ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Π.Μ.Σ. «ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΤΕΧΝΗΤΗΣ ΝΟΗΜΟΣΥΝΗΣ»

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Πλαίσιο εφαρμογής, ελέγχων και συμμόρφωσης της Οδηγίας NIS2 2022/2555

Κώστας Σαββίδης

Επιβλέπων Καθηγητής:
Στέφανος Γκρίτζαλης, Καθηγητής

ΠΕΙΡΑΙΑΣ

ΑΠΡΙΛΙΟΣ 2026
ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Πλαίσιο εφαρμογής, ελέγχων (auditing) και συμμόρφωσης (compliance) της Directive NIS2 2022/2555

Κώστας Σαββίδης
Α.Μ.: MTE24027

ΠΕΡΙΛΗΨΗ

Η παρούσα διπλωματική εργασία εξετάζει την Οδηγία (ΕΕ) 2022/2555 (NIS2) με έμφαση στην εφαρμογή, τους ελέγχους και τη συμμόρφωση σε επίπεδο οργανισμού. Στόχος είναι να αναδειχθεί ο τρόπος με τον οποίο οι κανονιστικές απαιτήσεις της Οδηγίας ενσωματώνονται στις οργανωτικές διαδικασίες και πώς οι εμπλεκόμενοι φορείς καλούνται να ανταποκριθούν σε αυτές στην πράξη.

Η εργασία βασίζεται σε βιβλιογραφική επισκόπηση και κανονιστική ανάλυση. Αρχικά χαρτογραφείται το νομικό και ρυθμιστικό πλαίσιο της NIS2, το πεδίο εφαρμογής της και οι βασικές απαιτήσεις διακυβέρνησης και εποπτείας. Στη συνέχεια αναλύεται η μετάφρασή της σε επίπεδο οργανισμού - από τις πολιτικές ασφάλειας πληροφοριών και τη διαχείριση κινδύνων έως την υλοποίηση συγκεκριμένων μέτρων κυβερνοασφάλειας. Ιδιαίτερη προσοχή δίνεται στο πλαίσιο ελέγχων και στη σύνδεση της NIS2 με το ISO/IEC 27001, καθώς και στη συμμόρφωση μέσα από τεκμηρίωση, παρακολούθηση, ανάλυση κενών και διορθωτικές ενέργειες. Ως εργαλείο αποτίμησης της συμμόρφωσης αξιοποιείται το Gap Analysis Tool της Εθνικής Αρχής Κυβερνοασφάλειας.

Από την ανάλυση προκύπτει ότι η συμμόρφωση με τη NIS2 αποτελεί διαρκή οργανωτική διαδικασία. Συνδέεται με τη διακυβέρνηση, τη διαχείριση κινδύνων, τον έλεγχο και τη συνεχή βελτίωση. Ταυτόχρονα, η εργασία δείχνει ότι η πρακτική εφαρμογή της Οδηγίας επηρεάζεται από την κανονιστική αβεβαιότητα, την οργανωτική και διοικητική ετοιμότητα, τους διαθέσιμους πόρους, το ανθρώπινο δυναμικό, καθώς και τις εξαρτήσεις από την εφοδιαστική αλυσίδα και τα τρίτα μέρη.

ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: Κυβερνοασφάλεια και κανονιστική συμμόρφωση

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: διακυβέρνηση κυβερνοασφάλειας, διαχείριση κινδύνων, έλεγχοι συμμόρφωσης, ανάλυση κενών, διαχείριση περιστατικών

ABSTRACT

This dissertation examines Directive (EU) 2022/2555 (NIS2), with emphasis on implementation, auditing, and compliance at organisational level. Its purpose is to provide an account of how the Directive's regulatory requirements are connected with organisational processes, control mechanisms, and the practical adaptation of entities falling within its scope.

The study is based on literature review and regulatory analysis. Firstly, it examines the legal and regulatory framework of NIS2, its scope of application, and its main governance and supervisory requirements. It then analyses the implementation framework of the Directive at organisational level, focusing on information security policies, risk management, and the implementation of cybersecurity measures. Furthermore, it focuses on the auditing framework, the link between NIS2 and ISO/IEC 27001, as well as the compliance framework through documentation, monitoring, gap analysis, and corrective actions. The Gap Analysis Tool of the Hellenic National Cybersecurity Authority is presented as a compliance assessment instrument.

The analysis shows that compliance with NIS2 constitutes an ongoing organisational process. It is closely linked to governance, risk management, auditing, and continuous improvement. At the same time, the study shows that the practical implementation of the Directive is influenced by regulatory uncertainty, organisational and administrative readiness, available resources, human capital, as well as dependencies on the supply chain and third parties.

SUBJECT AREA: Cybersecurity and regulatory compliance

KEYWORDS: cybersecurity governance, risk management, compliance audits, gap analysis, incident management

Περιεχόμενα

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

ΠΡΟΛΟΓΟΣ

Η κυβερνοασφάλεια αποτελεί σήμερα ζήτημα αυξημένης σημασίας για τη λειτουργία των οργανισμών, την προστασία των υποδομών και τη σταθερότητα του ψηφιακού περιβάλλοντος. Η συνεχής εξάρτηση από δίκτυα, πληροφοριακά συστήματα και ψηφιακές υπηρεσίες δημιουργεί νέες δυνατότητες για την οικονομία, τη διοίκηση και την κοινωνία. Ωστόσο, η ίδια εξάρτηση ενισχύει την έκθεση σε απειλές που γίνονται πιο συχνές, πιο σύνθετες και πιο απαιτητικές ως προς την αντιμετώπισή τους. Η ανάγκη για κυβερνοανθεκτικότητα συνδέεται πλέον άμεσα με τη συνέχεια λειτουργίας, τη διαχείριση κινδύνων και την εμπιστοσύνη στο ψηφιακό περιβάλλον.

Μέσα σε αυτό το πλαίσιο, η Οδηγία (ΕΕ) 2022/2555 (NIS2) κατέχει κεντρική θέση στο ευρωπαϊκό κανονιστικό πεδίο της κυβερνοασφάλειας. Αποτελεί το βασικό νομοθετικό πλαίσιο της Ευρωπαϊκής Ένωσης για την ασφάλεια δικτύων και συστημάτων πληροφοριών και εισάγει ένα πιο απαιτητικό σύστημα υποχρεώσεων για βασικές και σημαντικές οντότητες. Η σημασία της εκδηλώνεται στη διεύρυνση του πεδίου εφαρμογής, στην ενίσχυση των μέτρων ασφάλειας και στις αυστηρότερες υποχρεώσεις αναφοράς περιστατικών - με ιδιαίτερη έμφαση στη διακυβέρνηση, την εποπτεία και τη λογοδοσία.

Η μετάβαση από την προηγούμενη περίοδο εφαρμογής της NIS1 σε ένα νέο πλαίσιο με αυστηρότερες απαιτήσεις καταδεικνύει ότι η κυβερνοασφάλεια αντιμετωπίζεται πλέον ως κρίσιμο θεμέλιο της οικονομίας, της δημόσιας λειτουργίας και της κοινωνικής σταθερότητας. Η ενίσχυση της ανθεκτικότητας δεν περιορίζεται στην τυπική συμμόρφωση με νομικές υποχρεώσεις. Αφορά και τη δυνατότητα των οργανισμών να οργανώνουν αποτελεσματικά τις διαδικασίες τους, να εντοπίζουν και να διαχειρίζονται κινδύνους, να ανταποκρίνονται σε περιστατικά και να προσαρμόζονται σε ένα περιβάλλον που μεταβάλλεται διαρκώς. Σε αυτή την κατεύθυνση, η κυβερνοασφάλεια συνδέεται και με ευρύτερες έννοιες, όπως η ψηφιακή εμπιστοσύνη, η θεσμική ετοιμότητα και η συνολική αξιοπιστία.

Η μελέτη της NIS2 παρουσιάζει, για τον λόγο αυτό, ιδιαίτερο ενδιαφέρον. Πρόκειται για ένα πεδίο όπου συναντώνται η κανονιστική απαίτηση, η οργανωτική εφαρμογή και η ανάγκη για συστηματικό έλεγχο και συμμόρφωση. Η προσέγγιση της Οδηγίας μέσα από αυτές τις διαστάσεις συμβάλλει στην κατανόηση των απαιτήσεων που διαμορφώνονται στο σύγχρονο περιβάλλον κυβερνοασφάλειας και της σημασίας που αποκτούν για τους οργανισμούς που καλούνται να τις εφαρμόσουν.

1. ΕΙΣΑΓΩΓΗ

1.1. Ιστορικό και κίνητρα

Η κυβερνοασφάλεια συνιστά σήμερα κεντρικό ζήτημα για επιχειρήσεις, δημόσιους οργανισμούς και την κοινωνία ευρύτερα. Η επέκταση των ψηφιακών υπηρεσιών, σε συνδυασμό με την αυξανόμενη συχνότητα και πολυπλοκότητα των κυβερνοεπιθέσεων, έχει ανεβάσει σημαντικά τα επίπεδα κινδύνου για τα πληροφοριακά συστήματα της ΕΕ. Περιστατικά ασφάλειας που επηρέασαν παρόχους ενέργειας, φορείς υγείας, χρηματοπιστωτικά ιδρύματα και δημόσιους οργανισμούς έδειξαν ότι οι ελλείψεις στον τομέα της κυβερνοασφάλειας μπορούν να οδηγήσουν όχι μόνο σε οικονομικές απώλειες, αλλά και σε διακοπή βασικών λειτουργιών ενός κράτους. Σύμφωνα με τον ΣΕΒ, το 2024 οι κυβερνοεπιθέσεις στην ΕΕ αυξήθηκαν κατά 24%, ενώ μόλις το 29% των ευρωπαϊκών επιχειρήσεων είχε διαμορφώσει ή επικαιροποιήσει την πολιτική κυβερνοασφάλειάς τους κατά την ίδια περίοδο (ΣΕΒ σύνδεσμος επιχειρήσεων και βιομηχανιών - Τομέας Τεχνολογίας & Ψηφιακού Μετασχηματισμού, 2025).

Ως απάντηση στις παραπάνω προκλήσεις, η Ευρωπαϊκή Ένωση υιοθέτησε αρχικά την Οδηγία (ΕΕ) 2016/1148, γνωστή ως NIS, με σκοπό την εγκαθίδρυση ενός κοινού επιπέδου κυβερνοασφάλειας για το σύνολο των κρατών μελών. Εντούτοις, οι διαφορές στην εφαρμογή της Οδηγίας σε κάθε κράτος μέλος της ΕΕ, το περιορισμένο εύρος που κάλυπτε η υλοποίησή της και οι συνεχώς εξελισσόμενες απειλές που αναδύονταν, αποκάλυψαν σημαντικές ελλείψεις στο νέο νομικό πλαίσιο. Για να καλύψει τα κενά αυτά, η ΕΕ θέσπισε την Οδηγία (ΕΕ) 2022/2555, γνωστή ως NIS2, η οποία διευρύνει σημαντικά το εύρος εφαρμογής, ισχυροποιεί τις δυνατότητες ελέγχων και εισάγει αυστηρότερες υποχρεώσεις διαχείρισης κινδύνων κυβερνοασφάλειας και αναφοράς περιστατικών. Πιο συγκεκριμένα, το πεδίο εφαρμογής της NIS2 είναι πάνω από 10 φορές πιο ευρύ σε σχέση με της NIS1, τόσο σε ότι αφορά στον αριθμό των κλάδων που καλύπτονται, όσο και στην ακρίβεια των κριτηρίων ένταξης των οργανισμών σε αυτή (Puppet by Perforce).

Παρά το ενισχυμένο ρυθμιστικό πλαίσιο που εισήχθη μέσω της NIS2, οι διάφοροι οργανισμοί αντιμετωπίζουν σημαντικές προκλήσεις στην προσπάθειά τους να κατανοήσουν τον τρόπο με τον οποίο οφείλουν να εφαρμόσουν και να αποδείξουν τη συμμόρφωσή τους. Ειδικότερα, η απουσία μιας επίσημης μεθοδολογίας ελέγχων, εναρμονισμένης με τη νέα Οδηγία, προκαλεί αβεβαιότητα εξίσου σε ελεγκτές και ελεγχόμενους οργανισμούς. Το κενό

αυτό αναδεικνύει την ανάγκη ενός πρακτικού και δομημένου πλαισίου που θα υποστηρίζει τους οργανισμούς, ώστε να πετύχουν τη συμμόρφωσή τους με τη NIS2.

1.2. Ερευνητικό Πρόβλημα

Παρότι η Οδηγία NIS2 καθορίζει σαφείς νομικές υποχρεώσεις για τις οντότητες που υπάγονται σε αυτή, δεν υπαγορεύει μια συγκεκριμένη μεθοδολογία ελέγχων και συμμόρφωσης. Παρέχεται ευελιξία στα κράτη μέλη στη δημιουργία μηχανισμών επίβλεψης και επιβολής της Οδηγίας, κάτι που μπορεί να οδηγήσει σε αποκλίνουσες προσεγγίσεις μεταξύ των ευρωπαϊκών κρατών. Συνεπώς, οι οργανισμοί καταλήγουν συχνά δίχως σαφή καθοδήγηση σχετικά με το πώς να αποτιμήσουν το επίπεδο συμμόρφωσής τους ή το πώς να προετοιμαστούν για ελέγχους από τις εθνικές αρχές.

Επιπλέον, ορισμένα από τα υπάρχοντα πρότυπα και πλαίσια κυβερνοασφάλειας, όπως τα ISO/IEC 27001 και NIST, δεν αντιστοιχίζονται πλήρως στις απαιτήσεις της NIS2, ειδικά σε περιοχές όπως η ευθύνη της ανώτερης διοίκησης, τα χρονικά πλαίσια αναφοράς περιστατικών και η διαχείριση κινδύνων της εφοδιαστικής αλυσίδας. Αυτό οδηγεί σε ένα κενό μεταξύ των ρυθμιστικών απαιτήσεων και της πρακτικής υλοποίησης.

Επομένως, το βασικό ερευνητικό πρόβλημα που πραγματεύεται η παρούσα εργασία είναι η απουσία ενός ενοποιημένου και πρακτικού πλαισίου που θα ενσωματώνει τις κανονιστικές, οργανωτικές και ελεγκτικές διαστάσεις που απαιτούνται για την εφαρμογή και την τεκμηρίωση της συμμόρφωσης με την Οδηγία NIS2.

1.3. Αντικείμενο της Εργασίας

Ο κύριος σκοπός της παρούσας εργασίας είναι να σχεδιάσει και να προτείνει ένα οργανωμένο πλαίσιο το οποίο θα υποστηρίζει τους οργανισμούς στην εφαρμογή, τους ελέγχους και την επαλήθευση της συμμόρφωσης με την Οδηγία NIS2. Πιο συγκεκριμένα, θα αναλυθούν οι ρυθμιστικές απαιτήσεις της Οδηγίας NIS2 και οι επιπτώσεις τους στους οργανισμούς, ενώ ταυτόχρονα θα εξεταστεί ο τρόπος με τον οποίο οι οργανισμοί μπορούν να προσδιορίσουν εάν υπάγονται στο πεδίο εφαρμογής της. Ακόμη, θα αναζητηθούν υπάρχουσες προσεγγίσεις στις διαδικασίες ελέγχων και εξακρίβωσης της συμμόρφωσης

στο πλαίσιο της NIS2 και θα αξιολογηθεί ο ρόλος της ανάλυσης κενών (gap analysis) ως εργαλείο που μπορεί να χρησιμοποιηθεί στις παραπάνω διαδικασίες.

Η εργασία επικεντρώνεται στα θέματα της εφαρμογής και του ελέγχου υλοποίησης της Οδηγίας NIS2 σε επίπεδο οργανισμού. Παράλληλα, δεν αποτελεί στόχο της εργασίας η εξαντλητική τεχνική περιγραφή μέτρων κυβερνοασφάλειας. Αντιθέτως, δίνεται έμφαση σε ζητήματα διοίκησης, διαχείριση κινδύνων, διαδικασίες ελέγχων και μηχανισμούς επαλήθευσης της συμμόρφωσης.

1.4. Δομή της Εργασίας

Η εργασία είναι δομημένη ως εξής:

- το κεφάλαιο 2 παρουσιάζει το νομικό και ρυθμιστικό πλαίσιο της Οδηγίας NIS2
- το κεφάλαιο 3 εξετάζει το πλαίσιο εφαρμογής της NIS2 σε οργανωτικό επίπεδο
- το κεφάλαιο 4 αναλύει το πλαίσιο ελέγχων, τη μεθοδολογία τους και τη σύνδεσή τους με το ISO/IEC 27001
- το κεφάλαιο 5 πραγματεύεται το πλαίσιο συμμόρφωσης, την τεκμηρίωση, την παρακολούθηση και το Gap Analysis Tool της Εθνικής Αρχής Κυβερνοασφάλειας
- το κεφάλαιο 6 αναδεικνύει τις βασικές προκλήσεις εφαρμογής της Οδηγίας
- το κεφάλαιο 7 παρουσιάζει τα συμπεράσματα της μελέτης

2. ΝΟΜΙΚΟ ΚΑΙ ΡΥΘΜΙΣΤΙΚΟ ΠΛΑΙΣΙΟ

2.1. Οδηγία NIS

Η Οδηγία NIS, ή αλλιώς Οδηγία (ΕΕ) 2016/1148, αποτελεί το πρώτο νομοθετικό κείμενο της Ευρωπαϊκής Ένωσης που θεσπίζει ένα ενιαίο πλαίσιο κυβερνοασφάλειας σε ευρωπαϊκό επίπεδο. Τέθηκε σε ισχύ τον Αύγουστο του 2016 και η καταληκτική ημερομηνία για την ενσωμάτωσή της στο εθνικό δίκαιο των κρατών μελών ήταν η 9η Μαΐου του 2018. Στην ελληνική έννομη τάξη μεταφέρθηκε με το ν. 4577/2018. Σκοπός της ήταν η επίτευξη ενός υψηλού επιπέδου ασφάλειας σε δίκτυα και συστήματα πληροφοριών στο σύνολο της ΕΕ, μέσω τριών βασικών στρατηγικών στόχων πολιτικής:

1) ενίσχυση των εθνικών δυνατοτήτων κυβερνοασφάλειας
2) ανάπτυξη και εμβάθυνση της συνεργασίας σε επίπεδο Ευρωπαϊκής Ένωσης
3) θέσπιση υποχρεώσεων διαχείρισης κινδύνων και αναφοράς περιστατικών για τους φορείς εκμετάλλευσης βασικών υπηρεσιών και τους παρόχους ψηφιακών υπηρεσιών

(European Commission, 2018)

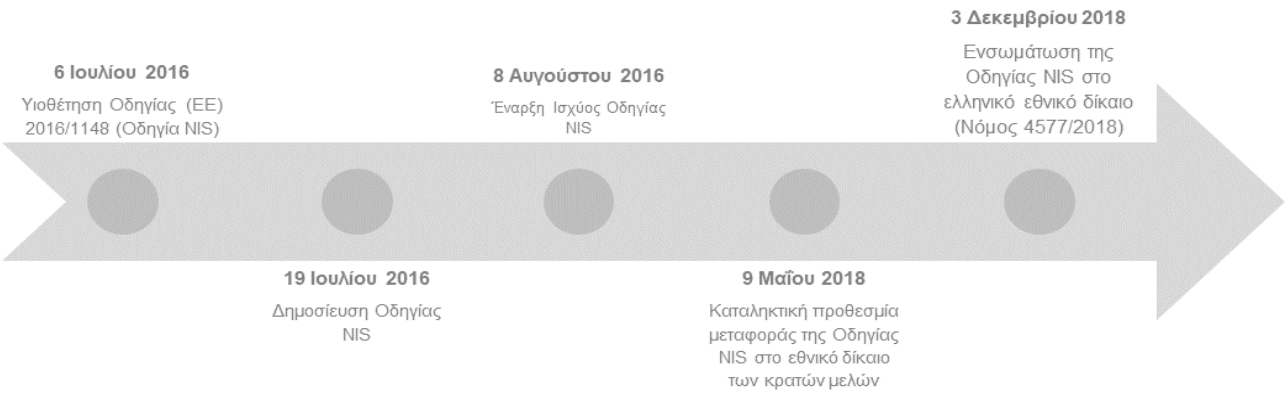
Η Οδηγία NIS αποτέλεσε το πρώτο ουσιαστικό βήμα της Ευρωπαϊκής Ένωσης προς τη διαμόρφωση ενός συνεκτικού πλαισίου κυβερνοασφάλειας, μετατοπίζοντας το ζήτημα της ασφάλειας δικτύων και συστημάτων πληροφοριών από την εθνική αποκλειστικότητα σε επίπεδο ενωσιακής πολιτικής. Μέχρι την υιοθέτησή της, τα κράτη μέλη εφάρμοζαν αποσπασματικές και ετερογενείς προσεγγίσεις, γεγονός που δημιουργούσε ανισότητες ως προς το επίπεδο ετοιμότητας και δυσχέραινε τη διασυνοριακή συνεργασία σε περιπτώσεις σοβαρών περιστατικών κυβερνοασφάλειας (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2016).

Η Οδηγία NIS αποτελείται από 6 κεφάλαια και 27 άρθρα, συνοδευόμενη από παραρτήματα. Το πρώτο κεφάλαιο καθορίζει το αντικείμενο, το πεδίο εφαρμογής και τους βασικούς ορισμούς της Οδηγίας, καθώς και τα κριτήρια για τον προσδιορισμό των φορέων εκμετάλλευσης βασικών υπηρεσιών και τους παράγοντες για την εκτίμηση της «σοβαρής διατάραξης». Στο δεύτερο κεφάλαιο περιγράφεται το εθνικό πλαίσιο που θα πρέπει να υιοθετήσουν τα κράτη μέλη για την ασφάλεια δικτύων και συστημάτων πληροφοριών. Μεταξύ αυτών περιλαμβάνεται η υποχρέωση για σύσταση μιας εθνικής στρατηγικής και ορισμό αρμόδιων αρχών, ενιαίου σημείου επαφής (Single Point of Contact - SPOC) και

ομάδων απόκρισης σε συμβάντα (Computer Security Incident Response Teams - CSIRTs). Στο τρίτο κεφάλαιο αναπτύσσεται το πλαίσιο συνεργασίας σε ενωσιακό επίπεδο, μέσω της Ομάδας Συνεργασίας και του Δικτύου CSIRT. Το τέταρτο κεφάλαιο πραγματεύεται τις απαιτήσεις ασφάλειας και υποχρεώσεις κοινοποίησης συμβάντων για τους φορείς εκμετάλλευσης βασικών υπηρεσιών και τους παρόχους ψηφιακών υπηρεσιών. Το πέμπτο κεφάλαιο εξετάζει την προώθηση προτύπων και την εθελούσια κοινοποίηση συμβάντων. Το έκτο κεφάλαιο περιέχει τις τελικές διατάξεις όπως κυρώσεις, διαδικασίες, επανεξέταση και κανόνες μεταφοράς στο εθνικό δίκαιο (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2016).

Κατά την αποτίμηση της εφαρμογής της Οδηγίας NIS, η Ευρωπαϊκή Επιτροπή αναγνώρισε ότι η Οδηγία συνέβαλε ουσιαστικά στη βελτίωση των εθνικών δυνατοτήτων κυβερνοασφάλειας και στην ενίσχυση του επιπέδου προστασίας των συστημάτων δικτύου και πληροφοριών εντός της Ένωσης. Ωστόσο, εντοπίστηκαν σημαντικά ζητήματα εκτέλεσης, κυρίως ως προς τη συνεκτικότητα και την ομοιομορφία του πλαισίου. Συγκεκριμένα, τα κράτη μέλη ανέπτυξαν διαφορετικές μεθοδολογίες για τον προσδιορισμό των φορέων εκμετάλλευσης βασικών υπηρεσιών, καθώς και για τον καθορισμό των ουσιωδών υπηρεσιών και των σχετικών κατωφλίων, με αποτέλεσμα την ανομοιόμορφη υλοποίηση των διατάξεων της Οδηγίας σε ενωσιακό επίπεδο. Επιπλέον, η διαφορετική ερμηνεία του όρου «βασικές υπηρεσίες» και ο βαθμός λεπτομέρειας των σχετικών καταλόγων δυσχέραναν τη συγκρισιμότητα μεταξύ των κρατών μελών, ενώ το πεδίο εφαρμογής της Οδηγίας παρουσίασε κατακερματισμό, με ορισμένους φορείς να υπόκεινται σε ρυθμιστικές υποχρεώσεις και άλλους, παρότι παρείχαν παρόμοιες υπηρεσίες, να εξαιρούνται. Τα παραπάνω ανέδειξαν την ανάγκη περαιτέρω εναρμόνισης και ενίσχυσης του κανονιστικού πλαισίου, αξιοποιώντας την εμπειρία από την πρακτική υλοποίηση της Οδηγίας NIS (Anna Zygierewicz, 2020).

