ενέργεια υψηλής προτεραιότητας ή απειλείται προθεσμία γνωστοποίησης. Ο κανόνας ορίζει αποδέκτη, αναπληρωτή, χρόνο ανταπόκρισης και προσωρινή ενέργεια. Η απόφαση καταγράφει πόρους, υπεύθυνο και ημερομηνία επανεξέτασης· η αποστολή μιας ειδοποίησης δεν αρκεί ως απόδειξη ότι η έκθεση αντιμετωπίστηκε.

5.7 Πρωτόκολλο εφαρμογής του προτύπου στο Κεφάλαιο 6

Ο Πίνακας 5.8 συνδέει τις έξι ενότητες τεκμηρίωσης με τα πέντε στάδια και με συγκεκριμένες θέσεις στο Κεφάλαιο 6. Η §6.5.1 και ο Πίνακας 6.10 εφαρμόζουν την ίδια ακολουθία σταδίων. Η διαχείριση του περιστατικού χρησιμοποιεί τα μέτρα του σταδίου 3, ελέγχεται μέσω ασκήσεων στο στάδιο 4 και τροφοδοτεί την ανασκόπηση του σταδίου 5. Δεν αποτελεί δεύτερη, ανταγωνιστική πεντασταδιακή μέθοδο.

Η εφαρμογή διατηρεί τις παραδοχές της LogiTrans: βασική οντότητα NIS2 λόγω της υποθετικής υπηρεσίας ITS και του μεγέθους της, ρόλοι GDPR ανά επεξεργασία και φυσική υπηρεσία διανομής προς τραπεζικό πελάτη. Η βοηθητική ψηφιακή διασύνδεση δεν θεωρείται αυτομάτως αυτοτελής υπηρεσία ΤΠΕ προς την

τράπεζα. Στοιχεία οργάνωσης, λειτουργίας και περιστατικού σημειώνονται ως παραδοχές, ενώ οι προτεινόμενες διορθώσεις διακρίνονται από ήδη υλοποιημένα μέτρα.

Η §6.7 συνδέει κάθε κενό με λύση, υπεύθυνο, υπηρεσία, προτεραιότητα, εξαρτήσεις και αναμενόμενο τεκμήριο. Οι χρόνοι του οδικού χάρτη αποτελούν παραδοχές σχεδιασμού και όχι νομοθετικές προθεσμίες ή μετρημένες διάρκειες έργου. Κόστος, τεχνική εφικτότητα και αναμενόμενη μείωση κινδύνου παραμένουν προς επιβεβαίωση όπου δεν υπάρχουν δεδομένα.

Πίνακας 5.8: Διαδρομή από το πρότυπο του Κεφαλαίου 4 στη μελέτη περίπτωσης

Ενότητα και στάδια	Είσοδος	Εφαρμογή	Θέση στο Κεφάλαιο 6
Πεδίο εφαρμογής· στάδιο 1	Οντότητα, δραστηριότητα, μέγεθος, χώρες και συμβάσεις.	Αιτιολόγηση NIS2, ρόλων GDPR και σχέσης με χρηματοοικονομικό πελάτη.	§6.1, Πίνακας 6.2: μητρώο εφαρμογής.
Υπηρεσίες και δεδομένα· στάδιο 1	Υπηρεσίες, συστήματα, δεδομένα, τρίτοι και στόχοι συνέχειας.	Χάρτης εξαρτήσεων και ρόλων ανά επεξεργασία.	§§6.2–6.3, Πίνακες 6.4–6.6: υπηρεσίες, ρόλοι και τρίτοι.
Κίνδυνος και περιστατικό· στάδιο 2 και ροή §5.4	Σενάρια, δικλίδες, γεγονότα και αβεβαιότητες.	Αιτιολόγηση προτεραιότητας και χωριστών αποφάσεων αναφοράς.	§6.4, Πίνακες 6.7–6.9: κίνδυνοι, χρονολόγιο και κανονιστική ενεργοποίηση.
Εφαρμογή μέτρων· στάδια 3–4	Απαιτήσεις, κίνδυνοι, κενά και προβλεπόμενες δοκιμές.	Σύνδεση επιλογής, υλοποίησης και επαλήθευσης, με διάκριση προτάσεων από υφιστάμενα μέτρα.	§6.5.1, Πίνακας 6.10 και §6.7: εφαρμογή σταδίων και σχέδιο ενεργειών.
Κενά και λύσεις· στάδια 2–5	Ευρήματα σεναρίου, περιορισμοί και εξαρτήσεις.	Σύνδεση κενών G με ενέργειες A, υπευθύνους και κριτήρια κλεισίματος.	§§6.6–6.7, Πίνακες 6.12–6.13: κενά και οδικός χάρτης.
Τεκμήρια και μέτρηση· στάδια 4–5	Προτεινόμενα τεκμήρια E και χρονικές παραδοχές.	Υπολογισμός μόνο υποστηριζόμενων δεικτών και δήλωση περιορισμών.	§§6.5.2–6.5.3, Πίνακας 6.11 και §6.8: φάκελος, τιμές και όρια.

Πηγή: Σύνθεση του συγγραφέα. Ο πίνακας εξειδικεύει το επαναχρησιμοποιήσιμο πρότυπο του Κεφαλαίου 4 και λειτουργεί ως πρωτόκολλο για το υποθετικό case study του Κεφαλαίου 6· δεν αποτελεί αποτέλεσμα εφαρμογής σε πραγματική εταιρεία.

Η αναλυτική επίδειξη κρίνεται με τέσσερα ερωτήματα: αιτιολογείται η εφαρμογή κάθε πλαισίου, υπολογίζονται οι προθεσμίες από το σωστό γεγονός, συνδέεται κάθε προτεινόμενη ενέργεια με κενό και τεκμήριο, και περιορίζονται οι δείκτες στα διαθέσιμα δεδομένα; Ασυνέπεια σε κάποιο ερώτημα απαιτεί αναθεώρηση της εφαρμογής. Η θετική απάντηση δείχνει εσωτερική συνέπεια της μεθόδου, όχι πραγματική συμμόρφωση ή μετρημένη αποτελεσματικότητα.

5.8 Συμπεράσματα

Το κεφάλαιο διαμορφώνει διαδικασία που αρχίζει από αιτιολογημένο πεδίο εφαρμογής και φθάνει σε υλοποίηση, επαλήθευση και διοικητική επανεξέταση. Τα σημεία απόφασης και οι υπεύθυνοι καθιστούν ελέγξιμη τη μετάβαση από μια γενική απαίτηση σε συγκεκριμένη ενέργεια.

Ως προς το RQ3, το προτεινόμενο πλαίσιο οργανώνει τη συμμόρφωση με μονάδα αναφοράς την επιχειρησιακή υπηρεσία και τον χάρτη των εξαρτήσεών της, διατηρεί χωριστές τις κανονιστικές κρίσεις, συνδέει κάθε κίνδυνο R με κενό G, ενέργεια A και τεκμήριο E, αναθέτει σαφείς ρόλους Responsible και Accountable και αποδέχεται την ολοκλήρωση μόνο όταν ικανοποιείται προκαθορισμένο κριτήριο

επαλήθευσης. Έτσι η απάντηση στο ερευνητικό ερώτημα λαμβάνει μορφή εφαρμόσιμης και ελέγξιμης διαδικασίας, της οποίας η εσωτερική συνέπεια εξετάζεται στο υποθετικό σενάριο του Κεφαλαίου 6.

Η πρωτότυπη συμβολή δεν περιορίζεται στην ονομασία πέντε σταδίων. Συνίσταται στη συστηματική μετατροπή των προβλημάτων που τεκμηριώθηκαν στα Κεφάλαια 2–4 σε έξι απαιτήσεις σχεδιασμού, στη λειτουργική υλοποίησή τους μέσω της πεντασταδιακής πορείας και στην ελεγχόμενη αλυσίδα $R \rightarrow G \rightarrow A \rightarrow E$, η οποία κλείνει με επαλήθευση και διοικητική επανεξέταση. Το αποτέλεσμα είναι μια αναπαραγώγιμη αρχιτεκτονική που επιτρέπει κοινή συλλογή επιχειρησιακών στοιχείων και επαναχρησιμοποίηση τεκμηρίων, χωρίς να συγχέει τις αυτοτελείς αποφάσεις NIS2, GDPR και DORA. Η εφαρμογή στη LogiTrans ελέγχει τη συνέπεια αυτής της αρχιτεκτονικής υπό δηλωμένες υποθετικές παραδοχές και δεν προβάλλεται ως εμπειρική επικύρωση της αποτελεσματικότητάς της.

ΚΕΦΑΛΑΙΟ 6 Εφαρμογή του ενοποιημένου πλαισίου στο υποθετικό σενάριο LogiTrans

Το κεφάλαιο αξιολογεί το πλαίσιο του Κεφαλαίου 5 μέσα από το υποθετικό οργανωτικό και περιστατικό σενάριο της LogiTrans Europe. Η αξιολόγηση είναι σεναριοκεντρική: εξετάζει αν η προτεινόμενη μέθοδος οργανώνει συνεκτικά τα δεδομένα, τις κανονιστικές αποφάσεις, τα κενά, τις ενέργειες και τα τεκμήρια. Δεν αποτελεί εμπειρική επικύρωση της αποτελεσματικότητας του πλαισίου ούτε αποτίμηση πραγματικού οργανισμού.

Η LogiTrans και ο πάροχος LogiLink Pro είναι υποθετικοί. Τα οργανωτικά, τεχνικά και χρονικά στοιχεία αποτελούν παραδοχές, χωρίς συνεντεύξεις, πραγματικά αρχεία ή μετρήσεις. Τα ονόματα εμπορικών προϊόντων δηλώνουν ενδεικτικές τεχνολογίες· οι αδυναμίες αποδίδονται στη διαμόρφωση του σεναρίου και δεν αποτελούν ευρήματα για τους κατασκευαστές.

Η αφήγηση διακρίνει την εκ των υστέρων ανακατασκευή από όσα γνωρίζει ο οργανισμός σε κάθε στιγμή. Νέα στοιχεία συμπληρώνουν τις αποφάσεις χωρίς να μεταθέτουν προγενέστερη γνώση της ίδιας παραβίασης. Όταν λείπει τεκμηρίωση, η αξιολόγηση παραμένει εκκρεμής αντί να συμπληρώνεται με υπόθεση επιτυχούς συμμόρφωσης.

Η εξέταση ακολουθεί το πρωτόκολλο και τα οκτώ προκαθορισμένα κριτήρια ΑΞ1–ΑΞ8 της §6.1.1. Στη συνέχεια εφαρμόζει τα πέντε στάδια του Κεφαλαίου 5, από την οριοθέτηση και τη χαρτογράφηση έως την αλυσίδα $R \rightarrow G \rightarrow A \rightarrow E$ και το σχέδιο υλοποίησης A-01–A-09. Η §6.8 αποτιμά τα αποτελέσματα έναντι των ίδιων κριτηρίων και προσθέτει δομική σύγκριση με βάση αναφοράς τη χωριστή ανάλυση ανά κανονιστικό πλαίσιο. Η κανονιστική βάση παραμένει εκείνη της 31ης Αυγούστου 2026.

6.1 Πρωτόκολλο αξιολόγησης, προφίλ και όρια εφαρμογής

6.1.1 Σχεδιασμός και κριτήρια αξιολόγησης

Το πρωτόκολλο ορίζει εκ των προτέρων τι θα εξεταστεί και με ποια βάση θα κριθεί το αποτέλεσμα. Μονάδα παρατήρησης είναι η απόφαση ή ο σύνδεσμος ιχνηλασιμότητας που παράγεται υπό τις δηλωμένες παραδοχές του σεναρίου, όχι άνθρωποι ή πραγματικές επιχειρησιακές μονάδες. Είσοδοι είναι οι παραδοχές του οργανισμού, ο χάρτης υπηρεσιών και εξαρτήσεων, το μητρώο κινδύνων, η χρονογραμμή του περιστατικού, οι κανονιστικές αποφάσεις και οι προδιαγραφές για κενά, ενέργειες και τεκμήρια. Ως αποδεικτική βάση χρησιμοποιείται η εσωτερική συνέπεια μεταξύ των πινάκων του κεφαλαίου και όχι πραγματικά αρχεία της LogiTrans.

Τα κριτήρια που ακολουθούν καθορίζονται πριν από την τελική αποτίμηση της §6.8, ώστε η κρίση να μη διαμορφώνεται εκ των υστέρων από το επιθυμητό αποτέλεσμα:

ΑΞ1: Κανονιστικό πεδίο και αιτιολόγηση. Το πλαίσιο πρέπει να αναγνωρίζει ποιο κανονιστικό καθεστώς εξετάζεται και να τεκμηριώνει γιατί εφαρμόζεται ή γιατί δεν μπορεί ακόμη να κριθεί.

ΑΞ2: Διακριτές χρονικές αφετηρίες. Οι προθεσμίες NIS2, GDPR και οι τυχόν συμβατικές υποχρεώσεις πρέπει να υπολογίζονται από τη δική τους κατάλληλη αφετηρία, χωρίς τεχνητή ενοποίηση.

ΑΞ3: Εντοπισμός ατεκμηρίωτων αποφάσεων. Η μέθοδος πρέπει να καθιστά ορατές αποφάσεις που δεν στηρίζονται επαρκώς από τα διαθέσιμα γεγονότα ή από καταγεγραμμένη αιτιολόγηση.

ΑΞ4: Ιχνηλασιμότητα $R \rightarrow G \rightarrow A \rightarrow E$. Κάθε κίνδυνος και κενό πρέπει να οδηγεί σε υπεύθυνη ενέργεια και σε προκαθορισμένο τεκμήριο επαλήθευσης.

ΑΞ5: Εντοπισμός ελλειπόντων τεκμηρίων. Το πλαίσιο πρέπει να διακρίνει μεταξύ σχεδιασμένης απόδειξης και τεκμηρίου που έχει πράγματι παραχθεί και ελεγχθεί.

ΑΞ6: Σύνδεση ανάκαμψης με στόχους υπηρεσίας. Η τεχνική αποκατάσταση πρέπει να αξιολογείται σε σχέση με RTO, RPO και αποδεκτό επίπεδο λειτουργίας της υπηρεσίας.

ΑΞ7: Αποφυγή μη υποστηριζόμενων ισχυρισμών συμμόρφωσης. Η ανάλυση δεν πρέπει να μετατρέπει επιμέρους θετικές ενδείξεις σε γενικό χαρακτηρισμό συμμόρφωσης ή αποτελεσματικότητας.

ΑΞ8: Καταγραφή ανοιχτών ζητημάτων. Οι αβεβαιότητες δικαιοδοσίας, ταξινόμησης, γνώσης, ανάκαμψης και αποδεικτικής πληρότητας πρέπει να παραμένουν ρητά ανοικτές μέχρι να επιλυθούν.

Για κάθε κριτήριο χρησιμοποιούνται οι καταστάσεις «ικανοποιείται», «ικανοποιείται εν μέρει» και «δεν αξιολογείται». Η αποτίμηση αφορά μόνο τη συνέπεια του σχεδιασμού στο παρόν σενάριο. Τα ΑΞ1–ΑΞ8 δεν ταυτίζονται με τους επιχειρησιακούς δείκτες K1–K8 του Κεφαλαίου 5, οι οποίοι προορίζονται για μέτρηση μετά από πραγματική εφαρμογή.

6.1.2 Παραδοχές του οργανωτικού σεναρίου

Η LogiTrans Europe υποτίθεται ότι είναι μεγάλη επιχείρηση παροχής υπηρεσιών εφοδιαστικής αλυσίδας, με έδρα την Αθήνα και λειτουργική παρουσία σε τέσσερα κράτη μέλη της Ευρωπαϊκής Ένωσης. Παρέχει αποθήκευση, εκτέλεση παραγγελιών, διαχείριση μεταφορών, διασύνδεση με συνεργαζόμενους μεταφορείς και υπηρεσίες τελευταίου μιλίου. Το πελατολόγιό της περιλαμβάνει επιχειρήσεις ηλεκτρονικού εμπορίου, διανομείς φαρμακευτικών προϊόντων και έναν τραπεζικό οργανισμό για τη φυσική διανομή καρτών και τερματικών.

Το σενάριο θεωρεί περίπου 1.850 εργαζομένους και τέσσερις εγκαταστάσεις σε ισάριθμα κράτη μέλη. Το μέγεθος υπερβαίνει το όριο προσωπικού μεσαίας επιχείρησης, αλλά η υπαγωγή προϋποθέτει και καλυπτόμενη δραστηριότητα. Οι χώρες εκτός Ελλάδας και η ακριβής νομική διάρθρωση των εγκαταστάσεων δεν εξειδικεύονται· αυτό περιορίζει τη διασυνοριακή αξιολόγηση. Δεν αποδίδονται πλασματικά ποσά ζημίας ή αριθμητικές πιθανότητες.

Ο Πίνακας 6.1 συγκεντρώνει τις βασικές οργανωτικές και τεχνικές παραδοχές του σεναρίου.

Πίνακας 6.1: Βασικές παραδοχές του υποθετικού οργανισμού LogiTrans

Πεδίο	Παραδοχή σεναρίου	Χρήση στην ανάλυση
Οργανωτικό μέγεθος	Περίπου 1.850 εργαζόμενοι, τέσσερις εγκαταστάσεις σε τέσσερα κράτη μέλη και διοίκηση στην Αθήνα.	Αποδίδει κατανεμημένη λειτουργία και ανάγκη διασυνοριακού συντονισμού· δεν αποτελεί πραγματικό εταιρικό στοιχείο.
Κρίσιμες υπηρεσίες	Παραλαβή, αποθήκευση, picking/packing, δρομολόγηση, παρακολούθηση αποστολών και επιστροφές.	Ορίζει τις λειτουργίες που εξετάζονται στην ανάλυση κινδύνου.
Ψηφιακό περιβάλλον	ERP, WMS, TMS, πύλη προμηθευτή, API gateway, Microsoft 365/Entra ID, SIEM/SOC και εφεδρικά αντίγραφα.	Υποστηρίζει τη χαρτογράφηση κοινών εξαρτήσεων και της εξάπλωσης στο δίκτυο.

Πεδίο	Παραδοχή σεναρίου	Χρήση στην ανάλυση
Τρίτα μέρη	Πάνω από 40 μεταφορείς, SaaS πάροχος πύλη προμηθευτή, πάροχοι υπηρεσιών νέφους, εξωτερικό SOC και HR SaaS.	Επιτρέπει έλεγχο κινδύνου αλυσίδας εφοδιασμού και συμβατικής ετοιμότητας.
Υπηρεσία ITS	Για τις ανάγκες του σεναρίου, αυτοτελής υπηρεσία πραγματικού χρόνου συντονίζει κυκλοφοριακά δεδομένα, δρομολόγηση στόλου και συνεργαζόμενους μεταφορείς.	Δηλώνει την ειδική παραδοχή υπαγωγής στη NIS2· δεν αρκεί η γενική ιδιότητα 3PL.
Ερευνητικό καθεστώς	Υποθετική, βιβλιογραφικά τεκμηριωμένη εφαρμογή χωρίς πραγματικούς συμμετέχοντες ή μετρήσεις.	Περιορίζει τα συμπεράσματα σε αναλυτική επάρκεια και όχι σε εμπειρική αποτελεσματικότητα.

Πηγή: Διαμόρφωση από τον συγγραφέα του υποθετικού οργανισμού. Όλα τα στοιχεία είναι παραδοχές.

6.1.3 Έλεγχος εφαρμογής NIS2, GDPR και DORA

Η NIS2 εξετάζεται για την αυτοτελή υπηρεσία ευφών συστημάτων μεταφορών (ITS), βάσει της υποκατηγορίας οδικών μεταφορών του Παραρτήματος I. Η γενική ιδιότητα επιχείρησης logistics δεν αρκεί. Για τις ανάγκες της εφαρμογής, θεωρείται ότι η υπηρεσία και το μέγεθος έχουν ελεγχθεί και η LogiTrans υπάγεται ως βασική οντότητα κατά τα άρθρα 2–3 και τον Ν. 5160/2024.

Η ελληνική καταχώριση είναι παραδοχή του σεναρίου και δεν υποκαθιστά τον έλεγχο υπαγωγής. Για τις άλλες εγκαταστάσεις απαιτείται χωριστή εξέταση εθνικής δικαιοδοσίας και υποχρεώσεων κατά το άρθρο 26 NIS2. Η ITS δραστηριότητα δεν υπάγεται αυτομάτως στην εξαίρεση της κύριας εγκατάστασης που ισχύει για συγκεκριμένους ψηφιακούς παρόχους. Το χρονολόγιο καταγράφει την ελληνική αναφορά· δεν αποδεικνύει εκπλήρωση όλων των υποχρεώσεων στα τέσσερα κράτη.

Ο GDPR εφαρμόζεται στις επεξεργασίες εργαζομένων, παραληπτών, οδηγών και χρηστών συστημάτων. Ο ρόλος της LogiTrans κρίνεται ανά σκοπό και ουσιώδη μέσα επεξεργασίας: εκτελούσα για ορισμένες παραγγελίες πελατών, υπεύθυνη για δικούς της σκοπούς προσωπικού και ασφάλειας. Ο Πίνακας 6.5 εξειδικεύει τις παραδοχές χωρίς ενιαία ετικέτα για όλη την εταιρεία.

Στο βασικό σενάριο η υπηρεσία προς την τράπεζα είναι φυσική διανομή καρτών και τερματικών, με βοηθητική ψηφιακή διεπαφή. Δεν θεωρείται αυτοτελής υπηρεσία ΤΠΕ κατά το άρθρο 3 σημείο 21 DORA και η LogiTrans δεν είναι χρηματοοικονομική οντότητα. Η ενημέρωση της τράπεζας είναι συμβατική. Οποιαδήποτε δική της ταξινόμηση ή αναφορά DORA απαιτεί στοιχεία για συμβάν ΤΠΕ και επίπτωση στις τραπεζικές λειτουργίες, τα οποία δεν παρέχει το σενάριο. Διαφορετικά χαρακτηριστικά υπηρεσίας θα επέβαλλαν νέα αξιολόγηση.

Ο Πίνακας 6.2 συνοψίζει τις αποφάσεις εφαρμογής και τα ανοικτά όρια κάθε κανονιστικού σκέλους.

Πίνακας 6.2: Απόφαση πεδίου εφαρμογής στο σενάριο LogiTrans

Πλαίσιο	Κριτήριο	Παραδοχή	Αποτέλεσμα και όριο
NIS2	Εμπίπτει η συγκεκριμένη δραστηριότητα σε κατηγορία του Παραρτήματος I ή II και πληρούνται τα λοιπά κριτήρια;	Καλυπτόμενη ITS δραστηριότητα Παραρτήματος I και μεγάλο μέγεθος· ελληνική καταχώριση ως βασικής οντότητας.	Ελληνικός κλάδος NIS2 προς ΕΑΚ (EL-CSIRT). Εκκρεμεί πλήρης έλεγχος των λοιπών εγκαταστάσεων κατά το άρθρο 26.

Πλαίσιο	Κριτήριο	Παραδοχή	Αποτέλεσμα και όριο
GDPR	Υπάρχει επεξεργασία δεδομένων προσωπικού χαρακτήρα και ποιος καθορίζει σκοπό και μέσα;	Υπεύθυνη για ίδιους σκοπούς· εκτελούσα για ορισμένες παραγγελίες πελατών.	Ρόλοι και αποφάσεις ανά επεξεργασία· άρθρο 28 όπου εφαρμόζεται και χωριστός έλεγχος αρμόδιας αρχής.
DORA	Είναι χρηματοοικονομική οντότητα; Παρέχει υπηρεσία ΤΠΕ κατά το άρθρο 3(21);	Όχι στο βασικό σενάριο. Η υπηρεσία προς την τράπεζα είναι φυσική διανομή με βοηθητική ψηφιακή διεπαφή.	Συμβατική ενημέρωση τράπεζας. Καμία δική της αναφορά DORA και κανένα τεκμηριωμένο τραπεζικό αποτέλεσμα ταξινόμησης.

Πηγή: Εφαρμογή του συγγραφέα βάσει NIS2, άρθρων 2–3 και 26 και Παραρτήματος I, Ν. 5160/2024, GDPR και DORA, άρθρων 2–3.

6.1.4 Δομή διακυβέρνησης και γραμμές ευθύνης

Στο οργανωτικό σενάριο, η ευθύνη για την κυβερνοασφάλεια ανατίθεται σε CISO που αναφέρεται στο διοικητικό όργανο, ενώ ο DPO είναι εξωτερικός συνεργάτης με άμεση πρόσβαση στη διοίκηση για θέματα προστασίας δεδομένων. Η επιχειρησιακή τεχνολογία υποστηρίζεται από κεντρική ομάδα IT, πέντε στελέχη ασφάλειας και εξωτερικό SOC εικοσιτετράωρης λειτουργίας. Η μικρή σχετικά εσωτερική ομάδα καθιστά αναγκαίο τον σαφή διαχωρισμό ανάμεσα στην τεχνική απόκριση, στη νομική αξιολόγηση και στην επιχειρησιακή απόφαση διακοπής υπηρεσίας.

Το SOC παρέχει ανίχνευση και τεχνική εισήγηση. Στον προτεινόμενο καταμερισμό, ο εξουσιοδοτημένος CISO αποφασίζει και υποβάλλει την ελληνική αναφορά NIS2, με αναπληρωτή και διαθέσιμη νομική συνδρομή. Η LogiTrans ως υπεύθυνη επεξεργασίας ορίζει εξουσιοδοτημένο αποφασίζοντα για GDPR, με ανεξάρτητη συμβουλή του DPO. Η απουσία στελέχους ή συνεδρίασης δεν αναστέλλει προθεσμία. Η εποπτεία της διοίκησης και η νομική ευθύνη δεν μεταφέρονται στον πάροχο· η αποδοχή κινδύνου δεν αίρει δεσμευτικές απαιτήσεις.

Οι προτεινόμενοι ρόλοι, τα όρια απόφασης και τα αντίστοιχα τεκμήρια παρουσιάζονται στον Πίνακα 6.3.

Πίνακας 6.3: Κατανομή ρόλων για την εφαρμογή του σεναρίου

Ρόλος	Λειτουργία	Όριο και απόφαση	Τεκμήριο
Διοίκηση	Εποπτεία, πολιτικές, πόροι και νόμιμα όρια αποδοχής κινδύνου.	Διατηρεί τη λογοδοσία· ορίζει εξουσιοδοτήσεις και αναπληρωτές χωρίς αναμονή συνεδρίασης.	Πρακτικά και πίνακας εξουσιοδοτήσεων.
CISO και διαχειριστής περιστατικού	Συντονισμός και τεχνική εισήγηση· ελληνική αναφορά NIS2 από εξουσιοδοτημένο ρόλο.	Απόφαση σημαντικότητας και υποβολή εντός εντολής· χωριστή απόφαση GDPR.	Χρονολόγιο, απόφαση και αποδεικτικό υποβολής.
Αποφασίζων GDPR	Εξουσιοδοτημένος εκπρόσωπος της LogiTrans ως υπευθύνου επεξεργασίας.	Αποφασίζει άρθρα 33–34, με συμβουλή DPO. Οι πελάτες αποφασίζουν για τις δικές τους επεξεργασίες.	Αιτιολογημένη απόφαση ανά σύνολο δεδομένων.
DPO	Ανεξάρτητη συμβουλή για ρόλους, κίνδυνο και γνωστοποίηση.	Δεν υποκαθιστά τον υπεύθυνο επεξεργασίας και δεν εγκρίνει επιχειρησιακή αποδοχή κινδύνου.	Γραπτή γνώμη και τυχόν διαφωνία.

Ρόλος	Λειτουργία	Όριο και απόφαση	Τεκμήριο
Νομική λειτουργία	Συμβάσεις, αρμόδιες αρχές και περιεχόμενο αναφορών.	Υποστηρίζει τον αποφασίζοντα· δεν αναστέλλει προθεσμία περιμένοντας πλήρη έρευνα.	Έλεγχος νομικής βάσης και εκδόσεις αναφορών.
IT και λειτουργίες	Περιορισμός, ανάκαμψη και επιχειρησιακή αποδοχή.	Ασφαλής επαναφορά βάσει κριτηρίων και ελέγχου επαναμόλυνσης.	Αλλαγές, δοκιμές και κατάσταση υπηρεσίας.
Εξωτερικό SOC	Ανίχνευση, διατήρηση στοιχείων και κλιμάκωση.	Δεν μεταφέρεται σε αυτό η νομική ευθύνη της LogiTrans.	Ειδοποιήσεις, χρόνοι και καταγραφή χειρισμών.

Πηγή: Σχεδιασμός ρόλων από τον συγγραφέα βάσει NIS2, άρθρου 20, GDPR, άρθρων 5(2), 24, 38–39 και NIST SP 800-61 Rev. 3 (Nelson et al., 2025).

6.2 Χαρτογράφηση υπηρεσιών, δεδομένων και ρόλων επεξεργασίας

6.2.1 Κρίσιμες επιχειρησιακές υπηρεσίες και πληροφοριακά συστήματα

Ο Πίνακας 6.4 συνδέει τις κρίσιμες υπηρεσίες με συστήματα, δεδομένα, τρίτους και προσωρινή λειτουργία. Ο ιδιοκτήτης λειτουργίας αποθήκης ελέγχει παραλαβή και εκτέλεση παραγγελιών, ο ιδιοκτήτης μεταφορών τη δρομολόγηση/ITS και ο υπεύθυνος εξυπηρέτησης την παρακολούθηση αποστολών. Ο διαχειριστής περιστατικού αναλαμβάνει την επικοινωνία κρίσης. Πρόκειται για κατανομή ευθυνών του σχεδιασμού.

Η διακοπή WMS επηρεάζει την τροφοδότηση TMS και την υπηρεσία ITS, ακόμη και αν το TMS παραμένει τεχνικά διαθέσιμο. Οι RTO μετρούν από την απώλεια του συμφωνημένου επιπέδου της αντίστοιχης υπηρεσίας. Στο χρονολόγιο η αφετηρία αποθήκης είναι η +10η ώρα. Το κριτήριο ανάκαμψης πρέπει να ορίζει εγκαταστάσεις, εύρος και αποδεκτή λειτουργία· απλή εκκίνηση εξυπηρετητή δεν αρκεί. Οι στόχοι είναι παραδοχές. Όπου δεν ορίζεται RPO ή χρόνος πλήρους επαναφοράς, δεν παράγεται αντίστοιχη τιμή επιτυχίας.

Πίνακας 6.4: Χαρτογράφηση κρίσιμων υπηρεσιών και εξαρτήσεων

Υπηρεσία	Συστήματα και εξαρτήσεις	Στόχος και προσωρινή λειτουργία	Σημείο αστοχίας
Εκτέλεση παραγγελιών	ERP, WMS, Entra ID. Στοιχεία παραγγελίας και παραλήπτη· e-commerce clients, cloud identity.	RTO 24 ώρες, RPO 4 ώρες· περιορισμένη χειροκίνητη λίστα picking για βασικά είδη.	Κοινή ταυτότητα και μη διαχωρισμένη διασύνδεση ERP–WMS.
Δρομολόγηση / ITS	TMS, API gateway, telematics. Θέση οχήματος, οδηγός, κυκλοφοριακά δεδομένα· cloud και μεταφορείς.	RTO 8 ώρες· στατικές διαδρομές και τηλεφωνική επικοινωνία. RPO προς ορισμό.	Συγκέντρωση σε cloud και ακεραιότητα δεδομένων API.
Ιχνηλάτηση αποστολής	Portal, API gateway, TMS. Tracking events, στοιχεία παραλήπτη· πελάτες και couriers.	RTO 12 ώρες· περιοδική ενημέρωση κατάστασης. RPO προς ορισμό.	SaaS portal με έμπιστη πρόσβαση προς εσωτερικά APIs.
Παραλαβή / αποθήκη	WMS, scanners, Wi-Fi. Κωδικοί ειδών, παρτίδες, χειριστές· τοπικός integrator.	RTO 12 ώρες· προσωρινή παραλαβή εκτός σύνδεσης και συμφωνία δεδομένων. RPO προς ορισμό.	Τοπική συνδεσιμότητα και διαθεσιμότητα WMS.

Υπηρεσία	Συστήματα και εξαρτήσεις	Στόχος και προσωρινή λειτουργία	Σημείο αστοχίας
Επικοινωνία κρίσης	M365, κινητή τηλεφωνία, out-of-band κανάλι. Στοιχεία στελεχών και αρχείων συμβάντος: telecom/cloud.	Άμεση χρήση ανεξάρτητου καναλιού· χρόνος και ελάχιστη λειτουργία προς δοκιμή.	Κοινή εξάρτηση M365 και Entra ID.

Πηγή: Χαρτογράφηση του συγγραφέα με αναφορά σε NIST CSF 2.0, ISO 22301:2019 και NIS2, άρθρο 21. Οι στόχοι RTO/RPO είναι παραδοχές, χωρίς πραγματικές δοκιμές.

6.2.2 Ρόλοι GDPR ανά δραστηριότητα επεξεργασίας

Οι έννοιες «υπεύθυνος» και «εκτελών την επεξεργασία» είναι λειτουργικές: κατά τις Κατευθυντήριες Γραμμές 07/2020 του EDPB (2021), ο ρόλος κρίνεται από το ποιος καθορίζει τον σκοπό και τα ουσιώδη μέσα κάθε συγκεκριμένης επεξεργασίας. Έτσι, η LogiTrans μπορεί να έχει διαφορετικό ρόλο στις αποστολές πελατών και στα δικά της αρχεία ασφάλειας.

Για τη διεκπεραίωση παραγγελιών θεωρείται ότι ο πελάτης καθορίζει σκοπό, κατηγορίες δεδομένων και ουσιώδεις όρους και η LogiTrans ενεργεί βάσει τεκμηριωμένων οδηγιών. Για δικούς της σκοπούς ασφάλειας, προσωπικού ή νομικών αξιώσεων ενεργεί ως υπεύθυνη. Ο ανεξάρτητος σκοπός δεν νομιμοποιεί αυτομάτως επαναχρησιμοποίηση: απαιτούνται νόμιμη βάση, διαφάνεια και έλεγχος του εφαρμοστέου πλαισίου. Από κοινού καθορισμός σκοπών και μέσων εξετάζεται κατά το άρθρο 26.

Πίνακας 6.5: Λειτουργική κατανομή ρόλων GDPR στη LogiTrans

Δραστηριότητα	Δεδομένα	Ρόλος και άλλο μέρος	Απαιτούμενη τεκμηρίωση
Παραγγελίες πελατών	Όνομα, διεύθυνση, τηλέφωνο και οδηγίες παράδοσης.	LogiTrans εκτελούσα βάσει οδηγιών· πελάτης υπεύθυνος. Ο ρόλος μεταφορέα εξετάζεται χωριστά.	Άρθρο 28, εγκεκριμένοι υπεργολάβοι, οδηγίες τήρησης και έγκαιρης ενημέρωσης.
Ίδια διαχείριση μεταφοράς	Οδηγοί, θέση οχήματος και συμβάντα διαδρομής.	LogiTrans υπεύθυνη για ίδιους σκοπούς. Τυχόν ανεξάρτητος ή από κοινού ρόλος μεταφορέα απαιτεί εξέταση.	Αρχείο επεξεργασιών, νόμιμη βάση, ενημέρωση, τήρηση και έλεγχος αναλογικότητας.
Προσωπικό και χειριστές	Στοιχεία απασχόλησης και ταυτοποιήσιμες ενέργειες χειριστών WMS· ειδικές κατηγορίες μόνο όπου υπάρχουν.	LogiTrans υπεύθυνη· πάροχοι μισθοδοσίας ή ανθρώπινου δυναμικού εκτελούντες όπου ενεργούν για λογαριασμό της.	Άρθρο 28 όπου απαιτείται, πρόσβαση και χρόνος τήρησης· έλεγχος άρθρου 9 σε σχετικές διαδικασίες.
Εποπτεία ασφάλειας	Αναγνωριστικά χρηστών, IP, αρχεία ενεργειών και ειδοποιήσεις.	LogiTrans υπεύθυνη για ίδιους σκοπούς ασφάλειας· SOC εκτελών στο ανατεθειμένο αντικείμενο.	Νόμιμη βάση και στάθμιση όπου απαιτείται, ενημέρωση, άρθρο 28, πρόσβαση και τήρηση.
Συμβάσεις προμηθευτών	Στοιχεία εκπροσώπων και αξιολογήσεις.	LogiTrans υπεύθυνη· κάθε προμηθευτής υπεύθυνος για τα δικά του εταιρικά αρχεία.	Νόμιμη βάση, ενημέρωση, περίοδος τήρησης και περιορισμός πρόσβασης.

Πηγή: Εφαρμογή του συγγραφέα βάσει GDPR, άρθρων 4(7)–(8), 5, 6, 9, 13–14, 26, 28 και 30 και EDPB Guidelines 07/2020 (2021). Οι ρόλοι είναι παραδοχές ανά επεξεργασία.

Κατά το περιστατικό εξετάζονται χωριστά η διαθεσιμότητα δεδομένων πελατών, τα ίδια δεδομένα χειριστών και η εξαγωγή αρχείων ασφάλειας. Η LogiTrans ως εκτελούσα ενημερώνει τους πελάτες χωρίς

αδικαιολόγητη καθυστέρηση, ενώ ως υπεύθυνη αξιολογεί τα άρθρα 33–34 για τις δικές της επεξεργασίες. Η υποχρέωση δεν αρχίζει κατ' ανάγκην με την επιβεβαίωση εξαγωγής: κατά τις Guidelines 9/2022 του EDPB (2023), παραβίαση μπορεί να αφορά και προσωρινή απώλεια διαθεσιμότητας.

6.3 Κρίσιμες εξαρτήσεις και κίνδυνος τρίτων μερών

6.3.1 Αλυσίδες τεχνικής και λειτουργικής εξάρτησης

Η LogiTrans δεν εξαρτάται απλώς από μεμονωμένους προμηθευτές. Εξαρτάται από αλυσίδες υπηρεσιών στις οποίες η αστοχία ενός κοινού συστατικού μεταφέρεται σε πολλές επιχειρησιακές λειτουργίες. Η ταυτότητα χρηστών αποτελεί χαρακτηριστικό παράδειγμα: αν η υπηρεσία Entra ID δεν είναι διαθέσιμη ή αν παραβιαστεί λογαριασμός υψηλών προνομίων, επηρεάζονται ταυτόχρονα το ERP, το WMS, το ηλεκτρονικό ταχυδρομείο και η πρόσβαση διαχειριστών. Η ύπαρξη πολλών εφαρμογών δεν σημαίνει πραγματική διαφοροποίηση όταν όλες στηρίζονται στον ίδιο μηχανισμό πρόσβασης.

Η διαδρομή portal–API–ERP/WMS ενώνει εξωτερική διαχείριση με εσωτερικά συστήματα. Το σενάριο θεωρεί υπερευρεία δικαιώματα λογαριασμού υποστήριξης και ελλιπή διαβίβαση αρχείων του παρόχου στο SIEM. Η τεχνική παραδοχή που επιτρέπει μετάβαση από API σε εκτέλεση εργασιών διατυπώνεται στη §6.4.2· η νόμιμη πρόσβαση σε API από μόνη της δεν αποδεικνύει δυνατότητα εκτέλεσης κακόβουλου κώδικα.

Η κρισιμότητα τρίτου εκτιμάται με βάση υπηρεσία, δεδομένα, πρόσβαση και δυνατότητα υποκατάστασης, όπως στον κύκλο της §5.3. Η ένδειξη «κρίσιμος» είναι εσωτερική κατηγορία κινδύνου και δεν αποτελεί χαρακτηρισμό κρίσιμου παρόχου ΤΠΕ κατά DORA. Πιστοποιήσεις και εκθέσεις αξιολόγησης συσχετίζονται με το εύρος και τις εξαιρέσεις τους. Τα ελλείποντα στοιχεία παραμένουν αβεβαιότητα.

Πίνακας 6.6: Αξιολόγηση κρίσιμων τρίτων μερών και εξαρτήσεων

Τρίτος ή υπηρεσία	Έκθεση	Υποκατάσταση	Κενό ή αβεβαιότητα
LogiLink Pro portal	Ευρεία διαπιστευτήρια και προνομιακή πρόσβαση· ελλιπής ταυτοποίηση και καταγραφή.	Χαμηλή άμεσα· μετάβαση ροών με πάνω από 40 συνεργάτες.	Παρωχημένη αξιολόγηση, ασαφείς χρόνοι ειδοποίησης και ρόλοι υπεργολάβων.
Κοινή ταυτότητα και επικοινωνία	Πολλές υπηρεσίες εξαρτώνται από κοινή πρόσβαση.	Περιορισμένη σε ώρες· επιλεκτικές εναλλακτικές σε μήνες.	Υπάρχει δυνατότητα έκτακτης πρόσβασης, αλλά δεν έχει δοκιμαστεί πλήρως.
Νέφος TMS και ITS	Εξάρτηση από περιοχή φιλοξενίας, συνδεσιμότητα και έλεγχο νέφους.	Χειροκίνητες διαδρομές περιορισμένης κλίμακας.	Ελλιπής απογραφή API και μη ολοκληρωμένη δοκιμή εναλλακτικής λειτουργίας.
Εξωτερικό SOC	Πρόσβαση σε αρχεία· κίνδυνος καθυστερημένης συσχέτισης.	Περιορισμένη εσωτερική παρακολούθηση για μικρό διάστημα.	Το SLA ειδοποίησης δεν καλύπτει όλα τα στοιχεία κανονιστικής απόφασης.
Αντίγραφα εκτός εγκατάστασης	Δηλώνονται αμετάβλητα αντίγραφα και χωριστός λογαριασμός· άγνωστη πλήρης αποτελεσματικότητα.	Ανάκαμψη από αντίγραφα, υπό δοκιμή υπηρεσίας και δεδομένων.	Δεν υπάρχει πρόσφατη επιτυχής πλήρης δοκιμή που να αποδεικνύει RTO/RPO.

Πηγή: Ανάλυση του συγγραφέα βάσει NIS2, άρθρον 21(2)(δ), ENISA (2023), NIST SP 800-161 Rev. 1, Update 1 (Boyens et al., 2024) και ISO/IEC 27001:2022. Δεν αξιολογούνται πραγματικοί πάροχοι.

6.3.2 Το κρίσιμο όριο εμπιστοσύνης της πύλης προμηθευτή

Το υποθετικό LogiLink Pro επιλέγεται επειδή συγκεντρώνει πρόσβαση σε δεδομένα παραληπτών και διασύνδεση με ERP/WMS. Το κρίσιμο όριο εμπιστοσύνης είναι η δυνατότητα ενός λογαριασμού που διαχειρίζεται εξωτερικός πάροχος να εκδίδει διαπιστευτήρια που γίνονται δεκτά με υπερβολικά δικαιώματα στο εσωτερικό περιβάλλον.

Στον Πίνακα 6.6 καταγράφονται χωριστά η τεχνική δυνατότητα πρόσβασης, η υποκατάσταση και όσα δεν έχουν δοκιμαστεί. Η αντιστοίχιση των συγκεκριμένων κενών με ενέργειες βρίσκεται στους Πίνακες 6.12–6.13, ώστε η αξιολόγηση του παρόχου να οδηγεί σε ελέγξιμες απαιτήσεις.

6.4 Ανάλυση κινδύνου και εξέλιξη του περιστατικού

6.4.1 Μέθοδος αξιολόγησης κινδύνου

Η αξιολόγηση του Πίνακα 6.7 αποτυπώνει την έκθεση πριν από το περιστατικό, με τις δηλωμένες δικλίδες και τα όρια γνώσης του σεναρίου. Δεν χρησιμοποιεί την εκ των υστέρων εκδήλωση της επίθεσης για να εμφανίσει κάθε κίνδυνο ως βέβαιο. Η πιθανότητα είναι ποιοτική, σύμφωνα με τη §5.1.3, και αιτιολογείται από έκθεση, δικαιώματα και δοκιμές. Δικλίδα χωρίς επαρκή επαλήθευση δεν λογίζεται ως αποδεδειγμένη μείωση. Η μελλοντική επίδραση των A-01–A-09 παραμένει χωριστή.

Οι επιπτώσεις εξετάζονται σε υπηρεσίες και δεδομένα, δικαιώματα προσώπων, ασφάλεια προσωπικού ή φορτίου, πελάτες και υποχρεώσεις. Η προτεραιότητα είναι κρίσιμη ή υψηλή για τους επιλεγμένους σοβαρούς κινδύνους του πίνακα, χωρίς αριθμητικό γινόμενο ή συμψηφισμό διαφορετικών βλαβών. Η κρισιμότητα της R-01 προκύπτει από τη συνδυασμένη εξάπλωση και διακοπή. Η άγνωστη αποτελεσματικότητα ανάκαμψης στις R-04/R-07 δεν δικαιολογεί τεκμηριωμένα χαμηλή πιθανότητα.