Στην εικόνα 1, παρουσιάζονται τα βασικά χρονικά ορόσημα που συνδέονται με την Οδηγία NIS, από την υιοθέτησή της ως την ενσωμάτωσή της στο εθνικό δίκαιο:



Εικόνα 1 - Χρονοδιάγραμμα Οδηγίας NIS

2.2. Οδηγία NIS2

Η Οδηγία NIS2, ή αλλιώς Οδηγία (ΕΕ) 2022/2555, καταργεί την Οδηγία (ΕΕ) 2016/1148 (NIS) και την αντικαθιστά, ενισχύοντας και διευρύνοντας το ρυθμιστικό πλαίσιο κυβερνοασφάλειας στην Ευρωπαϊκή Ένωση. Τέθηκε σε ισχύ τον Ιανουάριο του 2023 και η καταληκτική ημερομηνία για την ενσωμάτωσή της στο εθνικό δίκαιο των κρατών μελών ήταν η 17η Οκτωβρίου 2024. Στην ελληνική έννομη τάξη μεταφέρθηκε με το ν. 5160/2024 (Καλαντζής, 2024). Βασίζεται στους τρεις στρατηγικούς στόχους πολιτικής που είχαν τεθεί με την Οδηγία NIS, όπως αναφέρθηκαν στην ενότητα 2.1. Ωστόσο, η Οδηγία NIS2 δεν περιορίζεται στη διατήρηση των αρχικών στόχων της NIS, αλλά προχωρά στον επαναπροσδιορισμό και την περαιτέρω εξειδίκευσή τους, λαμβάνοντας υπόψη τις εμπειρίες από την εφαρμογή της προηγούμενης Οδηγίας και τις αυξημένες απαιτήσεις του σύγχρονου ψηφιακού περιβάλλοντος. Συγκεκριμένα:

1) ενισχύεται ο αρχικός στόχος της NIS περί ανάπτυξης εθνικών δυνατοτήτων κυβερνοασφάλειας, μέσω της εισαγωγής σαφώς καθορισμένων και δεσμευτικών υποχρεώσεων για τα κράτη μέλη. Ειδικότερα, τα κράτη μέλη υποχρεούνται:
    - να εγκρίνουν επικαιροποιημένη εθνική στρατηγική κυβερνοασφάλειας,
    - να ορίσουν αρμόδια εθνική αρχή, ομάδες απόκρισης σε συμβάντα ασφάλειας υπολογιστών (CSIRTs) και ενιαίο σημείο επαφής (SPOC)
    - να ενισχύσουν τη διακυβέρνηση και την εποπτεία σε εθνικό επίπεδο, προάγοντας τη λογοδοσία και τη θεσμική ετοιμότητα των κρατών μελών

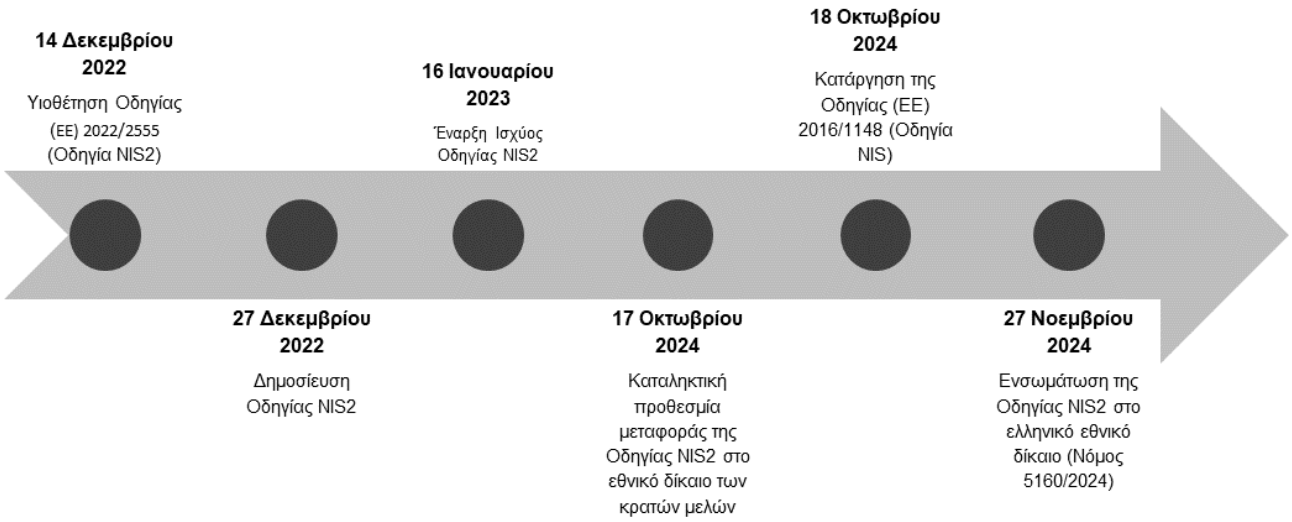
2) ισχυροποιείται η συνεργασία σε ενωσιακό και επιχειρησιακό επίπεδο, μέσω της διατήρησης του ρόλου της Ομάδας Συνεργασίας και του Δικτύου CSIRT και της διεύρυνσης του πεδίου της διασυνοριακής ανταλλαγής πληροφοριών

3) διευρύνονται και αυστηροποιούνται οι υποχρεώσεις που αφορούν τη διαχείριση κινδύνων και την κοινοποίηση συμβάντων, ενώ παράλληλα εισάγονται ενισχυμένες απαιτήσεις λογοδοσίας για τα διοικητικά όργανα των οντοτήτων

(European Commission, 2023)

Η Οδηγία NIS2 αποτελείται από περισσότερα κεφάλαια και άρθρα σε σύγκριση με την Οδηγία NIS, αντανακλώντας το διευρυμένο πεδίο εφαρμογής και τον ενισχυμένο κανονιστικό της χαρακτήρα. Τα αρχικά κεφάλαια καθορίζουν το αντικείμενο, το πεδίο εφαρμογής και τους βασικούς ορισμούς της Οδηγίας, καθώς και το νέο σύστημα κατηγοριοποίησης των οντοτήτων σε βασικές και σημαντικές, αντικαθιστώντας το προηγούμενο μοντέλο προσδιορισμού των φορέων εκμετάλλευσης βασικών υπηρεσιών. Στη συνέχεια, περιγράφεται το ενισχυμένο εθνικό πλαίσιο διακυβέρνησης κυβερνοασφάλειας, με έμφαση στην υποχρέωση υιοθέτησης εθνικής στρατηγικής κυβερνοασφάλειας, στον ορισμό αρμόδιων εθνικών αρχών, ενιαίου σημείου επαφής και ομάδων απόκρισης σε συμβάντα (CSIRTs), καθώς και στη σαφέστερη κατανομή αρμοδιοτήτων και ευθυνών. Ακολούθως, η Οδηγία NIS2 αναπτύσσει εκτενώς το πλαίσιο συνεργασίας σε ενωσιακό επίπεδο, διατηρώντας και ενισχύοντας τον ρόλο της Ομάδας Συνεργασίας και του Δικτύου CSIRT, με στόχο την αποτελεσματικότερη στρατηγική και επιχειρησιακή συνεργασία μεταξύ των κρατών μελών. Κεντρική θέση στην Οδηγία καταλαμβάνουν τα κεφάλαια που αφορούν τις απαιτήσεις διαχείρισης κινδύνων και τις υποχρεώσεις κοινοποίησης συμβάντων, οι οποίες εφαρμόζονται πλέον σε ευρύτερο φάσμα τομέων και οντοτήτων, συνοδεύονται από αυστηρότερες απαιτήσεις εταιρικής διακυβέρνησης και ενισχυμένους μηχανισμούς εποπτείας και επιβολής. Τέλος, τα καταληκτικά κεφάλαια της Οδηγίας περιλαμβάνουν διατάξεις σχετικά με τις κυρώσεις, τις διαδικασίες εποπτείας, την αξιολόγηση της εφαρμογής της, καθώς και τους κανόνες κατάργησης της Οδηγίας NIS και μεταφοράς της NIS2 στο εθνικό δίκαιο των κρατών μελών. Η δομή αυτή αποτυπώνει τον σαφώς πιο δεσμευτικό και εναρμονιστικό χαρακτήρα της Οδηγίας NIS2 σε σύγκριση με την προκάτοχό της (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2022; Αθήνα: Εθνικό Τυπογραφείο, 2024).

Αντίστοιχα με το χρονοδιάγραμμα της Οδηγίας NIS, στην εικόνα 2 αποτυπώνεται η μετάβαση στο νέο κανονιστικό πλαίσιο μέσω της χρονικής πορείας της Οδηγίας NIS2:

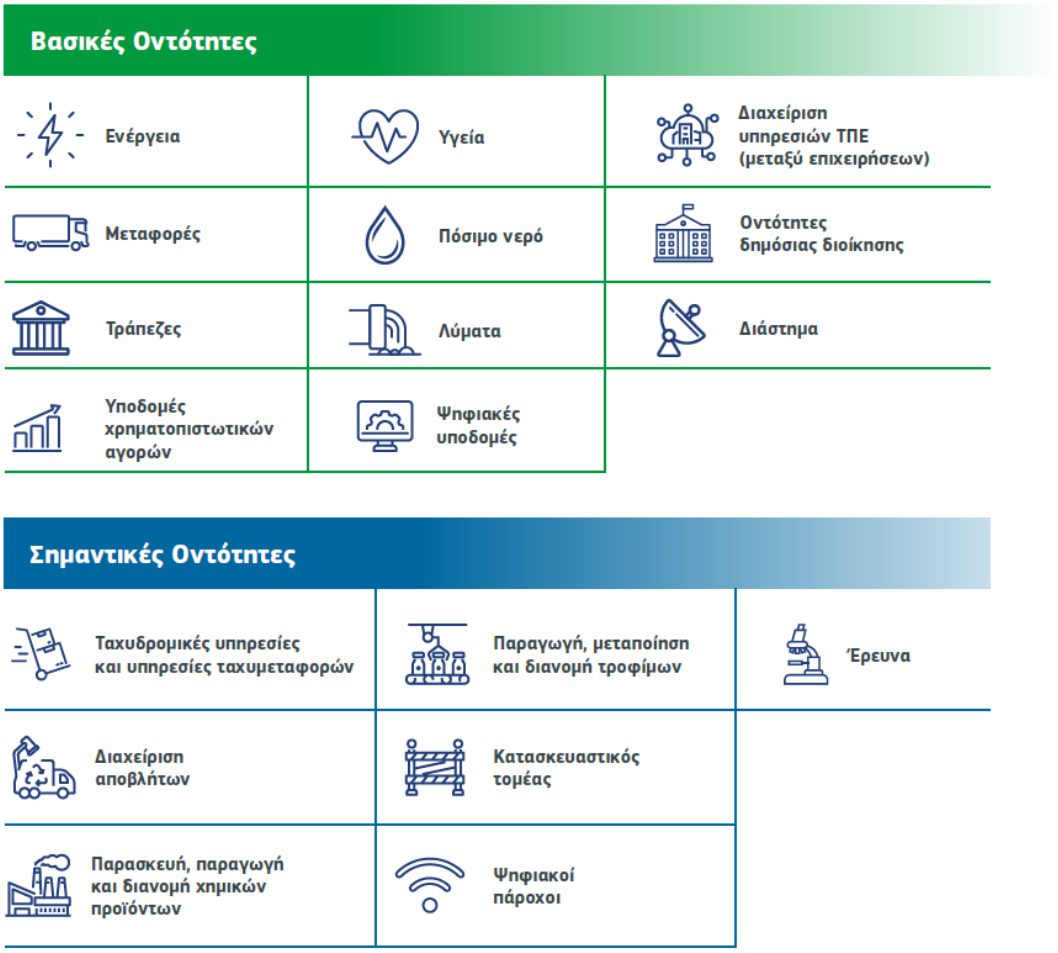


Εικόνα 2 - Χρονοδιάγραμμα Οδηγίας NIS2

2.3. Πεδίο Εφαρμογής

Η Οδηγία NIS2 καταργεί το προηγούμενο μοντέλο της Οδηγίας NIS, όπου προσδιορίζονταν οι φορείς εκμετάλλευσης βασικών υπηρεσιών και εισάγει ένα νέο σύστημα κατηγοριοποίησης, με βάση το οποίο οι οντότητες διακρίνονται σε βασικές και σημαντικές. Ως «οντότητες» νοούνται οι κρίσιμες υποδομές, επιχειρήσεις, φορείς και οργανισμοί που εμπίπτουν στο πεδίο εφαρμογής του ν. 5160/2024 και της Οδηγίας NIS2. Η κατηγοριοποίησή τους βασίζεται αφενός στον τομέα δραστηριότητάς τους και αφετέρου σε κριτήρια μεγέθους, δηλαδή στον αριθμό απασχολούμενων και σε οικονομικά όρια (κύκλος εργασιών ή/και σύνολο ισολογισμού).

Κατά κανόνα, η Οδηγία εφαρμόζεται σε δημόσιες ή ιδιωτικές οντότητες που παρέχουν τις υπηρεσίες τους ή ασκούν τις δραστηριότητές τους εντός της Ευρωπαϊκής Ένωσης και δραστηριοποιούνται σε τομείς που απαριθμούνται στα Παραρτήματα I και II. Οι συγκεκριμένοι τομείς αποτυπώνονται στην εικόνα 3:



Εικόνα 3 - Τομείς Δραστηριότητας Βασικών και Σημαντικών Οντοτήτων (Εθνική Αρχή Κυβερνοασφάλειας, 2024)

Για τις οντότητες αυτές, απαιτείται κατ' ελάχιστο να χαρακτηρίζονται ως μεσαίες επιχειρήσεις. Στην εικόνα 4 παρουσιάζεται αναλυτικά ο ορισμός των ΜμΕ (Πολύ Μικρών, Μικρών και Μεσαίων Επιχειρήσεων), σύμφωνα με τη σύσταση 2003/361/ΕΚ:

Κατηγορία Επιχείρησης	Αριθμός απασχολούμενων		Ετήσιος κύκλος εργασιών	<ή>	Ετήσιος συνολικός Ισολογισμός
Μεσαία	<250	ΚΑΙ	≤ € 50 εκατ.	<ή>	≤ € 43 εκατ.
Μικρή	<50		≤ € 10 εκατ.	<ή>	≤ € 10 εκατ.
Πολύ Μικρή	<10		≤ € 2 εκατ.	<ή>	≤ € 2 εκατ.

Εικόνα 4 - Ορισμός των ΜμΕ (Εθνική Αρχή Κυβερνοασφάλειας, 2024)

Αν και η Οδηγία παραπέμπει στην παραπάνω Σύσταση για τον ορισμό των ΜμΕ, εξαιρεί ρητά τον κανόνα σύμφωνα με τον οποίο δημόσια συμμετοχή άνω του 25% αποκλείει τον χαρακτηρισμό μιας επιχείρησης ως ΜμΕ. Κατά συνέπεια, για τους σκοπούς της Οδηγίας, η ύπαρξη τέτοιας δημόσιας συμμετοχής δεν εμποδίζει τον χαρακτηρισμό μιας οντότητας ως πολύ μικρής, μικρής ή μεσαίας επιχείρησης.

Παράλληλα, η NIS2 προβλέπει ότι ορισμένες οντότητες υπάγονται στο πεδίο εφαρμογής ανεξαρτήτως μεγέθους, λόγω της φύσης και της κρισιμότητας των υπηρεσιών τους. Αρχικά, περιλαμβάνονται οι πάροχοι δημόσιων δικτύων ηλεκτρονικών επικοινωνιών ή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, οι πάροχοι υπηρεσιών εμπιστοσύνης, καθώς και τα μητρώα ονομάτων τομέα ανωτάτου επιπέδου (TLD – Top Level Domain) και οι πάροχοι υπηρεσιών συστήματος ονομάτων τομέα (DNS – Domain Name System). Επιπλέον, εντός πεδίου εφαρμογής μπορεί να υπαχθεί ανεξαρτήτως μεγέθους μια οντότητα όταν, για παράδειγμα, αποτελεί τον μοναδικό πάροχο ουσιώδους υπηρεσίας σε ένα κράτος μέλος ή όταν η διατάραξη της υπηρεσίας της θα μπορούσε να έχει σημαντικό αντίκτυπο στη δημόσια ασφάλεια, στη δημόσια τάξη ή στη δημόσια υγεία, ή να προκαλέσει σημαντικό συστημικό κίνδυνο, ιδίως με διασυνοριακές επιπτώσεις. Ακόμη, η Οδηγία εφαρμόζεται ανεξαρτήτως μεγέθους σε φορείς της κεντρικής κυβέρνησης, όπως αυτοί ορίζονται από το εθνικό δίκαιο, καθώς και σε φορείς δημόσιας διοίκησης σε περιφερειακό επίπεδο, όταν, κατόπιν αξιολόγησης βάσει κινδύνου, παρέχουν υπηρεσίες των οποίων η διατάραξη θα μπορούσε να έχει σημαντικό αντίκτυπο σε κρίσιμες κοινωνικές ή οικονομικές δραστηριότητες. Ταυτόχρονα, τα κράτη μέλη δύνανται να επεκτείνουν το πεδίο εφαρμογής της Οδηγίας σε φορείς δημόσιας διοίκησης σε τοπικό επίπεδο και σε εκπαιδευτικά ιδρύματα, ιδίως όταν διεξάγουν κρίσιμες ερευνητικές δραστηριότητες. Τέλος, η Οδηγία NIS2 εφαρμόζεται επίσης ανεξαρτήτως μεγέθους σε φορείς που χαρακτηρίζονται ως κρίσιμες οντότητες σύμφωνα με την Οδηγία (ΕΕ) 2022/2557 (CER – Critical Entities Resilience Directive), καθώς και σε οργανισμούς που παρέχουν υπηρεσίες καταχώρισης ονομάτων τομέα.

Εκτός πεδίου εφαρμογής παραμένουν ρητά φορείς δημόσιας διοίκησης που ασκούν δραστηριότητες στους τομείς της εθνικής ασφάλειας, της άμυνας, της δημόσιας τάξης και της επιβολής του νόμου, σύμφωνα με τις ρητές προβλέψεις της Οδηγίας. Πέρα από αυτές, προβλέπονται εξαιρέσεις για οντότητες που υπόκεινται ταυτόχρονα σε τομεακές νομικές πράξεις της Ένωσης, όταν αυτές επιβάλλουν ισοδύναμες υποχρεώσεις ως προς την διαχείριση κινδύνων κυβερνοασφάλειας και την κοινοποίηση περιστατικών. Χαρακτηριστικό παράδειγμα αποτελεί ο Κανονισμός DORA, ή αλλιώς Κανονισμός (ΕΕ) 2022/2554 σχετικά

με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα αποτελεί τομεακή νομική πράξη της ΕΕ που εμπίπτει στη συγκεκριμένη κατηγορία.

Η Οδηγία NIS2 εισάγει σαφή διάκριση μεταξύ βασικών και σημαντικών οντοτήτων, με διαφορετικό επίπεδο εποπτείας και υποχρεώσεων. Από τη μια πλευρά, με κριτήριο το μέγεθος της οντότητας, η NIS2 προβλέπει ότι βασικές οντότητες θεωρούνται οι μεγάλες επιχειρήσεις, δηλαδή όσες:

A. απασχολούν τουλάχιστον 250 άτομα ή
B. έχουν ετήσιο κύκλο εργασιών μεγαλύτερο από 50 εκατ. ευρώ και ετήσιο συνολικό ισολογισμό μεγαλύτερο από 43 εκατ. ευρώ

και ασκούν δραστηριότητες στους ακόλουθους τομείς:

Πίνακας 1 - Τομείς Δραστηριότητας Βασικών Οντοτήτων

1. Ενέργεια	6. Πόσιμο νερό
2. Μεταφορές	7. Λύματα
3. Τράπεζες	8. Ψηφιακές υποδομές
4. Υποδομές χρηματοπιστωτικών αγορών	9. Διαχείριση υπηρεσιών ΤΠΕ (μεταξύ επιχειρήσεων)
5. Υγεία	10. Διάστημα

Έπειτα, ανεξαρτήτως μεγέθους, βασικές οντότητες αποτελούν οι:

a. πάροχοι υπηρεσιών εμπιστοσύνης και μητρώα ονομάτων τομέα ανωτάτου επιπέδου, καθώς και πάροχοι υπηρεσιών συστήματος ονομάτων τομέα (DNS)
b. πάροχοι δημόσιων δικτύων ηλεκτρονικών επικοινωνιών ή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών που χαρακτηρίζονται ως μεσαίες επιχειρήσεις, δυνάμει του παραρτήματος της Σύστασης της Επιτροπής 2003/361/ΕΚ
c. οντότητες δημόσιας διοίκησης που εντάσσονται στους φορείς της κεντρικής κυβέρνησης

d. οποιεσδήποτε άλλες οντότητες των τύπων που αναφέρονται στο παράρτημα I ή II του ν. 5160/2024, οι οποίες προσδιορίζονται ως βασικές οντότητες λόγω της κρισιμότητάς τους

e. οντότητες που προσδιορίζονται ως κρίσιμες οντότητες βάσει της Οδηγίας (ΕΕ) 2022/2557

f. οντότητες που αναγνωρίστηκαν, σύμφωνα με το ν. 4577/2018, ως φορείς εκμετάλλευσης βασικών υπηρεσιών

Από την άλλη πλευρά, σημαντικές οντότητες θεωρούνται το σύνολο των οντοτήτων των τομέων εκείνων που αναφέρονται στα παραρτήματα I και II της Οδηγίας και οι οποίες δεν έχουν χαρακτηριστεί ως βασικές. Πρόκειται για τις οργανισμούς που ανήκουν στους τομείς:

Πίνακας 2 - Τομείς Δραστηριότητας Σημαντικών Οντοτήτων

1. Ταχυδρομικές υπηρεσίες και υπηρεσίες ταχυμεταφορών	4. Παραγωγή, μεταποίηση και διανομή τροφίμων
2. Διαχείριση αποβλήτων	5. Κατασκευαστικός τομέας
3. Παρασκευή, παραγωγή και διανομή χημικών προϊόντων	6. Ψηφιακοί πάροχοι
	7. Έρευνα

καθώς και όσες οντότητες δραστηριοποιούνται στους τομείς του Παραρτήματος I της Οδηγίας, αλλά δεν καλύπτουν το κριτήριο μεγέθους ώστε να αποτελούν μεγάλη επιχείρηση (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2022; Εθνική Αρχή Κυβερνοασφάλειας, 2024).

2.4. Θεσμική Διακυβέρνηση και Συντονισμός

Η Οδηγία NIS2 προβλέπει ότι κάθε κράτος μέλος θεσπίζει εθνική στρατηγική κυβερνοασφάλειας, η οποία καθορίζει τους στρατηγικούς στόχους, τους αναγκαίους πόρους και τα κατάλληλα μέτρα πολιτικής και ρύθμισης για την επίτευξη και διατήρηση υψηλού επιπέδου κυβερνοασφάλειας. Η στρατηγική περιλαμβάνει, ιδίως, στόχους και προτεραιότητες που καλύπτουν τους τομείς του πεδίου εφαρμογής της Οδηγίας, πλαίσιο

διακυβέρνησης για την υλοποίησή τους, καθώς και σαφή κατανομή ρόλων και αρμοδιοτήτων μεταξύ των εμπλεκόμενων φορέων σε εθνικό επίπεδο. Παράλληλα, καθορίζεται μηχανισμός προσδιορισμού των σχετικών πάγιων στοιχείων και εκτίμησης κινδύνων, καθώς και μέτρα ετοιμότητας, απόκρισης και αποκατάστασης από περιστατικά, συμπεριλαμβανομένης της συνεργασίας δημόσιου και ιδιωτικού τομέα. Για τον σκοπό αυτό, τα κράτη μέλη θεσπίζουν ειδικές πολιτικές που αφορούν, μεταξύ άλλων, την ασφάλεια της αλυσίδας εφοδιασμού προϊόντων και υπηρεσιών ΤΠΕ, τη διαχείριση ευπαθειών, την ενσωμάτωση απαιτήσεων κυβερνοασφάλειας στις δημόσιες συμβάσεις, την ενίσχυση της ευαισθητοποίησης και της κατάρτισης, καθώς και την προώθηση της κυβερνοανθεκτικότητας των μικρών και μεσαίων επιχειρήσεων. Η εθνική στρατηγική κοινοποιείται στην Επιτροπή εντός τριών μηνών από την έγκρισή της και αξιολογείται σε τακτική βάση, τουλάχιστον ανά πενταετία.

Πέραν της εθνικής στρατηγικής, η Οδηγία προβλέπει ότι κάθε κράτος μέλος ορίζει ή συστήνει μία ή περισσότερες αρμόδιες αρχές ως υπεύθυνες για την κυβερνοασφάλεια και για την άσκηση των εποπτικών καθηκόντων. Οι αρμόδιες αρχές παρακολουθούν την εφαρμογή της Οδηγίας σε εθνικό επίπεδο και πρέπει να διαθέτουν τις αναγκαίες εξουσίες και επαρκείς πόρους για την αποτελεσματική άσκηση των καθηκόντων τους. Την ίδια στιγμή, κάθε κράτος μέλος ορίζει ένα ή περισσότερα ενιαία σημεία επαφής, κι εφόσον ορίζεται μία μόνο αρμόδια αρχή, αυτή μπορεί να λειτουργεί και ως ενιαίο σημείο επαφής. Το ενιαίο σημείο επαφής ασκεί καθήκοντα συνδέσμου για τη διασφάλιση της διασυνοριακής συνεργασίας με τις αρμόδιες αρχές άλλων κρατών μελών και, κατά περίπτωση, με την Επιτροπή και τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA), καθώς και για τον συντονισμό με άλλες αρμόδιες αρχές σε εθνικό επίπεδο. Η ταυτότητα των αρμόδιων αρχών και των ενιαίων σημείων επαφής κοινοποιείται στην Επιτροπή και δημοσιοποιείται σύμφωνα με τις προβλέψεις της Οδηγίας.