Η ποιοτική προσέγγιση χρησιμοποιεί τις αρχές αναλογικής διαχείρισης κινδύνου της NIS2, της KYA 1689/2025, του NIST CSF 2.0 και του ISO/IEC 27005:2022. Ο πίνακας είναι επιλεκτική ανάλυση σεναρίων, όχι πλήρης απογραφή απειλών ή πιστοποιημένη εφαρμογή προτύπου. Δεν υπάρχει μέτρηση αρχικής έναντι υπολειπόμενης έκθεσης που να αποδεικνύει πραγματικό μέγεθος μείωσης.

Πίνακας 6.7: Μητρώο βασικών κινδύνων του σεναρίου

Κίνδυνος	Πιθανότητα και επίπτωση	Δικλίδες και αβεβαιότητα	Προτεραιότητα και αιτιολόγηση
R-01 Παραβίαση λογαριασμού, κατάχρηση API και εξάπλωση ransomware.	Υψηλή· κρίσιμη επίπτωση.	SOC, SIEM, EDR και αντίγραφα· ελλείψεις σε πρόσβαση και αρχεία παρόχου.	Κρίσιμη: εξωτερικά ελεγχόμενη διαδρομή προς πολλές βασικές λειτουργίες.
R-02 Εξαγωγή δεδομένων παραδόσεων μέσω portal/API.	Μέτρια· υψηλή επίπτωση.	Ταυτοποίηση API· αποσπασματική καταγραφή και υπερευρεία δικαιώματα.	Υψηλή: συνδυασμός στοιχείων επικοινωνίας, διευθύνσεων και οδηγιών.
R-03 Παραβίαση κοινής ταυτότητας και απώλεια πρόσβασης/επικοινωνίας.	Μέτρια· κρίσιμη επίπτωση.	MFA σε μέρος χρηστών και πρόσβαση έκτακτης ανάγκης· ανεπαρκής δοκιμή.	Υψηλή: κοινή εξάρτηση πολλών υπηρεσιών χωρίς ελεγχόμενη εναλλακτική.

Κίνδυνος	Πιθανότητα και επίπτωση	Δικλίδες και αβεβαιότητα	Προτεραιότητα και αιτιολόγηση
R-04 Απώλεια αντιγράφων ή αδυναμία έγκαιρης επιχειρησιακής επαναφοράς.	Μέτρια με αβεβαιότητα· κρίσιμη επίπτωση.	Αμετάβλητα αντίγραφα εκτός εγκατάστασης και χωριστή ταυτότητα· μη επαληθευμένος χρόνος πλήρους ανάκαμψης.	Υψηλή: η διατήρηση αντιγράφου δεν αποδεικνύει αποκατάσταση υπηρεσίας.
R-05 Αλλοίωση δεδομένων δρομολόγησης χωρίς άμεση διακοπή.	Μέτρια· υψηλή επίπτωση.	Κανόνες επικύρωσης και επιχειρησιακός έλεγχος· ελλιπής δοκιμή μη εξουσιοδοτημένης αλλαγής.	Υψηλή: κίνδυνος για ασφάλεια, δρομολόγια και αποδείξεις παράδοσης.
R-06 Καθυστέρηση κανονιστικής απόφασης και ενημέρωσης.	Υψηλή· υψηλή επίπτωση.	Γενικό σχέδιο και DPO· ασαφείς εξουσιοδοτήσεις και καταγραφή πρώτης γνώσης.	Υψηλή: διαφορετικοί ρόλοι, σύνολα δεδομένων και αφετηρίες χρόνου.
R-07 Παρατεταμένη απώλεια TMS ή περιοχής νέφους.	Μέτρια με αβεβαιότητα· υψηλή επίπτωση.	Δηλωμένη ανθεκτικότητα νέφους και στατικές διαδρομές· μη δοκιμασμένη εναλλακτική.	Υψηλή: μικρή άμεση υποκατάσταση και διασυνοριακή επίπτωση.

Πηγή: Ποιοτική ανάλυση του συγγραφέα βάσει της §5.1.3, NIS2, άρθρου 21, KYA 1689/2025, NIST CSF 2.0 και ISO/IEC 27005:2022. Οι κατηγορίες δεν είναι στατιστικές εκτιμήσεις.

6.4.2 Σενάριο επίθεσης μέσω της αλυσίδας εφοδιασμού

Η επίθεση αρχίζει με στοχευμένο phishing σε διαχειριστή υποστήριξης του LogiLink Pro και παραβίαση λογαριασμού χωρίς ανθεκτική στο phishing πολυπαραγοντική ταυτοποίηση. Ο επιτιθέμενος εκδίδει νέο API token με δικαιώματα πέρα από τις αναγκαίες ροές αποστολών. Ως πρόσθετη τεχνική παραδοχή, κακώς περιορισμένη λειτουργία του εξυπηρετητή διασύνδεσης δέχεται εντολές διαχείρισης εργασιών μέσω αυτού του λογαριασμού. Η υπηρεσία εκτέλεσής τους διαθέτει υπερβολικά δικαιώματα προς WMS και κοινόχρηστα αρχεία. Αυτή η αλυσίδα εξηγεί τη δυνατότητα εξάπλωσης· δεν αποδίδεται σε συγκεκριμένη γνωστή ευπάθεια προϊόντος.

Στη +0 ώρα καταγράφεται ασυνήθιστος όγκος κλήσεων στην πύλη API. Τα λεπτομερή αρχεία του παρόχου δεν φτάνουν στο SIEM, οπότε λείπει η σύνδεση με την έκδοση διαπιστευτηρίων. Στη +6η ώρα απόπειρα πρόσβασης λογαριασμού υπηρεσίας εκτός αναμενόμενου εύρους καταγράφεται ως μεσαίας προτεραιότητας. Το κενό ανίχνευσης αφορά τη συσχέτιση εξωτερικής αλλαγής και εσωτερικής πρόσβασης, όχι μόνο τον όγκο συλλεγόμενων αρχείων.

Μετά την πρόσβαση σε εξυπηρετητή διασύνδεσης, ο επιτιθέμενος εξάγει περίπου 18.000 εγγραφές παραδόσεων και αναπτύσσει ransomware σε τμήμα του WMS και σε κοινόχρηστα αρχεία. Οι εγγραφές περιλαμβάνουν όνομα, διεύθυνση, τηλέφωνο και ελεύθερο πεδίο οδηγιών. Ο αριθμός των μοναδικών φυσικών προσώπων δεν είναι ακόμη γνωστός. Η εξαγωγή και τα πεδία αποτελούν παραδοχές του υποθετικού σεναρίου.

Στη +10η ώρα η κρυπτογράφηση WMS, η διακοπή τριών αποθηκών και η σοβαρή υποβάθμιση ITS θεμελιώνουν, στο σενάριο, γνώση σημαντικού περιστατικού NIS2. Παράλληλα, η μη διαθεσιμότητα δεδομένων παραδόσεων ενεργοποιεί την εξέταση GDPR ως εκτελούσας, χωρίς αναμονή εξαγωγής. Για τα ίδια ταυτοποιήσιμα δεδομένα χειριστών WMS απαιτείται χωριστή αξιολόγηση ως υπευθύνου. Η επιβεβαίωση στη +12η ή +26η ώρα δεν μηδενίζει ήδη αρχισμένη προθεσμία για το ίδιο επηρεασμένο σύνολο.

6.4.3 Χρονολόγιο γεγονότων, επίγνωσης και αποφάσεων

Ο χρόνος +0 αντιστοιχεί στο πρώτο καταγεγραμμένο σήμα στη LogiTrans, ενώ η ημέρα -3 προκύπτει από μεταγενέστερη ανακατασκευή στον πάροχο. Οι ώρες είναι σχετικές και δεν προσδιορίζουν πραγματική ημερομηνία· σε επιχειρησιακή εφαρμογή απαιτούνται απόλυτος χρόνος και ζώνη ώρας. Ο Πίνακας 6.8 διατηρεί τις ατελείς ή καθυστερημένες αποφάσεις ως ευρήματα. Η στήλη τεκμηρίων ορίζει τι θα έπρεπε να στηρίζει τα γεγονότα· δεν αντιστοιχεί σε πραγματικά αρχεία διαθέσιμα στον συγγραφέα.

Πίνακας 6.8: Χρονολόγιο του υποθετικού περιστατικού και σημεία απόφασης

Χρόνος	Γεγονός και διαθέσιμη γνώση	Απόφαση ή εκκρεμότητα	Απαιτούμενο τεκμήριο
Ημέρα -3	Παραβίαση λογαριασμού παρόχου και έκδοση API token.	Δεν υπάρχει γνώση στη LogiTrans· μεταγενέστερη ανακατασκευή.	Αρχεία παρόχου και χρονολόγιο έρευνας.
+0	Ασυνήθιστος όγκος API κλήσεων· ελλιπή αρχεία παρόχου.	Χαμηλής προτεραιότητας ένδειξη· καμία καταγεγραμμένη νομική απόφαση.	Αρχεία πύλης API.
+6	Λογαριασμός υπηρεσίας επιχειρεί πρόσβαση εκτός εύρους.	Μεσαίας προτεραιότητας ειδοποίηση SOC· δεν γίνεται η αναγκαία συσχέτιση.	Ειδοποίηση SIEM και δελτίο SOC.
+10	Κρυπτογράφηση WMS, διακοπή τριών αποθηκών και σοβαρή υποβάθμιση ITS. Μη διαθεσιμότητα δεδομένων παραδόσεων και ταυτοποιήσιμων στοιχείων χειριστών.	Γνώση σημαντικού περιστατικού NIS2. Χρειάζεται ενημέρωση πελατών ως εκτελούσας και χωριστή κρίση για ίδια δεδομένα χειριστών. Πρώτη ειδοποίηση πελατών καταγράφεται μόνο στη +20ή ώρα· η ίδια αξιολόγηση δεν τεκμηριώνεται.	Κατάσταση υπηρεσιών, τεχνικά στοιχεία και χωριστές εγγραφές παραβίασης.
+12	Το SOC συνδέει ransomware και δραστηριότητα API.	Εσωτερική κήρυξη σοβαρού περιστατικού. Δεν μεταθέτει ήδη υφιστάμενη γνώση· δεν ταυτίζεται με πρώτη νομική απόφαση.	Χρονοσημασμένο αρχείο απόφασης.
+14	Κίνδυνος εξάπλωσης μέσω διασύνδεσης· το TMS δεν έχει κρυπτογραφηθεί.	Απομόνωση διασυνδέσεων WMS/ERP, ανάκληση διαπιστευτηρίων και ανεξάρτητη επικοινωνία. Το τετράωρο από +10 χρειάζεται επιχειρησιακή αιτιολόγηση.	Εντολές αλλαγών και ανακλήσεις.
+18	Σοβαρή διατάραξη και πιθανός διασυννοριακός αντίκτυπος.	Ελληνική έγκαιρη προειδοποίηση NIS2, 8 ώρες από τη γνώση.	Αντίγραφο και απόδειξη υποβολής.
+20	Αξιόπιστες ενδείξεις μη εξουσιοδοτημένης πρόσβασης σε δεδομένα πελατών.	Πρώτη καταγεγραμμένη ενημέρωση πελατών και συμβατική ενημέρωση τράπεζας. Το δεκάωρο από τη γνωστή μη διαθεσιμότητα δεν αιτιολογείται επαρκώς. Δεν υποβάλλεται αναφορά DORA.	Περιεχόμενο, αποδέκτες και απόδειξη παραλαβής.
+26	Επιβεβαίωση εξαγωγής 18.000 εγγραφών παραδόσεων και ιδίων αρχείων ασφάλειας με αναγνωριστικά, IP και χρόνους. Άγνωστος αριθμός μοναδικών προσώπων.	Συμπλήρωση στοιχείων πελατών και αξιολόγηση ιδίων αρχείων. Η επιβεβαίωση δεν αποδεικνύει πρώτη γνώση· ελέγχονται προγενέστερα στοιχεία ανά σύνολο.	Έκθεση έρευνας, σύνολα δεδομένων και ιστορικό εκτιμήσεων.

Χρόνος	Γεγονός και διαθέσιμη γνώση	Απόφαση ή εκκρεμότητα	Απαιτούμενο τεκμήριο
+40	Καθαρό αντίγραφο WMS και σταδιακή λειτουργία δύο αποθηκών. Τρίτη αποθήκη και πλήρης εκτέλεση παραγγελιών παραμένουν ανεπιβεβαίωτες.	Μερική επαναφορά σε 30 ώρες από +10. Ο στόχος αποθήκης των 12 ωρών έχει ξεπεραστεί τουλάχιστον κατά 18 ώρες. Δεν τεκμηριώνεται πλήρης ανάκαμψη ή RPO.	Αρχεία επαναφοράς, έλεγχος καθαρότητας και επιχειρησιακή αποδοχή.
+58	Επικαιροποιημένα στοιχεία σοβαρότητας, έκτασης και περιορισμού.	Γνωστοποίηση NIS2, 48 ώρες μετά τη +10η ώρα.	Απόδειξη υποβολής και έκδοση αναφοράς.
+62	Η εκτίμηση για τα ίδια αρχεία ασφάλειας θεωρεί τον κίνδυνο μη απίθανο, χωρίς τεκμηριωμένο υψηλό κίνδυνο.	Γνωστοποίηση LogiTrans στην ΑΠΔΠΧ για αυτό το σύνολο. Οι 36 ώρες από +26 είναι διάστημα από επιβεβαίωση· η νομική αφετηρία χρειάζεται έλεγχο. Δεν καλύπτει αυτομάτως τα δεδομένα χειριστών WMS.	Γνωστοποίηση, αιτιολόγηση άρθρων 33–34 και στοιχεία πρώτης γνώσης.
+66	Οι πελάτες κρίνουν υψηλό κίνδυνο για μέρος των προσώπων των εξαγόμενων εγγραφών.	Ενημέρωση προσώπων από πελάτες με συνδρομή LogiTrans. Δεν αποδεικνύεται ότι ωρύτερα δεν μπορούσε να διαπιστωθεί υψηλός κίνδυνος· απαιτείται αιτιολόγηση χρόνου.	Αξιολόγηση, μοναδικοί αποδέκτες και αποστολή.
Εντός μήνα από +58	Προγραμματισμένο σημείο επανεξέτασης· δεν έχει δοθεί χρόνος ολοκλήρωσης χειρισμού του περιστατικού.	Τελική έκθεση NIS2 εφόσον έχει ολοκληρωθεί ο χειρισμός. Αν συνεχίζεται, έκθεση προόδου τότε και τελική εντός μήνα από την ολοκλήρωση. Δεν παρουσιάζεται ως ήδη αποδεδειγμένη υποβολή.	Κατάσταση χειρισμού και αποδεικτικό της απαιτούμενης έκθεσης.

Πηγή: Υποθετικό χρονολόγιο που διαμορφώθηκε για τις ανάγκες της μελέτης, με έλεγχο NIS2, άρθρων 23 και GDPR, άρθρων 33–34 βάσει EDPB Guidelines 9/2022 (2023). Οι 18.000 είναι εγγραφές, όχι μοναδικά πρόσωπα.

6.4.4 Αιτιολόγηση του περιστατικού ανά κανονιστικό πλαίσιο

Ο Πίνακας 6.9 εφαρμόζει τα κριτήρια των Κεφαλαίων 3–5 στα συγκεκριμένα δεδομένα. Διαχωρίζει τον ρόλο της LogiTrans, τον υπεύθυνο κάθε πελάτη και τη συμβατική σχέση με την τράπεζα. Η γνωστοποίηση στην ΑΠΔΠΧ του χρονολογίου είναι παραδοχή για την ίδια επεξεργασία της LogiTrans· πλήρης έλεγχος αρμόδιας ή επικεφαλής αρχής κατά GDPR απαιτεί την πραγματική διάρθρωση και τον τόπο λήψης αποφάσεων.

Η σημαντικότητα NIS2 στηρίζεται στη σοβαρή λειτουργική διατάραξη της καλυπτόμενης ITS υπηρεσίας λόγω απώλειας επίκαιρων δεδομένων από τρεις αποθήκες. Η ελληνική αναφορά απευθύνεται στην ΕΑΚ, μέσω της ομάδας απόκρισης EL-CSIRT (Εθνική Αρχή Κυβερνοασφάλειας, χ.χ.). Οι αναφορές +18 και +58 τηρούν αριθμητικά τα όρια από τη +10η ώρα, αλλά το διαθέσιμο περιθώριο δεν αποδεικνύει από μόνο του απουσία αδικαιολόγητης καθυστέρησης. Οι λοιπές εθνικές υποχρεώσεις παραμένουν εκτός ολοκληρωμένης αξιολόγησης.

Η πρώτη καταγεγραμμένη ειδοποίηση πελατών είναι στη +20ή ώρα, δέκα ώρες μετά τη γνωστή απώλεια διαθεσιμότητας. Δεν υπάρχει επαρκής αιτιολογία αυτού του διαστήματος και δεν μπορεί να χαρακτηριστεί αποδεδειγμένα έγκαιρη. Στη +26η επιβεβαιώνεται εξαγωγή 18.000 εγγραφών παραδόσεων και ιδίων αρχείων ασφάλειας. Η επιβεβαίωση δεν αποδεικνύει ότι τότε αποκτήθηκε για πρώτη φορά γνώση κάθε

παραβίασης. Για τα στοιχεία χειριστών WMS λείπει χωριστή τεκμηρίωση απόφασης. Οι πελάτες αξιολογούν με τη δική τους γνώση και τα δικά τους κριτήρια κινδύνου τα άρθρα 33–34.

Η συμβατική ενημέρωση της τράπεζας στη +20ή ώρα δεν ισοδυναμεί με αναφορά DORA ούτε αποδεικνύει τήρηση συμβατικού χρόνου, αφού το ακριβές SLA δεν ορίζεται. Η τράπεζα θα έπρεπε να εξετάσει αν προκύπτει δικό της συμβάν ΤΠΕ και αν πληρούνται τα κριτήρια μείζονος συμβάντος. Το σενάριο δεν δίνει ταξινόμηση, χρόνο γνώσης ή υποβολή της τράπεζας και συνεπώς δεν επιτρέπει υπολογισμό προθεσμίας DORA.

Πίνακας 6.9: Δελτίο αιτιολόγησης κανονιστικής ενεργοποίησης

Κλάδος	Στοιχείο και κριτήριο	Απόφαση και όριο	Υπόχρεος και τεκμήριο
NIS2	Σοβαρή υποβάθμιση ITS στη +10η ώρα.	Σημαντικό περιστατικό· ελληνικές υποβολές +18/+58. Εκκρεμεί έλεγχος άλλων εγκαταστάσεων και αδικαιολόγητης καθυστέρησης.	Εξουσιοδοτημένος ρόλος LogiTrans προς EAK (EL-CSIRT)· απόφαση και υποβολές.
GDPR εκτελούσα	Μη διαθεσιμότητα παραδόσεων +10· εξαγωγή επιβεβαιώνεται +26.	Πρώτη ειδοποίηση +20. Το δεκάωρο απαιτεί αιτιολογία· η +26 δεν μηδενίζει προγενέστερη γνώση.	LogiTrans προς κάθε πελάτη· χρόνος, περιεχόμενο και παραλαβή.
GDPR ίδια δεδομένα WMS	Μη διαθεσιμότητα ταυτοποιήσιμων δεδομένων χειριστών +10.	Απαιτείται κρίση άρθρων 33–34. Δεν παρέχεται απόφαση γνωστοποίησης ή μη· εκκρεμεί αξιολόγηση.	LogiTrans ως υπεύθυνη, με συμβουλή DPO· χωριστή εγγραφή και αιτιολόγηση.
GDPR ίδια αρχεία ασφάλειας	Επιβεβαιωμένη εξαγωγή +26· κίνδυνος μη απίθανος κατά την παραδοχή.	Γνωστοποίηση +62 και χωριστή κρίση άρθρου 34. Η πρώτη γνώση και η πληρότητα αιτιολόγησης παραμένουν προς έλεγχο.	Εξουσιοδοτημένος εκπρόσωπος προς ΑΠΔΠΧ στο σενάριο· αξιολόγηση και αποστολή.
GDPR πελάτες	Παραλαμβάνουν στοιχεία +20/+26· κρίνουν υψηλό κίνδυνο για μέρος προσώπων.	Δικές τους αποφάσεις 33–34. Η +66 δεν είναι καθολική προθεσμία. Δεν δίνονται χρόνοι γνωστοποίησης στις αρχές.	Κάθε πελάτης· δική του πρώτη γνώση, αξιολόγηση και ενημέρωση προσώπων.
DORA τράπεζα	Φυσική διανομή με βοηθητική διεπαφή· ενημέρωση +20.	Μόνο συμβατική διεπαφή. Απουσιάζουν στοιχεία δικού της συμβάντος ΤΠΕ, ταξινόμησης και υποβολής.	Τράπεζα για τυχόν DORA· LogiTrans για τις συμφωνημένες πληροφορίες.

Πηγή: Εφαρμογή του συγγραφέα βάσει NIS2, άρθρων 23 και 26, GDPR, άρθρων 4(12), 33–34 και 55–56, EDPB (2023), DORA, άρθρων 18–19 και Κανονισμών 2024/1772 και 2025/301.

6.5 Εφαρμογή του ενοποιημένου πλαισίου

6.5.1 Εφαρμογή των πέντε σταδίων

Ο Πίνακας 6.10 διατηρεί τα πέντε στάδια του Πίνακα 5.3, με ρητή κατάσταση ολοκλήρωσης. Η επιχειρησιακή απόκριση του χρονολογίου αποτελεί χωριστή ροή που τροφοδοτεί τα στάδια· δεν αποδεικνύει ότι υλοποιήθηκε και δοκιμάστηκε όλος ο προτεινόμενος οδικός χάρτης.

Τα στάδια 1–2 αποτυπώνονται στην αναλυτική χαρτογράφηση και στα μητρώα του σεναρίου. Για το στάδιο 3 προτείνονται οι A-01–A-09, με εκκρεμή υλοποίηση και εγκρίσεις. Στο στάδιο 4 σχεδιάζονται οι δοκιμές E-01–E-09, χωρίς αποτελέσματα εκτέλεσης. Στο στάδιο 5 υπολογίζονται μόνο οι διαθέσιμοι χρόνοι και προσδιορίζονται οι αναγκαίες αποφάσεις επανεξέτασης. Καμία προτεινόμενη ενέργεια δεν εμφανίζεται ως κλειστή.