Περαιτέρω, η Οδηγία επιβάλλει τη θέσπιση εθνικών πλαισίων διαχείρισης κυβερνοκρίσεων. Για τη διαχείριση περιστατικών μεγάλης κλίμακας, τα κράτη μέλη ορίζουν ειδική αρχή ή αρχές διαχείρισης περιστατικών και κρίσεων μεγάλης κλίμακας στον τομέα της κυβερνοασφάλειας και διασφαλίζουν ότι οι αρχές αυτές διαθέτουν επαρκείς πόρους για την άσκηση των καθηκόντων τους. Σε περίπτωση ύπαρξης περισσότερων αρχών, πρέπει να προσδιορίζεται ρητώς η αρχή που αναλαμβάνει τον συντονισμό. Επιπρόσθετα, τα κράτη μέλη θεσπίζουν εθνικό σχέδιο αντιμετώπισης περιστατικών και κρίσεων μεγάλης κλίμακας, στο οποίο καθορίζονται οι στόχοι ετοιμότητας, οι αρμοδιότητες των εμπλεκόμενων φορέων, οι διαδικασίες διαχείρισης και ο τρόπος ενσωμάτωσης στο γενικό εθνικό πλαίσιο διαχείρισης κρίσεων, καθώς και οι μηχανισμοί συμμετοχής δημόσιων και ιδιωτικών φορέων και η

διασύνδεση με τους ενωσιακούς μηχανισμούς συντονισμού κυβερνοκρίσεων. Η ταυτότητα των αρμόδιων αρχών και τα βασικά στοιχεία των εθνικών σχεδίων κοινοποιούνται στην Επιτροπή, με δυνατότητα εξαίρεσης πληροφοριών για λόγους εθνικής ασφάλειας.

Επιπλέον, η Οδηγία καθορίζει συγκεκριμένες απαιτήσεις για τη λειτουργία των CSIRT. Τα κράτη μέλη οφείλουν να διασφαλίζουν ότι κάθε CSIRT διαθέτει επαρκείς πόρους, κατάλληλη και ασφαλή υποδομή επικοινωνίας και πληροφοριών, καθώς και επαρκή στελέχωση ώστε να εξασφαλίζεται η συνεχής διαθεσιμότητα των υπηρεσιών της. Θεσπίζονται επίσης απαιτήσεις ως προς την ασφάλεια των εγκαταστάσεων, την ύπαρξη συστημάτων διαχείρισης αιτημάτων και την εξασφάλιση της εμπιστευτικότητας και αξιοπιστίας των δραστηριοτήτων τους. Ως προς τα καθήκοντά τους, οι CSIRT είναι επιφορτισμένες, μεταξύ άλλων, με την παρακολούθηση και ανάλυση κυβερνοαπειλών και περιστατικών σε εθνικό επίπεδο, την παροχή προειδοποιήσεων και σχετικών πληροφοριών σε βασικές και σημαντικές οντότητες, την αντιμετώπιση περιστατικών και, κατά περίπτωση, την παροχή τεχνικής συνδρομής, καθώς και τη συμμετοχή στο δίκτυο CSIRT και στη διαδικασία συντονισμένης γνωστοποίησης ευπαθειών.

Η Οδηγία προβλέπει επίσης τη θέσπιση μηχανισμού συντονισμένης γνωστοποίησης ευπαθειών. Κάθε κράτος μέλος αναθέτει σε μία από τις CSIRT του συντονιστικό ρόλο, ώστε να λειτουργεί ως διαμεσολαβητής μεταξύ του προσώπου που αναφέρει την ευπάθεια και του κατασκευαστή ή παρόχου του επηρεαζόμενου προϊόντος ή υπηρεσίας ΤΠΕ. Στο πλαίσιο αυτό, η αρμόδια CSIRT προσδιορίζει τις οικείες οντότητες, υποστηρίζει τον αναφέροντα και, όπου απαιτείται, συντονίζει το χρονοδιάγραμμα δημοσιοποίησης, ιδίως σε περιπτώσεις που η ευπάθεια αφορά περισσότερους του ενός φορείς ή έχει διασυνοριακή διάσταση. Η διαδικασία επιτρέπει ανώνυμη αναφορά και διασφαλίζει την εμπιστευτικότητα. Σε ενωσιακό επίπεδο, ο ENISA αναπτύσσει και τηρεί ευρωπαϊκή βάση δεδομένων ευπαθειών, στην οποία μπορούν να καταχωρίζονται, σε εθελοντική βάση, δημόσια γνωστές ευπάθειες προϊόντων και υπηρεσιών ΤΠΕ, μαζί με πληροφορίες για τη σοβαρότητά τους και τη διαθεσιμότητα διορθωτικών μέτρων.

Η NIS2 ρυθμίζει, επιπλέον, τη συνεργασία μεταξύ των βασικών «κομβικών» φορέων του εθνικού πλαισίου εφαρμογής της. Όταν οι αρμόδιες αρχές, το SPOC και οι CSIRTs είναι διακριτές οντότητες, οφείλουν να συνεργάζονται μεταξύ τους για την τήρηση των υποχρεώσεων της Οδηγίας. Στο ίδιο πλαίσιο, τα κράτη μέλη διασφαλίζουν ότι οι CSIRTs ή, κατά περίπτωση, οι αρμόδιες αρχές λαμβάνουν αναφορές σημαντικών περιστατικών και κυβερνοαπειλών, ενώ ορίζονται και ροές ενημέρωσης του SPOC για τις σχετικές

κοινοποιήσεις. Ιδιαίτερη σημασία για τη διακυβέρνηση έχει η πρόβλεψη διατομεακής συνεργασίας σε εθνικό επίπεδο. Συγκεκριμένα, η Οδηγία καλεί τα κράτη μέλη να διασφαλίζουν, στο μέτρο του δυνατού, κατάλληλη συνεργασία μεταξύ των φορέων NIS2 και άλλων αρχών, όπως αρχές επιβολής του νόμου, αρχές προστασίας δεδομένων, αρχές ασφάλειας πολιτικής αεροπορίας ((ΕΚ) 300/2008) και αερομεταφορών ((ΕΕ) 2018/1139), εποπτικές αρχές eIDAS ((ΕΕ) 910/2014), καθώς και αρμόδιες αρχές άλλων τομεακών πράξεων, συμπεριλαμβανομένου του κανονισμού DORA ((ΕΕ) 2022/2554). Τέλος, ορίζεται η απλούστευση της υποβολής αναφορών με τεχνικά μέσα για τις κοινοποιήσεις τόσο σημαντικών περιστατικών κυβερνοασφάλειας όσο και κυβερνοαπειλών ή παρ' ολίγον περιστατικών, με σκοπό τη διασφάλιση της έγκαιρης ενημέρωσης των αρμόδιων αρχών (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2022).

2.5. Εποπτεία και Μηχανισμοί Επιβολής

Πέραν της θεσμικής οργάνωσης και του πλαισίου διακυβέρνησης, η Οδηγία NIS2 θεσπίζει εκτενές σύστημα εποπτείας και επιβολής, με στόχο τη διασφάλιση της ουσιαστικής συμμόρφωσης των βασικών και σημαντικών οντοτήτων. Κεντρικό στοιχείο της NIS2 είναι η διαφοροποίηση της εποπτείας ανάμεσα σε βασικές και σημαντικές οντότητες, με στόχο την αναλογία μεταξύ κινδύνου, απαιτήσεων και διοικητικού φόρτου. Οι βασικές οντότητες υπάγονται σε καθεστώς που καλύπτει τόσο εκ των προτέρων (ex ante) όσο και εκ των υστέρων εποπτεία (ex post), ενώ οι σημαντικές οντότητες υπάγονται σε απλουστευμένη προσέγγιση που ενεργοποιείται εκ των υστέρων, όταν προκύπτουν ενδείξεις ή πληροφορίες πιθανής μη συμμόρφωσης. Για την αποτελεσματική άσκηση των καθηκόντων αυτών, η NIS2 υποχρεώνει τα κράτη μέλη να εξοπλίζουν τις αρμόδιες αρχές με τις αναγκαίες εξουσίες και επαρκείς πόρους.

Από τη μία πλευρά, για τις βασικές οντότητες η Οδηγία προβλέπει πληθώρα εποπτικών εργαλείων. Αρχικά, οι αρμόδιες αρχές μπορούν να διενεργούν επιτόπιες επιθεωρήσεις ή εποπτεία εκτός εγκαταστάσεων, τακτικούς ή στοχευμένους ελέγχους ασφάλειας (από ανεξάρτητο όργανο ή από την ίδια την αρχή), έκτακτους ειδικούς ελέγχους, καθώς και σαρώσεις ασφαλείας βάσει αντικειμενικών κριτηρίων κινδύνου. Ακόμη, μπορούν να ζητούν πληροφορίες, πρόσβαση σε δεδομένα/έγγραφα και αποδεικτικά στοιχεία σχετικά με την εφαρμογή των πολιτικών κυβερνοασφάλειας και των μέτρων διαχείρισης κινδύνων. Από την άλλη, οι σημαντικές οντότητες υπόκεινται επίσης σε ελέγχους και αιτήματα

πληροφοριών, όμως η λογική είναι κατασταλτική: η αρμόδια αρχή παρεμβαίνει όταν έχει αποδεικτικά στοιχεία, ενδείξεις ή πληροφορίες ότι υπάρχει πιθανή παραβίαση, ιδίως ως προς τα άρθρα για μέτρα κινδύνου και υποχρεώσεις αναφοράς. Έτσι, οι αρμόδιες αρχές δύνανται, μεταξύ άλλων, να διενεργούν επιτόπιες επιθεωρήσεις ή εποπτεία εκτός εγκαταστάσεων, τακτικούς ή στοχευμένους ελέγχους ασφάλειας, έκτακτους ειδικούς ελέγχους, καθώς και σαρώσεις ασφάλειας βάσει αντικειμενικών κριτηρίων κινδύνου. Παράλληλα, μπορούν να ζητούν πληροφορίες, πρόσβαση σε δεδομένα ή έγγραφα και αποδεικτικά στοιχεία που αφορούν την εφαρμογή των πολιτικών κυβερνοασφάλειας και των μέτρων διαχείρισης κινδύνων.

Ως προς την επιβολή, η NIS2 κατοχυρώνει μια κλιμάκωση μέτρων. Οι αρμόδιες αρχές μπορούν να εκδίδουν προειδοποιήσεις, δεσμευτικές οδηγίες με προθεσμίες, εντολές παύσης παραβατικής συμπεριφοράς, εντολές συμμόρφωσης με συγκεκριμένο τρόπο και εντός συγκεκριμένου χρόνου, καθώς και εντολές εφαρμογής συστάσεων που προκύπτουν από έλεγχο ασφάλειας. Προβλέπεται επίσης η δυνατότητα ορισμού υπεύθυνου παρακολούθησης, καθώς και, κατά περίπτωση, εντολή δημοσιοποίησης πτυχών παραβιάσεων με συγκεκριμένο τρόπο.

Σε περιπτώσεις μη συμμόρφωσης, η επιβολή συμπληρώνεται από το πλαίσιο των διοικητικών προστίμων, τα οποία διαφοροποιούνται ανάλογα με την κατηγορία της οντότητας. Οι βασικές οντότητες υπόκεινται σε πρόστιμα έως 10.000.000 ευρώ ή έως 2% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών, ενώ οι σημαντικές οντότητες έως 7.000.000 ευρώ ή έως 1,4%. Μεταξύ του απόλυτου ποσού και της ποσοστιαίας τιμής, επιλέγεται σε κάθε περίπτωση το υψηλότερο. Κατά τον καθορισμό του ύψους του προστίμου λαμβάνονται υπόψη παράγοντες όπως η σοβαρότητα, η διάρκεια, οι προηγούμενες παραβάσεις, η ζημία, η ύπαρξη πρόθεσης ή αμέλειας και ο βαθμός συνεργασίας. Το εθνικό δίκαιο μπορεί να ρυθμίζει ειδικά το αν και σε ποιο βαθμό επιβάλλονται πρόστιμα σε φορείς δημόσιας διοίκησης.

Ειδικά για τις βασικές οντότητες, εφόσον τα συνήθη μέτρα αποδειχθούν αναποτελεσματικά, προβλέπονται αυστηρότερα εργαλεία ως «έσχατη λύση»: προσωρινή αναστολή πιστοποίησης/εξουσιοδότησης που αφορά υπηρεσίες ή δραστηριότητες, ή προσωρινή απαγόρευση άσκησης διευθυντικών καθηκόντων σε επίπεδο CEO ή νομικού εκπροσώπου, μέχρι να διορθωθούν οι ελλείψεις και να επιτευχθεί συμμόρφωση. Τα μέτρα αυτά συνοδεύονται από διαδικαστικές εγγυήσεις (δικαιώματα υπεράσπισης κ.λπ.) και δεν εφαρμόζονται σε φορείς δημόσιας διοίκησης που υπάγονται στην Οδηγία.

Η Οδηγία λαμβάνει υπόψη την πιθανή επικάλυψη μεταξύ παραβιάσεων των υποχρεώσεων κυβερνοασφάλειας και παραβιάσεων δεδομένων προσωπικού χαρακτήρα. Όταν, στο πλαίσιο εποπτείας ή επιβολής, διαπιστώνεται ότι παράβαση υποχρεώσεων διαχείρισης κινδύνου ή κοινοποίησης περιστατικών ενδέχεται να συνεπάγεται παραβίαση δεδομένων προσωπικού χαρακτήρα, οι αρμόδιες αρχές οφείλουν να ενημερώνουν χωρίς αδικαιολόγητη καθυστέρηση την αρμόδια εποπτική αρχή προστασίας δεδομένων. Επιπλέον, η Οδηγία προβλέπει μηχανισμό αποφυγής διπλής κύρωσης για την ίδια συμπεριφορά, ώστε, όταν επιβάλλεται διοικητικό πρόστιμο βάσει του κανονισμού (ΕΕ) 2016/679, να μην επιβάλλεται δεύτερο πρόστιμο για το ίδιο πραγματικό περιστατικό δυνάμει της NIS2, χωρίς να αποκλείεται η λήψη λοιπών διοικητικών μέτρων.

Περαιτέρω, η Οδηγία υποχρεώνει τα κράτη μέλη να θεσπίσουν κανόνες κυρώσεων για παραβιάσεις των εθνικών μέτρων μεταφοράς της, διασφαλίζοντας ότι οι προβλεπόμενες κυρώσεις είναι αποτελεσματικές, αναλογικές και αποτρεπτικές. Η συγκεκριμενοποίηση των κυρώσεων και η διαδικασία επιβολής τους επαφίεται στο εθνικό δίκαιο, στο πλαίσιο των γενικών αρχών του ενωσιακού δικαίου.

Τέλος, η NIS2 αναγνωρίζει τη διασυνοριακή διάσταση της εποπτείας, ιδίως όταν μια οντότητα παρέχει υπηρεσίες σε περισσότερα κράτη μέλη ή όταν τα συστήματα δικτύου και πληροφοριών της βρίσκονται σε διαφορετικές δικαιοδοσίες. Στις περιπτώσεις αυτές, οι αρμόδιες αρχές των ενδιαφερόμενων κρατών μελών υποχρεούνται να συνεργάζονται και να παρέχουν αμοιβαία συνδρομή, περιλαμβανομένης της ανταλλαγής πληροφοριών και, όπου απαιτείται, της διενέργειας εποπτικών μέτρων κατόπιν αιτήματος άλλης αρχής. Ο μηχανισμός αυτός αποτελεί βασική προϋπόθεση για την αποφυγή κενών εποπτείας σε διασυνοριακά περιβάλλοντα (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2022).

3. ΠΛΑΙΣΙΟ ΕΦΑΡΜΟΓΗΣ

Η Οδηγία NIS2 διαμορφώνει ενιαίο ευρωπαϊκό πλαίσιο για τη διαχείριση κινδύνων κυβερνοασφάλειας σε οργανισμούς που δραστηριοποιούνται σε κρίσιμους τομείς της οικονομίας και της κοινωνίας. Οι οργανισμοί που εμπίπτουν στο πεδίο εφαρμογής της Οδηγίας υποχρεούνται να λαμβάνουν κατάλληλα τεχνικά, οργανωτικά και επιχειρησιακά μέτρα για την προστασία των συστημάτων δικτύου και πληροφοριών που χρησιμοποιούν για τη λειτουργία τους και για την παροχή των υπηρεσιών τους.

Η Οδηγία εισάγει μια προσέγγιση βασισμένη στη διαχείριση κινδύνου, σύμφωνα με την οποία τα μέτρα κυβερνοασφάλειας πρέπει να είναι ανάλογα με τον βαθμό έκθεσης της οντότητας σε κινδύνους, το μέγεθος και τα χαρακτηριστικά της, καθώς και τις πιθανές επιπτώσεις περιστατικών ασφάλειας. Ιδιαίτερη βαρύτητα αποδίδεται στον ρόλο της ανώτατης διοίκησης, η οποία καλείται να εγκρίνει και να επιβλέπει την εφαρμογή των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας.

Η αποτελεσματική εφαρμογή των απαιτήσεων της Οδηγίας προϋποθέτει μια οργανωμένη διαδικασία σχεδιασμού και υλοποίησης μέτρων κυβερνοασφάλειας σε επίπεδο οργανισμού. Για τον σκοπό αυτό, οι οργανισμοί καλούνται να αξιολογήσουν την υφιστάμενη κατάσταση ασφάλειας, να καθορίσουν πολιτικές και διαδικασίες διαχείρισης κινδύνων, να εφαρμόσουν τεχνικά και οργανωτικά μέτρα προστασίας και να αναπτύξουν μηχανισμούς ελέγχου και συνεχούς βελτίωσης.

Στο παρόν κεφάλαιο παρουσιάζεται ένα ενδεικτικό πλαίσιο εφαρμογής των απαιτήσεων της NIS2 σε οργανισμούς. Το πλαίσιο αυτό περιλαμβάνει βασικά στάδια προετοιμασίας, σχεδιασμού, υλοποίησης και αξιολόγησης των μέτρων κυβερνοασφάλειας, τα οποία μπορούν να υποστηρίξουν τη συστηματική ενσωμάτωση των απαιτήσεων της Οδηγίας στις λειτουργίες ενός οργανισμού (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2022; Αρχή Ψηφιακής Ασφάλειας, 2024; National Cyber Security Centre, 2025).

3.1. Προετοιμασία Εφαρμογής

Η αρχική φάση εφαρμογής των απαιτήσεων της Οδηγίας NIS2 περιλαμβάνει την αξιολόγηση της υφιστάμενης κατάστασης κυβερνοασφάλειας του οργανισμού μέσω

διαδικασίας ανάλυσης κενών (gap analysis). Η ανάλυση αυτή αποσκοπεί στη σύγκριση των υφιστάμενων πρακτικών ασφάλειας, πολιτικών και διαδικασιών με τις απαιτήσεις που προβλέπει η Οδηγία, προκειμένου να εντοπιστούν τυχόν αποκλίσεις ή ελλείψεις που ενδέχεται να επηρεάσουν τη συμμόρφωση του οργανισμού. Βάσει της ανάλυσης αυτής εξετάζονται βασικοί τομείς, όπως η διακυβέρνηση και η διαχείριση κινδύνων κυβερνοασφάλειας, οι μηχανισμοί διαχείρισης περιστατικών, η επιχειρησιακή συνέχεια, καθώς και η ασφάλεια της εφοδιαστικής αλυσίδας. Μέσω της συγκεκριμένης διαδικασίας, ο οργανισμός αποκτά σαφή εικόνα της υφιστάμενης ωριμότητας των μέτρων κυβερνοασφάλειας και μπορεί να προσδιορίσει τις περιοχές που απαιτούν βελτίωση ή ενίσχυση. Η ανάλυση κενών αποτελεί συνεπώς κρίσιμο αρχικό στάδιο της διαδικασίας συμμόρφωσης, καθώς επιτρέπει τον προσδιορισμό των βασικών αναγκών συμμόρφωσης και τον σχεδιασμό των απαραίτητων ενεργειών για την ενίσχυση της ασφάλειας των συστημάτων δικτύου και πληροφοριών ενός οργανισμού (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2022; Advisera, 2024; Kosutic, 2024; Άννα Πέλλα, 2025; Κωτσικοπούλου, 2025; Commugen, χ.χ.).

Πέραν της αρχικής αξιολόγησης της υφιστάμενης κατάστασης κυβερνοασφάλειας, η αποτελεσματική εφαρμογή των απαιτήσεων της Οδηγίας NIS2 προϋποθέτει την ενεργή συμμετοχή και υποστήριξη της ανώτατης διοίκησης του οργανισμού. Σύμφωνα με το άρθρο 20 της Οδηγίας, η διοίκηση των βασικών και σημαντικών οντοτήτων οφείλει να εγκρίνει τα μέτρα διαχείρισης κινδύνων κυβερνοασφάλειας που λαμβάνει η οντότητα και να επιβλέπει την εφαρμογή τους, ενώ φέρει ευθύνη για ενδεχόμενη μη συμμόρφωση με τις σχετικές υποχρεώσεις. Η διάταξη αυτή αναδεικνύει τον στρατηγικό ρόλο της διοίκησης στη διακυβέρνηση της κυβερνοασφάλειας, μεταφέροντας την ευθύνη για τη λήψη και υλοποίηση των μέτρων προστασίας σε επίπεδο οργανωτικής ηγεσίας. Κατά συνέπεια, τα διοικητικά όργανα καλούνται να εγκρίνουν τις πολιτικές ασφάλειας, να διαθέτουν τους απαραίτητους πόρους για την υλοποίηση των μέτρων διαχείρισης κινδύνων και να διασφαλίζουν ότι υφίσταται κατάλληλη δομή διακυβέρνησης για την παρακολούθηση της εφαρμογής τους. Την ίδια στιγμή, η Οδηγία προβλέπει ότι τα μέλη της διοίκησης πρέπει να διαθέτουν επαρκείς γνώσεις σχετικά με τους κινδύνους κυβερνοασφάλειας και να παρακολουθούν σχετική εκπαίδευση, ώστε να μπορούν να αξιολογούν αποτελεσματικά τις πρακτικές διαχείρισης κινδύνων και τις επιπτώσεις τους στις υπηρεσίες του οργανισμού (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2022; Kosutic, 2024; Αλεξάνδρα Εξάρχου, 2024; Αρχή Ψηφιακής Ασφάλειας, 2024; National Cyber Security Centre, 2025).

Ακόμη, η εφαρμογή των απαιτήσεων της Οδηγίας αποτελεί σύνθετη οργανωτική διαδικασία, η οποία απαιτεί συστηματικό σχεδιασμό και συντονισμό πολλαπλών δραστηριοτήτων. Για τον λόγο αυτό, η υλοποίηση των μέτρων κυβερνοασφάλειας δεν μπορεί να αντιμετωπιστεί ως μεμονωμένη τεχνική εργασία, αλλά πρέπει να οργανώνεται ως έργο με σαφώς καθορισμένα στάδια, στόχους και αρμοδιότητες. Η προσέγγιση αυτή επιτρέπει τον καθορισμό συγκεκριμένων βημάτων υλοποίησης, χρονοδιαγραμμάτων, υπευθύνων και αναμενόμενων αποτελεσμάτων, διευκολύνοντας τον συντονισμό των εμπλεκόμενων οργανωτικών μονάδων και τη διαχείριση των απαιτούμενων πόρων. Επιπλέον, η ενσωμάτωση της κυβερνοασφάλειας στη διαχείριση έργων αποτελεί καθιερωμένη πρακτική σε διεθνή πρότυπα ασφάλειας πληροφοριών. Σύμφωνα με το πρότυπο ISO/IEC 27002, οι απαιτήσεις ασφάλειας πληροφοριών πρέπει να λαμβάνονται υπόψη σε όλα τα στάδια του κύκλου ζωής ενός έργου, ώστε οι σχετικοί κίνδυνοι να εντοπίζονται και να αντιμετωπίζονται εγκαίρως. Με τον τρόπο αυτό διασφαλίζεται ότι τα μέτρα κυβερνοασφάλειας ενσωματώνονται συστηματικά στον σχεδιασμό και την υλοποίηση των οργανωτικών και τεχνολογικών αλλαγών που απαιτούνται για τη συμμόρφωση με την Οδηγία (ISO/IEC, 2022; Kosutic, 2024).

Η προετοιμασία για την εφαρμογή της Οδηγίας NIS2 περιλαμβάνει, μεταξύ άλλων, την αρχική εκπαίδευση των εμπλεκομένων στελεχών. Η παροχή κατάλληλης εκπαίδευσης, ήδη από τα πρώτα στάδια της διαδικασίας εφαρμογής, επιτρέπει στα στελέχη του οργανισμού να κατανοήσουν το περιεχόμενο και τις υποχρεώσεις που απορρέουν από την Οδηγία, καθώς και τον ρόλο που καλούνται να διαδραματίσουν στην υλοποίηση των μέτρων κυβερνοασφάλειας. Η σημασία της εκπαίδευσης αναγνωρίζεται και από την ίδια την Οδηγία, καθώς το άρθρο 20 προβλέπει ότι τα μέλη της ανώτατης διοίκησης των βασικών και σημαντικών οντοτήτων οφείλουν να παρακολουθούν κατάλληλη κατάρτιση, ενθαρρύνοντας ταυτόχρονα την παροχή αντίστοιχης εκπαίδευσης και στους εργαζομένους των οργανισμών. Η ανάπτυξη γνώσεων και δεξιοτήτων σε θέματα κυβερνοασφάλειας συμβάλλει στην αποτελεσματική αναγνώριση και αξιολόγηση των κινδύνων που απειλούν τα συστήματα δικτύου και πληροφοριών του οργανισμού. Στο ίδιο πνεύμα, διεθνή πρότυπα ασφάλειας πληροφοριών, όπως τα ISO/IEC 27001 και ISO/IEC 27002, επισημαίνουν ότι οι οργανισμοί πρέπει να διασφαλίζουν την επάρκεια και την κατάλληλη εκπαίδευση του προσωπικού τους, ώστε οι εργαζόμενοι να γνωρίζουν τις ευθύνες τους και να συμβάλλουν ενεργά στην προστασία των πληροφοριακών πόρων του οργανισμού (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2022; ISO/IEC, 2022a, 2022b; Kosutic, 2024).

3.2. Πολιτικές Ασφάλειας Πληροφοριών και Διαχείρισης Κινδύνων

Η εφαρμογή των απαιτήσεων κυβερνοασφάλειας της NIS2 προϋποθέτει τον καθορισμό σαφών πολιτικών ασφάλειας που καθοδηγούν τη διαχείριση των κινδύνων και τη λειτουργία των πληροφοριακών συστημάτων ενός οργανισμού. Στο πλαίσιο αυτό, οι οργανισμοί καλούνται να διαμορφώσουν μια κεντρική πολιτική ασφάλειας πληροφοριών, η οποία καθορίζει τη γενική κατεύθυνση και τους στόχους της κυβερνοασφάλειας, καθώς και τους βασικούς ρόλους και τις αρμοδιότητες που σχετίζονται με την προστασία των πληροφοριακών πόρων. Η ύπαρξη μιας τέτοιας πολιτικής αποτελεί καθιερωμένη πρακτική στα διεθνή πρότυπα διαχείρισης ασφάλειας πληροφοριών. Σύμφωνα με το πρότυπο ISO/IEC 27001, η ανώτατη διοίκηση ενός οργανισμού οφείλει να καθορίζει και να εγκρίνει μια πολιτική ασφάλειας πληροφοριών η οποία είναι κατάλληλη για τον σκοπό και τις δραστηριότητες του οργανισμού, περιλαμβάνει δεσμεύσεις για την τήρηση των σχετικών απαιτήσεων και παρέχει το πλαίσιο για τον καθορισμό στόχων ασφάλειας πληροφοριών. Η πολιτική αυτή πρέπει να τεκμηριώνεται, να κοινοποιείται εντός του οργανισμού και να αποτελεί σημείο αναφοράς για την ανάπτυξη επιμέρους πολιτικών και διαδικασιών ασφάλειας. Σε ένα σύστημα διαχείρισης ασφάλειας πληροφοριών (Information Security Management System – ISMS), η πολιτική ασφάλειας λειτουργεί ως θεμελιώδες στοιχείο διακυβέρνησης, καθώς συγκεντρώνει τις βασικές αρχές προστασίας των πληροφοριών και καθοδηγεί τη συστηματική εφαρμογή μέτρων κυβερνοασφάλειας στον οργανισμό (ISO/IEC, 2022; Kosutic, 2024; CYBERDAY, χ.χ.).

Η αποτελεσματική εφαρμογή των μέτρων κυβερνοασφάλειας προϋποθέτει ακόμη την ύπαρξη σαφώς καθορισμένης μεθοδολογίας διαχείρισης κινδύνων, η οποία καθοδηγεί τον τρόπο με τον οποίο ένας οργανισμός εντοπίζει, αξιολογεί και αντιμετωπίζει τους κινδύνους που απειλούν τα συστήματα δικτύου και πληροφοριών του. Η Οδηγία NIS2 υιοθετεί προσέγγιση βασισμένη στη διαχείριση κινδύνων, καθώς προβλέπει ότι οι βασικές και σημαντικές οντότητες οφείλουν να λαμβάνουν κατάλληλα τεχνικά, οργανωτικά και επιχειρησιακά μέτρα για τη διαχείριση των κινδύνων κυβερνοασφάλειας και την ελαχιστοποίηση των επιπτώσεων πιθανών περιστατικών. Για την υποστήριξη της διαδικασίας αυτής, οι οργανισμοί καλούνται να καθορίσουν μια μεθοδολογία διαχείρισης κινδύνων η οποία να περιγράφει τα κριτήρια αξιολόγησης κινδύνων, τις διαδικασίες εκτίμησης και αντιμετώπισής τους, καθώς και τα κριτήρια αποδοχής κινδύνου. Η ύπαρξη μιας τέτοιας μεθοδολογίας συμβάλλει στη συστηματική και ομοιόμορφη αντιμετώπιση των κινδύνων σε όλο τον οργανισμό και διασφαλίζει ότι οι αποφάσεις σχετικά με την προστασία

των πληροφοριακών συστημάτων λαμβάνονται με βάση αντικειμενικά και προκαθορισμένα κριτήρια. Αντίστοιχη προσέγγιση υιοθετεί το πρότυπο ISO/IEC 27001, το οποίο προβλέπει ότι οι οργανισμοί πρέπει να εντοπίζουν τους κινδύνους που επηρεάζουν την ασφάλεια πληροφοριών και να σχεδιάζουν τις κατάλληλες ενέργειες για την αντιμετώπισή τους στο πλαίσιο του συστήματος διαχείρισης ασφάλειας πληροφοριών (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2022; ISO/IEC, 2022; Kosutic, 2024).

3.3. Αποτίμηση και Αντιμετώπιση Κινδύνων

Κεντρικό στοιχείο της διαχείρισης κυβερνοασφάλειας ενός οργανισμού είναι η διαδικασία αποτίμησης και αντιμετώπισης κινδύνων. Η διαδικασία αποτίμησης κινδύνων (risk assessment) αποσκοπεί στον εντοπισμό των απειλών και των ευπαθειών που μπορούν να επηρεάσουν τα συστήματα δικτύου και πληροφοριών, καθώς και στην αξιολόγηση της πιθανότητας εκδήλωσης και της σοβαρότητας των πιθανών επιπτώσεών τους. Για τον λόγο αυτό, πραγματοποιείται καταγραφή των κρίσιμων πληροφοριακών πόρων και περιουσιακών στοιχείων του οργανισμού, καθώς και των σχετικών απειλών και ευπαθειών που ενδέχεται να τα επηρεάσουν. Ταυτόχρονα, αξιολογείται η πιθανότητα εκδήλωσης περιστατικών και το μέγεθος των επιπτώσεων που θα μπορούσαν να προκύψουν για τις λειτουργίες και τις υπηρεσίες του οργανισμού. Η διαδικασία αυτή οδηγεί στον προσδιορισμό του επιπέδου κινδύνου για κάθε σενάριο απειλής και επιτρέπει την ιεράρχηση των κινδύνων, αναλόγως της σοβαρότητάς τους.

Με βάση τα αποτελέσματα της αποτίμησης κινδύνων, οι οργανισμοί προχωρούν στον καθορισμό κατάλληλων τρόπων αντιμετώπισης κινδύνων (risk treatment). Οι στρατηγικές αντιμετώπισης κινδύνων μπορεί να περιλαμβάνουν τη μείωση του κινδύνου μέσω της εφαρμογής κατάλληλων μέτρων ασφάλειας, την αποφυγή δραστηριοτήτων που δημιουργούν υψηλό επίπεδο κινδύνου, τη μεταφορά του κινδύνου σε τρίτους (π.χ. μέσω ασφαλιστικών ή συμβατικών μηχανισμών), ή την αποδοχή κινδύνων που κρίνονται ανεκτοί βάσει της στρατηγικής του οργανισμού. Για τον σκοπό αυτό, οι οργανισμοί καθορίζουν τα κατάλληλα τεχνικά, οργανωτικά και επιχειρησιακά μέτρα προστασίας, τα οποία επιλέγονται με γνώμονα τη σοβαρότητα των εντοπισμένων κινδύνων και το απαιτούμενο επίπεδο προστασίας των συστημάτων και των υπηρεσιών του οργανισμού. Η προσέγγιση αυτή αντανακλά τη βασική αρχή της Οδηγίας NIS2, σύμφωνα με την οποία οι βασικές και σημαντικές οντότητες οφείλουν να λαμβάνουν κατάλληλα και αναλογικά μέτρα διαχείρισης

κινδύνων για την προστασία των συστημάτων δικτύου και πληροφοριών τους. Παράλληλα, τα διεθνή πρότυπα διαχείρισης ασφάλειας πληροφοριών, όπως το ISO/IEC 27001, προβλέπουν ότι οι οργανισμοί πρέπει να εφαρμόζουν συστηματική διαδικασία αποτίμησης κινδύνων ώστε να εντοπίζονται οι σημαντικότεροι κίνδυνοι και να καθορίζονται οι κατάλληλες ενέργειες για την αντιμετώπισή τους στο πλαίσιο του συστήματος διαχείρισης ασφάλειας πληροφοριών (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2022; ISO/IEC, 2022; ΣΕΒ σύνδεσμος επιχειρήσεων και βιομηχανιών - Τομέας Τεχνολογίας & Ψηφιακού Μετασχηματισμού, 2025).

Μετά τον προσδιορισμό των κατάλληλων τρόπων αντιμετώπισης των κινδύνων, οι οργανισμοί προχωρούν στη διαμόρφωση ενός συγκεκριμένου σχεδίου αντιμετώπισης κινδύνων (Risk Treatment Plan), που περιγράφει πώς θα υλοποιηθούν τα μέτρα μείωσης των εντοπισμένων κινδύνων. Το σχέδιο αυτό λειτουργεί ως πρακτικός οδηγός υλοποίησης των μέτρων προστασίας και περιλαμβάνει τις δραστηριότητες, τις διαδικασίες και τις τεχνολογικές λύσεις που πρέπει να εφαρμοστούν για την ενίσχυση του επιπέδου κυβερνοασφάλειας του οργανισμού. Για την επίτευξη του στόχου αυτού, καθορίζονται τα συγκεκριμένα μέτρα που πρόκειται να υλοποιηθούν, οι αρμόδιοι για την εφαρμογή τους, οι απαιτούμενοι πόροι, καθώς και το χρονοδιάγραμμα υλοποίησης των σχετικών ενεργειών. Με τον τρόπο αυτό διασφαλίζεται ότι τα μέτρα κυβερνοασφάλειας εφαρμόζονται με οργανωμένο και συντονισμένο τρόπο, ενώ παράλληλα καθίσταται δυνατή η παρακολούθηση της προόδου και της αποτελεσματικότητας των ενεργειών που υλοποιούνται. Ιδιαίτερη σημασία έχει η έγκριση του σχεδίου από την ανώτατη διοίκηση του οργανισμού, η οποία φέρει την ευθύνη για την εποπτεία των μέτρων διαχείρισης κινδύνων και για τη διάθεση των απαραίτητων πόρων για την υλοποίησή τους (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2022; ISO/IEC, 2022; National Cyber Security Centre, 2025).

3.4. Υλοποίηση Μέτρων Κυβερνοασφάλειας

Μετά την κατάρτιση και έγκριση του σχεδίου αντιμετώπισης κινδύνων, οι οργανισμοί προχωρούν στην υλοποίηση των μέτρων κυβερνοασφάλειας που έχουν προσδιοριστεί κατά τη διαδικασία διαχείρισης κινδύνων. Τα μέτρα αυτά προστατεύουν τα συστήματα δικτύου και πληροφοριών από απειλές που μπορούν να επηρεάσουν τη διαθεσιμότητα, την ακεραιότητα και την εμπιστευτικότητα των πληροφοριών. Τα μέτρα κυβερνοασφάλειας

υλοποιούνται με τρόπο ανάλογο προς τον εκάστοτε κίνδυνο, λαμβάνοντας υπόψη το μέγεθος και τη φύση των δραστηριοτήτων του οργανισμού, το επίπεδο έκθεσης σε κινδύνους, καθώς και τις πιθανές επιπτώσεις περιστατικών ασφάλειας. Τα μέτρα αυτά καλύπτουν διαφορετικές πτυχές της ασφάλειας των πληροφοριακών συστημάτων. Ενδεικτικά, περιλαμβάνουν την ανάπτυξη και εφαρμογή πολιτικών ασφάλειας δικτύων και συστημάτων πληροφοριών, τη διαχείριση και προστασία των πληροφοριακών πόρων, τον έλεγχο πρόσβασης στα συστήματα, την υιοθέτηση πρακτικών βασικής υγιεινής κυβερνοασφάλειας, καθώς και την εφαρμογή μηχανισμών κρυπτογράφησης και ασφαλούς επικοινωνίας. Επιπλέον, ιδιαίτερη σημασία αποδίδεται στην ασφάλεια της εφοδιαστικής αλυσίδας, στην ασφαλή ανάπτυξη και συντήρηση πληροφοριακών συστημάτων, καθώς και στη διασφάλιση της επιχειρησιακής συνέχειας και της φυσικής ασφάλειας των υποδομών. Η υλοποίηση των μέτρων αυτών πραγματοποιείται μέσω της θέσπισης συγκεκριμένων πολιτικών, διαδικασιών και τεχνικών ελέγχων, οι οποίοι καθορίζουν τους κανόνες και τις πρακτικές που πρέπει να ακολουθούνται για την προστασία των πληροφοριακών συστημάτων (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2022; ISO/IEC, 2022; Άννα Πέλλα, 2025).

Οι βασικές θεματικές περιοχές των μέτρων κυβερνοασφάλειας που προβλέπει η Οδηγία NIS2 παρουσιάζονται συνοπτικά στην εικόνα 5:

Εικόνα 5 - Τεχνικές και μεθοδολογικές απαιτήσεις των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας (European Union Agency for Cybersecurity, 2025)

Σημαντική διάσταση της κυβερνοασφάλειας των οργανισμών αφορά την ασφάλεια της εφοδιαστικής αλυσίδας, καθώς η λειτουργία των πληροφοριακών συστημάτων εξαρτάται σε μεγάλο βαθμό από προμηθευτές τεχνολογικών λύσεων, παρόχους υπηρεσιών και άλλους εξωτερικούς συνεργάτες. Η Οδηγία NIS2 αναγνωρίζει τον κίνδυνο που μπορεί να προκύψει από αδυναμίες ασφάλειας σε προϊόντα, υπηρεσίες ή διαδικασίες τρίτων οργανισμών και προβλέπει τη λήψη μέτρων που αφορούν τις σχέσεις μεταξύ των οντοτήτων και των προμηθευτών ή παρόχων υπηρεσιών τους. Σε αυτό το πλαίσιο, οι οργανισμοί εφαρμόζουν διαδικασίες διαχείρισης κινδύνων εφοδιαστικής αλυσίδας που περιλαμβάνουν

την αναγνώριση και καταγραφή των προμηθευτών με πρόσβαση σε συστήματα ή δεδομένα, καθώς και την αξιολόγηση του επιπέδου κυβερνοασφάλειας που διαθέτουν. Η διαδικασία αξιολόγησης μπορεί να βασίζεται σε ερωτηματολόγια ασφάλειας, σε πιστοποιήσεις που διαθέτουν οι προμηθευτές ή σε εσωτερικούς ελέγχους συμμόρφωσης με απαιτήσεις κυβερνοασφάλειας. Παράλληλα, οι απαιτήσεις κυβερνοασφάλειας ενσωματώνονται στις συμβάσεις και στις συμφωνίες παροχής υπηρεσιών με τους προμηθευτές, μέσω ρητρών που καθορίζουν τις υποχρεώσεις ασφάλειας, τις διαδικασίες γνωστοποίησης περιστατικών και τα ελάχιστα τεχνικά και οργανωτικά μέτρα προστασίας που πρέπει να εφαρμόζονται. Επιπλέον, η διαχείριση της ασφάλειας της εφοδιαστικής αλυσίδας περιλαμβάνει τη συνεχή παρακολούθηση της συμμόρφωσης των προμηθευτών με τις απαιτήσεις κυβερνοασφάλειας του οργανισμού, μέσω περιοδικών αξιολογήσεων, ελέγχων συμμόρφωσης και σχετικών δεικτών απόδοσης (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2022; Kosutic, 2024; ΣΕΒ σύνδεσμος επιχειρήσεων και βιομηχανιών - Τομέας Τεχνολογίας & Ψηφιακού Μετασχηματισμού, 2025).

Η εφαρμογή των μέτρων κυβερνοασφάλειας συνοδεύεται από διαδικασίες αξιολόγησης της αποτελεσματικότητάς τους, ώστε να διασφαλίζεται ότι τα μέτρα που έχουν υιοθετηθεί λειτουργούν όπως προβλέπεται και συμβάλλουν στη μείωση των κινδύνων κυβερνοασφάλειας. Η Οδηγία NIS2 προβλέπει τη θέσπιση πολιτικών και διαδικασιών για την αξιολόγηση της αποτελεσματικότητας των μέτρων διαχείρισης κινδύνων, με στόχο την παρακολούθηση της εφαρμογής τους και την έγκαιρη αναγνώριση αποκλίσεων ή αδυναμιών. Για την ορθή εφαρμογή της διαδικασίας, οι οργανισμοί καθορίζουν μηχανισμούς παρακολούθησης και μέτρησης της λειτουργίας των διαδικασιών και των ελέγχων ασφάλειας. Η παρακολούθηση μπορεί να περιλαμβάνει τη συλλογή και ανάλυση δεικτών απόδοσης ασφάλειας, την αξιολόγηση της αποτελεσματικότητας των εφαρμοζόμενων ελέγχων και την καταγραφή των αποτελεσμάτων σε τεκμηριωμένες αναφορές. Ακόμη, εφαρμόζονται διαδικασίες εσωτερικού ελέγχου που αποσκοπούν στον εντοπισμό αποκλίσεων από τις καθορισμένες πολιτικές και διαδικασίες κυβερνοασφάλειας. Επιπλέον, η διοίκηση του οργανισμού πραγματοποιεί περιοδικές ανασκοπήσεις των αποτελεσμάτων των διαδικασιών παρακολούθησης και ελέγχου, με στόχο την αξιολόγηση της συνολικής απόδοσης του πλαισίου κυβερνοασφάλειας και την υιοθέτηση των αναγκαίων βελτιωτικών ενεργειών (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2022; ISO/IEC, 2022; Kosutic, 2024; Άννα Πέλλα, 2025).

Στο πλαίσιο της Οδηγίας NIS2, οι βασικές και σημαντικές οντότητες υποχρεούνται να κοινοποιούν σημαντικά περιστατικά κυβερνοασφάλειας. Ως περιστατικό νοείται κάθε

συμβάν που επηρεάζει τη διαθεσιμότητα, την ακεραιότητα, την αυθεντικότητα ή την εμπιστευτικότητα των δεδομένων ή των υπηρεσιών που παρέχονται μέσω συστημάτων δικτύου και πληροφοριών. Οι οργανισμοί υποχρεούνται να κοινοποιούν τα σημαντικά περιστατικά στις αρμόδιες αρχές ή στις ομάδες αντιμετώπισης περιστατικών ασφάλειας υπολογιστών (CSIRT), καθώς και στους αποδέκτες των υπηρεσιών τους όταν ενδέχεται να επηρεαστούν από το περιστατικό. Η διαδικασία κοινοποίησης πραγματοποιείται μέσω συγκεκριμένων σταδίων αναφοράς που προβλέπονται από τη νομοθεσία. Αρχικά, υποβάλλεται έγκαιρη προειδοποίηση (early warning) εντός είκοσι τεσσάρων ωρών από τη στιγμή που η οντότητα αντιληφθεί την ύπαρξη σημαντικού περιστατικού. Στη συνέχεια, εντός εβδομήντα δύο ωρών αποστέλλεται αναλυτικότερη κοινοποίηση περιστατικού, η οποία περιλαμβάνει αρχική αξιολόγηση της σοβαρότητας και των επιπτώσεων του συμβάντος. Επιπλέον, μπορεί να ζητηθεί ενδιάμεση έκθεση από την αρμόδια αρχή με επικαιροποιημένες πληροφορίες σχετικά με την εξέλιξη του περιστατικού. Τέλος, υποβάλλεται τελική έκθεση εντός ενός μηνός από την κοινοποίηση του περιστατικού, η οποία περιλαμβάνει αναλυτική περιγραφή του συμβάντος, την πιθανή αιτία του, τις επιπτώσεις του και τα μέτρα αντιμετώπισης που εφαρμόστηκαν. Για την αποτελεσματική εφαρμογή των υποχρεώσεων αυτών, οι οργανισμοί οφείλουν να θεσπίζουν διαδικασίες εσωτερικής διαχείρισης και αναφοράς περιστατικών, οι οποίες καθορίζουν τον τρόπο αναγνώρισης, καταγραφής και κλιμάκωσης των συμβάντων ασφάλειας. Οι διαδικασίες αυτές περιλαμβάνουν τον καθορισμό υπευθύνων για την καταγραφή και αξιολόγηση των περιστατικών, τη διατήρηση σχετικών αρχείων και την έγκαιρη επικοινωνία με τις αρμόδιες αρχές (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2022; ISO/IEC, 2022; Εθνική Αρχή Κυβερνοασφάλειας, 2024; Kosutic, 2024).

3.5. Παρακολούθηση και Βελτίωση

Η συνεχής ενίσχυση της κυβερνοασφάλειας ενός οργανισμού προϋποθέτει την κατάλληλη εκπαίδευση και ευαισθητοποίηση του προσωπικού. Η Οδηγία NIS2 προβλέπει ότι τα μέλη της ανώτατης διοίκησης των βασικών και σημαντικών οντοτήτων οφείλουν να παρακολουθούν κατάλληλη εκπαίδευση και να ενθαρρύνουν την παροχή αντίστοιχης κατάρτισης στους εργαζομένους, ώστε να αναπτύσσονται οι απαραίτητες γνώσεις και δεξιότητες για την αναγνώριση και διαχείριση κινδύνων κυβερνοασφάλειας. Επιπλέον, η Οδηγία περιλαμβάνει τη βασική κυβερνοϋγιεινή και την εκπαίδευση στην κυβερνοασφάλεια

μεταξύ των ελάχιστων μέτρων διαχείρισης κινδύνων που πρέπει να εφαρμόζονται από τους οργανισμούς. Για την υλοποίηση των απαιτήσεων αυτών, οι οργανισμοί οργανώνουν προγράμματα ευαισθητοποίησης και εκπαίδευσης που απευθύνονται τόσο στη διοίκηση όσο και στους εργαζομένους, με στόχο την κατανόηση των βασικών αρχών ασφάλειας πληροφοριών και των υποχρεώσεων που απορρέουν από τις πολιτικές κυβερνοασφάλειας του οργανισμού. Τα προγράμματα αυτά μπορούν να περιλαμβάνουν εκπαιδευτικά σεμινάρια, διαδικτυακά μαθήματα, ενημερωτικές δράσεις ή εξειδικευμένη τεχνική κατάρτιση για προσωπικό με αυξημένες αρμοδιότητες ασφάλειας πληροφοριών. Η εκπαίδευση σε θέματα κυβερνοασφάλειας πραγματοποιείται σε τακτική βάση και συνδέεται με τις απαιτήσεις επάρκειας προσωπικού που προβλέπονται από τα διεθνή πρότυπα διαχείρισης ασφάλειας πληροφοριών. Σύμφωνα με το ISO/IEC 27001, οι οργανισμοί οφείλουν να διασφαλίζουν ότι τα άτομα που επηρεάζουν την απόδοση της ασφάλειας πληροφοριών διαθέτουν την απαραίτητη κατάρτιση και ικανότητα για την εκτέλεση των καθηκόντων τους, καθώς και να διατηρούν τεκμηριωμένες αποδείξεις σχετικά με την εκπαίδευση και τις δεξιότητές τους. Με τον τρόπο αυτό ενισχύεται η ικανότητα του οργανισμού να προλαμβάνει περιστατικά κυβερνοασφάλειας και να υποστηρίζει την αποτελεσματική εφαρμογή των μέτρων προστασίας (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2022; ISO/IEC, 2022; Kosutic, 2024).

Για την παρακολούθηση της εφαρμογής των μέτρων κυβερνοασφάλειας, οι οργανισμοί διενεργούν περιοδικούς εσωτερικούς ελέγχους. Αν και η Οδηγία NIS2 δεν αναφέρεται ρητά στη διαδικασία εσωτερικού ελέγχου, προβλέπει ότι η διοίκηση των βασικών και σημαντικών οντοτήτων οφείλει να επιβλέπει την εφαρμογή των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας. Η απαίτηση αυτή προϋποθέτει την ύπαρξη μηχανισμών που επιτρέπουν την αντικειμενική αξιολόγηση της εφαρμογής και της αποτελεσματικότητας των μέτρων προστασίας. Αντιστοίχως, τα διεθνή πρότυπα διαχείρισης ασφάλειας πληροφοριών προβλέπουν τη διενέργεια εσωτερικών ελέγχων σε τακτικά χρονικά διαστήματα. Οι έλεγχοι αυτοί αποσκοπούν στην αξιολόγηση της συμμόρφωσης του οργανισμού με τις καθορισμένες πολιτικές και διαδικασίες κυβερνοασφάλειας, καθώς και στον εντοπισμό πιθανών αποκλίσεων ή αδυναμιών στην εφαρμογή των μέτρων προστασίας. Οι εσωτερικοί έλεγχοι πραγματοποιούνται σύμφωνα με προκαθορισμένο πρόγραμμα, το οποίο καθορίζει τη συχνότητα των ελέγχων, το αντικείμενο αξιολόγησης, τα κριτήρια ελέγχου και τις αρμοδιότητες των ελεγκτών. Ο μηχανισμός περιλαμβάνει τον καθορισμό του πεδίου και των κριτηρίων του ελέγχου, τη συλλογή και αξιολόγηση αποδεικτικών στοιχείων, καθώς και την καταγραφή των αποτελεσμάτων σε σχετικές

αναφορές. Τα ευρήματα των ελέγχων γνωστοποιούνται στη διοίκηση του οργανισμού, η οποία οφείλει να λάβει τα απαραίτητα μέτρα για την αντιμετώπιση των εντοπισμένων αποκλίσεων και τη βελτίωση των πρακτικών κυβερνοασφάλειας (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2022; ISO/IEC, 2022).