Πίνακας 6.10: Εφαρμογή του πλαισίου του Κεφαλαίου 5 στη LogiTrans

Στάδιο	Εφαρμογή	Παραδοτέο και κατάσταση	Κριτήριο μετάβασης
1. Οριοθέτηση και χαρτογράφηση	Υπηρεσίες, ρόλοι, τρίτοι και ελληνική υπαγωγή.	Πίνακες 6.1–6.6· αναλυτική αποτύπωση με κενά δικαιοδοσίας και RPO.	Επιβεβαίωση πραγματικού πεδίου και υπεύθυνος για κάθε άγνωστο στοιχείο.
2. Κίνδυνοι και αποκλίσεις	Σύνδεση R-01–R-07 με G-01–G-09.	Πίνακες 6.7/6.12· αξιολόγηση βάσει παραδοχών.	Αιτιολόγηση κατάταξης και χωριστή δήλωση αβεβαιότητας.
3. Μέτρα και αντιμετώπιση	Πρόταση A-01–A-09 και εξαρτήσεις.	Πίνακας 6.13· σχεδιασμένο πρόγραμμα, εκκρεμούν έγκριση και υλοποίηση.	Πραγματικά τεκμήρια εγκατάστασης/εφαρμογής πριν από δοκιμή.
4. Δοκιμή και ετοιμότητα	Προδιαγραφές δοκιμών πρόσβασης, απόφασης και ανάκαμψης.	E-01–E-09· απαιτούμενα τεκμήρια, χωρίς εκτέλεση ή επιτυχή αποτελέσματα.	Επιτυχής έλεγχος κριτηρίων ή επιστροφή στο στάδιο 3.
5. Μέτρηση και βελτίωση	Διαθέσιμοι χρόνοι, αβεβαιότητες και προτεινόμενη ανασκόπηση.	Πίνακας 6.11· υπολογισμοί σεναρίου, χωρίς πραγματική διοικητική έγκριση.	Απόφαση με υπεύθυνο, προθεσμία και στάδιο επανεκτέλεσης.

Πηγή: Εφαρμογή του συγγραφέα των σταδίων του Κεφαλαίου 5. Η κατάσταση διαχωρίζει ανάλυση σεναρίου, σχεδιασμό και εκκρεμή υλοποίηση.

6.5.2 Ενιαίο μητρώο αποφάσεων και διατήρηση τεκμηρίων

Το αρχείο αποφάσεων της §5.4 εξειδικεύεται με χωριστή εγγραφή ανά οντότητα, επεξεργασία και νομικό κλάδο. Κάθε εγγραφή συνδέει χρόνο και πηγή γνώσης, κριτήριο, αποφασίζοντα, ενέργεια και αποδεικτικό. Διατηρούνται οι αρχικές εκτιμήσεις και οι αναθεωρήσεις. Οι 18.000 εγγραφές δεν μετατρέπονται σε αριθμό μοναδικών προσώπων χωρίς αποδιπλοποίηση.

Ο φάκελος τεκμηρίων προβλέπει ελεγχόμενη πρόσβαση, προέλευση, συγχρονισμένη ώρα και προστασία ακεραιότητας, με καταγραφή χειρισμών όπου απαιτείται. Η διάρκεια τήρησης αιτιολογείται ανά σκοπό και υποχρέωση. Οι εκδόσεις αποφάσεων και γνωστοποιήσεων τηρούνται σε σταθερό αρχείο, με περιορισμό περιττών προσωπικών δεδομένων. Η ελλιπής πρόσβαση στα αρχεία παρόχου καταγράφεται ως κενό και δεν θεραπεύεται με τη δήλωση ότι υπάρχει φάκελος.

Τα E-01–E-09 ορίζουν απαιτούμενα τεκμήρια κλεισίματος. Για παράδειγμα, το E-01 θα πρέπει να καταγράφει πληθυσμό λογαριασμών, κάλυψη και εξαιρέσεις και να περιέχει επιτυχή αρνητική δοκιμή πρόσβασης. Η δοκιμή δεν έχει πραγματοποιηθεί στο σενάριο. Αντίστοιχα, η υπογραφή όρου προμήθειας χρειάζεται χωριστό λειτουργικό έλεγχο έγκαιρης παράδοσης αρχείων.

6.5.3 Αποτίμηση χρόνων και επιχειρησιακής επίδοσης

Ο Πίνακας 6.11 χρησιμοποιεί τις χρονικές παραδοχές του Πίνακα 6.8 και δηλώνει τη σχέση τους με τους K1–K8 του Κεφαλαίου 5. Ο K5 υπολογίζεται για τις δύο αναφορές NIS2. Για τα ίδια αρχεία ασφάλειας, οι

36 ώρες είναι διάστημα επιβεβαίωσης εξαγωγής–γνωστοποίησης και αποτελούν νομικό δείκτη μόνο εφόσον τεκμηριωθεί η +26η ως πρώτη γνώση. Οι K1–K3, K6–K8 δεν υπολογίζονται: λείπουν πληθυσμοί, ολοκληρωμένες δοκιμές και περίοδοι. Ο K4 απαιτεί χρόνο πρώτης νομικής απόφασης, όχι εσωτερικής κήρυξης.

Πίνακας 6.11: Ενδεικτικοί δείκτες επίδοσης από το περιστατικό

Μέτρηση	Υπολογισμός σεναρίου	Σχέση με Κεφάλαιο 5	Ερμηνεία
Σήμα έως εσωτερική κήρυξη	$12 - 0 = 12$ ώρες.	Διαγνωστικός χρόνος· δεν είναι ο K4.	Λείπει ακριβής πρώτη νομική απόφαση ανά κλάδο για υπολογισμό K4.
NIS2 προειδοποίηση	Διάρκεια: $18 - 10 = 8$ ώρες. Όριο +34· περιθώριο $34 - 18 = 16$ ώρες.	K5, αρχικό στάδιο.	Αριθμητικά εντός 24 ωρών· δεν αποδεικνύεται απουσία αδικαιολόγητης καθυστέρησης.
NIS2 γνωστοποίηση	Διάρκεια: $58 - 10 = 48$ ώρες. Όριο +82· περιθώριο $82 - 58 = 24$ ώρες.	K5, γνωστοποίηση περιστατικού.	Ίδια αφετηρία +10· παραμένει χωριστός έλεγχος καθυστέρησης.
GDPR ειδοποίηση πελατών	$20 - 10 = 10$ ώρες από μη διαθεσιμότητα.	Δεν υπολογίζεται K5: το άρθρο 33(2) δεν ορίζει αριθμητικό περιθώριο.	Η καθυστέρηση δεν αιτιολογείται επαρκώς· δεν εφαρμόζεται 72ωρο στην εκτελούσα.
GDPR ίδια αρχεία ασφάλειας	$62 - 26 = 36$ ώρες από επιβεβαίωση. Αν πρώτη γνώση = +26, όριο +98 και K5 = 36 ώρες.	Υπό όρο υπολογισμός· πρώτη γνώση δεν έχει επαληθευθεί.	Αν γνώση προϋπήρχε, ο χρόνος αλλάζει. Δεν καλύπτονται τα ίδια δεδομένα WMS ή οι πελάτες.
Αποθήκη, μερική επαναφορά	$40 - 10 = 30$ ώρες. $30 - 12 = 18$ ώρες ελάχιστης απόκλισης RTO.	Σύγκριση υπηρεσίας· δεν είναι επιτυχής δοκιμή K6.	Άγνωστος χρόνος πλήρους λειτουργίας. Δεν αποδεικνύεται RPO ή πλήρης ανάκαμψη παραγγελιών.
Κάλυψη και δοκιμές	Δεν υπολογίζονται K1–K3 και K6–K8.	Λείπουν πληθυσμοί, ολοκληρωμένες δοκιμές και περίοδοι.	Δεν χρησιμοποιούνται 0% ή 100% για να καλυφθούν ελλείποντα δεδομένα.

Πηγή: Υπολογισμοί του συγγραφέα από τον Πίνακα 6.8 και τους ορισμούς της §5.6. Οι τιμές είναι υποθετικές και οι νομικές κρίσεις διατηρούν τους δηλωμένους όρους.

6.6 Κενά, αιτίες και προτεραιότητες βελτίωσης

6.6.1 Διάκριση κενού ελέγχου και νομικής παράβασης

Ο Πίνακας 6.12 συνδέει κάθε κενό με συγκεκριμένο κριτήριο και νομική συνάφεια. Οι καταστάσεις «μη ικανοποίηση του κριτηρίου», «μερική ικανοποίηση του κριτηρίου» και «εκκρεμεί αξιολόγηση» περιγράφουν το αποτέλεσμα του ελέγχου στο υποθετικό σενάριο. Η διαπίστωση νομικής παράβασης απαιτεί χωριστή εξέταση της εφαρμοστέας υποχρέωσης και των σχετικών πραγματικών στοιχείων.

Η R-01 συνδέεται με G-01, A-01 και το απαιτούμενο E-01, αλλά η ιχνηλασιμότητα δεν είναι πάντοτε μία προς μία. Η A-02 καλύπτει πρόσβαση, εξαγωγή και αλλοίωση δεδομένων (R-01, R-02, R-05), ενώ η A-08

συνδέεται με ταυτότητα και TMS/ITS (R-03, R-07). Όλοι οι R-01–R-07 συνδέονται με τουλάχιστον ένα κενό και κάθε G με ενέργεια και τεκμήριο.

Πίνακας 6.12: Μητρώο κενών και προτεραιοτήτων

Κενό και κίνδυνος	Κριτήριο και διαπιστωμένο όριο	Νομική συνάφεια	Κατάσταση και προτεραιότητα	Ενέργεια
G-01 R-01	Ανθεκτική προστασία προνομιούχου πρόσβασης παρόχου· δεν καλύπτει τον λογαριασμό του σεναρίου.	NIS2, άρθρο 21(2)(θ)–(ι), GDPR, άρθρο 32.	Μη ικανοποίηση του κριτηρίου· κρίσιμη.	A-01
G-02 R-01, R-02, R-05	Μόνο αναγκαίες λειτουργίες API και απόρριψη μη εγκεκριμένης ανάγνωσης/αλλοίωσης· υπερευρεία δικαιώματα.	NIS2, άρθρο 21(2)(ε),(θ), GDPR, άρθρο 32.	Μη ικανοποίηση του κριτηρίου· κρίσιμη.	A-02
G-03 R-01, R-02	Συσχέτιση κρίσιμων γεγονότων παρόχου και εσωτερικών συστημάτων· αποσπασματική ροή αρχείων.	NIS2, άρθρο 21(2)(β),(στ), GDPR, άρθρο 32.	Μερική ικανοποίηση του κριτηρίου· κρίσιμη.	A-03
G-04 R-02, R-06	Τεκμηριωμένος ρόλος και εφαρμοστέοι συμβατικοί όροι ανά ροή· λείπει πλήρης αντιστοίχιση.	GDPR, άρθρο 24, 26, 28, 30 κατά περίπτωση.	Εκκρεμεί αξιολόγηση· υψηλή.	A-06
G-05 R-06	Απόφαση, αφετηρία και αιτιολογία ανά κλάδο· λείπει κρίση WMS και αιτιολογία δεκαώρου.	NIS2, άρθρο 20, 23· GDPR, άρθρα 33–34.	Μερική ικανοποίηση του κριτηρίου· κρίσιμη.	A-04
G-06 R-01, R-03, R-05, R-07	Επίκαιρες εξαρτήσεις API, ταυτότητας και TMS/ITS· ανακαλύπτονται διασυνδέσεις κατά τον περιορισμό.	NIS2, άρθρο 21(2)(α),(γ)· GDPR, άρθρο 30 όπου εφαρμόζεται.	Μερική ικανοποίηση του κριτηρίου· υψηλή.	A-09
G-07 R-04	Επαναφορά αποθήκης εντός RTO 12 ωρών· στη +40ή μόνο μερική λειτουργία μετά 30 ώρες.	NIS2, άρθρο 21(2)(γ),(στ), GDPR, άρθρο 32(1)(γ)–(δ).	Μη επίτευξη του εσωτερικού στόχου· υψηλή.	A-07
G-08 R-03, R-07	Ελεγμένη εναλλακτική πρόσβαση και λειτουργία TMS/ITS· λείπει πλήρης δοκιμή.	NIS2, άρθρο 21(2)(γ)–(δ),(στ).	Εκκρεμεί αξιολόγηση αποτελέσματος· υψηλή.	A-08
G-09 R-01, R-02	Κρίσιμοι τρίτοι με υπηρεσία, πρόσβαση, αποδεκτά τεκμήρια και επανεξέταση· ατελείς εγγραφές.	NIS2, άρθρο 21(2)(δ), 21(3)· GDPR, άρθρο 28 όπου εφαρμόζεται.	Μερική ικανοποίηση του κριτηρίου· υψηλή.	A-05

Πηγή: Αντιστοίχιση του συγγραφέα με NIS2, GDPR και ΚΥΑ 1689/2025. Η κατάσταση αφορά το συγκεκριμένο κριτήριο του σεναρίου και δεν αποτελεί συνολική διαπίστωση νομικής συμμόρφωσης.

6.6.2 Λογική ιεράρχησης

Τα G-01–G-03 έχουν κρίσιμη προτεραιότητα λόγω της ενεργής διαδρομής επίθεσης και το G-05 λόγω της εκκρεμούς έγκαιρης απόφασης. Τα υπόλοιπα χαρακτηρίζονται υψηλής προτεραιότητας. Η σοβαρότητα διαχωρίζεται από τον χρόνο ολοκλήρωσης του Πίνακα 6.13: μακρά τεχνική υλοποίηση δεν καθιστά χαμηλό τον κίνδυνο ούτε επιτρέπει αναμονή πριν από προσωρινά μέτρα.

Ο υπεύθυνος υλοποίησης εκτελεί την ενέργεια και ο ιδιοκτήτης υπηρεσίας ή κινδύνου αξιολογεί το αποτέλεσμα. Ο DPO συμβουλεύει, χωρίς να αναλαμβάνει την επιχειρησιακή αποδοχή κινδύνου. Καθυστέρηση καταγράφεται με προσωρινό μέτρο, υπεύθυνο και ημερομηνία επανεξέτασης. Δεσμευτική απαίτηση ή γνωστοποίηση δεν υποκαθίσταται από απόφαση αποδοχής· η σχετική ενέργεια παραμένει ανοικτή.

6.7 Πιθανές λύσεις και σχέδιο υλοποίησης

Οι ορίζοντες του Πίνακα 6.13 αφορούν το προτεινόμενο πρόγραμμα μετά τη σταθεροποίηση και την έγκρισή του, όχι περιθώριο αναμονής κατά το ενεργό περιστατικό. Η ανάκληση στη +14η ώρα είναι ήδη γεγονός περιορισμού. Οι μόνιμες διορθώσεις, οι υπεύθυνοι και τα κριτήρια κλεισίματος παραμένουν προτάσεις. Εξαρτώνται από πρόσβαση στον πάροχο, πόρους, ασφαλές περιβάλλον δοκιμών και ελεγχόμενες αλλαγές.

6.7.1 Άμεσες λύσεις: 0–30 ημέρες

Η A-01 ελέγχει την πληρότητα της ήδη πραγματοποιημένης ανάκλησης, επανεκδίδει όσα διαπιστευτήρια χρειάζονται και ενισχύει την ταυτοποίηση προνομιούχων χρηστών. Για λογαριασμούς μηχανής περιορίζει δικαιώματα, διάρκεια και έκδοση μυστικών· δεν αντιμετωπίζει το MFA ως μέτρο για κάθε API token. Οι εξαιρέσεις είναι προσωρινές και η αρνητική δοκιμή E-01 ελέγχει την απόρριψη απαγορευμένης πρόσβασης.

Η A-02 περιορίζει τη διαδρομή portal–ERP/WMS και ελέγχει την ακεραιότητα δεδομένων δρομολόγησης. Το E-02 περιλαμβάνει μη εξουσιοδοτημένη ανάγνωση, εξαγωγή και αλλαγή, μαζί με έλεγχο ότι οι αναγκαίες ροές συνεχίζονται. Η A-03 συσχετίζει έκδοση διαπιστευτηρίων, μαζική εξαγωγή και ασυνήθιστη πρόσβαση. Το E-03 απαιτεί μετρημένο χρόνο και περιεχόμενο ειδοποίησης.

Η A-04 ορίζει αποφασίζοντες, υποβάλλοντες και αναπληρωτές για NIS2, GDPR και συμβατική ενημέρωση της τράπεζας. Το βασικό ανεξάρτητο κανάλι έχει ήδη ενεργοποιηθεί στη +14η ώρα· η ενέργεια οργανώνει επαφές, ασφαλή πρόσβαση υποβολής και δοκιμή εκτός ωραρίου. Η A-08 επεκτείνει αργότερα την ανεξαρτησία και την εναλλακτική λειτουργία υπηρεσιών, χωρίς να αναβάλλει την άμεση επικοινωνία.

6.7.2 Βραχυπρόθεσμες λύσεις: 1–3 μήνες

Η A-05 ολοκληρώνει τις εγγραφές κρίσιμων προμηθευτών με υπηρεσία, πρόσβαση, δεδομένα, αποδεκτά τεκμήρια, υπεύθυνο και επανεξέταση. Το E-05 ελέγχει τον προκαθορισμένο πληθυσμό και τις εκκρεμότητες. Πλήρης καταχώριση δεν αρκεί για τον K3, αν τα τεκμήρια παραμένουν μη αποδεκτά ή μη ελεγμένα.

Η A-06 αντιστοιχίζει τις συμβάσεις σε πραγματικές υπηρεσίες και επεξεργασίες. Το άρθρο 28 εφαρμόζεται όπου υπάρχει σχέση υπευθύνου–εκτελούντος, με έλεγχο υπεργολάβων, συνδρομής, επιστροφής/διαγραφής και δικαιωμάτων ελέγχου. Οι επιχειρησιακοί όροι εξειδικεύουν πληροφορίες περιστατικού και συνεργασία. Υποχρεωτικός όρος δεν αντικαθίσταται από αποδοχή κινδύνου. Η σχέση με τραπεζικό πελάτη δεν μετατρέπει κάθε σύμβαση φυσικής διανομής σε σύμβαση υπηρεσίας TΠΕ DORA.

Η A-07 σχεδιάζει χωριστά άσκηση αποφάσεων και δοκιμή ανάκαμψης. Η δεύτερη ελέγχει την παραλαβή/αποθήκη έναντι RTO 12 ωρών και την πλήρη εκτέλεση παραγγελιών έναντι RTO 24 και RPO 4 ωρών, με καθορισμένο εύρος, ακεραιότητα δεδομένων και επιχειρησιακή αποδοχή. Η μερική επαναφορά στη +40ή ώρα δεν αντικαθιστά αυτές τις δοκιμές ούτε αποτελεί επιτυχία του K6.

6.7.3 Μεσοπρόθεσμες λύσεις: 3–12 μήνες

Η A-08 εξετάζει εναλλακτική πρόσβαση όταν αστοχεί η κοινή ταυτότητα και περιορισμένη λειτουργία TMS/ITS όταν δεν είναι διαθέσιμη η υποδομή νέφους. Προηγούνται ελάχιστο αποδεκτό επίπεδο υπηρεσίας, όριο χρόνου μετάβασης και προσωρινά μέτρα. Η επιλογή δεν προϋποθέτει αντικατάσταση κάθε πλατφόρμας ούτε θεωρεί τις χειροκίνητες διαδρομές επαρκείς χωρίς δοκιμή.

Για το portal προβλέπονται ελεγχόμενη εξαγωγή δεδομένων, ανάκληση πρόσβασης και πιλοτική μετάβαση περιορισμένων ροών. Το E-08 ορίζει χωριστά αποτελέσματα για ταυτότητα, TMS/ITS και portal, ώστε επιτυχία μιας ροής να μην εμφανίζεται ως συνολική ικανότητα εξόδου. Τυχόν αποτυχία διατηρεί ανοικτό το αντίστοιχο μέρος της A-08.

Η A-09 συνδέει αλλαγές σε API, αποθήκη, πάροχο ή περιοχή νέφους με επανεξέταση υπηρεσιών, ρόλων GDPR και επαφών. Μέχρι την ολοκλήρωση της διαδικασίας απαιτείται χειροκίνητη ενημέρωση για κρίσιμες αλλαγές. Σε πραγματική εφαρμογή, το E-09 θα ελέγχει προκαθορισμένο δείγμα ολοκληρωμένων αλλαγών και τις αντίστοιχες εγκρίσεις· δεν προϋποθέτει αυτοματοποίηση.

Πίνακας 6.13: Οδικός χάρτης πιθανών λύσεων για τη LogiTrans

Ενέργεια και ορίζοντας	Κενό και προτεινόμενη λύση	Υλοποίηση και ευθύνη	Απαιτούμενο τεκμήριο κλεισίματος
A-01 0–30 ημέρες	G-01: έλεγχος ανάκλησης, ισχυρή ταυτοποίηση χρηστών, περιορισμός και ασφαλής έκδοση διαπιστευτηρίων μηχανής.	Ομάδα πρόσβασης και πάροχος· CISO/ιδιοκτήτης υπηρεσίας εγκρίνει.	E-01: πληθυσμός λογαριασμών, εξαιρέσεις και αρνητική δοκιμή που απορρίπτει απαγορευμένη πρόσβαση.
A-02 0–30 ημέρες	G-02: διαχωρισμός διασύνδεσης, ελάχιστα δικαιώματα, έλεγχος δεδομένων και περιορισμός κλήσεων.	Αρχιτεκτονική IT· ιδιοκτήτες αποθήκης και μεταφορών αποδέχονται λειτουργία.	E-02: απόρριψη μη εξουσιοδοτημένης ανάγνωσης, μαζικής εξαγωγής και αλλοίωσης δρομολόγησης· επιτυχείς αναγκαίες ροές.
A-03 0–30 ημέρες	G-03: κρίσιμα αρχεία παρόχου στο SIEM ή ασφαλής προσωρινή εξαγωγή, με κανόνες συσχέτισης.	Υπεύθυνος SOC και πάροχος· CISO εγκρίνει κριτήρια.	E-03: δοκιμή έκδοσης token/εξαγωγής με ειδοποίηση εντός προεγκεκριμένου χρόνου και απαιτούμενα στοιχεία.
A-04 0–30 ημέρες	G-05: αποφασίζοντας, υποβάλλοντας, αναπληρωτές και εκτίμηση διαθεσιμότητας από το πρώτο κατάλληλο γεγονός.	CISO και εξουσιοδοτημένος εκπρόσωπος· νομική συνδρομή και συμβουλή DPO.	E-04: εγκρίσεις ρόλων, δοκιμή εκτός ωραρίου και χωριστές αιτιολογημένες αποφάσεις γνώσης/αναφοράς.
A-05 1–3 μήνες	G-09: ενιαίες εγγραφές κρίσιμων τρίτων και έλεγχος εύρους/επικαιρότητας τεκμηρίων.	Προμήθειες και ασφάλεια· ιδιοκτήτης κάθε υπηρεσίας.	E-05: έλεγχος όλων των εγγραφών του ορισμένου πληθυσμού, αριθμητής/παρονομαστής, εκκρεμότητες και αποδεκτά τεκμήρια.
A-06 1–3 μήνες	G-04: ρόλοι, εφαρμοστέοι όροι άρθρου 28, συνδρομή, υπεργολάβοι, πληροφορίες και έξοδος. Άμεση κλιμάκωση υποχρεωτικών ελλείψεων.	Νομική λειτουργία και ιδιοκτήτης σύμβασης· DPO συμβουλεύει.	E-06: υπογεγραμμένοι εφαρμοστέοι όροι και έλεγχος κάλυψης. Εκκρεμής δεσμευτική απαίτηση κρατά ανοικτή την A-06· δεν κλείνει με αποδοχή κινδύνου.