Η διοίκηση των οργανισμών πραγματοποιεί σε τακτά χρονικά διαστήματα ανασκόπηση της κυβερνοασφάλειας. Η Οδηγία NIS2 προβλέπει ότι η ανώτατη διοίκηση των βασικών και σημαντικών οντοτήτων εγκρίνει τα μέτρα διαχείρισης κινδύνων κυβερνοασφάλειας και επιβλέπει την εφαρμογή τους, καθιστώντας αναγκαία την ύπαρξη διαδικασιών συστηματικής ενημέρωσης και αξιολόγησης. Η περιοδική ανασκόπηση από τη διοίκηση αποτελεί τον μηχανισμό μέσω του οποίου τα διοικητικά στελέχη λαμβάνουν συγκεντρωμένη πληροφόρηση σχετικά με την απόδοση και την αποτελεσματικότητα των μέτρων κυβερνοασφάλειας. Κατά τη προσέγγιση αυτή παρουσιάζονται στη διοίκηση τα βασικά στοιχεία που αφορούν τη λειτουργία του πλαισίου κυβερνοασφάλειας, όπως τα αποτελέσματα της παρακολούθησης και μέτρησης των διαδικασιών ασφάλειας, τα ευρήματα των εσωτερικών ελέγχων, η πρόοδος των σχεδίων αντιμετώπισης κινδύνων, καθώς και τυχόν περιστατικά ασφάλειας που έχουν καταγραφεί. Η ανασκόπηση επιτρέπει στη διοίκηση να αξιολογεί κατά πόσο τα εφαρμοζόμενα μέτρα ανταποκρίνονται στις ανάγκες του οργανισμού και να εντοπίζει περιοχές όπου απαιτούνται βελτιώσεις. Με βάση τα αποτελέσματα της ανασκόπησης, η διοίκηση μπορεί να λάβει αποφάσεις σχετικά με την αναθεώρηση πολιτικών και διαδικασιών, την τροποποίηση ρόλων και αρμοδιοτήτων, τον καθορισμό νέων στόχων ασφάλειας ή τη διάθεση πρόσθετων πόρων για την ενίσχυση των μέτρων προστασίας (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2022; ISO/IEC, 2022).

Η συνεχής βελτίωση του πλαισίου κυβερνοασφάλειας επιτυγχάνεται μέσω της εφαρμογής κατάλληλων διορθωτικών ενεργειών. Οι διορθωτικές ενέργειες ενεργοποιούνται όταν εντοπίζονται αποκλίσεις από τις καθορισμένες πολιτικές και διαδικασίες ασφάλειας ή όταν διαπιστώνονται αδυναμίες στη λειτουργία των μέτρων προστασίας. Οι αποκλίσεις αυτές μπορεί να προκύψουν από τα αποτελέσματα εσωτερικών ελέγχων, από διαδικασίες παρακολούθησης της απόδοσης των μέτρων ασφάλειας ή από την ανάλυση περιστατικών κυβερνοασφάλειας. Η υλοποίηση των διορθωτικών ενεργειών περιλαμβάνει τη συστηματική διερεύνηση των αιτίων που οδήγησαν στη μη συμμόρφωση, καθώς και τον καθορισμό και την εφαρμογή κατάλληλων μέτρων για την εξάλειψη των αιτιών αυτών. Μέσω της ανάλυσης των αιτιών διασφαλίζεται ότι οι ενέργειες που λαμβάνονται δεν περιορίζονται στην αντιμετώπιση των άμεσων συνεπειών ενός προβλήματος, αλλά στοχεύουν στην αποτροπή

της επανάληψής του στο μέλλον. Οι διορθωτικές ενέργειες μπορεί να περιλαμβάνουν την αναθεώρηση πολιτικών και διαδικασιών ασφάλειας, την ενίσχυση τεχνικών ελέγχων προστασίας, την τροποποίηση οργανωτικών πρακτικών ή την υλοποίηση πρόσθετων εκπαιδευτικών δράσεων για το προσωπικό. Παράλληλα, οι οργανισμοί καταγράφουν τις μη συμμορφώσεις που εντοπίζονται, τις ενέργειες που εφαρμόζονται για την αντιμετώπισή τους και τα αποτελέσματα των ενεργειών αυτών, ώστε να αξιολογείται η αποτελεσματικότητα των μέτρων που λαμβάνονται (ISO/IEC, 2022).

4. ΠΛΑΙΣΙΟ ΕΛΕΓΧΩΝ

Μετά την παρουσίαση του πλαισίου εφαρμογής της Οδηγίας NIS2 στους οργανισμούς, είναι αναγκαίο να εξεταστούν οι μηχανισμοί μέσω των οποίων μπορεί να ελεγχθεί η ορθή υλοποίηση των απαιτήσεων κυβερνοασφάλειας. Η εφαρμογή μέτρων ασφάλειας πληροφοριών πρέπει να συνοδεύεται από διαδικασίες ελέγχου, ώστε να επαληθεύεται ότι τα μέτρα αυτά εφαρμόζονται αποτελεσματικά και σύμφωνα με τις κανονιστικές απαιτήσεις. Σε πολλούς τομείς κρίσιμων υπηρεσιών, οι οργανισμοί βασίζονται σε σύνθετες πληροφοριακές υποδομές που περιλαμβάνουν δίκτυα, πληροφοριακά συστήματα και υπηρεσίες που παρέχονται από διαφορετικούς παρόχους. Η διασφάλιση ενός επαρκούς επιπέδου ασφάλειας σε τέτοια περιβάλλοντα προϋποθέτει την ύπαρξη μηχανισμών εποπτείας και ελέγχου, μέσω των οποίων οι αρμόδιες αρχές ή άλλοι φορείς μπορούν να επαληθεύουν ότι οι πάροχοι εφαρμόζουν τα απαιτούμενα μέτρα προστασίας.

Στο πλαίσιο αυτό, οι έλεγχοι κυβερνοασφάλειας (audits) αποτελούν βασικό εργαλείο για την αξιολόγηση της εφαρμογής πολιτικών, διαδικασιών και τεχνικών μέτρων ασφάλειας πληροφοριών. Μέσω των ελέγχων συλλέγονται αποδεικτικά στοιχεία σχετικά με τον τρόπο λειτουργίας των μηχανισμών ασφάλειας και αξιολογείται ο βαθμός συμμόρφωσης ενός οργανισμού με τα καθορισμένα κριτήρια, τα οποία μπορεί να προκύπτουν από κανονιστικές απαιτήσεις, πρότυπα ασφάλειας ή εσωτερικές πολιτικές.

Στο παρόν κεφάλαιο εξετάζεται ο ρόλος των ελέγχων στο πλαίσιο της κυβερνοασφάλειας και παρουσιάζονται οι βασικές αρχές και μεθοδολογίες που μπορούν να χρησιμοποιηθούν για τον έλεγχο της εφαρμογής των απαιτήσεων της Οδηγίας NIS2. Ειδικότερα, αναλύεται το θεσμικό πλαίσιο των ελέγχων, η σχέση τους με τα πρότυπα διαχείρισης ασφάλειας πληροφοριών, καθώς και τα βασικά στάδια σχεδιασμού, διεξαγωγής και αναφοράς ενός ελέγχου (European Network and Information Security Agency, 2013; ISO/IEC, 2018).

4.1. Έλεγχοι Ασφάλειας Πληροφοριών

Οι διαδικασίες ελέγχου ασφάλειας πληροφοριών χρησιμοποιούνται για την αξιολόγηση της εφαρμογής πολιτικών και μέτρων προστασίας πληροφοριακών συστημάτων. Για τον σκοπό αυτό, οι οργανισμοί εφαρμόζουν διαδικασίες ελέγχου με στόχο

την επαλήθευση ότι οι καθορισμένες απαιτήσεις ασφάλειας τηρούνται στην πράξη και ότι οι σχετικές διαδικασίες λειτουργούν αποτελεσματικά.

Σύμφωνα με το πρότυπο ISO 19011, ένας έλεγχος ορίζεται ως μια συστηματική, ανεξάρτητη και τεκμηριωμένη διαδικασία για τη συλλογή αντικειμενικών αποδεικτικών στοιχείων και την αντικειμενική αξιολόγησή τους, προκειμένου να διαπιστωθεί ο βαθμός στον οποίο πληρούνται τα καθορισμένα κριτήρια ελέγχου. Στο πλαίσιο της διαδικασίας αυτής, ο έλεγχος περιλαμβάνει τη συλλογή αποδεικτικών στοιχείων σχετικά με τον τρόπο με τον οποίο εφαρμόζονται στην πράξη οι πολιτικές και τα μέτρα ασφάλειας. Με βάση το ίδιο πρότυπο, τα κριτήρια ελέγχου αποτελούν το σύνολο των απαιτήσεων έναντι των οποίων συγκρίνονται τα αποδεικτικά στοιχεία που συλλέγονται κατά τη διάρκεια του ελέγχου. Οι απαιτήσεις αυτές μπορεί να περιλαμβάνουν πολιτικές, διαδικασίες, οδηγίες εργασίας, συμβατικές υποχρεώσεις ή κανονιστικές και νομοθετικές απαιτήσεις.

Η σημασία των ελέγχων καθίσταται ιδιαίτερα εμφανής σε περιβάλλοντα όπου οι οργανισμοί παρέχουν κρίσιμες υπηρεσίες και βασίζονται σε σύνθετες πληροφοριακές υποδομές. Σε τέτοια περιβάλλοντα, οι αρμόδιες αρχές ή άλλοι εποπτικοί φορείς συχνά απαιτούν από τους παρόχους υπηρεσιών να εφαρμόζουν συγκεκριμένα μέτρα ασφάλειας και να αποδεικνύουν την εφαρμογή τους μέσω διαδικασιών ελέγχου (European Network and Information Security Agency, 2013; ISO/IEC, 2018).

4.2. Μέτρα Εποπτείας

Η Οδηγία NIS2, πέρα από τις υποχρεώσεις που θέτει για τη διαχείριση κινδύνων και την κοινοποίηση περιστατικών, περιλαμβάνει συγκεκριμένο πλαίσιο εποπτείας και επιβολής για την παρακολούθηση της εφαρμογής των απαιτήσεών της. Για τον σκοπό αυτό, τα κράτη μέλη οφείλουν να διασφαλίζουν ότι οι αρμόδιες αρχές διαθέτουν τις κατάλληλες εξουσίες, ώστε να ελέγχουν αν οι οντότητες εφαρμόζουν τα απαιτούμενα μέτρα κυβερνοασφάλειας και τηρούν τις σχετικές υποχρεώσεις.

Η μορφή και η ένταση της εποπτείας διαφοροποιούνται ανάλογα με την κατηγορία της οντότητας. Οι βασικές οντότητες υπάγονται σε πληρέστερο εποπτικό καθεστώς, το οποίο περιλαμβάνει τόσο εκ των προτέρων όσο και εκ των υστέρων παρεμβάσεις. Στις σχετικές εξουσίες των αρμόδιων αρχών περιλαμβάνονται οι επιτόπιες επιθεωρήσεις, η εποπτεία εκτός εγκαταστάσεων, οι τακτικοί και στοχευμένοι έλεγχοι ασφάλειας, καθώς και

οι έκτακτοι ειδικοί έλεγχοι, ιδίως σε περιπτώσεις σημαντικών περιστατικών ή πιθανών παραβιάσεων της Οδηγίας. Επιπλέον, προβλέπονται σαρώσεις ασφαλείας βάσει αντικειμενικών και διαφανών κριτηρίων αξιολόγησης κινδύνου, καθώς και αιτήματα παροχής πληροφοριών, πρόσβασης σε δεδομένα και έγγραφα, αλλά και αποδεικτικών στοιχείων σχετικά με την εφαρμογή των πολιτικών κυβερνοασφάλειας.

Για τις σημαντικές οντότητες, η Οδηγία προβλέπει ηπιότερο εποπτικό καθεστώς, το οποίο ενεργοποιείται κυρίως όταν υπάρχουν αποδεικτικά στοιχεία, ενδείξεις ή πληροφορίες περί πιθανής μη συμμόρφωσης. Η προσέγγιση αυτή αντιστοιχεί σε εκ των υστέρων ή κατασταλτική εποπτεία. Οι αρμόδιες αρχές διατηρούν, ωστόσο, την εξουσία να διενεργούν επιτόπιες επιθεωρήσεις, στοχευμένους ελέγχους ασφάλειας και σαρώσεις ασφαλείας, καθώς και να ζητούν πληροφορίες, έγγραφα και αποδεικτικά στοιχεία για την εφαρμογή των πολιτικών κυβερνοασφάλειας. Ωστόσο, η εποπτεία των σημαντικών οντοτήτων δεν οργανώνεται ως πλήρης και συνεχής εκ των προτέρων παρακολούθηση, αλλά συνδέεται με την ύπαρξη συγκεκριμένων ενδείξεων κινδύνου ή παραβίασης.

Η Οδηγία παρέχει επίσης στις αρμόδιες αρχές εξουσίες επιβολής σε περίπτωση διαπιστωμένων παραβάσεων. Στις εξουσίες αυτές περιλαμβάνονται η έκδοση προειδοποιήσεων, δεσμευτικών οδηγιών και εντολών για την αποκατάσταση ελλείψεων, καθώς και η δυνατότητα επιβολής διοικητικών κυρώσεων. Περιλαμβάνεται ακόμη η δυνατότητα να ζητείται από τις οντότητες η εφαρμογή των συστάσεων που προκύπτουν από ελέγχους ασφάλειας εντός εύλογης προθεσμίας (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2022; Εθνική Αρχή Κυβερνοασφάλειας, 2024).

4.3. Σύνδεση NIS2 με ISO/IEC 27001

Η εφαρμογή και ο έλεγχος των απαιτήσεων της Οδηγίας NIS2 μπορούν να υποστηριχθούν από υφιστάμενα πρότυπα διαχείρισης ασφάλειας πληροφοριών, με κυριότερο το ISO/IEC 27001. Η σύνδεση αυτή είναι ιδιαίτερα χρήσιμη, καθώς η Οδηγία θέτει υποχρεώσεις σε επίπεδο διακυβέρνησης, διαχείρισης κινδύνων, χειρισμού περιστατικών, επιχειρησιακής συνέχειας και εκπαίδευσης, ενώ το πρότυπο παρέχει δομημένες απαιτήσεις για την οργάνωση, την τεκμηρίωση, την εφαρμογή και την αξιολόγηση ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών.

Κατ' αρχάς, η σχέση αυτή διακρίνεται ήδη στο επίπεδο της διακυβέρνησης. Το άρθρο 20 της NIS2 προβλέπει ότι η ανώτατη διοίκηση εγκρίνει τα μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας, επιβλέπει την εφαρμογή τους και παρακολουθεί σχετική εκπαίδευση. Αντίστοιχα, το ISO/IEC 27001 αποδίδει κεντρικό ρόλο στην ανώτατη διοίκηση μέσω της πολιτικής ασφάλειας πληροφοριών, της ανασκόπησης του ISMS και της ευαισθητοποίησης των εμπλεκομένων προσώπων.

Η σύνδεση αυτή είναι ιδιαίτερα εμφανής στο πεδίο της διαχείρισης κινδύνων. Το άρθρο 21 της NIS2 απαιτεί κατάλληλα και αναλογικά τεχνικά, επιχειρησιακά και οργανωτικά μέτρα, βασισμένα σε ολιστική προσέγγιση του κινδύνου. Αντίστοιχα, το ISO/IEC 27001 περιλαμβάνει απαιτήσεις για την αξιολόγηση των κινδύνων, τον σχεδιασμό της αντιμετώπισής τους και τη διατήρηση σχετικής τεκμηρίωσης. Για τον λόγο αυτό, το πρότυπο μπορεί να λειτουργήσει ως πρακτικό πλαίσιο αναφοράς για τον έλεγχο της εφαρμογής των μέτρων που απαιτεί η NIS2.

Αντίστοιχη συνάφεια εμφανίζεται και σε επιμέρους υποχρεώσεις της Οδηγίας. Ο χειρισμός περιστατικών, η επιχειρησιακή συνέχεια, η ασφάλεια της εφοδιαστικής αλυσίδας, η βασική κυβερνοϋγιεινή και η εκπαίδευση προσωπικού, όπως προβλέπονται στο άρθρο 21, αντιστοιχούν σε απαιτήσεις και ελέγχους του ISO/IEC 27001 που αφορούν οργανωμένες διαδικασίες αντιμετώπισης συμβάντων, αντίγραφα ασφαλείας, σχέδια συνέχειας, σχέσεις με προμηθευτές, επικοινωνία και ευαισθητοποίηση. Παράλληλα, το πρότυπο περιλαμβάνει διαδικασίες παρακολούθησης, εσωτερικού ελέγχου και διοικητικής ανασκόπησης, οι οποίες προσφέρουν συγκεκριμένη βάση για την αξιολόγηση της εφαρμογής των μέτρων αυτών.

Επιπλέον, το άρθρο 23 της NIS2 προβλέπει συγκεκριμένες υποχρεώσεις αναφοράς περιστατικών, με καθορισμένα χρονικά στάδια και απαιτήσεις ενημέρωσης. Το ISO/IEC 27001 δεν αναπαράγει το ίδιο κανονιστικό σχήμα κοινοποιήσεων, υποστηρίζει όμως την ανάγκη ύπαρξης οργανωμένων διαδικασιών καταγραφής, επικοινωνίας και διαχείρισης σχετικών συμβάντων. Κατά συνέπεια, η σχέση της Οδηγίας με το πρότυπο δεν συνιστά ταύτιση των δύο πλαισίων, αλλά αναδεικνύει ότι το ISO/IEC 27001 μπορεί να διευκολύνει την οργάνωση των διαδικασιών που απαιτούνται για την εφαρμογή και τον έλεγχο των υποχρεώσεων της NIS2.

Η αντιστοίχιση μεταξύ NIS2 και ISO/IEC 27001 είναι ιδιαίτερα χρήσιμη στο πεδίο του auditing. Μέσω αυτής, οι κανονιστικές απαιτήσεις της Οδηγίας μπορούν να συνδεθούν με τεκμηριωμένες διαδικασίες, αρχεία, εσωτερικούς ελέγχους και διοικητικές ανασκοπήσεις, τα οποία λειτουργούν ως αποδεικτικά στοιχεία για την αξιολόγηση της εφαρμογής τους. Για τον

λόγο αυτό, το ISO/IEC 27001 δεν υποκαθιστά τη NIS2, αλλά μπορεί να αξιοποιηθεί ως οργανωμένο πλαίσιο αναφοράς για τον έλεγχο απαιτήσεων της Οδηγίας (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2022; ISO/IEC, 2022; Αλεξάνδρα Εξάρχου, 2024; Άννα Πέλλα, 2025).

Για την αποτύπωση της σχέσης αυτής, ακολουθεί ο Πίνακας 3, στον οποίο συσχετίζονται επιμέρους απαιτήσεις της NIS2 με σχετικές διατάξεις του ISO/IEC 27001:

Πίνακας 3 - Αντιστοίχιση απαιτήσεων της NIS2 με διατάξεις και ελέγχους του ISO/IEC 27001 (BSI group, χ.χ.)

Μέτρα NIS2	**ISO/IEC 27001**	
Άρθρο 20: Διακυβέρνηση		
	Παράρτημα Α	
	A.5.1	Πολιτικές για την ασφάλεια των πληροφοριών
	A.5.31	Νομικές, καταστατικές, κανονιστικές και συμβατικές απαιτήσεις
	A.5.34	Ιδιωτικότητα και προστασία των αναγνωριστικών στοιχείων ταυτότητας
	A.5.35	Ανεξάρτητη επανεξέταση της ασφάλειας πληροφοριών
	A.5.36	Συμμόρφωση με πολιτικές, κανόνες και πρότυπα για την ασφάλεια πληροφοριών
	A.6.3	Ενημέρωση, εκπαίδευση και κατάρτιση για την ασφάλεια πληροφοριών
Άρθρο 21: Μέτρα Διαχείρισης Κινδύνων Κυβερνοασφάλειας		
(Α) Πολιτικές ανάλυσης κινδύνων και ασφάλειας συστημάτων πληροφοριών	5.2	Πολιτική ασφάλειας πληροφοριών
	6.1.2	Διαδικασία αξιολόγησης κινδύνων ασφάλειας πληροφοριών
	6.1.3	Διαδικασία αντιμετώπισης κινδύνων ασφάλειας πληροφοριών
	8.2	Αποτίμηση κινδύνων ασφάλειας πληροφοριών
	8.3	Αντιμετώπιση κινδύνων ασφάλειας πληροφοριών
	Παράρτημα Α	
	A.5.1	Πολιτικές για την ασφάλεια των πληροφοριών

Μέτρα NIS2	**ISO/IEC 27001**	
Άρθρο 21: Μέτρα Διαχείρισης Κινδύνων Κυβερνοασφάλειας (συνέχεια)		
(Β) Διαχείριση περιστατικών	**Παράρτημα Α**	
	Α.5.24	Σχεδιασμός και προετοιμασία διαχείρισης περιστατικών ασφάλειας πληροφοριών
	Α.5.25	Αποτίμηση και απόφαση σχετικά με συμβάντα ασφάλειας πληροφοριών
	Α.5.26	Απόκριση σε περιστατικά ασφάλειας πληροφοριών
	Α.5.27	Μάθηση από περιστατικά ασφάλειας πληροφοριών
	Α.5.28	Συλλογή αποδεικτικών στοιχείων
	Α.6.8	Αναφορά συμβάντων ασφάλειας πληροφοριών
	Α.8.16	Δραστηριότητες παρακολούθησης
(Γ) Επιχειρησιακή συνέχεια, όπως διαχείριση αντιγράφων ασφάλειας και ανάκαμψη από καταστροφή, και διαχείριση κρίσεων	**Παράρτημα Α**	
	Α.5.29	Ασφάλεια πληροφοριών κατά τη διάρκεια διαταραχής
	Α.5.30	Ετοιμότητα ΤΠΕ για επιχειρησιακή συνέχεια
	Α.8.13	Δημιουργία αντιγράφων ασφαλείας πληροφοριών
	Α.8.14	Εφεδρεία εγκαταστάσεων επεξεργασίας πληροφοριών
	Α.8.15	Δημιουργία και αποθήκευση καταγραφών
	Α.8.16	Δραστηριότητες παρακολούθησης
(Δ) Ασφάλεια εφοδιαστικής αλυσίδας, συμπεριλαμβανομένης της ασφάλειας που σχετίζεται με τη σχέση κάθε οντότητας με τους άμεσους προμηθευτές της ή τους παρόχους υπηρεσιών της	**Παράρτημα Α**	
	Α.5.19	Ασφάλεια πληροφοριών στις σχέσεις με προμηθευτές
	Α.5.20	Αντιμετώπιση ασφάλειας πληροφοριών στο πλαίσιο συμφωνιών με προμηθευτές
	Α.5.21	Διαχείριση της ασφάλειας των πληροφοριών στην αλυσίδα εφοδιασμού ΤΠΕ
	Α.5.22	Παρακολούθηση, αναθεώρηση και διαχείριση αλλαγών σε υπηρεσίες προμηθευτών
	Α.5.23	Ασφάλεια πληροφοριών για τη χρήση υπηρεσιών νέφους
(Ε) Ασφάλεια στην απόκτηση, ανάπτυξη και συντήρηση συστημάτων δικτύου και πληροφοριών, συμπεριλαμβανομένου του χειρισμού και της γνωστοποίησης ευπαθειών	**Παράρτημα Α**	
	Α.5.20	Αντιμετώπιση ασφάλειας πληροφοριών στο πλαίσιο συμφωνιών με προμηθευτές
	Α.5.24	Σχεδιασμός και προετοιμασία διαχείρισης περιστατικών ασφάλειας πληροφοριών
	Α.5.37	Τεκμηριωμένες διαδικασίες λειτουργίας
	Α.6.8	Αναφορά συμβάντων ασφάλειας πληροφοριών
	Α.8.8	Διαχείριση τεχνικών ευπαθειών
	Α.8.9	Διαχείριση παραμετροποιήσεων
	Α.8.20	Ασφάλεια δικτύων
	Α.8.21	Ασφάλεια υπηρεσιών δικτύου

Μέτρα NIS2	**ISO/IEC 27001**	
Άρθρο 21: Μέτρα Διαχείρισης Κινδύνων Κυβερνοασφάλειας (συνέχεια)		
(ΣΤ) Πολιτικές και διαδικασίες για την αξιολόγηση της αποτελεσματικότητας των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας	9.1	Παρακολούθηση, μέτρηση, ανάλυση και αξιολόγηση
	9.2	Εσωτερική επιθεώρηση
	9.3	Ανασκόπηση από τη Διοίκηση
	Παράρτημα Α	
	Α.5.35	Ανεξάρτητη επανεξέταση της ασφάλειας πληροφοριών
	Α.5.36	Συμμόρφωση με πολιτικές, κανόνες και πρότυπα για την ασφάλεια πληροφοριών
(Ζ) Βασικές πρακτικές κυβερνοϋγιεινής και κατάρτιση στην κυβερνοασφάλεια	7.3	Ευαισθητοποίηση
	7.4	Επικοινωνία
	Παράρτημα Α	
	Α.5.15	Έλεγχος πρόσβασης
	Α.5.16	Διαχείριση ταυτότητας
	Α.5.18	Δικαιώματα πρόσβασης
	Α.5.24	Σχεδιασμός και προετοιμασία διαχείρισης περιστατικών ασφάλειας πληροφοριών
	Α.6.3	Ενημέρωση, εκπαίδευση και κατάρτιση για την ασφάλεια πληροφοριών
	Α.6.5	Ευθύνες μετά τη λήξη ή την αλλαγή απασχόλησης
	Α.6.8	Αναφορά συμβάντων ασφάλειας πληροφοριών
	Α.8.2	Επαυξημένα δικαιώματα πρόσβασης
	Α.8.3	Περιορισμός πρόσβασης σε πληροφορίες
	Α.8.5	Ασφαλής αυθεντικοποίηση
	Α.8.7	Προστασία από κακόβουλο λογισμικό
	Α.8.9	Διαχείριση παραμετροποιήσεων
	Α.8.13	Δημιουργία αντιγράφων ασφαλείας πληροφοριών
	Α.8.15	Δημιουργία και αποθήκευση καταγραφών
	Α.8.19	Εγκατάσταση λογισμικού σε λειτουργικά συστήματα
	Α.8.22	Διαχωρισμός δικτύων
(Η) Πολιτικές και διαδικασίες σχετικά με τη χρήση κρυπτογραφίας και, κατά περίπτωση, κρυπτογράφησης	**Παράρτημα Α**	
	Α.8.24	Χρήση κρυπτογραφίας

Μέτρα NIS2	**ISO/IEC 27001**	
Άρθρο 21: Μέτρα Διαχείρισης Κινδύνων Κυβερνοασφάλειας (συνέχεια)		
(Θ) Ασφάλεια ανθρώπινων πόρων, πολιτικές ελέγχου πρόσβασης και διαχείριση πάγιων στοιχείων	**Παράρτημα Α**	
	Α.5.9	Απογραφή πληροφοριών και άλλων συναφών περιουσιακών στοιχείων
	Α.5.10	Αποδεκτή χρήση πληροφοριών και άλλων σχετιζόμενων περιουσιακών στοιχείων
	Α.5.11	Επιστροφή περιουσιακών στοιχείων
	Α.5.15	Έλεγχος πρόσβασης
	Α.5.16	Διαχείριση ταυτότητας
	Α.5.17	Πληροφορίες αυθεντικοποίησης
	Α.5.18	Δικαιώματα πρόσβασης
	Α.6.1	Διαλογή
	Α.6.2	Όροι και προϋποθέσεις απασχόλησης
	Α.6.4	Πειθαρχική διαδικασία
	Α.6.5	Ευθύνες μετά τη λήξη ή την αλλαγή απασχόλησης
	Α.6.6	Συμφωνίες εμπιστευτικότητας ή μη δημοσιοποίησης
(Ι) Χρήση λύσεων πολυπαραγοντικής επαλήθευσης ταυτότητας ή συνεχούς επαλήθευσης ταυτότητας, ασφαλών φωνητικών επικοινωνιών, επικοινωνιών βίντεο και κειμένου και ασφαλών συστημάτων επικοινωνιών έκτακτης ανάγκης εντός της οντότητας, κατά περίπτωση	**Παράρτημα Α**	
	Α.5.14	Μεταφορά πληροφοριών
	Α.5.16	Διαχείριση ταυτότητας
	Α.5.17	Πληροφορίες αυθεντικοποίησης
Άρθρο 23: Υποχρεώσεις αναφοράς περιστατικών		
	Παράρτημα Α	
	Α.5.14	Μεταφορά πληροφοριών
	Α.6.8	Αναφορά συμβάντων ασφάλειας πληροφοριών
Άρθρο 24: Χρήση των ευρωπαϊκών συστημάτων πιστοποίησης της κυβερνοασφάλειας		
	Παράρτημα Α	
	Α.5.1	Πολιτικές για την ασφάλεια των πληροφοριών

4.4. Μεθοδολογία Ελέγχου

Η διενέργεια ενός ελέγχου προϋποθέτει σαφή μεθοδολογική οργάνωση, ώστε η αξιολόγηση να βασίζεται σε προκαθορισμένα κριτήρια και σε επαληθεύσιμα αποδεικτικά στοιχεία. Σύμφωνα με το ISO 19011, κάθε επιμέρους έλεγχος πρέπει να στηρίζεται σε καθορισμένους στόχους, πεδίο εφαρμογής και κριτήρια ελέγχου, τα οποία πρέπει να είναι συνεπή με το γενικό πρόγραμμα ελέγχου. Σκοπός αυτής της προσέγγισης είναι να καθορίζεται με σαφήνεια τι επιδιώκει να εξετάσει ο έλεγχος, σε ποια οργανωτικά ή λειτουργικά όρια θα κινηθεί και με βάση ποιες απαιτήσεις θα γίνει η αξιολόγηση.