Ενέργεια και ορίζοντας	Κενό και προτεινόμενη λύση	Υλοποίηση και ευθύνη	Απαιτούμενο τεκμήριο κλεισίματος
A-07 1–3 μήνες	G-07: άσκηση αποφάσεων και πλήρης δοκιμή WMS/παραγγελιών με επιχειρησιακή αποδοχή.	Συνέχεια, IT και λειτουργίες· ιδιοκτήτης υπηρεσίας αποδέχεται.	E-07: χρόνος ανάκαμψης, RTO/RPO όπου ορίζονται, ακεραιότητα, αποδεκτό εύρος και επανέλεγχος αποτυχιών.
A-08 3–12 μήνες	G-08: εναλλακτική ταυτότητα, προσωρινή λειτουργία TMS/ITS και δοκιμή εξαγωγής/μετάβασης portal.	IT και επιχειρησιακή διοίκηση· ιδιοκτήτες υπηρεσιών.	E-08: δοκιμές ανά υπηρεσία με προεγκεκριμένο ελάχιστο επίπεδο και χρόνο μετάβασης· ανοικτές αστοχίες καταγράφονται.
A-09 3–12 μήνες	G-06: σύνδεση υπηρεσιών, δεδομένων και τρίτων με αλλαγές. Ενδιάμεσα χειροκίνητη ενημέρωση κρίσιμων μεταβολών.	Αρχιτεκτονική και ιδιοκτήτες υπηρεσιών· DPO συμβουλεύει για επεξεργασίες.	E-09: προκαθορισμένο δείγμα αλλαγών, ενεργοποιημένοι έλεγχοι, ενημερωμένα αρχεία και ολοκληρωμένες εγκρίσεις.

Πηγή: Σχέδιο του συγγραφέα βάσει των Πινάκων 6.7 και 6.12, NIS2, άρθρου 21, GDPR, άρθρων 25, 28 και 32, ENISA (2023), NIST CSF 2.0 και NIST SP 800-61 Rev. 3/800-161 Rev. 1, Update 1. Όλες οι A παραμένουν προτεινόμενες και τα E απαιτούμενα τεκμήρια.

6.7.4 Εφικτότητα, κόστος και υπολειπόμενος κίνδυνος

Η ταχύτητα υλοποίησης εξαρτάται από συμβατότητα, δικαιώματα διαχείρισης, εξάρτηση από τον πάροχο και παράθυρα αλλαγών. Δεν θεωρείται δεδομένο ότι ενεργοποίηση MFA ή αντικατάσταση πλατφόρμας ολοκληρώνεται άμεσα. Οι A-01/A-02 στηρίζουν τις δοκιμές πρόσβασης, η A-03 χρειάζεται διαθέσιμα αρχεία και η A-07 επαρκή χαρτογράφηση και καθαρό περιβάλλον ανάκαμψης. Κόστος και στελέχωση δεν εκτιμώνται αριθμητικά χωρίς προσφορές ή στοιχεία.

Η περιορισμένη εσωτερική ομάδα δίνει βάθος ελέγχου στους κρίσιμους προμηθευτές και ελαφρύτερη, τεκμηριωμένη διαδικασία στους υπόλοιπους. Η παρακολούθηση επιλέγει γεγονότα που μπορούν να στηρίξουν συγκεκριμένη απόφαση, όχι κάθε διαθέσιμο αρχείο. Ο ιδιοκτήτης κινδύνου εγκρίνει τις προτεραιότητες και καταγράφει προσωρινά αντισταθμιστικά μέτρα.

Η αναμενόμενη μείωση αφορά τις διαδρομές πρόσβασης, εξάπλωσης, ανίχνευσης και ανάκαμψης που στοχεύει κάθε ενέργεια. Παραμένει προς επαλήθευση με τα E-01–E-09. Χωρίς υλοποίηση και επιτυχή δοκιμή δεν αποδίδεται χαμηλότερος υπολειπόμενος κίνδυνος. Τυχόν μελλοντική αποδοχή χρειάζεται σαφές εύρος, λήξη και έλεγχο των δεσμευτικών υποχρεώσεων.

6.8 Αξιολόγηση της εφαρμογής, περιορισμοί και συμπεράσματα

6.8.1 Αποτελέσματα βάσει των προκαθορισμένων κριτηρίων

Η τελική αποτίμηση εφαρμόζει τα ΑΞ1–ΑΞ8 στα στοιχεία που έχουν ήδη δηλωθεί και συνδεθεί στους Πίνακες 6.1–6.13. Δεν προσθέτει μεταγενέστερα κριτήρια ούτε αντιμετωπίζει την εσωτερική συνέπεια του σεναρίου ως απόδειξη πραγματικής οργανωτικής επίδοσης.

ΑΞ1 Ικανοποιείται εν μέρει. Η εφαρμογή NIS2 και οι ρόλοι GDPR αιτιολογούνται υπό τις δηλωμένες παραδοχές, ενώ για τη DORA τεκμηριώνεται μόνο συμβατική ενημέρωση χρηματοπιστωτικού πελάτη. Η πλήρης διασυννοριακή δικαιοδοσία και η τελική τραπεζική ταξινόμηση παραμένουν ανοικτές.

ΑΞ2 Ικανοποιείται εν μέρει. Η NIS2 έχει σαφή αφετηρία στην +10η ώρα. Για ορισμένα σύνολα δεδομένων δεν τεκμηριώνεται με βεβαιότητα η πρώτη γνώση κατά GDPR, ενώ χωρίς τελική ταξινόμηση DORA δεν υπολογίζεται αντίστοιχη κανονιστική προθεσμία.

ΑΞ3 Ικανοποιείται ως προς τον αναλυτικό εντοπισμό. Οι πίνακες αναδεικνύουν την ανεπαρκώς αιτιολογημένη δεκάωρη αναμονή για ενημέρωση πελατών, καθώς και αποφάσεις ή εγκρίσεις που απουσιάζουν. Το εύρημα δεν αποδεικνύει αυτοτελώς παράβαση.

ΑΞ4 Ικανοποιείται στο επίπεδο του σχεδιασμού. Τα 9/9 κενά G-01–G-09 συνδέονται με ενέργεια A και προγραμματισμένο τεκμήριο E, ενώ όλοι οι κίνδυνοι R-01–R-07 συνδέονται με τουλάχιστον ένα κενό. Η πληρότητα αυτή αφορά τη δομή ιχνηλασιμότητας και όχι ολοκληρωμένη υλοποίηση.

ΑΞ5 Ικανοποιείται ως προς τον εντοπισμό. Τα εννέα αναμενόμενα τεκμήρια E-01–E-09 είναι ορατά ακριβώς επειδή κανένα δεν έχει ακόμη παραχθεί ή ελεγχθεί. Επομένως το πλαίσιο αποκαλύπτει το αποδεικτικό κενό χωρίς να το εμφανίζει ως κλειστό.

ΑΞ6 Ικανοποιείται εν μέρει. Οι υπηρεσίες έχουν δηλωμένους RTO/RPO, όμως η μερική επαναφορά της αποθήκης στην +40ή ώρα συνεπάγεται 30 ώρες διακοπής από την +10η ώρα και τουλάχιστον 18 ώρες υπέρβασης του RTO των 12 ωρών. Η πλήρης ανάκαμψη και η επίτευξη RPO δεν επαληθεύονται.

ΑΞ7 Ικανοποιείται. Το κεφάλαιο αποφεύγει τον συνολικό ισχυρισμό ότι η απόκριση ήταν «συμμορφωμένη» και διατηρεί χωριστές τις θετικές ενδείξεις, τα κενά και τις μη αξιολογημένες διαστάσεις.

ΑΞ8 Ικανοποιείται. Παραμένουν ρητά ανοικτά η διασυνοριακή δικαιοδοσία, ο χρόνος πρώτης γνώσης κατά GDPR, η ταξινόμηση DORA, η πλήρης ανάκαμψη και η παραγωγή των τεκμηρίων.

Συνολικά, το σενάριο δείχνει ότι το πλαίσιο είναι εσωτερικά συνεπές ως μηχανισμός οργάνωσης αποφάσεων και ανάδειξης ελλείψεων. Δεν αποδεικνύει ότι οι σχεδιασμένες ενέργειες μειώνουν χρόνο, κόστος ή κίνδυνο ούτε ότι επιτυγχάνεται κανονιστική συμμόρφωση στην πράξη.

6.8.2 Συγκριτική αποτίμηση έναντι βάσης αναφοράς

Η δομική σύγκριση χρησιμοποιεί ως βάση αναφοράς τη χωριστή ανάλυση ανά κανονιστικό πλαίσιο, όπως αυτή ορίζεται στον Πίνακα 6.14 για τα ίδια δεδομένα του σεναρίου. Στη συγκεκριμένη βάση δεν προβλέπονται κοινό μητρώο και ενιαίες συνδέσεις $R \rightarrow G \rightarrow A \rightarrow E$. Πρόκειται για παραδοχές της σύγκρισης και όχι για χαρακτηριστικά όλων των υφιστάμενων μεθόδων χωριστής ανάλυσης. Εξετάζεται η οργάνωση γεγονότων, αποφάσεων, ανοικτών ζητημάτων και τεκμηρίων, χωρίς πείραμα πριν και μετά ή μέτρηση χρόνου, κόστους και αποτελεσματικότητας.

Πίνακας 6.14: Σύγκριση χωριστής και ενοποιημένης ανάλυσης στο σενάριο

Διάσταση σύγκρισης	Βάση αναφοράς του σεναρίου	Ενοποιημένο πλαίσιο	Αποτίμηση και όριο
Κοινά πραγματικά στοιχεία	Οι ίδιες 14 εγγραφές ελέγχονται χωριστά ανά εφαρμοστέο σκέλος, χωρίς κοινό μητρώο στη συγκεκριμένη βάση.	Οι 14 εγγραφές τηρούνται στον Πίνακα 6.8 και συνδέονται με διακριτές αποφάσεις. Η τελευταία είναι προγραμματισμένο στάδιο.	Στη συγκεκριμένη δομή προβλέπεται μία κοινή καταγραφή· δεν μετρήθηκε εξοικονόμηση χρόνου.

Διάσταση σύγκρισης	Βάση αναφοράς του σεναρίου	Ενοποιημένο πλαίσιο	Αποτίμηση και όριο
Χωριστές κανονιστικές αποφάσεις	Τρία αυτοτελή σκέλη: NIS2, GDPR και DORA.	Διατηρούνται τρεις αυτοτελείς αποφάσεις με κοινό πραγματικό υπόβαθρο.	Η ενοποίηση δεν συγχωνεύει ούτε υποκαθιστά τη νομική κρίση ανά πλαίσιο.
Ανοιχτά ζητήματα	Το σενάριο δεν παρέχει ενιαίο παρονομαστή, επομένως δεν είναι δυνατή άμεση καταμέτρηση.	Καταγράφονται εννέα κενά G-01–G-09 στον Πίνακα 6.12, μαζί με εκκρεμότητες δικαιοδοσίας και ταξινόμησης.	Ο αριθμός δείχνει ορατότητα εκκρεμοτήτων, όχι αποδεδειγμένες νομικές παραβάσεις.
Ιχνηλασιμότητα $R \rightarrow G \rightarrow A \rightarrow E$	Στην ορισμένη βάση αναφοράς δεν προβλέπονται κοινές συνδέσεις $R \rightarrow G \rightarrow A \rightarrow E$ ούτε συγκρίσιμος παρονομαστής.	Τα 9/9 κενά συνδέονται με ενέργεια A και προγραμματισμένο τεκμήριο E, ενώ όλοι οι R-01–R-07 συνδέονται με τουλάχιστον ένα G.	Πρόκειται για 100% ιχνηλασιμότητα σχεδιασμού, όχι για 100% υλοποίηση ή αποτελεσματικότητα.
Ελλείποντα τεκμήρια	Η συγκεκριμένη βάση δεν ορίζει ενιαίο κατάλογο τεκμηρίων· δεν υπολογίζεται συγκρίσιμο ποσοστό.	Και τα 9/9 τεκμήρια E-01–E-09 παραμένουν προς παραγωγή.	Το αποτέλεσμα αποδεικνύει εντοπισμό ελλείψεων, όχι ολοκληρωμένη συμμόρφωση.

Πηγή: Συγκριτική αποτίμηση του συγγραφέα βάσει των Πινάκων 6.8 και 6.10–6.13. Η σύγκριση είναι αναλυτική και δεν αποτελεί μέτρηση πραγματικού χρόνου ή κόστους.

Το καταγράψιμο αποτέλεσμα του υποθετικού σεναρίου είναι η ρητή σύνδεση των στοιχείων: οι 14 εγγραφές του χρονολογίου, συμπεριλαμβανομένου του προγραμματισμένου τελικού σταδίου αναφοράς, τροφοδοτούν τρία χωριστά κανονιστικά σκέλη. Τα 9/9 κενά έχουν σχεδιασμένη συνέχεια προς A και E και τα 9/9 τεκμήρια εμφανίζονται ως εκκρεμή. Οι αριθμοί αποτυπώνουν την πληρότητα της συγκεκριμένης δομής, χωρίς να τεκμηριώνουν λειτουργική υπεροχή.

6.8.3 Περιορισμοί της μελέτης περίπτωσης

Η αποτίμηση αφορά μόνο τον σχεδιασμό στο συγκεκριμένο σενάριο. Τα E παραμένουν προδιαγραφές μελλοντικής επαλήθευσης και οι οργανωτικές αποφάσεις προτάσεις. Η απουσία πραγματικής υλοποίησης και ανεξάρτητης αξιολόγησης και οι συνέπειές της αναπτύσσονται συγκεντρωτικά στη §7.7.

Η υπαγωγή ITS, το μέγεθος και οι ρόλοι επεξεργασίας είναι παραδοχές που σε πραγματικό οργανισμό χρειάζονται εταιρικά στοιχεία, συμβάσεις και έλεγχο των εφαρμοστέων εθνικών κανόνων. Δεν έχει συμπληρωθεί πίνακας δικαιοδοσίας για τα τέσσερα κράτη ούτε εξέταση τραπεζικής ταξινόμησης DORA. Η χρονική βάση περιορίζεται σε εκείνη των Κεφαλαίων 3–5.

Η τεχνική ανακατασκευή απλοποιεί τις επιμέρους προσβάσεις, τη διάρκεια έρευνας και το εύρος επαναφοράς. Δεν υπάρχουν πραγματικά αρχεία για επαλήθευση ούτε πλήρης ανάλυση επιχειρησιακών επιπτώσεων για τους RTO/RPO. Λείπουν χρόνοι πλήρους ανάκαμψης, αναλυτικά στοιχεία γνώσης ανά επεξεργασία και ανεξάρτητη επιβεβαίωση των εκτιμήσεων κινδύνου.

6.8.4 Συνολικά συμπεράσματα

Ως προς το RQ4, η εφαρμογή δείχνει ότι το προτεινόμενο πλαίσιο μπορεί, υπό δηλωμένες παραδοχές, να συνδέσει κανονιστικό πεδίο, υπηρεσίες, γεγονότα, κινδύνους, κενά, ενέργειες και τεκμήρια χωρίς να συγχέει

τις αυτοτελείς κρίσεις NIS2, GDPR και DORA. Η αξιολόγηση ΑΞ1–ΑΞ8 εντοπίζει τόσο τα σημεία εσωτερικής συνέπειας όσο και τις περιοχές που παραμένουν μερικές ή μη επαληθευμένες.

Η συμβολή του κεφαλαίου είναι η ελέγξιμη σεναριακή αξιολόγηση με προκαθορισμένα κριτήρια και ρητή βάση αναφοράς. Το Κεφάλαιο 7 συνθέτει τα συμπεράσματα και προτείνει τη μελλοντική αξιοποίηση του πρωτοκόλλου σε πραγματική ή πιλοτική εφαρμογή, με επαληθευμένα χρονολόγια, παραγόμενα τεκμήρια, τιμές των Κ1–Κ8 και ανεξάρτητη αποτίμηση μετά την υλοποίηση.

ΚΕΦΑΛΑΙΟ 7 Συμπεράσματα, συμβολή και κατευθύνσεις μελλοντικής έρευνας

7.1 Σύνοψη

Η εργασία διερεύνησε πώς μπορούν να οργανωθούν από κοινού οι επιχειρησιακές πληροφορίες που χρειάζονται η κυβερνοασφάλεια, η προστασία δεδομένων και η ανθεκτικότητα της εφοδιαστικής αλυσίδας, χωρίς να συγχωνεύονται οι αυτοτελείς κρίσεις NIS2, GDPR και DORA. Η βιβλιογραφική και κανονιστική σύνθεση οδήγησε σε έξι απαιτήσεις σχεδιασμού, ένα πλαίσιο πέντε σταδίων και την αλυσίδα ιχνηλασιμότητας $R \rightarrow G \rightarrow A \rightarrow E$. Η σεναριακή εφαρμογή στη LogiTrans αξιολόγησε την εσωτερική συνέπεια αυτής της πρότασης με τα προκαθορισμένα κριτήρια $A\Xi 1 - A\Xi 8$. Το κεντρικό συμπέρασμα είναι ότι μία κοινή βάση πραγματικών στοιχείων μπορεί να βελτιώνει την ορατότητα και την ιχνηλασιμότητα, αλλά η νομική υπαγωγή, οι χρονικές αφετηρίες, οι αποφάσεις γνωστοποίησης και η αποδοχή των τεκμηρίων πρέπει να παραμένουν διακριτές και αιτιολογημένες.

7.2 Απάντηση στο RQ1 Ψηφιακές εξαρτήσεις

RQ1: Πώς οι ψηφιακές και οργανωτικές εξαρτήσεις υπηρεσιών, συστημάτων και τρίτων διαμορφώνουν τον κυβερνοκίνδυνο στην εφοδιαστική αλυσίδα; Η απάντηση είναι ότι ο κίνδυνος διαμορφώνεται από αλυσίδες αλληλεξάρτησης και όχι από μεμονωμένα περιουσιακά στοιχεία. Κοινές υπηρεσίες ταυτότητας, API, υποδομές νέφους, πάροχοι και εξωτερικές ομάδες δημιουργούν κοινά σημεία αστοχίας: μία τεχνική παραβίαση μπορεί έτσι να μεταφερθεί σε περισσότερα συστήματα, να διακόψει υπηρεσίες και να επηρεάσει ταυτόχρονα επιχειρησιακές, κανονιστικές και συμβατικές υποχρεώσεις.

Η κατάλληλη μονάδα ανάλυσης είναι συνεπώς η επιχειρησιακή υπηρεσία μαζί με τα συστήματα, τα δεδομένα, τους ανθρώπους και τα τρίτα μέρη που την υποστηρίζουν. Στο σενάριο, το TMS παραμένει τεχνικά διαθέσιμο, αλλά η αστοχία WMS υποβαθμίζει τη δρομολόγηση και την υπηρεσία ITS. Το εύρημα επιβεβαιώνει την ανάγκη χαρτογράφησης εξαρτήσεων, στόχων RTO/RPO και εναλλακτικής λειτουργίας ανά υπηρεσία (§§2.4, 5.2 και 6.2–6.3). Δεν ποσοτικοποιεί πιθανότητες ούτε αποδεικνύει το μέγεθος πραγματικής μείωσης του κινδύνου.

7.3 Απάντηση στο RQ2 Κανονιστική σύγκριση

RQ2: Ποια στοιχεία των NIS2, GDPR και DORA μπορούν να υποστηριχθούν από κοινή επιχειρησιακή οργάνωση και ποιες κρίσεις πρέπει να παραμένουν διακριτές; Κοινά μπορούν να οργανωθούν ο κατάλογος υπηρεσιών και εξαρτήσεων, το χρονολόγιο γεγονότων, οι πηγές γνώσης, τα επηρεαζόμενα δεδομένα, οι τρίτοι, οι υπεύθυνοι, οι ενέργειες και τα μεταδεδομένα των τεκμηρίων. Τα ίδια πραγματικά στοιχεία μπορούν να επαναχρησιμοποιούνται, αρκεί να διατηρούνται η προέλευση, ο χρόνος, η έκδοση και η αβεβαιότητά τους.

Διακριτές παραμένουν η υπαγωγή και η αρμόδια δικαιοδοσία, ο ρόλος υπευθύνου ή εκτελούντος ανά επεξεργασία, η σημασία περιστατικού NIS2, η ύπαρξη και ο κίνδυνος παραβίασης προσωπικών δεδομένων, η ταξινόμηση συμβάντος DORA, η χρονική αφετηρία κάθε προθεσμίας και η τελική απόφαση γνωστοποίησης. Επομένως, η σύνθεση των Κεφαλαίων 3–4 δεν προτείνει μία ενιαία κρίση συμμόρφωσης αλλά κοινή επιχειρησιακή βάση με χωριστές εγγραφές απόφασης, αρμόδιους αποφασίζοντες και αιτιολογία. Η εφαρμογή στη LogiTrans επιβεβαιώνει αυτή τη διάκριση: τεκμηριώνει ελληνικές παραδοχές NIS2 και

ρόλους GDPR, αλλά αφήνει ανοικτές τη διασυννοριακή δικαιοδοσία και την τραπεζική ταξινόμηση DORA (§§6.1.3 και 6.4.4).

7.4 Απάντηση στο RQ3 Σχεδιασμός του πλαισίου

RQ3: Πώς οργανώνεται ένα πλαίσιο που συνδέει απαιτήσεις, υπηρεσίες, κινδύνους, διορθώσεις, υπευθύνους και κριτήρια επαλήθευσης; Το πλαίσιο οργανώνεται από τις έξι απαιτήσεις σχεδιασμού DR1–DR6 και εφαρμόζεται σε πέντε στάδια: οριοθέτηση και χαρτογράφηση, αξιολόγηση κινδύνων και αποκλίσεων, επιλογή και υλοποίηση μέτρων, δοκιμή και ετοιμότητα, και μέτρηση με αναθεώρηση. Η επιχειρησιακή υπηρεσία λειτουργεί ως σημείο σύνδεσης των απαιτήσεων με τις εξαρτήσεις και τις επιπτώσεις.

Η ελεγκτική ραχοκοκαλιά είναι η αλυσίδα $R \rightarrow G \rightarrow A \rightarrow E$: κάθε κίνδυνος R συνδέεται με κενό G , κάθε κενό με διορθωτική ενέργεια A και κάθε ενέργεια με προκαθορισμένο τεκμήριο E . Η ανάθεση Responsible και Accountable οργανώνει την εκτέλεση χωρίς να μεταφέρει τη νομική ευθύνη, ενώ τα κριτήρια αποδοχής εμποδίζουν το κλείσιμο ενεργειών μόνο με βάση την ύπαρξη πολιτικής ή σχεδίου. Οι δείκτες K1–K8 χρησιμοποιούνται μετά την εφαρμογή για κάλυψη, χρόνο, τρίτα μέρη, αποφάσεις, γνωστοποιήσεις, ανάκαμψη, επικαιρότητα τεκμηρίων και επανάληψη αιτίων (§§5.1–5.6). Έτσι η μέθοδος παράγει ιχνηλατήσιμη πορεία από την απαίτηση έως την επαλήθευση, χωρίς να προεξοφλεί επιτυχία πριν παραχθούν τα τεκμήρια.

7.5 Απάντηση στο RQ4 Σεναριακή αξιολόγηση

RQ4: Ποιες δυνατότητες και ποια όρια αναδεικνύει η εφαρμογή του πλαισίου σε υποθετικό περιστατικό εταιρείας logistics; Η εφαρμογή δείχνει ότι το πλαίσιο μπορεί να διατηρήσει κοινό πραγματικό υπόβαθρο και ταυτόχρονα να απομονώσει τις αποφάσεις που χρειάζονται διαφορετική νομική αιτιολόγηση. Οι 14 εγγραφές του χρονολογίου, συμπεριλαμβανομένου του προγραμματισμένου τελικού σταδίου αναφοράς, καταγράφονται μία φορά και τροφοδοτούν τρία διακριτά κανονιστικά σκέλη. Όλοι οι R-01–R-07 συνδέονται με τουλάχιστον ένα κενό και τα 9/9 κενά G-01–G-09 με ενέργεια A και προγραμματισμένο τεκμήριο E . Παράλληλα, τα 9/9 τεκμήρια εμφανίζονται ως μη παραχθέντα, γεγονός που καθιστά ορατή την απόσταση ανάμεσα στον σχεδιασμό και στην ολοκλήρωση.

Η αξιολόγηση AΞ1–AΞ8 εντοπίζει επίσης τα όρια: το πεδίο εφαρμογής και οι χρονικές αφηρημένες ικανοποιούνται μόνο εν μέρει, η πλήρης ανάκαμψη και το RPO δεν επαληθεύονται, ενώ η μερική επαναφορά στην +40ή ώρα συνεπάγεται τουλάχιστον 18 ώρες υπέρβασης του RTO. Η διασυννοριακή δικαιοδοσία, η πρώτη γνώση για ορισμένες επεξεργασίες GDPR και η ταξινόμηση DORA παραμένουν ανοικτές. Άρα η εφαρμογή υποστηρίζει εσωτερική συνέπεια, ορατότητα ελλείψεων και ιχνηλασιμότητα σχεδιασμού· δεν αποδεικνύει πραγματική συμμόρφωση, ταχύτερη απόκριση, χαμηλότερο κόστος ή λειτουργική αποτελεσματικότητα (§§6.8.1–6.8.3).

Ο Πίνακας 7.1 συμπυκνώνει τις τελικές απαντήσεις, την κύρια τεκμηρίωσή τους και το όριο μέσα στο οποίο μπορούν να υποστηριχθούν.

Πίνακας 7.1: Αντιστοίχιση ερευνητικών ερωτημάτων, απαντήσεων και ορίων

RQ	Τελική απάντηση	Κύρια τεκμηρίωση	Όριο συμπεράσματος
RQ1	Οι αλληλεξαρτήσεις μεταφέρουν και ενισχύουν τον κίνδυνο μεταξύ υπηρεσιών, συστημάτων και τρίτων· η υπηρεσία είναι η κατάλληλη μονάδα ανάλυσης.	Χαρτογράφηση υπηρεσιών και εξαρτήσεων των Κεφαλαίων 2, 5 και 6.	Ποιοτική ανάλυση σεναρίου, χωρίς μέτρηση πιθανότητας ή πραγματικής μείωσης κινδύνου.
RQ2	Κοινά οργανώνονται τα πραγματικά και αποδεικτικά στοιχεία· χωριστές παραμένουν οι κρίσεις NIS2, GDPR και DORA.	Συγκριτική χαρτογράφηση Κεφαλαίων 3–4 και αποφάσεις του Κεφαλαίου 6.	Ανοικτές δικαιοδοσίες, χρονικές αφετηρίες και ταξινόμηση DORA δεν επιτρέπουν συνολική κρίση συμμόρφωσης.
RQ3	Οι DR1–DR6, τα πέντε στάδια και η αλυσίδα $R \rightarrow G \rightarrow A \rightarrow E$ συνδέουν απαιτήσεις, ευθύνες, ενέργειες και επαλήθευση.	Αρχιτεκτονική, μητρώα, κριτήρια κλεισίματος και K1–K8 του Κεφαλαίου 5.	Η πληρότητα του σχεδιασμού δεν ισοδυναμεί με υλοποίηση ή επιτυχή δοκιμή.
RQ4	Το σενάριο δείχνει ορατότητα, διακριτές αποφάσεις και πλήρη ιχνηλασιμότητα σχεδιασμού, αλλά και μη παραχθέντα τεκμήρια και ανοικτές κρίσεις.	Πρωτόκολλο ΑΞ1–ΑΞ8 και βάση αναφοράς των §§6.1.1 και 6.8.	Υποθετική εφαρμογή χωρίς ανεξάρτητη αξιολόγηση, μετρήσεις πριν/μετά ή απόδειξη αποτελεσματικότητας.

Πηγή: Σύνθεση του συγγραφέα των ερευνητικών ερωτημάτων του Κεφαλαίου 1 και των αποτελεσμάτων των Κεφαλαίων 2–6.

7.6 Συμβολή της εργασίας

Η συμβολή της εργασίας δεν βρίσκεται στην παραγωγή νέου νομικού κανόνα ούτε στην απόδειξη υπεροχής έναντι όλων των υφιστάμενων πλαισίων. Βρίσκεται στη συστηματική σύνθεση του προβλήματος και στη μετατροπή του σε ελέγξιμη λειτουργική μέθοδο. Για να αποφεύγεται ένας γενικός και ασαφής ισχυρισμός πρωτοτυπίας, η συμβολή διακρίνεται σε εννοιολογική, μεθοδολογική και πρακτική.

7.6.1 Εννοιολογική συμβολή

Η εννοιολογική συμβολή είναι η σαφής διάκριση ανάμεσα σε κοινή επιχειρησιακή πληροφορία και χωριστή κανονιστική απόφαση. Η υπηρεσία και οι εξαρτήσεις της αποτελούν κοινό σημείο αναφοράς, ενώ κάθε νομικό πλαίσιο διατηρεί δικό του πεδίο, υπόχρεο, αφετηρία, κριτήριο και αιτιολογία. Αυτή η διάκριση συνδέει τη βιβλιογραφία για τον κίνδυνο εφοδιαστικής αλυσίδας με τη συγκριτική ανάλυση NIS2, GDPR και DORA χωρίς να τα παρουσιάζει ως ενιαίο καθεστώς.

7.6.2 Μεθοδολογική συμβολή

Η μεθοδολογική συμβολή συνίσταται στη μετάβαση από έξι ρητές απαιτήσεις σχεδιασμού σε πλαίσιο πέντε σταδίων, στον κλειστό κύκλο ιχνηλασιμότητας $R \rightarrow G \rightarrow A \rightarrow E$ και στην απαίτηση προκαθορισμένου κριτηρίου αποδοχής πριν από το κλείσιμο μιας ενέργειας. Η αξιολόγηση δεν περιορίζεται σε αφηγηματική εφαρμογή· χρησιμοποιεί τα προκαθορισμένα ΑΞ1–ΑΞ8 και βάση δομικής σύγκρισης. Έτσι ο αναγνώστης μπορεί να ελέγξει ποιο στοιχείο στηρίζει κάθε συμπέρασμα, ποιο λείπει και σε ποιο επίπεδο παραμένει η αβεβαιότητα.

7.6.3 Πρακτική συμβολή

Η πρακτική συμβολή είναι ένα σύνολο επαναχρησιμοποιήσιμων παραδοτέων: χάρτης υπηρεσιών και εξαρτήσεων, μητρώο κανονιστικών αποφάσεων, μητρώα κινδύνων, κενών, ενεργειών, τρίτων και τεκμηρίων, δείκτες K1–K8 και υποδείγματα εφαρμογής. Τα παραδοτέα μπορούν να υποστηρίξουν διοίκηση, ασφάλεια, νομική λειτουργία, προστασία δεδομένων, προμήθειες και εσωτερικό έλεγχο, εφόσον προσαρμοστούν στο πραγματικό πεδίο, στους διαθέσιμους πόρους και στο τότε ισχύον δίκαιο.

Ο Πίνακας 7.2 αποτυπώνει τι είναι νέο σε κάθε διάσταση, ποιο παραδοτέο την υλοποιεί και ποιο όριο πρέπει να συνοδεύει τη χρήση της.

Πίνακας 7.2: Διαστάσεις, παραδοτέα και όρια της συμβολής

Διάσταση	Στοιχείο συμβολής	Κύριο παραδοτέο	Όριο
Εννοιολογική	Κοινή επιχειρησιακή πληροφορία με χωριστές κανονιστικές αποφάσεις και μονάδα αναφοράς την υπηρεσία.	Συγκριτική χαρτογράφηση πεδίων, αφετηριών, ρόλων και τεκμηρίων.	Σύνθεση και επιχειρησιακή εξειδίκευση υφιστάμενων απαιτήσεων, όχι νέα νομική θεωρία.
Μεθοδολογική	DR1–DR6, πέντε στάδια, R→G→A→E, κριτήρια κλεισίματος και αξιολόγηση AΞ1–AΞ8.	Αναπαραγωγή ροή από απαίτηση και υπηρεσία έως επαλήθευση και επανεξέταση.	Η εσωτερική συνέπεια του σχεδιασμού δεν αποδεικνύει εμπειρική αποτελεσματικότητα.
Πρακτική	Επαναχρησιμοποιήσιμα μητρώα, αρχεία αποφάσεων, δείκτες και υποδείγματα.	Εργαλεία για διοίκηση, απόκριση, DPO, νομική λειτουργία, προμήθειες και έλεγχο.	Απαιτούν πραγματικά δεδομένα, ιδιοκτησία, συντήρηση, πόρους και ανεξάρτητη δοκιμή.

Πηγή: Σύνθεση του συγγραφέα της συμβολής που αναπτύσσεται στα Κεφάλαια 4–6.

7.7 Περιορισμοί της εργασίας

Πρώτον, η βιβλιογραφική σύνθεση είναι δομημένη αλλά δεν αποτελεί πλήρη συστηματική ανασκόπηση με προκαθορισμένο πρωτόκολλο, εξαντλητικές βάσεις και διάγραμμα ροής επιλογής. Συνεπώς, δεν υποστηρίζεται ισχυρισμός καθολικής κάλυψης. Η κανονιστική ανάλυση διατηρεί χρονικό όριο την 31η Αυγούστου 2026 και κάθε πραγματική εφαρμογή απαιτεί έλεγχο του τότε ισχύοντος δικαίου και των αρμόδιων εθνικών κανόνων.

Δεύτερον, δεν πραγματοποιήθηκε πρωτογενής έρευνα σε οργανισμούς ούτε ανεξάρτητη αξιολόγηση από επαγγελματίες. Το πλαίσιο και το σενάριο αναπτύχθηκαν στην ίδια εργασία, γεγονός που περιορίζει τη δυνατότητα γενίκευσης και αυξάνει τον κίνδυνο εσωτερικής μεροληψίας. Η ευχρηστία, η συμφωνία μεταξύ αξιολογητών, ο φόρτος συντήρησης και η επίδραση στην ποιότητα των αποφάσεων παραμένουν άγνωστα.

Τρίτον, η LogiTrans, οι τεχνικές διαδρομές, τα μεγέθη και οι χρόνοι είναι υποθετικές παραδοχές. Δεν ολοκληρώθηκε πίνακας δικαιοδοσίας για όλες τις εγκαταστάσεις ούτε εφαρμόστηκε πραγματικό χρηματοπιστωτικό σενάριο DORA. Οι ενέργειες A-01–A-09 δεν υλοποιήθηκαν και τα E-01–E-09 δεν παρήχθησαν· επομένως, η ιχνηλασιμότητα είναι σχεδιαστική και όχι απόδειξη επιτυχούς ελέγχου ή συμμόρφωσης.

Τέταρτον, δεν υπάρχουν μετρήσεις πριν και μετά, ομάδα σύγκρισης, πραγματικά κόστη, επαρκείς σειρές περιστατικών ή πλήρης ανάλυση επιχειρησιακών επιπτώσεων. Οι K1–K8 δεν υπολογίστηκαν στο σύνολό

τους και η πλήρης ανάκαμψη δεν επαληθεύτηκε. Ως αποτέλεσμα, η εργασία δεν τεκμηριώνει αιτιώδη μείωση κινδύνου, εξοικονόμηση χρόνου, απόδοση επένδυσης ή λειτουργική υπεροχή έναντι άλλης μεθόδου.

7.8 Κατευθύνσεις μελλοντικής έρευνας

Η επόμενη ερευνητική φάση χρειάζεται να μεταφέρει το πλαίσιο από την εσωτερική συνέπεια στη διαψεύσιμη εμπειρική αξιολόγηση. Προτεραιότητα δεν είναι η προσθήκη περισσότερων πεδίων, αλλά ο έλεγχος αν τα υπάρχοντα πεδία, οι ρόλοι και τα κριτήρια βελτιώνουν πράγματι την πληρότητα και την ποιότητα των αποφάσεων με αποδεκτό οργανωτικό κόστος. Ο Πίνακας 7.3 προτείνει πέντε συμπληρωματικά σχέδια που καλύπτουν εγκυρότητα, εφαρμογή, μέτρηση, μεταφερσιμότητα και τεχνική υποστήριξη.

Συνολικά, η εργασία απαντά στα τέσσερα ερευνητικά ερωτήματα με μία ενιαία αλλά οριοθετημένη θέση: οι οργανισμοί μπορούν να μοιράζονται το κοινό επιχειρησιακό πληροφοριακό υπόβαθρο, τη χαρτογράφηση εξαρτήσεων και την αλυσίδα τεκμηρίωσης, αλλά οφείλουν να διατηρούν χωριστές τις κανονιστικές κρίσεις και να θεωρούν μια ενέργεια ολοκληρωμένη μόνο όταν έχει παραχθεί και ελεγχθεί το απαιτούμενο τεκμήριο. Η συνεισφορά είναι η λειτουργική και ελέγξιμη οργάνωση αυτής της θέσης.

Πίνακας 7.3: Προτεινόμενα σχέδια μελλοντικής έρευνας

Κατεύθυνση	Ερευνητικός σχεδιασμός	Κύρια δεδομένα	Κριτήριο αξιολόγησης
Επικύρωση από ειδικούς	Δομημένη ομάδα ή Delphi με επαγγελματίες ασφάλειας, νομικής, προστασίας δεδομένων, λειτουργιών και ελέγχου.	Συνάφεια DR1–DR6, σαφήνεια πεδίων, διαφωνίες και προτεινόμενες αλλαγές.	Τεκμηριωμένη συμφωνία και διατήρηση των χωριστών κανονιστικών κρίσεων.
Πιλοτικές εφαρμογές	Μελέτες σε πραγματικούς οργανισμούς logistics διαφορετικού μεγέθους με ανεξάρτητη αποτίμηση.	Πληρότητα μητρώων, αποδεκτά τεκμήρια, χρόνος εργασίας, σφάλματα και φόρτος συντήρησης.	Βιώσιμη χρήση χωρίς απώλεια ιχνηλασιμότητας ή παράκαμψη δεσμευτικών απαιτήσεων.
Μετρήσεις πριν και μετά	Επαναλαμβανόμενες ασκήσεις ή συγκρίσιμες περιόδους με τους ίδιους ορισμούς K1–K8.	Χρόνος απόφασης, περιθώριο γνωστοποίησης, κάλυψη τρίτων, επιτυχία ανάκαμψης και ηλικία τεκμηρίων.	Σταθερή βελτίωση με έλεγχο παράλληλων αλλαγών σε στελέχωση, συστήματα και περιστατικά.
Δικαιοδοσίες και DORA	Συγκριτικές περιπτώσεις σε διαφορετικά κράτη μέλη και σενάριο με πραγματικό χρηματοπιστωτικό αντισυμβαλλόμενο.	Εθνικοί κανόνες, αρμόδιες αρχές, συμβάσεις, ταξινόμηση συμβάντος ΤΠΕ και υποχρεώσεις ανταλλαγής πληροφοριών.	Ορθή μεταφορά του κοινού μοντέλου χωρίς εξομίωση δικαιοδοσιών ή υποχρέων.
Ανάκαμψη και ψηφιακή υποστήριξη	Ασκήσεις ανά υπηρεσία και πρωτότυπο εργαλείου με εκδόσεις, δικαιώματα και αρχείο ελέγχου.	RTO/RPO, αποδεκτό επίπεδο λειτουργίας, αποτυχίες δοκιμών, αλλαγές συνδέσεων και χρόνος ενημέρωσης.	Επαληθεύσιμη ανάκαμψη και λιγότερα σφάλματα ιχνηλασιμότητας χωρίς μεταφορά της νομικής κρίσης στο εργαλείο.

Πηγή: Πρόταση του συγγραφέα ερευνητικού σχεδιασμού βάσει των περιορισμών της παρούσας εργασίας.

Η επόμενη δοκιμασία της πρότασης δεν είναι ακόμη μία θεωρητική επέκταση, αλλά η ανεξάρτητη εφαρμογή της σε πραγματικές συνθήκες.

ΒΙΒΛΙΟΓΡΑΦΙΑ

- Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (2018). Απόφαση 65/2018 και κατάλογος πράξεων επεξεργασίας που υπόκεινται σε εκτίμηση αντικτύπου κατά το άρθρο 35 παράγραφος 4 GDPR. <https://www.dpa.gr/el/enimerwtiko/prakseisArxis/katalogos-me-ta-eidi-ton-praxeon-epexergasias-poy-ypokeintai-stin>
- Εθνική Αρχή Κυβερνοασφάλειας (2026). Εγκύκλιος 28427/30.07.2026, Διαχείριση ευπαθειών πληροφοριακών συστημάτων από τις βασικές οντότητες του Ν. 5160/2024. <https://cyber.gov.gr/wp-content/uploads/2026/09/%CE%94%CE%B9%CE%B1%CF%87%CE%B5%CE%AF%CF%81%CE%B9%CF%83%CE%B7-%CE%B5%CF%85%CF%80%CE%B1%CE%B8%CE%B5%CE%B9%CF%8E%CE%BD-%CE%B1%CF%80%CF%8C-%CF%84%CE%B9%CF%82-%CE%B2%CE%B1%CF%83%CE%B9%CE%BA%CE%AD%CF%82-%CE%BF%CE%BD%CF%84%CF%8C%CF%84%CE%B7%CF%84%CE%B5%CF%82-%CF%84%CE%BF%CF%85-%CE%BD.-5160-2024.pdf>
- Εθνική Αρχή Κυβερνοασφάλειας (χ.χ.). EL CSIRT: αρμοδιότητες και πεδίο δράσης της ομάδας απόκρισης. <https://cyber.gov.gr/el-csirt/>
- Ελληνική Δημοκρατία (2019). 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. https://www.dpa.gr/el/enimerwtiko/nomothesia/proswpika/nomothesia_prwsopikwn
- Ελληνική Δημοκρατία (2024). Ν. 5160/2024, Ενσωμάτωση της Οδηγίας (ΕΕ) 2022/2555 και άλλες διατάξεις. ΦΕΚ Α' 195/27.11.2024. https://cyber.gov.gr/wp-content/uploads/2024/12/ENOTHTA_5_%CE%9D%CE%9F%CE%9C%CE%9F%CE%98%CE%95%CE%A3%CE%99%CE%91_fek_a_195_2024-5160-2024.pdf
- Ελληνική Δημοκρατία (2025a). ΚΥΑ 1381/2025, Δημιουργία ψηφιακής πλατφόρμας για την εγγραφή των βασικών και σημαντικών οντοτήτων του άρθρου 4 του Ν. 5160/2024. ΦΕΚ Β' 463/10.02.2025, όπως τροποποιήθηκε. https://cyber.gov.gr/wp-content/uploads/2025/03/KYA_APOFASI_10-Feb-2025_FEK-463_DEFTERO-TEFHOS.pdf
- Ελληνική Δημοκρατία (2025b). ΚΥΑ 1689/2025, Εθνικό Πλαίσιο Απαιτήσεων Κυβερνοασφάλειας Βασικών και Σημαντικών Οντοτήτων. ΦΕΚ Β' 2186/06.05.2025. <https://cyber.gov.gr/wp-content/uploads/2025/05/20250202186.pdf>
- Ελληνική Δημοκρατία (2025c). ΥΑ 1899/2025, Καθορισμός προσόντων, καθηκόντων, ασυμβιβάστων και υποχρεώσεων των Υπεύθυνων Ασφαλείας Συστημάτων Πληροφορικής και Επικοινωνιών. ΦΕΚ Β' 4250/05.08.2025. 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