Οι στόχοι του ελέγχου προσδιορίζουν το επιδιωκόμενο αποτέλεσμα της ελεγκτικής διαδικασίας. Πιο συγκεκριμένα, μπορούν να αφορούν τον βαθμό συμμόρφωσης ενός συστήματος ή μιας διαδικασίας με τα καθορισμένα κριτήρια, την ικανότητα του οργανισμού να ανταποκρίνεται σε κανονιστικές ή άλλες απαιτήσεις, την αποτελεσματικότητα των εφαρμοζόμενων μέτρων, καθώς και τον εντοπισμό δυνατοτήτων βελτίωσης. Το πεδίο εφαρμογής του ελέγχου καθορίζει την έκταση και τα όριά του και συνήθως περιλαμβάνει τις εγκαταστάσεις, τις λειτουργίες, τις οργανωτικές μονάδες, τις δραστηριότητες, τις διαδικασίες και το χρονικό διάστημα που θα εξεταστούν. Τα κριτήρια ελέγχου αποτελούν το σύνολο των απαιτήσεων έναντι των οποίων συγκρίνονται τα αποδεικτικά στοιχεία και μπορεί να περιλαμβάνουν πολιτικές, διαδικασίες, οδηγίες εργασίας, κανονιστικές και νομοθετικές απαιτήσεις ή άλλες δεσμεύσεις του οργανισμού. Στην περίπτωση ελέγχου εφαρμογής της NIS2, τα κριτήρια αυτά μπορούν να αντλούνται από την ίδια την Οδηγία, από το ISO/IEC 27001, καθώς και από τις εσωτερικές πολιτικές και διαδικασίες του οργανισμού.

Ο σχεδιασμός του ελέγχου ακολουθεί προσέγγιση βασισμένη στον κίνδυνο, ώστε οι ελεγκτικές δραστηριότητες να οργανώνονται με τρόπο κατάλληλο για την επίτευξη των στόχων του ελέγχου. Για τον σκοπό αυτό, ο σχεδιασμός λαμβάνει υπόψη το αντικείμενο και την πολυπλοκότητα του ελέγχου, τις μεθόδους που θα χρησιμοποιηθούν, τις απαιτήσεις δειγματοληψίας, τους διαθέσιμους πόρους, τους ρόλους της ελεγκτικής ομάδας, καθώς και τα χαρακτηριστικά των χώρων ή διαδικασιών που θα εξεταστούν. Επιπλέον, ο έλεγχος μπορεί να περιλαμβάνει δραστηριότητες επιτόπιας ή εξ αποστάσεως αξιολόγησης, ανάλογα με το αντικείμενο, το περιβάλλον του οργανισμού και τα διαθέσιμα μέσα.

Κεντρικό στάδιο της μεθοδολογίας αποτελεί η συλλογή και επαλήθευση των πληροφοριών που σχετίζονται με τους στόχους, το πεδίο εφαρμογής και τα κριτήρια του ελέγχου. Το ISO 19011 προβλέπει ότι οι πληροφορίες αυτές πρέπει να συλλέγονται με

κατάλληλες μεθόδους, όπως συνεντεύξεις, παρατήρηση και ανασκόπηση τεκμηριωμένων πληροφοριών. Η συλλογή τους μπορεί να βασίζεται και σε δειγματοληψία, υπό την προϋπόθεση ότι τα στοιχεία που αξιοποιούνται είναι επαληθεύσιμα. Ως αποδεικτικά στοιχεία γίνονται δεκτά αρχεία, διαπιστωμένα γεγονότα και άλλες πληροφορίες που είναι σχετικές με τα κριτήρια ελέγχου και μπορούν να ελεγχθούν ως προς την αξιοπιστία τους. Η απαίτηση αυτή είναι ιδιαίτερα σημαντική σε ελέγχους κυβερνοασφάλειας, όπου η αξιολόγηση δεν στηρίζεται μόνο στην ύπαρξη πολιτικών και διαδικασιών, αλλά και σε στοιχεία που αποδεικνύουν την πραγματική εφαρμογή τους.

Μετά τη συλλογή των αποδεικτικών στοιχείων ακολουθεί η αξιολόγησή τους σε σχέση με τα κριτήρια ελέγχου, προκειμένου να διαμορφωθούν τα ευρήματα. Τα ευρήματα εκφράζουν το αποτέλεσμα της σύγκρισης αυτής και μπορούν να υποδηλώνουν συμμόρφωση ή μη συμμόρφωση. Όταν τα κριτήρια ελέγχου προέρχονται από κανονιστικές ή νομοθετικές απαιτήσεις, τα ευρήματα μπορούν να διατυπώνονται και ως συμμόρφωση ή μη συμμόρφωση προς τις συγκεκριμένες υποχρεώσεις. Παράλληλα, τα ευρήματα μπορούν να αναδείξουν κινδύνους, δυνατότητες βελτίωσης καθώς και ορθές πρακτικές. Με βάση τους στόχους του ελέγχου και το σύνολο των ευρημάτων διαμορφώνεται στη συνέχεια το τελικό συμπέρασμα του ελέγχου.

Στην επόμενη ενότητα εξετάζονται πιο συγκεκριμένα οι τρόποι με τους οποίους η μεθοδολογία αυτή εφαρμόζεται κατά τη διεξαγωγή ενός ελέγχου (ISO/IEC, 2018, 2022; Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2022).

4.5. Διεξαγωγή Ελέγχου

Η διεξαγωγή ενός ελέγχου περιλαμβάνει μια διαδοχή οργανωμένων ενεργειών, οι οποίες εξασφαλίζουν ότι η ελεγκτική διαδικασία εφαρμόζεται με συνέπεια, διαφάνεια και επαρκή τεκμηρίωση. Σύμφωνα με το ISO 19011, η ευθύνη για τη διεξαγωγή του ελέγχου παραμένει στον επικεφαλής της ελεγκτικής ομάδας έως την ολοκλήρωσή του. Πριν από την έναρξη των ελεγκτικών δραστηριοτήτων, απαιτείται επικοινωνία με την ελεγχόμενη οντότητα, προκειμένου να επιβεβαιωθούν οι δίαυλοι επικοινωνίας, η αρμοδιότητα διενέργειας του ελέγχου, οι στόχοι, το πεδίο εφαρμογής, τα κριτήρια και οι μέθοδοι που θα χρησιμοποιηθούν, καθώς και πρακτικά ζητήματα που αφορούν το χρονοδιάγραμμα, την πρόσβαση στις πληροφορίες και τις απαιτήσεις εμπιστευτικότητας.

Στο αρχικό αυτό στάδιο εξετάζεται επίσης η σκοπιμότητα και η εφικτότητα του ελέγχου. Για να θεωρηθεί εφικτός, θα πρέπει να υπάρχει επαρκής και κατάλληλη πληροφορία για τον σχεδιασμό και τη διεξαγωγή του, κατάλληλη συνεργασία από την πλευρά της ελεγχόμενης οντότητας, καθώς και επαρκής χρόνος και πόροι. Η εκτίμηση αυτή είναι σημαντική, διότι επιτρέπει να διαπιστωθεί αν μπορούν πράγματι να επιτευχθούν οι στόχοι του ελέγχου και αν απαιτούνται προσαρμογές πριν από την έναρξή του.

Μετά την προετοιμασία ακολουθεί η εναρκτήρια συνάντηση, η οποία πραγματοποιείται με τη διοίκηση της ελεγχόμενης οντότητας και, κατά περίπτωση, με τα πρόσωπα που είναι υπεύθυνα για τις λειτουργίες ή τις διαδικασίες που θα εξεταστούν. Σκοπός της είναι η επιβεβαίωση του σχεδίου ελέγχου, η παρουσίαση της ελεγκτικής ομάδας και των ρόλων της, καθώς και η διασφάλιση ότι όλες οι προβλεπόμενες δραστηριότητες μπορούν να πραγματοποιηθούν. Κατά τη συνάντηση αυτή επιβεβαιώνονται, μεταξύ άλλων, οι στόχοι, το πεδίο εφαρμογής και τα κριτήρια του ελέγχου, οι τρόποι επικοινωνίας, η διαθεσιμότητα των απαιτούμενων πόρων, ζητήματα εμπιστευτικότητας και ασφάλειας πληροφοριών, καθώς και ειδικές ρυθμίσεις που αφορούν την πρόσβαση στους χώρους ή στα πληροφοριακά συστήματα του οργανισμού.

Κατά τη διάρκεια του ελέγχου, η ελεγκτική ομάδα συλλέγει και επαληθεύει πληροφορίες σχετικές με τους στόχους, το πεδίο εφαρμογής και τα κριτήρια του ελέγχου. Η συλλογή αυτή μπορεί να πραγματοποιείται μέσω συνεντεύξεων, παρατήρησης, ανασκόπησης τεκμηριωμένων πληροφοριών και κατάλληλης δειγματοληψίας. Οι ελεγκτικές δραστηριότητες μπορούν να λάβουν χώρα επιτόπου ή εξ αποστάσεως, ανάλογα με τη φύση του ελέγχου, το περιβάλλον της οντότητας και τα διαθέσιμα μέσα. Το ISO 19011 επισημαίνει ότι μόνο πληροφορίες που μπορούν να επαληθευθούν σε ικανοποιητικό βαθμό θα πρέπει να γίνονται αποδεκτές ως αποδεικτικά στοιχεία. Για τον λόγο αυτό, η διεξαγωγή του ελέγχου περιλαμβάνει και επιβεβαίωση του τρόπου με τον οποίο οι σχετικές διαδικασίες εφαρμόζονται στην πράξη.

Η επικοινωνία κατά τη διάρκεια του ελέγχου αποτελεί επίσης κρίσιμο στοιχείο της διαδικασίας. Η ελεγκτική ομάδα οφείλει να ανταλλάσσει περιοδικά πληροφορίες εσωτερικά, να αξιολογεί την πρόοδο του ελέγχου και, όπου απαιτείται, να ανακατανέμει τις εργασίες μεταξύ των μελών της. Παράλληλα, ο επικεφαλής της ομάδας επικοινωνεί με την ελεγχόμενη οντότητα σχετικά με την πρόοδο, τυχόν σημαντικά ευρήματα και ζητήματα που ενδέχεται να απαιτούν άμεση προσοχή. Εάν, κατά τη διάρκεια του ελέγχου, προκύψουν νέα δεδομένα ή

μεταβληθούν οι συνθήκες υπό τις οποίες αυτός σχεδιάστηκε, ενδέχεται να απαιτηθεί αναθεώρηση του σχεδίου ελέγχου.

Η ολοκλήρωση της ελεγκτικής διαδικασίας πραγματοποιείται με την καταληκτική συνάντηση, κατά την οποία παρουσιάζονται τα ευρήματα και τα συμπεράσματα του ελέγχου. Η συνάντηση αυτή πραγματοποιείται με τη συμμετοχή της διοίκησης της ελεγχόμενης οντότητας και, κατά περίπτωση, των υπευθύνων για τις λειτουργίες που ελέγχθηκαν. Κατά τη διάρκειά της επεξηγείται ο τρόπος με τον οποίο προέκυψαν τα ευρήματα, επισημαίνεται ότι τα αποδεικτικά στοιχεία βασίζονται σε δείγμα των διαθέσιμων πληροφοριών και παρέχεται η δυνατότητα συζήτησης τυχόν αποκλίσεων ή διαφορετικών ερμηνειών. Στο στάδιο αυτό μπορούν επίσης να τεθούν τα χρονικά περιθώρια για ενδεχόμενο σχέδιο ενεργειών, καθώς και ζητήματα που σχετίζονται με διορθωτικές παρεμβάσεις ή παρακολούθηση μετά τον έλεγχο (ISO/IEC, 2018; Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2022).

4.6. Ευρήματα και Αναφορά Ελέγχου

Μετά τη συλλογή και επαλήθευση των αποδεικτικών στοιχείων ακολουθεί η αξιολόγησή τους σε σχέση με τα κριτήρια ελέγχου, ώστε να προκύψουν τα ευρήματα του ελέγχου. Ανάλογα με το αποτέλεσμα της αξιολόγησης, τα ευρήματα μπορούν να υποδηλώνουν συμμόρφωση ή μη συμμόρφωση, ενώ είναι δυνατό να αναδεικνύουν και κινδύνους, δυνατότητες βελτίωσης ή ορθές πρακτικές.

Ιδιαίτερη σημασία έχει η καταγραφή των μη συμμορφώσεων και των αντίστοιχων αποδεικτικών στοιχείων που τις υποστηρίζουν. Το ISO 19011 προβλέπει ότι οι μη συμμορφώσεις μπορούν, ανάλογα με το πλαίσιο του οργανισμού και το επίπεδο κινδύνου, να διαβαθμίζονται ποιοτικά ή ποσοτικά. Παράλληλα, τα ευρήματα θα πρέπει να εξετάζονται μαζί με την ελεγχόμενη οντότητα, ώστε να επιβεβαιώνεται ότι τα αποδεικτικά στοιχεία έχουν γίνει ορθά κατανοητά και ότι οι αποκλίσεις αποτυπώνονται με σαφήνεια. Σε περίπτωση διαφορετικών απόψεων ως προς τα ευρήματα ή την ερμηνεία τους, επιδιώκεται η επίλυσή τους κατά τη διάρκεια της διαδικασίας. Εάν αυτό δεν καταστεί δυνατό, οι σχετικές αποκλίσεις καταγράφονται στην αναφορά ελέγχου.

Με βάση τα ευρήματα και τους στόχους του ελέγχου διαμορφώνεται το τελικό συμπέρασμα του ελέγχου. Το συμπέρασμα αυτό συνοψίζει την έκβαση της ελεγκτικής

διαδικασίας και αποτυπώνει σε ποιο βαθμό πληρούνται τα καθορισμένα κριτήρια. Στην περίπτωση ελέγχων που στηρίζονται σε κανονιστικές ή νομοθετικές απαιτήσεις, όπως συμβαίνει με την Οδηγία NIS2, τα ευρήματα και τα συμπεράσματα μπορούν να διατυπώνονται και με όρους συμμόρφωσης ή μη συμμόρφωσης προς τις σχετικές υποχρεώσεις.

Τα αποτελέσματα του ελέγχου αποτυπώνονται στην αναφορά ελέγχου, η οποία πρέπει να αποτελεί σαφή, ακριβή και συνοπτική καταγραφή της ελεγκτικής διαδικασίας. Σύμφωνα με το ISO 19011, η αναφορά αυτή περιλαμβάνει συνήθως τους στόχους και το πεδίο εφαρμογής του ελέγχου, τα κριτήρια βάσει των οποίων πραγματοποιήθηκε, τα ευρήματα και τα σχετικά αποδεικτικά στοιχεία, καθώς και τα τελικά συμπεράσματα. Μπορεί επίσης να περιλαμβάνει τον βαθμό εκπλήρωσης των κριτηρίων ελέγχου, τυχόν άλυτες αποκλίσεις απόψεων μεταξύ ελεγκτικής ομάδας και ελεγχόμενης οντότητας, καθώς και επισήμανση ότι ο έλεγχος βασίζεται σε δειγματοληψία και, επομένως, υπάρχει πάντοτε ο κίνδυνος τα εξεταζόμενα στοιχεία να μην αποτυπώνουν πλήρως το σύνολο της λειτουργίας του οργανισμού.

Η αναφορά ελέγχου εκδίδεται εντός συμφωνημένου χρονικού διαστήματος και διαβιβάζεται στα αρμόδια ενδιαφερόμενα μέρη, με τήρηση των αναγκαίων μέτρων εμπιστευτικότητας. Η ολοκλήρωση του ελέγχου δεν σημαίνει κατ’ ανάγκην και το τέλος της διαδικασίας αξιολόγησης, καθώς τα αποτελέσματά του μπορεί να υποδεικνύουν την ανάγκη λήψης διορθώσεων, διορθωτικών ενεργειών ή περαιτέρω βελτιώσεων. Η υλοποίηση και η αποτελεσματικότητα των ενεργειών αυτών μπορούν να παρακολουθούνται και να επαληθεύονται σε μεταγενέστερο στάδιο, ακόμη και μέσω επόμενου ελέγχου (ISO/IEC, 2018; Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2022).

4.7. Έλεγχοι και Συνεχής Βελτίωση

Οι έλεγχοι λειτουργούν τόσο ως μέσο αποτύπωσης της υφιστάμενης κατάστασης ενός οργανισμού όσο και ως μηχανισμός βελτίωσης του επιπέδου ασφάλειας πληροφοριών. Τα αποτελέσματα ενός ελέγχου μπορούν να αναδείξουν μη συμμορφώσεις, αδυναμίες, κινδύνους ή πεδία στα οποία απαιτούνται παρεμβάσεις. Για τον λόγο αυτό, η αξία του ελέγχου δεν περιορίζεται στην καταγραφή ευρημάτων, αλλά συνδέεται και με τις ενέργειες που ακολουθούν μετά την ολοκλήρωσή του.

Σύμφωνα με το ISO 19011, το αποτέλεσμα του ελέγχου μπορεί να υποδεικνύει την ανάγκη για διορθώσεις, διορθωτικές ενέργειες ή ευκαιρίες βελτίωσης. Οι ενέργειες αυτές συνήθως αποφασίζονται και υλοποιούνται από την ελεγχόμενη οντότητα εντός συμφωνημένου χρονικού διαστήματος. Παράλληλα, η οντότητα οφείλει, κατά περίπτωση, να ενημερώνει για την πορεία των ενεργειών αυτών τα πρόσωπα που διαχειρίζονται το πρόγραμμα ελέγχου ή την ελεγκτική ομάδα. Η ολοκλήρωση και η αποτελεσματικότητά τους πρέπει να επαληθεύονται, ενώ η επαλήθευση αυτή μπορεί να αποτελέσει μέρος μεταγενέστερου ελέγχου.

Η προσέγγιση αυτή συνδέεται άμεσα με τη λογική του ISO/IEC 27001, σύμφωνα με το οποίο, όταν προκύπτει μη συμμόρφωση, ο οργανισμός οφείλει να αντιδρά, να λαμβάνει μέτρα για τον έλεγχο και τη διόρθωσή της, να εξετάζει τα αίτιά της και να εφαρμόζει τις αναγκαίες διορθωτικές ενέργειες ώστε να αποτρέπεται η επανεμφάνισή της. Επιπλέον, απαιτείται η ανασκόπηση της αποτελεσματικότητας των ενεργειών αυτών και, όπου χρειάζεται, η πραγματοποίηση αλλαγών στο σύστημα διαχείρισης ασφάλειας πληροφοριών.

Σημαντικός είναι και ο ρόλος της διοικητικής ανασκόπησης στη διαδικασία αυτή. Το ISO/IEC 27001 προβλέπει ότι η ανώτατη διοίκηση ανασκοπεί σε προγραμματισμένα διαστήματα το σύστημα διαχείρισης ασφάλειας πληροφοριών, λαμβάνοντας υπόψη, μεταξύ άλλων, τις μη συμμορφώσεις, τις διορθωτικές ενέργειες, τα αποτελέσματα των ελέγχων, τα αποτελέσματα της παρακολούθησης και μέτρησης, καθώς και τις ευκαιρίες για συνεχή βελτίωση. Τα αποτελέσματα της ανασκόπησης αυτής μπορούν να οδηγήσουν σε αποφάσεις για αλλαγές στο σύστημα, για πρόσθετα μέτρα ή για νέες παρεμβάσεις με στόχο την ενίσχυση της αποτελεσματικότητάς του.

Πέρα από το επίπεδο του επιμέρους ελέγχου, το ISO 19011 συνδέει τη βελτίωση και με το ίδιο το πρόγραμμα ελέγχων. Η ανασκόπηση του προγράμματος μπορεί να αναδείξει διδάγματα, τάσεις, αδυναμίες ή νέα πεδία ενδιαφέροντος, τα οποία αξιοποιούνται για τη βελτίωση της συνολικής ελεγκτικής διαδικασίας. Έτσι, οι έλεγχοι υπηρετούν διπλό σκοπό: βελτιώνουν τόσο την ελεγχόμενη οντότητα όσο και το ίδιο το σύστημα εποπτείας που εφαρμόζεται (ISO/IEC, 2018, 2022; Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2022).

5. ΠΛΑΙΣΙΟ ΣΥΜΜΟΡΦΩΣΗΣ

Η συμμόρφωση με την Οδηγία NIS2 αφορά την οργανωμένη ανταπόκριση των βασικών και σημαντικών οντοτήτων στις υποχρεώσεις που απορρέουν από το κανονιστικό πλαίσιο κυβερνοασφάλειας. Οι υποχρεώσεις αυτές συνδέονται με τη διακυβέρνηση της κυβερνοασφάλειας, τη λήψη μέτρων διαχείρισης κινδύνων, την τεκμηρίωση της εφαρμογής τους και τη δυνατότητα επίδειξης σχετικών αποδεικτικών στοιχείων στις αρμόδιες αρχές. Στο άρθρο 20 της Οδηγίας προβλέπεται ότι η ανώτατη διοίκηση εγκρίνει τα μέτρα διαχείρισης κινδύνων, επιβλέπει την εφαρμογή τους και λογοδοτεί για παραβιάσεις των υποχρεώσεων του άρθρου 21.

Η συμμόρφωση προϋποθέτει επίσης σαφή κατανομή ρόλων, αρμοδιοτήτων και γραμμών αναφοράς. Η τεχνική καθοδήγηση του ENISA προβλέπει ότι οι οντότητες καθορίζουν ευθύνες για την ασφάλεια συστημάτων δικτύου και πληροφοριών, τις αποδίδουν σε συγκεκριμένους ρόλους και τις γνωστοποιούν στα διοικητικά όργανα. Στα σχετικά τεκμήρια περιλαμβάνονται, μεταξύ άλλων, περιγραφές θέσεων, κατάλογοι ρόλων ασφάλειας, οργανογράμματα, πρακτικά συναντήσεων με τη διοίκηση και τεκμήρια αποφάσεων σχετικών με την κυβερνοασφάλεια.

Στην ίδια κατεύθυνση, το ISO/IEC 27002 προβλέπει ότι η διοίκηση απαιτεί από το προσωπικό να εφαρμόζει την ασφάλεια πληροφοριών σύμφωνα με τις καθιερωμένες πολιτικές και διαδικασίες του οργανισμού. Παράλληλα, το ISO/IEC 27001 περιλαμβάνει απαιτήσεις για τη διατήρηση τεκμηριωμένης πληροφορίας, την παρακολούθηση και την αξιολόγηση των σχετικών αποτελεσμάτων, καθώς και για τη λήψη διορθωτικών ενεργειών όταν εντοπίζονται μη συμμορφώσεις.

Το παρόν κεφάλαιο εξετάζει τη συμμόρφωση με τη NIS2, με ιδιαίτερη έμφαση στο Gap Analysis Tool της Εθνικής Αρχής Κυβερνοασφάλειας ως εργαλείο αποτύπωσης του επιπέδου συμμόρφωσης, εντοπισμού κενών και υποστήριξης διορθωτικών ενεργειών (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2022; ISO/IEC, 2022; European Union Agency for Cybersecurity, 2025).

5.1. Απαιτήσεις Συμμόρφωσης

Το άρθρο 21 της Οδηγίας NIS2 καθορίζει τις βασικές απαιτήσεις συμμόρφωσης. Σύμφωνα με αυτό, οι βασικές και σημαντικές οντότητες οφείλουν να λαμβάνουν κατάλληλα και αναλογικά τεχνικά, επιχειρησιακά και οργανωτικά μέτρα. Τα μέτρα αυτά αφορούν τη διαχείριση των κινδύνων που σχετίζονται με την ασφάλεια των συστημάτων δικτύου και πληροφοριών που χρησιμοποιούν για τη λειτουργία τους και για την παροχή των υπηρεσιών τους. Η ίδια διάταξη συνδέει τα μέτρα αυτά με την πρόληψη ή την ελαχιστοποίηση των επιπτώσεων των περιστατικών στους αποδέκτες των υπηρεσιών και σε άλλες υπηρεσίες. Για την αξιολόγηση της αναλογικότητας των μέτρων λαμβάνονται υπόψη ο βαθμός έκθεσης της οντότητας σε κινδύνους, το μέγεθός της, καθώς και η πιθανότητα και η σοβαρότητα των περιστατικών, μαζί με τις κοινωνικές και οικονομικές επιπτώσεις τους.

Το άρθρο 21 ορίζει επίσης ότι τα μέτρα αυτά βασίζονται σε ολιστική προσέγγιση του κινδύνου και καλύπτουν ένα ελάχιστο σύνολο θεματικών περιοχών. Στις περιοχές αυτές περιλαμβάνονται οι πολιτικές για την ανάλυση κινδύνου και την ασφάλεια των πληροφοριακών συστημάτων, ο χειρισμός περιστατικών, η επιχειρησιακή συνέχεια, η διαχείριση αντιγράφων ασφαλείας, η αποκατάσταση έπειτα από καταστροφή και η διαχείριση κρίσεων. Στο ίδιο σύνολο εντάσσονται ακόμη η ασφάλεια της αλυσίδας εφοδιασμού, η ασφάλεια στην απόκτηση, ανάπτυξη και συντήρηση συστημάτων δικτύου και πληροφοριών, καθώς και ο χειρισμός και η γνωστοποίηση ευπαθειών.

Στο ίδιο άρθρο περιλαμβάνονται και οι πολιτικές και οι διαδικασίες για την αξιολόγηση της αποτελεσματικότητας των μέτρων διαχείρισης κινδύνων κυβερνοασφάλειας. Η αναφορά αυτή δείχνει ότι οι απαιτήσεις της Οδηγίας δεν αφορούν μόνο τη θέσπιση μέτρων, αλλά και την παρακολούθηση της λειτουργίας τους. Επιπρόσθετα, προδιαγράφονται οι βασικές πρακτικές κυβερνοϋγιεινής και η κατάρτιση σε θέματα κυβερνοασφάλειας, οι πολιτικές και οι διαδικασίες σχετικά με τη χρήση κρυπτογραφίας και, κατά περίπτωση, κρυπτογράφησης, καθώς και η ασφάλεια ανθρώπινων πόρων, οι πολιτικές ελέγχου πρόσβασης και η διαχείριση πάγιων στοιχείων.

Στις απαιτήσεις του άρθρου 21 περιλαμβάνεται ακόμη η χρήση λύσεων πολυπαραγοντικής επαλήθευσης ταυτότητας ή συνεχούς επαλήθευσης ταυτότητας, καθώς και η χρήση ασφαλών επικοινωνιών, όπου αυτό κρίνεται κατάλληλο. Παράλληλα, η Οδηγία δίνει ιδιαίτερη βαρύτητα στην ασφάλεια της αλυσίδας εφοδιασμού, προβλέποντας ότι οι οντότητες λαμβάνουν υπόψη τις ευπάθειες των άμεσων προμηθευτών και παρόχων

υπηρεσιών, καθώς και τη συνολική ποιότητα των προϊόντων και των πρακτικών κυβερνοασφάλειας που αυτοί εφαρμόζουν.

Ιδιαίτερη σημασία έχει και η παράγραφος 4 του άρθρου 21, σύμφωνα με την οποία μια οντότητα που διαπιστώνει ότι δεν συμμορφώνεται με τα μέτρα της παραγράφου 2 λαμβάνει αμελλητί όλα τα αναγκαία, κατάλληλα και αναλογικά διορθωτικά μέτρα (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2022).

5.2. Τεκμηρίωση και Παρακολούθηση

Η συμμόρφωση με τη NIS2 συνδέεται με την ύπαρξη τεκμηριωμένης πληροφορίας και με τη συστηματική παρακολούθηση της εφαρμογής των σχετικών απαιτήσεων. Το ISO/IEC 27001 προβλέπει ότι το σύστημα διαχείρισης ασφάλειας πληροφοριών περιλαμβάνει την τεκμηριωμένη πληροφορία που απαιτείται από το ίδιο το πρότυπο, καθώς και όση τεκμηριωμένη πληροφορία κρίνει αναγκαία ο οργανισμός για την αποτελεσματική εφαρμογή του. Το ίδιο πρότυπο απαιτεί η πληροφορία αυτή να δημιουργείται, να επικαιροποιείται και να ελέγχεται με κατάλληλο τρόπο ως προς την ταυτοποίηση, τη μορφή, την έγκριση, τη διανομή, την αποθήκευση, την προστασία και τη διατήρησή της. Στο επίπεδο της συμμόρφωσης, η τεκμηριωμένη πληροφορία περιλαμβάνει πολιτικές, διαδικασίες, αρχεία, αναφορές και λοιπά στοιχεία που αποτυπώνουν την εφαρμογή των απαιτήσεων κυβερνοασφάλειας.

Η σημασία της τεκμηρίωσης συνδέεται και με το κανονιστικό πλαίσιο της NIS2. Στα άρθρα 32 και 33 προβλέπεται ότι οι αρμόδιες αρχές μπορούν να ζητούν από τις οντότητες τεκμηριωμένες πολιτικές κυβερνοασφάλειας, έγγραφα, πληροφορίες και αποδεικτικά στοιχεία που σχετίζονται με την εφαρμογή των μέτρων διαχείρισης κινδύνων. Στα τεκμήρια αυτά μπορούν να περιλαμβάνονται πολιτικές και διαδικασίες ασφάλειας, στοιχεία παρακολούθησης, αρχεία εξαιρέσεων, αποτελέσματα αξιολογήσεων, πρακτικά διοικητικής ανασκόπησης και καταγραφές διορθωτικών ενεργειών.

Η συμμόρφωση προϋποθέτει επίσης τακτική παρακολούθηση. Το ISO/IEC 27001 προβλέπει ότι ο οργανισμός καθορίζει τι πρέπει να παρακολουθείται και να μετράται, με ποιες μεθόδους, πότε, από ποιον και με ποια συχνότητα τα αποτελέσματα πρέπει να αναλύονται και να αξιολογούνται. Προβλέπεται επίσης η διατήρηση τεκμηριωμένης πληροφορίας ως αποδεικτικού στοιχείου των αποτελεσμάτων. Η τεχνική καθοδήγηση του

ENISA αναφέρει ότι οι οντότητες διενεργούν περιοδικές ανασκοπήσεις συμμόρφωσης, διατηρούν διαδικασίες παρακολούθησης της συμμόρφωσης και ενημερώνουν τα διοικητικά όργανα μέσω τακτικής αναφοράς. Στις σχετικές αναφορές μπορούν να περιλαμβάνονται δείκτες, κατάσταση συμμόρφωσης, εξαιρέσεις πολιτικών, εντοπισμένοι κίνδυνοι και προτεινόμενες ενέργειες.

Αντίστοιχη πρόβλεψη υπάρχει για τη διοικητική ανασκόπηση. Το ISO/IEC 27001 προβλέπει ότι η ανώτατη διοίκηση εξετάζει σε προγραμματισμένα διαστήματα την καταλληλότητα, την επάρκεια και την αποτελεσματικότητα του συστήματος διαχείρισης ασφάλειας πληροφοριών. Στα στοιχεία που λαμβάνονται υπόψη περιλαμβάνονται οι μη συμμορφώσεις, οι διορθωτικές ενέργειες, τα αποτελέσματα παρακολούθησης και μέτρησης, τα αποτελέσματα ελέγχων, η πρόοδος του σχεδίου αντιμετώπισης κινδύνων και οι δυνατότητες βελτίωσης (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2022; ISO/IEC, 2022; European Union Agency for Cybersecurity, 2025).

5.3. Το Gap Analysis Tool της Εθνικής Αρχής Κυβερνοασφάλειας ως Εργαλείο Αποτίμησης Συμμόρφωσης

Το Gap Analysis Tool της Εθνικής Αρχής Κυβερνοασφάλειας (ΕΑΚ) αποτελεί ένα ολοκληρωμένο πλαίσιο αξιολόγησης, το οποίο έχει αναπτυχθεί για χρήση από την ΕΑΚ και από τις οντότητες που εμπίπτουν στο πεδίο εφαρμογής του Ν. 5160/2024. Το εργαλείο αποσκοπεί στην αποτίμηση της συμμόρφωσης των οργανισμών με τις απαιτήσεις του νόμου και της ΚΥΑ 1689/2025, καθώς και στην εκτίμηση της ωριμότητας των μέτρων κυβερνοασφάλειας που εφαρμόζονται. Το εργαλείο περιλαμβάνει και επιπρόσθετα τεχνικά και οργανωτικά μέτρα, μέσω των οποίων υλοποιούνται οι αντίστοιχες απαιτήσεις.

Η δομή του εργαλείου βασίζεται σε λίστα ελέγχου με συνολικά 169 σημεία ελέγχου, τα οποία κατανέμονται σε 24 θεματικές ενότητες. Οι ενότητες αυτές καλύπτουν ευρύ φάσμα απαιτήσεων, όπως οι υποχρεώσεις και η ευθύνη των ανωτάτων οργάνων διοίκησης, το πλαίσιο διαχείρισης κινδύνων, οι πολιτικές και διαδικασίες ασφάλειας πληροφοριών, οι ρόλοι και οι αρμοδιότητες, οι διαδικασίες παρακολούθησης της συμμόρφωσης, η ασφάλεια της αλυσίδας εφοδιασμού, η αξιολόγηση της αποτελεσματικότητας των μέτρων, η εκπαίδευση και ευαισθητοποίηση, η διαχείριση περιστατικών ασφάλειας και η επιχειρησιακή συνέχεια.

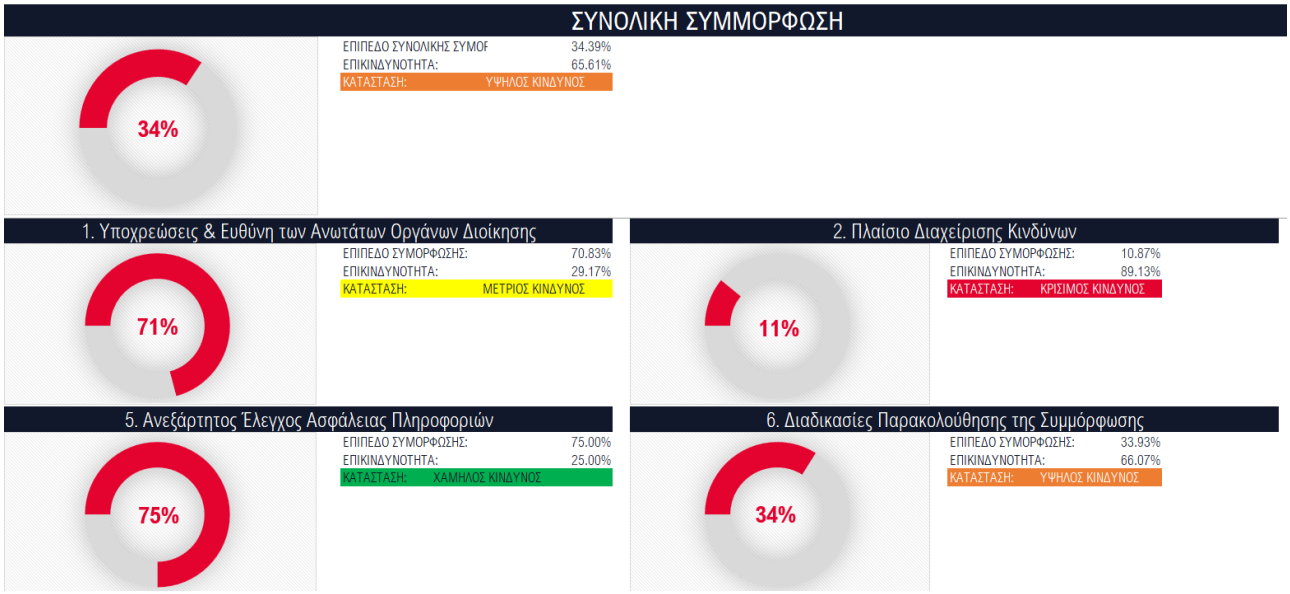
Η χρήση του εργαλείου ακολουθεί καθοδηγούμενη λογική. Για κάθε επιμέρους σημείο ελέγχου, ο χρήστης επιλέγει την τρέχουσα κατάσταση υλοποίησης μέσα από προκαθορισμένες κατηγορίες. Οι κατηγορίες αυτές περιλαμβάνουν τις τιμές «Δεν έχει ξεκινήσει», «Σχεδιάζεται», «Μερική υλοποίηση», «Σχεδόν ολοκληρωμένο» και «Πλήρως υλοποιημένο». Για ορισμένες απαιτήσεις προβλέπεται και η επιλογή «Δεν εφαρμόζεται», όταν η απαίτηση αφορά περιπτώσεις που δεν υφίστανται στον συγκεκριμένο οργανισμό. Σε κάθε κατηγορία αντιστοιχεί προκαθορισμένο ποσοστό υλοποίησης, από 0% έως 100%, ώστε η επιλογή του χρήστη να μετατρέπεται σε μετρήσιμο αποτέλεσμα. Στην εικόνα 6 παρουσιάζονται ενδεικτικά τα σημεία ελέγχου του εργαλείου και οι βασικοί δείκτες αξιολόγησής τους:

ΑΠΑΙΤΗΣΕΙΣ ΣΥΜΜΟΡΦΩΣΗΣ		ΣΥΝΟΛΙΚΗ ΣΥΜΜΟΡΦΩΣΗ: 34.05%			
#	ΜΕΤΡΑ	ΚΑΤΑΣΤΑΣΗ	ΠΟΣΟΣΤΟ ΥΛΟΠΟΙΗΣΗΣ (%)	ΒΑΡΥΤΗΤΑ (1-5)	ΕΠΙΠΕΔΟ ΣΥΜΜΟΡΦΩΣΗΣ
1	**Υποχρεώσεις & Ευθύνη των Ανωτάτων Οργάνων Διοίκησης**	**Μερική υλοποίηση**	**71%**	**Μέγιστη Δυνατή Βαθμολογία: 30**	**Επιτευχθείσα Βαθμολογία: 21.25**
1.1	Ο οργανισμός διαμορφώνει και υλοποιεί, με ευθύνη της ανώτατης διοίκησης, ολοκληρωμένο πρόγραμμα διαχείρισης των κινδύνων κυβερνοασφάλειας, που αποτελείται από πολιτικές, διαδικασίες, ανάθεση ρόλων, αρμοδιοτήτων και ευθυνών, καθώς και από ένα σύνολο τεχνικών, οργανωτικών και επιχειρησιακών μέτρων για την ασφάλεια των συστημάτων δικτύου και επικοινωνιών του.	Σχεδιάζεται	25%	5	1.25
1.2	Το ανώτατο όργανο διοίκησης της οντότητας εγκρίνει το πρόγραμμα διαχείρισης των κινδύνων κυβερνοασφάλειας και λαμβάνει μέριμνα για τη συνολική υλοποίηση, επίβλεψη, περιοδική αξιολόγηση και συνεχή βελτίωσή του.	Σχεδόν ολοκληρωμένο	75%	5	3.75
1.3	Το ανώτατο όργανο διοίκησης της οντότητας διασφαλίζει ότι παρέχονται οι απαραίτητοι πόροι για την υλοποίηση του προγράμματος διαχείρισης των κινδύνων κυβερνοασφάλειας και για τη λήψη των κατάλληλων και αναλογικών τεχνικών, επιχειρησιακών και οργανωτικών μέτρων διαχείρισης των εν λόγω κινδύνων.	Σχεδόν ολοκληρωμένο	75%	5	3.75
1.4	Το ανώτατο όργανο διοίκησης της οντότητας διασφαλίζει ότι το σύνολο του προσωπικού ενημερώνεται για τις υποχρεώσεις και τις ευθύνες του όσον αφορά στην τήρηση και εφαρμογή της πολιτικής ασφάλειας, των θεματικών πολιτικών ασφάλειας και των συναφών διαδικασιών της οντότητας.	Μερική υλοποίηση	50%	5	2.5
1.5	Το ανώτατο όργανο διοίκησης της οντότητας διασφαλίζει ότι η οικεία οντότητα τηρεί στοιχεία τεκμηρίωσης στην υποδομή της που αφορούν σε έγγραφα ψηφιακής ή φυσικής μορφής (όπως, πολιτικές ασφάλειας και διαδικασίες, πρακτικά διοικητικού συμβουλίου, οικονομικά στοιχεία, συμβάσεις, βεβαιώσεις εκπαίδευσης, διαγράμματα δικτύου, πλάνα επιχειρησιακής συνέχειας, έγγραφα περιοδικής αξιολόγησης μέτρων και διαδικασιών, αναφορές ελέγχων ασφάλειας, μηνύματα ηλεκτρονικού ταχυδρομείου).	Πλήρως υλοποιημένο	100%	5	5
1.6	Το ανώτατο όργανο διοίκησης της οντότητας παρακολουθεί σε περιοδική βάση πρόγραμμα εκπαίδευσης για θέματα κυβερνοασφάλειας και διασφαλίζει ότι παρέχεται αντίστοιχο πρόγραμμα και στο προσωπικό της.	Πλήρως υλοποιημένο	100%	5	5
2	**Πλαίσιο Διαχείρισης Κινδύνων**	**Σχεδιάζεται**	**10%**	**Μέγιστη Δυνατή Βαθμολογία: 23**	**Επιτευχθείσα Βαθμολογία: 2.5**
2.1	Η οντότητα αναπτύσσει και τηρεί κατάλληλο πλαίσιο για τη διαχείριση των κινδύνων κυβερνοασφάλειας, το οποίο ευθυγραμμίζεται με τη συνολική στρατηγική διαχείρισης των επιχειρηματικών κινδύνων της ή των κινδύνων που προκύπτουν κατά την άσκηση των αρμοδιοτήτων της, εφόσον πρόκειται για οντότητα της περ. στ΄ της παρ. 2 του άρθρου 3 του ν. 5160/2024. Για τη διαμόρφωση του εν λόγω πλαισίου λαμβάνονται υπόψη και οι σχέσεις της οντότητας με τρίτα μέρη, καθώς και με προμηθευτές και παρόχους υπηρεσιών.	Μερική υλοποίηση	50%	5	2.5
2.2	Η οντότητα διενεργεί, σε περιοδική βάση (προτείνεται ετησίως) και με αναλογικό τρόπο, εκτίμηση κινδύνων (risk assessment), εφαρμόζοντας διαδικασίες αναγνώρισης, ανάλυσης και αξιολόγησης των κινδύνων που απειλούν την ασφάλεια των συστημάτων δικτύου και πληροφοριών της. Για την υλοποίηση των εν λόγω διαδικασιών, εφαρμόζονται μεθοδολογίες που βασίζονται σε διεθνή πρότυπα ή / και βέλτιστες πρακτικές.	Δεν έχει ξεκινήσει	0%	5	0
2.3	Η οντότητα αναπτύσσει, υλοποιεί και επιβλέπει κατάλληλο πλάνο αντιμετώπισης των κινδύνων (risk treatment plan).	Δεν έχει ξεκινήσει	0%	5	0

Εικόνα 6 - Συνοπτική εικόνα των σημείων ελέγχου του εργαλείου της ΕΑΚ (Κωτσικοπούλου, 2025)

Πέρα από την κατάσταση υλοποίησης, κάθε σημείο ελέγχου συνοδεύεται από βαρύτητα. Με βάση το ποσοστό υλοποίησης και τη βαρύτητα, το εργαλείο υπολογίζει το επίπεδο συμμόρφωσης για κάθε επιμέρους σημείο. Ο υπολογισμός αυτός γίνεται με πολλαπλασιασμό του ποσοστού υλοποίησης με τη βαρύτητα του σημείου ελέγχου. Στη συνέχεια, το εργαλείο υπολογίζει τη συνολική συμμόρφωση του οργανισμού ως ποσοστό, με βάση τη συνολική επιτευχθείσα βαθμολογία σε σχέση με τη μέγιστη δυνατή βαθμολογία όλων των σημείων ελέγχου. Τα αποτελέσματα της αξιολόγησης αποτυπώνονται συγκεντρωτικά σε ξεχωριστή καρτέλα του εργαλείου (Dashboard), όπου παρουσιάζονται η συνολική συμμόρφωση του οργανισμού, η συνολική επικινδυνότητα και η αντίστοιχη

κατάσταση κινδύνου, καθώς και τα επιμέρους επίπεδα συμμόρφωσης ανά θεματική ενότητα, όπως φαίνεται στην εικόνα 7:



Εικόνα 7 - Διαγραμματική απεικόνιση επιπέδων συμμόρφωσης μέσω του εργαλείου της ΕΑΚ (Κωτσικοπούλου, 2025)

Η λειτουργία αυτή διευκολύνει την αναγνώριση ελλείψεων και την ιεράρχηση παρεμβάσεων. Μέσα από τις επιμέρους επιλογές και τους αυτόματους υπολογισμούς, το εργαλείο επιτρέπει στον οργανισμό να εντοπίσει τα σημεία στα οποία η εφαρμογή είναι περιορισμένη ή δεν έχει ξεκινήσει, καθώς και τις θεματικές ενότητες στις οποίες εμφανίζονται χαμηλότερα επίπεδα συμμόρφωσης. Παράλληλα, η ύπαρξη βαρύτητας ανά σημείο ελέγχου επιτρέπει τη διαφοροποίηση της σημασίας των απαιτήσεων και διευκολύνει την ιεράρχηση των επόμενων ενεργειών. Οι επιμέρους καρτέλες του εργαλείου εξειδικεύουν περαιτέρω τα παραπάνω, όπου καταγράφονται στοιχεία τεκμηρίωσης, κενά συμμόρφωσης, προτεινόμενες διορθωτικές ή βελτιωτικές ενέργειες και αντιστοίχιση των σημείων ελέγχου με τις σχετικές κανονιστικές διατάξεις.

Ειδικότερα, το εργαλείο περιλαμβάνει και πεδία τεκμηρίωσης για κάθε σημείο ελέγχου. Σε αυτά καταγράφονται η τωρινή κατάσταση ή οι σχετικές παρατηρήσεις, τα διαθέσιμα τεκμήρια και το αντίστοιχο κενό συμμόρφωσης. Η καταγραφή αυτή διευκολύνει τον οργανισμό να αποτυπώσει όχι μόνο τι έχει υλοποιηθεί, αλλά και ποια σημεία υπολείπονται, ποια αποδεικτικά στοιχεία υπάρχουν ήδη και ποια λείπουν. Η λειτουργία αυτή φαίνεται ενδεικτικά στην εικόνα 8:

ΑΠΑΙΤΗΣΕΙΣ ΣΥΜΜΟΡΦΩΣΗΣ		ΣΤΟΙΧΕΙΑ ΤΕΚΜΗΡΙΩΣΗΣ/ΥΛΟΠΟΙΗΣΗΣ		
#	ΜΕΤΡΑ	ΤΩΡΙΝΗ ΚΑΤΑΣΤΑΣΗ/ ΠΑΡΑΤΗΡΗΣΗ	ΤΕΚΜΗΡΙΑ	ΚΕΝΟ ΣΥΜΜΟΡΦΩΣΗΣ
3	Πολιτικές και Διαδικασίες Ασφάλειας Πληροφοριών			
3.1	Η οντότητα έχει εκπονήσει γραπτή γενική πολιτική ασφάλειας πληροφοριών, η οποία εγκρίνεται από το ανώτατο όργανο διοίκησης και καθορίζει την προσέγγιση της οντότητας για τη διαχείριση της ασφάλειας των συστημάτων δικτύου και πληροφοριών της.	Υπάρχει εγκεκριμένη γενική πολιτική ασφάλειας πληροφοριών, η οποία έχει εγκριθεί από τη διοίκηση και κοινοποιείται στα αρμόδια στελέχη.	Εγκεκριμένη Πολιτική Ασφάλειας Πληροφοριών, πρακτικό έγκρισης από διοίκηση, έκδοση εγγράφου με αριθμό αναθεώρησης, δημοσίευση στο εσωτερικό αποθετήριο πολιτικών.	Δεν εντοπίζεται ουσιώδες κενό συμμόρφωσης.
3.2	Η οντότητα έχει εκπονήσει γραπτές και εγκεκριμένες θεματικές πολιτικές ασφάλειας που καλύπτουν ειδικές πτυχές κυβερνοασφάλειας αυτής, όσον αφορά ανθρώπινο δυναμικό, διαδικασίες και τεχνολογίες (π.χ. πολιτική ελέγχου πρόσβασης, πολιτική ασφάλειας δικτύων, πολιτική ορθής χρήσης κ.λπ.).	Υπάρχουν ορισμένες θεματικές πολιτικές ασφάλειας, αλλά η κάλυψη δεν είναι πλήρης και δεν έχουν όλες εγκριθεί ή επικαιροποιηθεί.	Πολιτική ελέγχου πρόσβασης, πολιτική ορθής χρήσης, σχέδιο πολιτικής ασφάλειας δικτύων, πίνακας υφιστάμενων πολιτικών.	Δεν υπάρχει πλήρες και ενοποιημένο σύνολο θεματικών πολιτικών για όλες τις απαιτούμενες περιοχές.
3.3	Η γενική πολιτική ασφάλειας και οι θεματικές πολιτικές αξιολογούνται και, κατά περίπτωση, επικαιροποιούνται τακτικά σε προγραμματισμένα χρονικά διαστήματα, καθώς και όταν λαμβάνουν χώρα σοβαρά περιστατικά κυβερνοασφάλειας ή σημαντικές αλλαγές στις λειτουργίες του οργανισμού.	Δεν έχει θεσπιστεί ακόμη τυπική διαδικασία περιοδικής αναθεώρησης και επικαιροποίησης των πολιτικών ασφάλειας.	Υφιστάμενες πολιτικές χωρίς τεκμηριωμένο χρονοδιάγραμμα ανασκόπησης, απουσία εγκεκριμένης διαδικασίας επανεξέτασης, περιορισμένα στοιχεία version history.	Απουσιάζει καθορισμένη διαδικασία τακτικής αναθεώρησης, καθώς και μηχανισμός επικαιροποίησης μετά από περιστατικά ή σημαντικές αλλαγές.