- Ευρωπαϊκή Ένωση (2016). Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών. Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, L 119, 4.5.2016, σ. 1–88. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- Ευρωπαϊκή Ένωση (2022a). Οδηγία (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση (NIS2). Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, L 333, 27.12.2022, σ. 80–152. <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>
- Ευρωπαϊκή Ένωση (2022b). Κανονισμός (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα (DORA). Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, L 333, 27.12.2022, σ. 1–79. <https://eur-lex.europa.eu/eli/reg/2022/2554/oj>
- Ευρωπαϊκή Επιτροπή (2003). Σύσταση 2003/361/ΕΚ, της 6ης Μαΐου 2003, σχετικά με τον ορισμό των πολύ μικρών, των μικρών και των μεσαίων επιχειρήσεων. Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, L 124, 20.5.2003, σ. 36–41. <https://eur-lex.europa.eu/eli/reco/2003/361/oj>
- Ευρωπαϊκή Επιτροπή (2024a). Εκτελεστικός Κανονισμός (ΕΕ) 2024/2690 σχετικά με τις τεχνικές και μεθοδολογικές απαιτήσεις εφαρμογής της NIS2 και τα σημαντικά περιστατικά συγκεκριμένων ψηφιακών παρόχων. https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj
- Ευρωπαϊκή Επιτροπή (2024b). Κατ' εξουσιοδότηση Κανονισμός (ΕΕ) 2024/1772 σχετικά με την ταξινόμηση περιστατικών ΤΠΕ και τα όρια ουσιαστικότητας κατά DORA. https://eur-lex.europa.eu/eli/reg_del/2024/1772/oj
- Ευρωπαϊκή Επιτροπή (2024c). Κατ' εξουσιοδότηση Κανονισμός (ΕΕ) 2024/1773 σχετικά με την πολιτική συμβατικών ρυθμίσεων για υπηρεσίες ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες. https://eur-lex.europa.eu/eli/reg_del/2024/1773/oj
- Ευρωπαϊκή Επιτροπή (2024d). Κατ' εξουσιοδότηση Κανονισμός (ΕΕ) 2024/1774 σχετικά με τα εργαλεία, τις μεθόδους, τις διαδικασίες και τις πολιτικές διαχείρισης κινδύνων ΤΠΕ και το απλουστευμένο πλαίσιο. https://eur-lex.europa.eu/eli/reg_del/2024/1774/oj
- Ευρωπαϊκή Επιτροπή (2024e). Εκτελεστικός Κανονισμός (ΕΕ) 2024/2956 σχετικά με τα τυποποιημένα υποδείγματα του μητρώου πληροφοριών κατά DORA. https://eur-lex.europa.eu/eli/reg_impl/2024/2956/oj
- Ευρωπαϊκή Επιτροπή (2025a). Κατ' εξουσιοδότηση Κανονισμός (ΕΕ) 2025/301 σχετικά με το περιεχόμενο και τις προθεσμίες των αναφορών μείζονων περιστατικών ΤΠΕ. https://eur-lex.europa.eu/eli/reg_del/2025/301/oj
- Ευρωπαϊκή Επιτροπή (2025b). Εκτελεστικός Κανονισμός (ΕΕ) 2025/302 σχετικά με τα έντυπα, τα υποδείγματα και τις διαδικασίες αναφοράς μείζονων περιστατικών ΤΠΕ. https://eur-lex.europa.eu/eli/reg_impl/2025/302/oj

- Ευρωπαϊκή Επιτροπή (2025c). Κατ' εξουσιοδότηση Κανονισμός (ΕΕ) 2025/532 σχετικά με την υπεργολαβία υπηρεσιών ΤΠΕ που υποστηρίζουν κρίσιμες ή σημαντικές λειτουργίες. https://eur-lex.europa.eu/eli/reg_del/2025/532/oj
- Ευρωπαϊκή Επιτροπή (2025d). Κατ' εξουσιοδότηση Κανονισμός (ΕΕ) 2025/1190 σχετικά με τις προηγμένες δοκιμές διείσδυσης βάσει απειλών κατά DORA. https://eur-lex.europa.eu/eli/reg_del/2025/1190/oj
- Ευρωπαϊκή Επιτροπή (2026, 8 Ιουλίου). Commission refers Ireland, Spain, France and the Netherlands to the Court of Justice for failing to fully transpose the NIS2 Directive. <https://digital-strategy.ec.europa.eu/en/news/commission-refers-ireland-spain-france-and-netherlands-court-justice-failing-transpose-rules>
- Συμβούλιο της Ευρωπαϊκής Ένωσης (2013). Κανονισμός (ΕΕ) 1024/2013, της 15ης Οκτωβρίου 2013, σχετικά με την ανάθεση ειδικών καθηκόντων στην Ευρωπαϊκή Κεντρική Τράπεζα όσον αφορά πολιτικές σχετικές με την προληπτική εποπτεία των πιστωτικών ιδρυμάτων. Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, L 287, 29.10.2013, σ. 63–89. <https://eur-lex.europa.eu/eli/reg/2013/1024/oj>
- Boyens, J., Smith, A., Bartol, N., Winkler, K., Holbrook, A., & Fallon, M. (2024). Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (NIST SP 800-161 Rev. 1, Update 1· αρχική έκδοση 2022). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-161r1-upd1>
- Boyson, S. (2014). Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. *Technovation*, 34(7), 342–353. <https://doi.org/10.1016/j.technovation.2014.02.001>
- Büyükoçkan, G., & Göçer, F. (2018). Digital Supply Chain: Literature review and a proposed framework for future research. *Computers in Industry*, 97, 157–177. <https://doi.org/10.1016/j.compind.2018.02.010>
- EDPB (2020). Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, version 2.0. https://www.edpb.europa.eu/documents/guideline/guidelines-42019-on-article-25-data-protection-by-design-and-by-default_en
- EDPB (2021). Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.1, adopted 7 July 2021. https://www.edpb.europa.eu/documents/guideline/guidelines-072020-on-the-concepts-of-controller-and-processor-in-the-gdpr_en
- EDPB (2022). Guidelines 01/2021 on Examples regarding Personal Data Breach Notification, version 2.0. Υιοθέτηση: 14 Δεκεμβρίου 2021· δημοσίευση τελικού κειμένου: 3 Ιανουαρίου 2022. https://www.edpb.europa.eu/documents/guideline/guidelines-012021-on-examples-regarding-personal-data-breach-notification_en
- EDPB (2023). Guidelines 9/2022 on Personal Data Breach Notification under GDPR, version 2.0. https://www.edpb.europa.eu/documents/guideline/guidelines-92022-on-personal-data-breach-notification-under-gdpr_en
- ENISA (2021). Threat Landscape for Supply Chain Attacks. ENISA. <https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks>

- ENISA (2023). Good Practices for Supply Chain Cybersecurity. ENISA. <https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity>
- Faber, N., de Koster, R., & Smidts, A. (2013). Organizing warehouse management. *International Journal of Operations & Production Management*, 33(9), 1230–1256. <https://doi.org/10.1108/IJOPM-12-2011-0471>
- Gellert, R. (2018). Understanding the notion of risk in the General Data Protection Regulation. *Computer Law & Security Review*, 34(2), 279–288. <https://doi.org/10.1016/j.clsr.2017.12.003>
- Ghadge, A., Weiß, M., Caldwell, N. D., & Wilding, R. (2020). Managing cyber risk in supply chains: A review and research agenda. *Supply Chain Management: An International Journal*, 25(2), 223–240. <https://doi.org/10.1108/SCM-10-2018-0357>
- Hendricks, K. B., Singhal, V. R., & Stratman, J. K. (2007). The impact of enterprise systems on corporate performance: A study of ERP, SCM, and CRM system implementations. *Journal of Operations Management*, 25(1), 65–82. <https://doi.org/10.1016/j.jom.2006.02.002>
- Ingram Micro Holding Corporation (2025, 5 Ιουλίου). Ingram Micro Issues Statement Regarding Cybersecurity Incident. Εταιρική ανακοίνωση, κατατεθειμένη στην SEC. <https://www.sec.gov/Archives/edgar/data/1897762/000162828025034372/pressrelease-cybersecurity.htm>
- ISO (2018). ISO 31000:2018, Risk management — Guidelines. ISO. Επίσημη περιγραφή του προτύπου. <https://www.iso.org/standard/65694.html>
- ISO (2019). ISO 22301:2019, Security and resilience — Business continuity management systems — Requirements. ISO. Επίσημη περιγραφή του προτύπου. <https://www.iso.org/standard/75106.html>
- ISO/IEC (2022a). ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection: Information security management systems: Requirements. Επίσημη περιγραφή του προτύπου. <https://www.iso.org/standard/27001>
- ISO/IEC (2022b). ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection: Guidance on managing information security risks. Επίσημη περιγραφή του προτύπου. <https://www.iso.org/standard/80585.html>
- Ivanov, D., & Dolgui, A. (2020). Viability of intertwined supply networks: extending the supply chain resilience angles towards survivability. A position paper motivated by COVID-19 outbreak. *International Journal of Production Research*, 58(10), 2904–2915. <https://doi.org/10.1080/00207543.2020.1750727>
- Latsiou, A., & Lambrinoudakis, C. (2026). Cyber Supply Chain Risk Management: From Threats to Treatment. *International Journal of Information Security*, 25, άρθρο 40. <https://doi.org/10.1007/s10207-025-01207-9>
- Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing. NIST SP 800-145. NIST. <https://doi.org/10.6028/NIST.SP.800-145>

- Nelson, A., Rekhi, S., Souppaya, M., & Scarfone, K. (2025). Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile (NIST SP 800-61 Rev. 3). Gaithersburg, MD: National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-61r3>
- NIST (2024). The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. <https://doi.org/10.6028/NIST.CSWP.29>
- Seid, E., Ilter, D., Blix, F., & Popov, O. (2025). Cyber Supply Chain Resilience: Analyzing ISO, NIST, and NIS2 Frameworks for Mitigating Third-Party Risks. *Procedia Computer Science*, 263, 591–599. <https://doi.org/10.1016/j.procs.2025.07.071>
- SolarWinds Corporation (2021). Annual Report on Form 10-K for the fiscal year ended December 31, 2020. Υποβολή στην SEC την 1.3.2021, ενότητα Cyber Incident. <https://www.sec.gov/Archives/edgar/data/1739942/000173994221000043/swi-20201231.htm>
- Yu, F., Carton, F., & Xiong, H. (2026). From policy to action: a cross-regulatory conceptual framework to address data and AI regulations. *Journal of Decision Systems*, 35(1), άρθρο 2669329. <https://doi.org/10.1080/12460125.2026.2669329>

ΠΑΡΑΡΤΗΜΑΤΑ

Πρακτικός οδηγός εφαρμογής

Υποδείγματα και χάρτες ροών

Τα παραρτήματα υποστηρίζουν την εφαρμογή του ενοποιημένου πλαισίου του Κεφαλαίου 5 σε μία συγκεκριμένη επιχειρησιακή υπηρεσία. Το Παράρτημα Α οργανώνει την πορεία εργασίας, το Παράρτημα Β συγκεντρώνει τα επαναχρησιμοποιήσιμα υποδείγματα και το Παράρτημα Γ παρουσιάζει τους χάρτες και τις εγγραφές ροών. Το υλικό χρησιμοποιείται μαζί με τις κανονιστικές διακρίσεις των Κεφαλαίων 3–4 και τα κριτήρια αξιολόγησης του Κεφαλαίου 6.

ΠΑΡΑΡΤΗΜΑ Α — Πρακτικός οδηγός εφαρμογής

A.1 Σκοπός και τρόπος χρήσης

Ο οδηγός απευθύνεται στον συντονιστή της εφαρμογής, στους ιδιοκτήτες υπηρεσιών και συστημάτων, στην ασφάλεια, στις προμήθειες και στις αρμόδιες κανονιστικές λειτουργίες. Η εργασία αρχίζει από σαφώς οριοθετημένη υπηρεσία, συνεχίζεται με κινδύνους, κενά και μέτρα και ολοκληρώνεται με δοκιμή και διοικητική ανασκόπηση. Σε ενεργό περιστατικό, η απόκριση και οι απαιτούμενες αποφάσεις εκτελούνται παράλληλα και δεν περιμένουν την ολοκλήρωση του κύκλου εφαρμογής.

Οι πίνακες του Παραρτήματος Β παρέχουν πεδία προς συμπλήρωση και όχι έτοιμες κρίσεις συμμόρφωσης. Οι χάρτες του Παραρτήματος Γ δείχνουν τον τρόπο τεκμηρίωσης των ροών. Οι χρόνοι, οι ρόλοι, οι κατηγορίες δεδομένων και τα κριτήρια προσαρμόζονται στην πραγματική υπηρεσία και επιβεβαιώνονται από τους αρμόδιους ιδιοκτήτες.

A.2 Προετοιμασία του φακέλου εφαρμογής

Επιλέγεται μία υπηρεσία με σαφή αρχή και τέλος, ιδιοκτήτη και αποδεκτό επίπεδο λειτουργίας. Καταγράφονται η νομική οντότητα, οι εγκαταστάσεις, οι χώρες, τα συστήματα, οι τρίτοι, οι στόχοι RTO/RPO και οι απαιτήσεις που ενδέχεται να εφαρμόζονται. Άγνωστα στοιχεία δεν συμπληρώνονται με παραδοχές: σημειώνονται ως εκκρεμότητες με συνέπεια για την αξιολόγηση, προσωρινό χειρισμό, υπεύθυνο και προθεσμία επιβεβαίωσης. Το υπόδειγμα B.2 αποτελεί την ελάχιστη εγγραφή έναρξης.

Η κατανομή εργασιών διακρίνει τον εκτελούντα, τον εσωτερικά υπόλογο, τους συμβουλευόμενους και τους ενημερούμενους. Ορίζονται επίσης αναπληρωτές, αρμόδιοι υποβολής και κανάλια κλιμάκωσης. Η οργανωτική ανάθεση δεν συγχωνεύει τις χωριστές αποφάσεις NIS2, GDPR και DORA ούτε μεταφέρει τη νομική ευθύνη από τον κατά περίπτωση υπόχρεο.

A.3 Στάδιο 1 Οριοθέτηση και χαρτογράφηση

Πρώτα αποτυπώνεται το περιβάλλον της υπηρεσίας και έπειτα οι εφαρμογές, οι αποθήκες δεδομένων, οι διασυνδέσεις και οι εξαρτήσεις της. Κάθε ουσιαστικής ροής αποκτά σταθερό κωδικό F, κατεύθυνση, σκοπό, ιδιοκτήτη και σχετικό τεκμήριο. Τα Σχήματα Γ.1–Γ.2 και οι Πίνακες Γ.1–Γ.2 δείχνουν τη μετάβαση από τον συνοπτικό χάρτη στην αναλυτική καρτέλα.

Ο χάρτης επαληθεύεται με ρυθμίσεις, συμβάσεις, τεχνική τεκμηρίωση και ελεγχόμενα δείγματα καταγραφών. Η μετάβαση στο στάδιο 2 επιτρέπεται όταν κάθε κρίσιμη ροή έχει πηγή, προορισμό, σκοπό,

υπεύθυνο και τεκμήριο ή ρητή εκκρεμότητα. Ο χάρτης μπορεί να τροφοδοτεί ειδικά αρχεία, όπως το αρχείο δραστηριοτήτων επεξεργασίας, χωρίς να τα αντικαθιστά.

A.4 Στάδιο 2 Από τη ροή στον κίνδυνο και στο κενό

Για κάθε κρίσιμη ροή ή κοινή εξάρτηση καταγράφεται η ακριβής απαίτηση και το ελέγξιμο κριτήριό της. Δημιουργείται εγγραφή κινδύνου R με απειλή ή αστοχία, αδυναμία, υπηρεσία, συνέπεια, υφιστάμενες δικλίδες και αβεβαιότητα. Η διαθεσιμότητα της υπηρεσίας και η επίπτωση στα δικαιώματα προσώπων αιτιολογούνται χωριστά, ακόμη και όταν προκύπτουν από το ίδιο γεγονός.

Η εγγραφή κενού G περιγράφει τι λείπει ή ποιο κριτήριο αποτυγχάνει, ποιος κίνδυνος επηρεάζεται και ποια τεκμηρίωση απαιτείται. Η μετάβαση στο στάδιο 3 προϋποθέτει ότι δεν υπάρχουν ασύνδετοι κίνδυνοι, κενά χωρίς κριτήριο ή κρίσεις που στηρίζονται μόνο στην απουσία στοιχείων. Η προτεραιότητα του κινδύνου διατηρείται χωριστά από τον χρόνο και τη δυσκολία υλοποίησης της διόρθωσης.

A.5 Στάδιο 3 Επιλογή και υλοποίηση μέτρων

Κάθε επιλεγμένη ενέργεια A συνδέεται με τα σχετικά G, R και F και αποκτά υπεύθυνο υλοποίησης, αρμόδιο αποδοχής, αρχική προθεσμία, πόρους, εξαρτήσεις, προσωρινά μέτρα και προκαθορισμένο τεκμήριο E. Το υπόδειγμα B.3 δείχνει αυτή την αλυσίδα. Τα κριτήρια επιτυχίας ορίζονται πριν από την αλλαγή, ώστε η ύπαρξη πολιτικής ή σχεδίου να μην εμφανίζεται ως απόδειξη λειτουργίας.

Οι καταστάσεις διακρίνονται ως προτεινόμενη, εγκεκριμένη, υλοποιημένη, ελεγμένη και κλειστή. Για τη μετάβαση σε «υλοποιημένη» απαιτείται απόδειξη της πραγματικής αλλαγής· για το κλείσιμο απαιτούνται αποδεκτό αποτέλεσμα και έγκριση. Αποτυχημένη δοκιμή επιστρέφει την ενέργεια σε διόρθωση, ενώ κάθε παράταση διατηρεί ορατή την αρχική προθεσμία.

A.6 Στάδιο 4 Δοκιμές και ετοιμότητα περιστατικών

Η δοκιμή εκτελείται με εγκεκριμένο πεδίο, εξουσιοδοτημένους συμμετέχοντες, κατάλληλα δεδομένα και προκαθορισμένες συνθήκες διακοπής. Εξετάζει τόσο την απόρριψη μη επιτρεπτών ενεργειών όσο και την επιτυχή λειτουργία των εγκεκριμένων ροών. Στην ανάκαμψη μετρώνται η αποκατάσταση του συμφωνημένου επιπέδου υπηρεσίας, το RTO/RPO, η ακεραιότητα και η επιχειρησιακή αποδοχή, όχι μόνο η επανεκκίνηση ενός συστήματος.

Σε περιστατικό ή άσκηση τηρείται κοινό χρονολόγιο πραγματικών στοιχείων και χωριστή εγγραφή απόφασης ανά υπόχρεο, επεξεργασία και κανονιστικό κλάδο. Καταγράφονται η πηγή και ο χρόνος γνώσης, το εφαρμοζόμενο κριτήριο, ο αποφασίζων, ο αποδέκτης, η προθεσμία και η απόδειξη υποβολής ή η αιτιολογία μη αναφοράς. Το δελτίο B.4 χρησιμοποιείται για την αποδοχή του τεκμηρίου και τον επανέλεγχο.

A.7 Στάδιο 5 Μέτρηση και διοικητική ανασκόπηση

Οι δείκτες K1–K8 χρησιμοποιούνται με τους ορισμούς και τους πληθυσμούς του Κεφαλαίου 5. Πριν από κάθε υπολογισμό επιβεβαιώνονται η πληρότητα των δεδομένων, η περίοδος, ο παρονομαστής και η σχέση με το αντίστοιχο κριτήριο. Άγνωστα δεδομένα και μηδενικοί παρονομαστές δεν μετατρέπονται σε 0% ή 100%, ενώ ένας θετικός χρόνος δεν αποδεικνύει από μόνος του έγκαιρη ή επαρκή απόφαση.

Η διοικητική ανασκόπηση παρουσιάζει τιμή, περίοδο, εύρος, αβεβαιότητες και απόφαση που απαιτείται. Κάθε απόφαση αποκτά υπεύθυνο και προθεσμία και παραπέμπει στο στάδιο που πρέπει να επανεκτελεστεί.

Το υπόδειγμα B.5 συγκεντρώνει τα ελάχιστα δεδομένα για κάλυψη, κλείσιμο ενεργειών, απόκριση, ανάκαμψη και επανάληψη αιτίων.

A.8 Ολοκλήρωση και επαναχρησιμοποίηση

Ο πρώτος κύκλος συγκεντρώνει εγγραφή ορίων και απαιτήσεων, χάρτη με λεξικό ροών, μητρώα R/G/A/E, φάκελο δοκιμών και αιτιολογημένη ανασκόπηση. Θεωρείται τεκμηριωμένος για το επιλεγμένο πεδίο όταν οι αποφάσεις συνδέονται με πραγματικά στοιχεία, οι ενέργειες έχουν ελεγχόμενη κατάσταση και κάθε ανοικτό θέμα έχει ιδιοκτήτη και ημερομηνία επανεξέτασης. Η διαπίστωση αυτή δεν ισοδυναμεί με πιστοποίηση συνολικής συμμόρφωσης.

Κατά την επέκταση σε άλλη υπηρεσία αντιγράφονται η δομή, οι κωδικοί και τα κριτήρια, όχι οι πραγματικές τιμές ή οι αποφάσεις του προηγούμενου φακέλου. Οι ροές, οι υπόχρεοι, οι στόχοι συνέχειας και οι απαιτήσεις επιβεβαιώνονται εκ νέου. Ο Πίνακας A.1 συνοψίζει τις πύλες μετάβασης που διατηρούν αυτή την πειθαρχία.

Πίνακας A.1: Πύλες μετάβασης του κύκλου εφαρμογής

Στάδιο	Ελάχιστη είσοδος	Κριτήριο μετάβασης	Κύριο αποτέλεσμα
1	Επιλεγμένη υπηρεσία, ιδιοκτήτης και αρχικά όρια.	Κάθε κρίσιμη ροή έχει πηγή, προορισμό, σκοπό, υπεύθυνο και τεκμήριο ή εκκρεμότητα.	Εγγραφή οριοθέτησης, χάρτης και λεξικό ροών.
2	Ροές, εξαρτήσεις και ακριβή κριτήρια απαιτήσεων.	Κάθε R συνδέεται με αξιολογημένο G· δεν υπάρχουν κενά χωρίς κριτήριο.	Μητρώα κινδύνων και κενών με προτεραιότητες.
3	Εγκεκριμένα κενά και προτεραιότητες.	Κάθε A έχει ιδιοκτήτη, προθεσμία, εξαρτήσεις και προκαθορισμένο E.	Σχέδιο ενεργειών και πραγματικά στοιχεία υλοποίησης.
4	Υλοποιημένες αλλαγές και εγκεκριμένο σχέδιο δοκιμής.	Το αποτέλεσμα καλύπτει όλα τα κριτήρια ή επιστρέφει την A σε διόρθωση.	Αναφορά δοκιμής, αποδεκτό E και ενημερωμένη κατάσταση A.
5	Επαληθευμένα δεδομένα δεικτών και ανοικτές αποφάσεις.	Η ανασκόπηση ορίζει απόφαση, υπεύθυνο, προθεσμία και στάδιο επανεκτέλεσης.	Δείκτες, πρακτικό ανασκόπησης και νέος κύκλος.

Πηγή: Σύνθεση του συγγραφέα βάσει της πεντασταδιακής μεθόδου και των παραδοτέων των Κεφαλαίων 5–6.

ΠΑΡΑΡΤΗΜΑ Β — Υποδείγματα και επεξήγηση πινάκων

Τα υποδείγματα μπορούν να τηρούνται σε ελεγχόμενο υπολογιστικό φύλλο ή αποθετήριο. Κάθε εγγραφή χρειάζεται σταθερό αναγνωριστικό, ιδιοκτήτη, έκδοση, ημερομηνία και σύνδεση με τα σχετικά τεκμήρια. Τα παραδείγματα συμπλήρωσης δείχνουν τη μορφή της πληροφορίας και δεν μεταφέρονται ως πραγματικά στοιχεία άλλου οργανισμού. Τα υποδείγματα μπορούν να συνυπάρχουν στο ίδιο σύστημα, εφόσον διατηρούν κοινά αναγνωριστικά και ιστορικό εκδόσεων, χωρίς να καταργούνται οι χωριστές εγκρίσεις, οι περίοδοι τήρησης ή τα δικαιώματα πρόσβασης κάθε εγγραφής.

B.1 Επιλογή υποδείγματος ανά ανάγκη

Ο Πίνακας B.1 λειτουργεί ως σημείο εισόδου. Ο χρήστης επιλέγει την ανάγκη, συμβουλευτεί την αντίστοιχη ανάλυση της κύριας εργασίας και δημιουργεί δική του εγγραφή με τη δομή του υποδείγματος. Η επιλογή ενός παραδοτέου δεν περιορίζει τον έλεγχο των λοιπών εφαρμοστέων απαιτήσεων.

Πίνακας B.1: Επιλογές υποδειγμάτων και παραδοτέων

Ανάγκη	Αναφορά	Δομή που προσαρμόζεται	Αναμενόμενο αποτέλεσμα
Πεδίο και απαιτήσεις	Πίνακας 4.1	Πίνακας 4.5 και παράδειγμα 6.2	Αιτιολογημένη εφαρμογή ανά οντότητα, υπηρεσία και διάταξη.
Οργάνωση έργου	Πίνακες 5.1–5.3	Πίνακες 6.3 και 6.10	Ρόλοι, αναπληρωτές και κατάσταση κάθε σταδίου.
Υπηρεσίες και δεδομένα	§5.1.1	Πίνακες 6.4–6.5, B.2 και Γ.1–Γ.2	Χάρτης εξαρτήσεων, ροές και ρόλοι ανά επεξεργασία.
Αξιολόγηση τρίτου	Πίνακας 5.4	Πίνακες 6.6 και 4.5	Πρόσβαση, κρισιμότητα, συμβάσεις και αποδεκτά τεκμήρια.
Κίνδυνοι και κενά	Πίνακες 4.3 και 4.5	Πίνακες 6.7 και 6.12	Κίνδυνοι R και κενά G με συγκεκριμένα κριτήρια.
Διορθωτικές ενέργειες	Πίνακας 5.6	Πίνακας 6.13 και B.3	Ενέργειες A, ιδιοκτήτες, προθεσμίες και απαιτούμενα E.
Περιστατικό και αναφορές	Πίνακες 4.2 και 5.4	Πίνακες 6.8–6.9	Χρονολόγιο και χωριστές αποφάσεις ανά υπόχρεο και κλάδο.
Σχέση με τράπεζα	Πίνακες 4.1 και 4.4	Πίνακες 6.2 και 6.9	Διάκριση είδους υπηρεσίας και συμβατικών ή κανονιστικών υποχρεώσεων.
Ανάκαμψη και μέτρηση	Πίνακες 5.6–5.7	Πίνακες B.4–B.5 και παράδειγμα 6.11	Δοκιμή υπηρεσίας, υποστηριζόμενοι δείκτες και αποφάσεις ανασκόπησης.

Πηγή: Αντιστοίχιση του συγγραφέα των πινάκων των Κεφαλαίων 4–6 με τις ανάγκες εφαρμογής.

B.2 Ελάχιστη εγγραφή έναρξης εφαρμογής

Ο Πίνακας B.2 συγκεντρώνει τα ελάχιστα πεδία για την έναρξη ενός νέου φακέλου εφαρμογής.

Πίνακας B.2: Ελάχιστη εγγραφή έναρξης εφαρμογής

Πεδίο	Τι συμπληρώνεται
Ταυτότητα υπηρεσίας	Κωδικός, περιγραφή αρχής και τέλους της λειτουργίας, πελάτες και ιδιοκτήτης.

Πεδίο	Τι συμπληρώνεται
Όρια	Νομική οντότητα, χώρες, εγκαταστάσεις, συστήματα, τρίτοι και αιτιολογημένες εξαιρέσεις.
Συνέχεια	Αποδεκτό επίπεδο υπηρεσίας, RTO, RPO, εύρος ανάκαμψης και πηγή έγκρισης. Άγνωστοι στόχοι παραμένουν εκκρεμείς.
Απαιτήσεις	Ακριβής διάταξη ή ρήτρα, υπόχρεος, αιτιολογία εφαρμογής και χωριστή ένδειξη νόμου, σύμβασης ή εσωτερικού στόχου.
Ρόλοι	Συντονιστής, ιδιοκτήτες δεδομένων και συστημάτων, αποφασίζοντες, υποβάλλοντες, αναπληρωτές και συμβουλευτικοί ρόλοι.
Έλεγχος έκδοσης	Ημερομηνία, έκδοση, εγκρίνων, επόμενη ανασκόπηση και αλλαγές που απαιτούν επανεξέταση.
Εκκρεμότητες	Άγνωστο στοιχείο, συνέπεια για την αξιολόγηση, προσωρινός χειρισμός, υπεύθυνος και προθεσμία επιβεβαίωσης.

Πηγή: Σύνθεση του συγγραφέα βάσει των §§5.1–5.2 και των Πινάκων 6.1–6.5.

B.3 Σύνδεση ροής κινδύνου κενού ενέργειας και τεκμηρίου

Το παράδειγμα δείχνει τη λογική σύνδεσης και όχι πραγματικό εύρημα. Οι κωδικοί T είναι αυτοτελείς και δεν προστίθενται στο μητρώο της LogiTrans.

Ο Πίνακας B.3 συνδέει μια διδακτική ροή με κίνδυνο, κενό, ενέργεια και απαιτούμενο τεκμήριο.

Πίνακας B.3: Παράδειγμα σύνδεσης $R \rightarrow G \rightarrow A \rightarrow E$

Εγγραφή	Διδακτική συμπλήρωση
Ροή και απαίτηση	F-02/F-03. Επιτρέπονται μόνο οι εγκεκριμένες εντολές και τα αναγκαία πεδία. Συνδέονται οι εφαρμοστέες διατάξεις, ρήτρες και τεχνικά κριτήρια.
T-R01 Κίνδυνος	Κατάχρηση διαπιστευτηρίου portal και υπερευρείων δικαιωμάτων με εξαγωγή ή αλλοίωση παραγγελιών και επίπτωση σε WMS/TMS. Η αδυναμία αποτελεί παραδοχή του παραδείγματος.
T-G01 Κενό	Ο λογαριασμός διασύνδεσης επιτρέπει ενέργειες πέρα από την εγκεκριμένη λειτουργία. Καταγράφονται η ρύθμιση και το αποτυχημένο κριτήριο πριν από τον τελικό χαρακτηρισμό.
T-A01 Ενέργεια	Περιορισμός λειτουργιών και δικαιωμάτων, έλεγχος δεδομένων και διαχωρισμός πρόσβασης. Υλοποιεί ο τεχνικός ιδιοκτήτης API και αποδέχεται ο ιδιοκτήτης υπηρεσίας με συνδρομή ασφάλειας.
Προθεσμία και εξάρτηση	Ορίζονται αρχική ημερομηνία, παράθυρο αλλαγής, συνδρομή παρόχου και προσωρινός περιορισμός. Τα πεδία παραμένουν εκκρεμή μέχρι την οργανωτική έγκριση.
T-E01 Τεκμήριο	Έκδοση ρυθμίσεων και αναφορά δοκιμής: απόρριψη μη εξουσιοδοτημένης ανάγνωσης, εξαγωγής και αλλαγής, μαζί με επιτυχία των εγκεκριμένων ροών παραγγελίας.
Κατάσταση	Προτεινόμενη ενέργεια και προδιαγραφή δοκιμής. Χωρίς εκτέλεση και αποδεκτό αποτέλεσμα δεν εμφανίζεται ως κλειστή.

Πηγή: Σύνθεση του συγγραφέα με τη λογική G-02/A-02/E-02 του Κεφαλαίου 6.

B.4 Δελτίο δοκιμής και αποδοχής τεκμηρίου

Ο Πίνακας B.4 οργανώνει το δελτίο δοκιμής και την αιτιολογημένη αποδοχή ή απόρριψη του τεκμηρίου.

Πίνακας B.4: Δελτίο δοκιμής και αποδοχής τεκμηρίου

Πεδίο	Οδηγία συμπλήρωσης
Σύνδεση	Κωδικοί δοκιμής/Ε, ενέργειας Α, απαίτησης, ροής F και υπηρεσίας.
Πεδίο και έκδοση	Συστήματα, εγκαταστάσεις, έκδοση ρυθμίσεων, εξαιρέσεις, ημερομηνία και ζώνη ώρας.
Εξουσιοδότηση	Εγκρίνων, εκτελών, αρμόδιος αποδοχής, παράθυρο δοκιμής και συνθήκες διακοπής.
Αναμενόμενο αποτέλεσμα	Μετρήσιμα κριτήρια πριν από την εκτέλεση. Στην T-E01 απορρίπτονται οι απαγορευμένες πράξεις και ολοκληρώνονται οι εγκεκριμένες.
Αποτέλεσμα εκτέλεσης	Πραγματικό αποτέλεσμα ανά περίπτωση, ώρα, απόκλιση και θέση σχετικού αρχείου. Σε μη εκτελεσμένο υπόδειγμα σημειώνεται ρητά «Δεν εκτελέστηκε».
Ανάκαμψη όπου αφορά	Χρόνος απώλειας και αποκατάστασης συμφωνημένου επιπέδου υπηρεσίας, RTO/RPO, ακεραιότητα και επιχειρησιακή αποδοχή.
Τελική κρίση	Επιτυχία, αποτυχία ή ατελής δοκιμή με αιτιολογία. Αποτυχίες και ακυρώσεις παραμένουν ορατές.
Επόμενη ενέργεια	Υπεύθυνος διόρθωσης, προθεσμία επανελέγχου, αποδοχή του Ε και ενημερωμένη κατάσταση της Α.

Πηγή: Σύνθεση του συγγραφέα βάσει της §5.5 και των κριτηρίων Ε του Πίνακα 6.13.

B.5 Επιλογή δεικτών και ελάχιστα δεδομένα

Ο Πίνακας B.5 συνδέει την ανάγκη μέτρησης με τον κατάλληλο δείκτη και τα ελάχιστα δεδομένα του.

Πίνακας B.5: Επιλογή δεικτών και ελάχιστα δεδομένα

Ανάγκη και δείκτες	Δεδομένα εισόδου	Έλεγχος πριν από την ερμηνεία
Κάλυψη K1, K3, K7	Πλήρεις πληθυσμοί υπηρεσιών, κρίσιμων τρίτων ή εφαρμοζόμενων ελέγχων· αποδεκτά και επίκαιρα στοιχεία.	Εξετάζονται όλα τα πεδία του αντίστοιχου ορισμού, όχι μόνο αν υπάρχει εγγραφή.
Κλείσιμο K2	Ενέργειες υψηλής προτεραιότητας, αρχικές προθεσμίες και ημερομηνία επαληθευμένου κλεισίματος.	Οι παρατάσεις δεν αλλάζουν τον αρχικό πληθυσμό της περιόδου.
Απόκριση K4, K5	Πρώτο σήμα, πρώτη τεκμηριωμένη απόφαση, αφετηρία γνώσης, καταληκτική ώρα και πραγματική υποβολή.	Χωριστά ανά κλάδο και υπόχρεο. Ο K4 δεν είναι νομική προθεσμία· ο K5 χρειάζεται αριθμητικό όριο.
Ανάκαμψη K6	Ολοκληρωμένες δοκιμές με προεγκεκριμένα κριτήρια και χωριστά πλήθη προγραμματισμένων και ακυρωμένων.	Επιτυχία μόνο όταν πληρούνται όλα τα κριτήρια του καθορισμένου πεδίου.
Επανάληψη K8	Ολοκληρωμένες αναλύσεις αιτίας, σταθερή περίοδος και κοινή ταξινόμηση· χωριστές εκκρεμότητες.	Η απουσία καταγεγραμμένης επανάληψης δεν αποδεικνύει εξάλειψη κινδύνου.

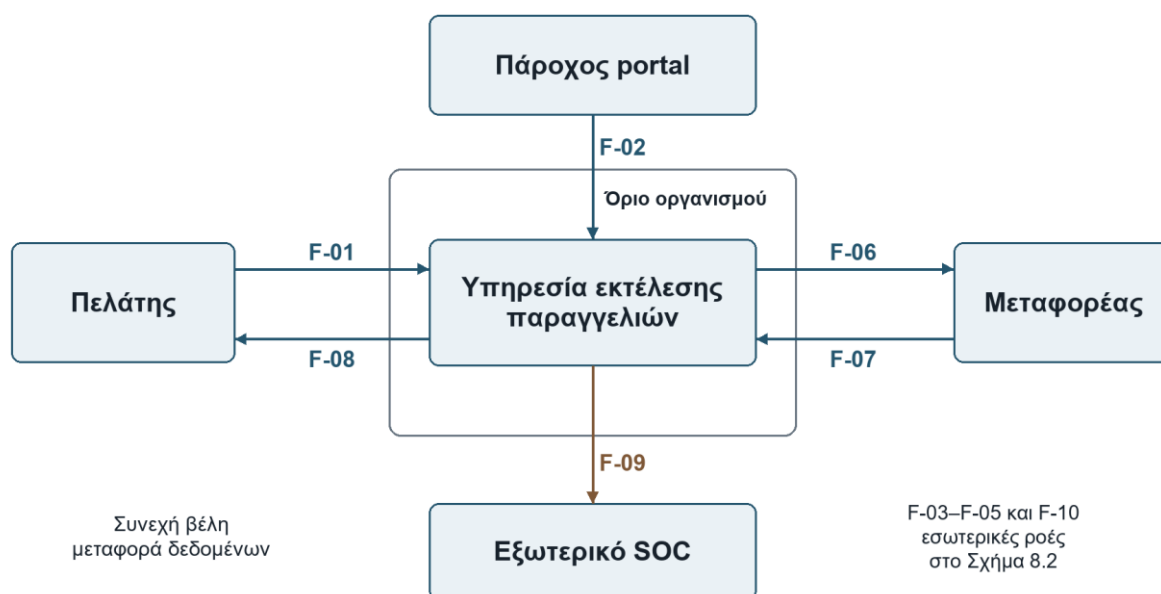
Πηγή: Σύνοψη του συγγραφέα του Πίνακα 5.7. Οι πλήρεις τύποι και οι κανόνες του διατηρούνται.

ΠΑΡΑΡΤΗΜΑ Γ — Χάρτες και παραδείγματα ροών

Γ.1 Τρόπος ανάγνωσης των χαρτών

Η χαρτογράφηση αρχίζει με το περιβάλλον της υπηρεσίας και συνεχίζει με το αναλυτικό εσωτερικό πεδίο. Κάθε βέλος έχει κατεύθυνση και σταθερό κωδικό F. Οι κωδικοί συνδέουν το σχήμα με το λεξικό ροών, τις απαιτήσεις, τους κινδύνους και τα τεκμήρια. Οι χάρτες αποτελούν διδακτικό παράδειγμα υπηρεσίας παραγγελιών και προσαρμόζονται μόνο μετά την επιβεβαίωση των πραγματικών καναλιών, χωρών, ζωνών και παρόχων.

Σχήμα Γ.1: Χάρτης περιβάλλοντος υπηρεσίας παραγγελιών



Πηγή: Σύνθεση του συγγραφέα. Οι εξωτερικές ροές χρησιμοποιούν τους ίδιους κωδικούς με τον αναλυτικό χάρτη· οι F-03–F-05 και F-10 αναπτύσσονται μέσα στο οργανωτικό όριο.

Το παράδειγμα δείχνει δύο κανάλια εισόδου παραγγελιών, απευθείας από πελάτη και μέσω portal. Στην πραγματική εφαρμογή διατηρούνται μόνο τα υπαρκτά κανάλια και καταγράφεται ο τρόπος αποτροπής διπλής καταχώρισης. Το οργανωτικό όριο δηλώνει ευθύνη χαρτογράφησης και όχι ίσο επίπεδο εμπιστοσύνης για όλα τα εσωτερικά συστήματα.

Γ.2 Αναλυτικός χάρτης ροών και εξαρτήσεων

Το Σχήμα Γ.2 εξειδικεύει τις επιλεγμένες ροές και τη διακριτή εξάρτηση πρόσβασης του συνοπτικού χάρτη.

Ροή	Πηγή → προορισμός	Κατηγορίες δεδομένων	Σκοπός και βασικός έλεγχος
F-02	Portal → πύλη API	Εντολή παραγγελίας και αναγνωριστικό συνεργάτη.	Παραλαβή εξωτερικού αιτήματος· επιτρεπτές λειτουργίες και πεδία.
F-03	Πύλη API → ERP	Ελεγμένα στοιχεία παραγγελίας.	Εσωτερική προώθηση· δικαιώματα λογαριασμού υπηρεσίας.
F-04	ERP → WMS	Είδη, ποσότητες, θέσεις ή οδηγίες συλλογής και παράδοσης.	Προετοιμασία· ακεραιότητα και συμφωνία αποθέματος.
F-05	WMS → TMS	Έτοιμη αποστολή, όγκος και αναγκαία στοιχεία προορισμού.	Δρομολόγηση· πληρότητα και επικαιρότητα.
F-06	TMS → μεταφορέας	Ανάθεση, διεύθυνση, επικοινωνία και οδηγίες παράδοσης.	Διανομή· ελάχιστα αναγκαία δεδομένα και εξουσιοδοτημένος αποδέκτης.
F-07	Μεταφορέας → TMS	Κατάσταση, χρόνος και αναγκαία απόδειξη παράδοσης.	Επιβεβαίωση· προέλευση και δικαιώματα ενημέρωσης.
F-08	TMS → πελάτης	Κωδικός αποστολής και κατάσταση παράδοσης.	Ενημέρωση· διαχωρισμός δεδομένων διαφορετικών πελατών.
F-09	API/ERP/WMS/TMS → συλλέκτης → SOC	Χρόνος, αναγνωριστικό χρήστη ή υπηρεσίας, ενέργεια και αποτέλεσμα.	Ανίχνευση· κάλυψη πηγών, συγχρονισμός και περιορισμός πρόσβασης.
F-10	WMS → αντίγραφα	Επιλεγμένα δεδομένα και ρυθμίσεις προς ανάκτηση.	Ανάκαμψη· εύρος, διαχωρισμός πρόσβασης και ελεγχόμενη επαναφορά.

Πηγή: Σύνθεση του συγγραφέα από τα Σχήματα Γ.1–Γ.2. Τα πεδία επιβεβαιώνονται ανά υλοποίηση.

Γ.4 Αναλυτική καρτέλα ροής

Για κάθε κρίσιμη ροή δημιουργείται αναλυτική εγγραφή. Το παράδειγμα F-02 δείχνει τα πεδία που απαιτούνται για να συνδεθεί η τεχνική διασύνδεση με ρόλους, όρια, τεκμήρια και εκκρεμότητες.

Πίνακας Γ.2: Αναλυτική καρτέλα ροής με παράδειγμα F-02

Πεδίο	Παράδειγμα και οδηγία συμπλήρωσης
Ταυτότητα και σκοπός	F-02, portal προς πύλη API, για λήψη παραγγελίας. Δηλώνονται η υπηρεσία, η έκδοση και η σχέση με την F-03.
Δεδομένα και πρόσωπα	Καταγράφονται τα πραγματικά πεδία, οι κατηγορίες προσώπων και τυχόν ελεύθερα πεδία. Το υπόδειγμα αφορά παραλήπτες· η παρουσία ειδικών κατηγοριών δεν προεξοφλείται.
Ρόλοι και βάση	Καθορίζονται σκοπός, ουσιαστικά μέσα, υπεύθυνος ή εκτελών ανά επεξεργασία, εφαρμοστέα βάση και συμβατικοί όροι. Οι ρόλοι δεν αποδίδονται μόνο από το βέλος.
Μηχανισμός και συχνότητα	API ανά παραγγελία ως παραδοχή. Πρωτόκολλο, κρυπτογράφηση, ταυτοποίηση, περιορισμοί κλήσεων και χειρισμός επανάλληψης επιβεβαιώνονται από την IT.
Πρόσβαση και όρια	Οντότητες στα δύο άκρα, χώρες, ζώνες πρόσβασης, λογαριασμοί και επιτρεπόμενες ενέργειες. Τρίτες χώρες και περαιτέρω διαβιβάσεις εξετάζονται χωριστά.

Πεδίο	Παράδειγμα και οδηγία συμπλήρωσης
Αποθήκευση και τήρηση	Θέσεις αντιγράφων στο portal, στο API και στα αρχεία ελέγχου· σκοπός, αιτιολογημένος χρόνος τήρησης και διαγραφή ανά θέση. Δεν ορίζεται κοινός αυθαίρετος χρόνος.
Ευθύνη και απόδειξη	Ιδιοκτήτης υπηρεσίας και τεχνικός διαχειριστής· σύμβαση, ρύθμιση, δείγμα σχήματος μηνύματος και ημερομηνία επαλήθευσης.
Ανοικτά σημεία	Όσα δεν έχουν ελεγχθεί σημειώνονται «Προς επιβεβαίωση», με υπεύθυνο και προθεσμία. Το διδακτικό παράδειγμα δεν υποκαθιστά έλεγχο πραγματικών ρυθμίσεων.

Πηγή: Σύνθεση του συγγραφέα βάσει της χαρτογράφησης και της διαχείρισης τεκμηρίων των Κεφαλαίων 4–5.

Η καρτέλα Γ.2 τροφοδοτεί τα μητρώα R/G/A/E του Παραρτήματος Β. Η σύνδεση θεωρείται πλήρης όταν ο ίδιος κωδικός ροής εμφανίζεται στην απαίτηση, στον κίνδυνο, στο κενό, στην ενέργεια και στο τεκμήριο, με ελεγχόμενη έκδοση και υπεύθυνο για κάθε μεταβολή.