Εικόνα 8 - Καταγραφή στοιχείων τεκμηρίωσης στο εργαλείο της ΕΑΚ (Κωτσικοπούλου, 2025)

Σε επόμενο στάδιο, το εργαλείο υποστηρίζει τη διαμόρφωση πλάνου διορθωτικών και βελτιωτικών ενεργειών. Για κάθε σημείο ελέγχου μπορούν να καταγραφούν οι προτεινόμενες ενέργειες, η προτεραιότητά τους, η καταληκτική ημερομηνία, ο υπεύθυνος υλοποίησης, η κατάσταση προόδου και συμπληρωματικά σχόλια. Η δομή αυτή επιτρέπει τη μετατροπή της αξιολόγησης σε οργανωμένο σχέδιο παρακολούθησης της συμμόρφωσης, με σαφή προσδιορισμό ενεργειών και ευθυνών. Η λειτουργία αυτή αποτυπώνεται στην εικόνα 9:

ΑΠΑΙΤΗΣΕΙΣ ΣΥΜΜΟΡΦΩΣΗΣ		ΠΛΑΝΟ ΔΙΟΡΘΩΤΙΚΩΝ/ΒΕΛΤΙΩΤΙΚΩΝ ΕΝΕΡΓΕΙΩΝ					
#	ΜΕΤΡΑ	ΠΡΟΤΕΙΝΟΜΕΝΕΣ ΕΝΕΡΓΕΙΕΣ	ΠΡΟΤΕΡΑΙΟΤΗΤΑ	ΚΑΤΑΛΗΚΤΙΚΗ ΗΜΕΡΟΜΗΝΙΑ	ΥΠΕΥΘΥΝΟΣ	ΚΑΤΑΣΤΑΣΗ	ΣΧΟΛΙΑ
3	Πολιτικές και Διαδικασίες Ασφάλειας Πληροφοριών						
3.1	Η οντότητα έχει εκπονήσει γραπτή γενική πολιτική ασφάλειας πληροφοριών, η οποία εγκρίνεται από το ανώτατο όργανο διοίκησης και καθορίζει την προσέγγιση της οντότητας για τη διαχείριση της ασφάλειας των συστημάτων δικτύου και πληροφοριών της.	Διατήρηση της πολιτικής σε ισχύ, έλεγχος έκδοσης και προγραμματισμένη επανεξέταση.	ΧΑΜΗΛΗ	31-12-26	Ανώτατη Διοίκηση / Υ.Α.Σ.Π.Ε.	Ολοκληρώθηκε	Να επιβεβαιώνεται ετησίως η επικαιρότητα του εγγράφου.
3.2	Η οντότητα έχει εκπονήσει γραπτές και εγκεκριμένες θεματικές πολιτικές ασφάλειας που καλύπτουν ειδικές πτυχές κυβερνοασφάλειας αυτής, όσον αφορά ανθρώπινο δυναμικό, διαδικασίες και τεχνολογίες (π.χ. πολιτική ελέγχου πρόσβασης, πολιτική ασφάλειας δικτύων, πολιτική ορθής χρήσης κ.λπ.).	Κατάρτιση και έγκριση πλήρους συνόλου θεματικών πολιτικών, ευθυγράμμιση με τη γενική πολιτική ασφάλειας, κοινοποίηση στους εμπλεκόμενους.	ΧΑΜΗΛΗ	30-09-26	Υ.Α.Σ.Π.Ε. / Διεύθυνση Πληροφορικής	Σε εξέλιξη	Υφίστανται μεμονωμένες πολιτικές, απαιτείται ολοκλήρωση και ομοιομορφία.
3.3	Η γενική πολιτική ασφάλειας και οι θεματικές πολιτικές αξιολογούνται και, κατά περίπτωση, επικαιροποιούνται τακτικά σε προγραμματισμένα χρονικά διαστήματα, καθώς και όταν λαμβάνουν χώρα σοβαρά περιστατικά κυβερνοασφάλειας ή σημαντικές αλλαγές στις λειτουργίες του οργανισμού.	Θέσπιση διαδικασίας αναθεώρησης πολιτικών, ορισμός συχνότητας επανεξέτασης, καθορισμός triggers για ad hoc επικαιροποίηση, τήρηση ιστορικού εκδόσεων.	ΥΨΗΛΗ	30-06-26	Υ.Α.Σ.Π.Ε. / Ιδιοκτήτες πολιτικών / Ανώτατη Διοίκηση	Δεν ξεκίνησε	Να συνδεθεί με incident management, change management και management review.

Εικόνα 9 - Αποτύπωση προτεινόμενων διορθωτικών/βελτιωτικών ενεργειών στο εργαλείο της ΕΑΚ (Κωτσικοπούλου, 2025)

Επιπλέον, το εργαλείο περιλαμβάνει καρτέλα αναφοράς, στην οποία κάθε σημείο ελέγχου αντιστοιχίζεται με τις σχετικές διατάξεις του Ν. 5160/2024, της ΚΥΑ 1689/2025 και της Οδηγίας NIS2. Η αντιστοίχιση αυτή υποστηρίζει την ιχνηλασιμότητα της αξιολόγησης και την αποτύπωση της κανονιστικής βάσης κάθε απαίτησης. Παράλληλα, επιτρέπει στον οργανισμό να συνδέει τα ευρήματα της αξιολόγησης με συγκεκριμένες ρυθμιστικές υποχρεώσεις και να οργανώνει με μεγαλύτερη σαφήνεια την τεκμηρίωση και τις παρεμβάσεις συμμόρφωσης. Ενδεικτική αποτύπωση της λειτουργίας αυτής παρουσιάζεται στην Εικόνα 10:

ΑΠΑΙΤΗΣΕΙΣ ΣΥΜΜΟΡΦΩΣΗΣ		ΑΝΑΦΟΡΑ		
#	ΜΕΤΡΑ	Ν.5160/2024	ΚΥΑ 1689/2025	ΟΔΗΓΙΑ NIS2
3	Πολιτικές και Διαδικασίες Ασφάλειας Πληροφοριών	Άρθρο 14 Διακυβέρνηση & Άρθρο 15 Μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας	Άρθρο 6	Άρθρο 20 & 21 της Οδηγίας
3.1	Η οντότητα έχει εκπονήσει γραπτή γενική πολιτική ασφάλειας πληροφοριών, η οποία εγκρίνεται από το ανώτατο όργανο διοίκησης και καθορίζει την προσέγγιση της οντότητας για τη διαχείριση της ασφάλειας των συστημάτων δικτύου και πληροφοριών της.	Άρθρο 14 Διακυβέρνηση & Άρθρο 15 Μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας παρ. 2α	Άρθρο 6 παρ. α	Άρθρο 20 & 21 παρ. 2α
3.2	Η οντότητα έχει εκπονήσει γραπτές και εγκεκριμένες θεματικές πολιτικές ασφάλειας που καλύπτουν ειδικές πτυχές κυβερνοασφάλειας αυτής, όσον αφορά ανθρώπινο δυναμικό, διαδικασίες και τεχνολογίες (π.χ. πολιτική ελέγχου πρόσβασης, πολιτική ασφάλειας δικτύων, πολιτική ορθής χρήσης κ.λπ.).	Άρθρο 15 Μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας	Άρθρο 6 παρ. β	Άρθρο 21
3.3	Η γενική πολιτική ασφάλειας και οι θεματικές πολιτικές αξιολογούνται και, κατά περίπτωση, επικαιροποιούνται τακτικά σε προγραμματισμένα χρονικά διαστήματα, καθώς και όταν λαμβάνουν χώρα σοβαρά περιστατικά κυβερνοασφάλειας ή σημαντικές αλλαγές στις λειτουργίες του οργανισμού.	Άρθρο 15 Μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας	Άρθρο 6 παρ. γ	Άρθρο 21

Εικόνα 10 - Αντιστοίχιση σημείων ελέγχου με το κανονιστικό πλαίσιο στο εργαλείο της ΕΑΚ (Κωτσικοπούλου, 2025)

Συνολικά, το εργαλείο της ΕΑΚ δεν περιορίζεται στην αρχική αποτύπωση του επιπέδου συμμόρφωσης, αλλά αξιοποιείται και για την τεκμηρίωση της υφιστάμενης κατάστασης, την ιεράρχηση των αναγκαίων ενεργειών και τη σύνδεση της αξιολόγησης με το εφαρμοστέο κανονιστικό πλαίσιο (Κωτσικοπούλου, 2025).

5.4. Διορθωτικές Ενέργειες

Η συμμόρφωση με τη NIS2 συνδέεται και με την υποχρέωση λήψης διορθωτικών μέτρων όταν εντοπίζονται ελλείψεις. Η Οδηγία προβλέπει ότι, όταν μια οντότητα διαπιστώνει μη συμμόρφωση, λαμβάνει αμελλητί όλα τα αναγκαία, κατάλληλα και αναλογικά διορθωτικά μέτρα.

Αντίστοιχες προβλέψεις περιλαμβάνονται και στο ISO/IEC 27001. Ειδικότερα, προβλέπεται ότι, όταν προκύπτει μη συμμόρφωση, ο οργανισμός αντιδρά, λαμβάνει μέτρα για τον έλεγχο και τη διόρθωσή της, αντιμετωπίζει τις συνέπειες και αξιολογεί την ανάγκη λήψης ενεργειών για την εξάλειψη των αιτίων της. Το ίδιο κείμενο περιλαμβάνει την ανασκόπηση της μη συμμόρφωσης, τον προσδιορισμό των αιτίων της, την εξέταση τυχόν παρόμοιων περιπτώσεων, την εφαρμογή των αναγκαίων ενεργειών και τον έλεγχο της αποτελεσματικότητάς τους. Προβλέπεται επίσης η τήρηση τεκμηριωμένης πληροφορίας ως αποδεικτικού στοιχείου για τη φύση των μη συμμορφώσεων, τις ενέργειες που λήφθηκαν και τα αποτελέσματά τους.

Στην ίδια κατεύθυνση, το ISO/IEC 27002 προβλέπει ότι η συμμόρφωση με τις πολιτικές, τους κανόνες και τα πρότυπα ασφάλειας πληροφοριών εξετάζεται σε τακτική βάση. Όταν εντοπίζεται μη συμμόρφωση, οι αρμόδιοι εξετάζουν τα αίτιά της, αξιολογούν την ανάγκη

λήψης διορθωτικών ενεργειών, εφαρμόζουν τις κατάλληλες παρεμβάσεις και επανεξετάζουν την αποτελεσματικότητά τους. Τα αποτελέσματα των ανασκοπήσεων και των διορθωτικών ενεργειών καταγράφονται και διατηρούνται, ενώ η ολοκλήρωσή τους πρέπει να γίνεται εντός χρονικού διαστήματος ανάλογου προς τον σχετικό κίνδυνο.

Η τεχνική καθοδήγηση του ENISA προβλέπει επίσης ότι οι πολιτικές και οι διαδικασίες για την αξιολόγηση της αποτελεσματικότητας των μέτρων επανεξετάζονται σε προγραμματισμένα διαστήματα και επικαιροποιούνται όταν προκύπτουν σημαντικά περιστατικά ή ουσιώδεις μεταβολές στις λειτουργίες ή στους κινδύνους. Στα σχετικά τεκμήρια περιλαμβάνονται αρχεία προηγούμενων ανασκοπήσεων, προγραμματισμένες επόμενες αξιολογήσεις, πρακτικά συναντήσεων και σχέδια αντιμετώπισης κινδύνων που λαμβάνουν υπόψη τα αποτελέσματα των αξιολογήσεων. Οι διορθωτικές ενέργειες περιλαμβάνουν και παρακολούθηση, επανεξέταση και επικαιροποίηση των σχετικών διαδικασιών.

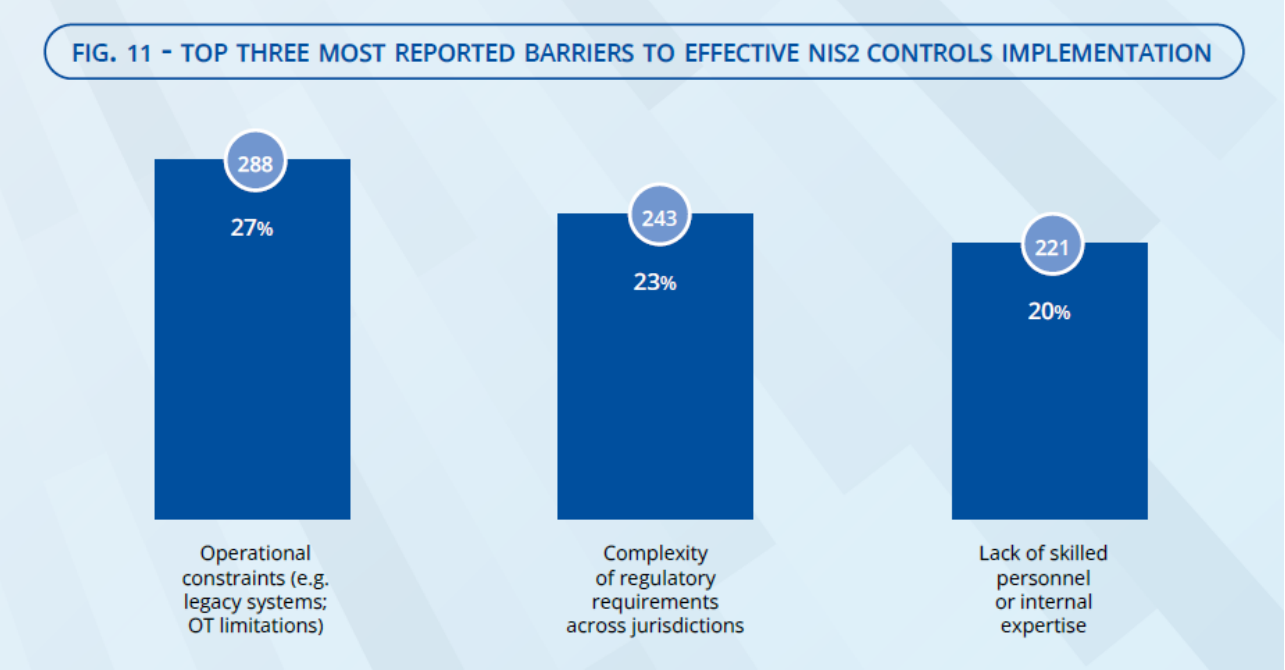
Η λογική αυτή αποτυπώνεται και στο Gap Analysis Tool της ΕΑΚ. Μετά την καταγραφή του κενού συμμόρφωσης, το εργαλείο προβλέπει πεδία για προτεινόμενες ενέργειες, προτεραιότητα, καταληκτική ημερομηνία, υπεύθυνο, κατάσταση προόδου και σχόλια. Παράλληλα, υποστηρίζει την παρακολούθηση της αποκατάστασης και την τεκμηριωμένη αποτύπωση της προόδου (Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης, 2022; ISO/IEC, 2022a, 2022b; European Union Agency for Cybersecurity, 2025).

6. ΠΡΟΚΛΗΣΕΙΣ ΕΦΑΡΜΟΓΗΣ

Η εφαρμογή της Οδηγίας NIS2 αποτελεί ένα απαιτητικό εγχείρημα για τους οργανισμούς που εμπίπτουν στο πεδίο εφαρμογής της. Στην πράξη, η υλοποίησή της επηρεάζεται από ένα σύνολο κανονιστικών, οργανωτικών, τεχνικών και επιχειρησιακών δυσκολιών. Οι δυσκολίες αυτές συνδέονται με την ερμηνεία και εναρμόνιση των απαιτήσεων, τη διαθεσιμότητα πόρων και την ύπαρξη κατάλληλων μηχανισμών διακυβέρνησης, καθώς και με ζητήματα που αφορούν την εφοδιαστική αλυσίδα, την αναφορά περιστατικών και την εφαρμογή σε περιβάλλοντα διαφορετικής ωριμότητας.

6.1. Κανονιστική και Ερμηνευτική Αβεβαιότητα

Παρά τον στόχο της Οδηγίας NIS2 για την επίτευξη υψηλού κοινού επιπέδου κυβερνοασφάλειας στην Ένωση, η εφαρμογή της δεν εξελίσσεται με ενιαίο τρόπο σε όλα τα κράτη μέλη. Κατά την εθνική ενσωμάτωσή της παρατηρούνται αποκλίσεις στην κατηγοριοποίηση των οντοτήτων, στο εύρος του πεδίου εφαρμογής και στα κατώφλια υπαγωγής. Η αβεβαιότητα αυτή αποτυπώνεται ιδιαίτερα και στον δημόσιο τομέα, όπου η αναγνώριση των φορέων που εμπίπτουν στο πεδίο εφαρμογής της NIS2 παραμένει σε εξέλιξη, ενώ τα κράτη μέλη διατηρούν σημαντική ευχέρεια ως προς τον προσδιορισμό των οντοτήτων που θεωρούνται δημόσιες διοικήσεις. Η ευχέρεια αυτή συνδέεται και με χαμηλότερο επίπεδο επίγνωσης του γενικού πεδίου και των βασικών προβλέψεων της Οδηγίας σε ορισμένα τμήματα του τομέα. Ορισμένα κράτη μέλη υιοθετούν διαφορετικά μοντέλα ταξινόμησης ή επεκτείνουν το πεδίο εφαρμογής σε πρόσθετους τομείς, ενώ άλλα εξαιρούν δραστηριότητες που ρυθμίζονται ήδη από ειδικότερα καθεστώτα. Οι αποκλίσεις αυτές αυξάνουν την πολυπλοκότητα για οργανισμούς που δραστηριοποιούνται σε περισσότερα από ένα κράτη μέλη, καθώς ενδέχεται να υπάγονται σε διαφορετικές απαιτήσεις, παρότι παρέχουν τις ίδιες υπηρεσίες. Όπως αποτυπώνεται στην εικόνα 11, για οργανισμούς της Ένωσης που δραστηριοποιούνται σε τομείς υψηλής κρισιμότητας, η πολυπλοκότητα των κανονιστικών απαιτήσεων μεταξύ διαφορετικών χωρών αποτελεί ένα από τα σημαντικότερα εμπόδια στην εφαρμογή της NIS2:



Εικόνα 11 - Βασικότερες δυσκολίες στην αποτελεσματική εφαρμογή των μέτρων της NIS2 (European Union Agency for Cybersecurity κ.ά., 2025)

Το ζήτημα δεν περιορίζεται μόνο στην υπαγωγή των οντοτήτων. Επεκτείνεται και στην ερμηνεία ορισμένων απαιτήσεων εφαρμογής, ιδίως όταν δεν υπάρχουν επαρκώς σαφείς και ομοιόμορφες κατευθύνσεις. Η ασάφεια αυτή δυσκολεύει τους οργανισμούς να κρίνουν ποια μέτρα θεωρούνται επαρκή, ποια τεκμηρίωση απαιτείται και με ποιον τρόπο πρέπει να οργανωθεί η εφαρμογή σε πρακτικό επίπεδο. Το πρόβλημα εντείνεται από την ανάγκη ευθυγράμμισης της NIS2 με άλλα πρότυπα και κανονιστικά πλαίσια, όπως το ISO 27001, ο GDPR και ο DORA, καθώς τα κράτη μέλη δεν ακολουθούν πάντοτε κοινή προσέγγιση ως προς την αναγνώριση ή την αντιστοίχιση των πλαισίων αυτών. Η δυσκολία αυτή γίνεται εντονότερη σε τομείς με έντονη ετερογένεια, διασυνοριακή δραστηριότητα και συμμετοχή οντοτήτων που μέχρι πρόσφατα δεν υπάγονταν σε αντίστοιχο κανονιστικό πλαίσιο. Στις περιπτώσεις αυτές, η εφαρμογή των απαιτήσεων περιπλέκεται ακόμη περισσότερο, καθώς ούτε οι εποπτικές αρχές διαθέτουν πάντοτε τον ίδιο βαθμό εξοικείωσης με τα ιδιαίτερα χαρακτηριστικά της σχετικής αγοράς.

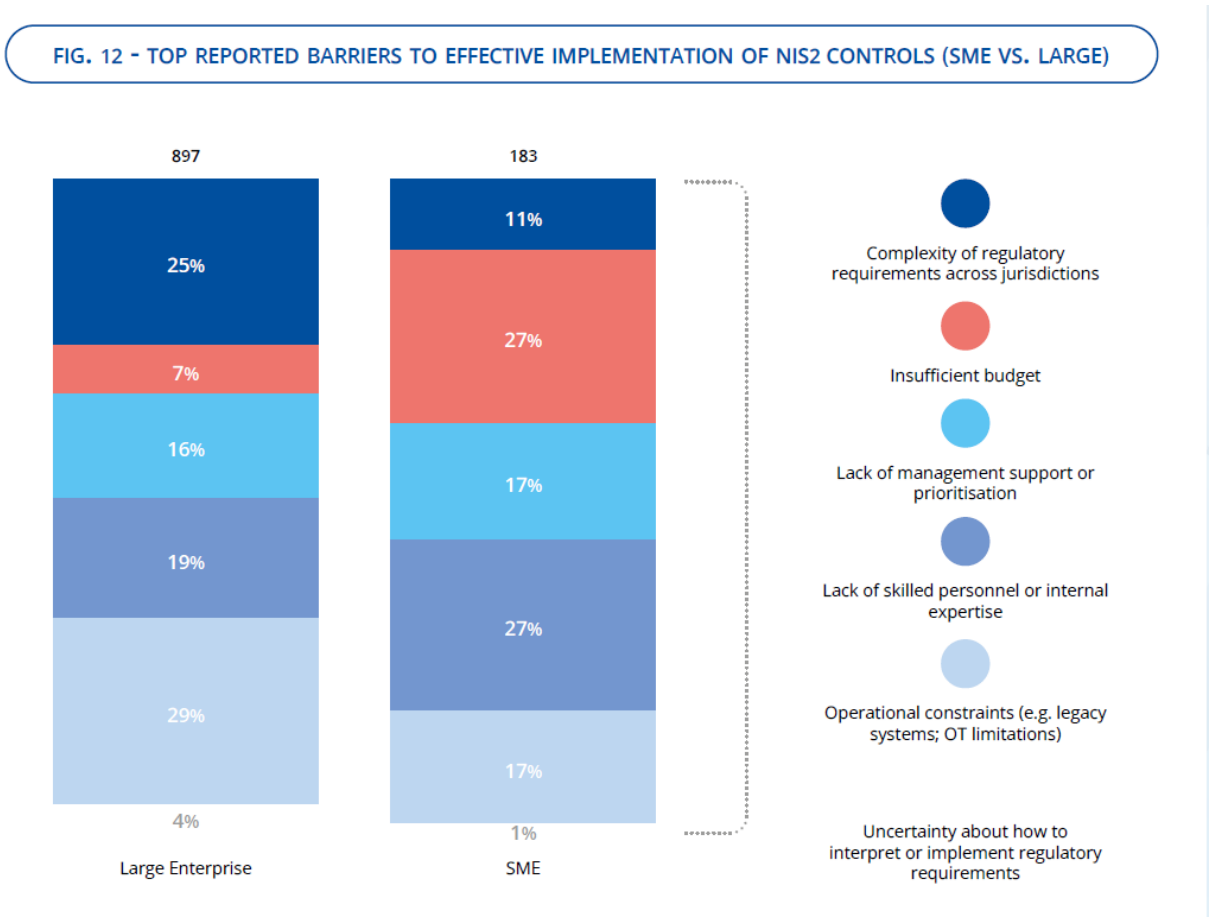
Ζητήματα ερμηνείας εμφανίζονται και στις υποχρεώσεις αναφοράς περιστατικών, ιδίως ως προς το πότε ενεργοποιείται η σχετική υποχρέωση και ποιο περιστατικό θεωρείται αναφερόμενο. Οι αποκλίσεις αυτές αυξάνουν την κανονιστική πολυπλοκότητα, ιδίως για οργανισμούς με διασυνοριακή παρουσία (European Cyber Security Organisation, 2025;

European Union Agency for Cybersecurity., 2025; European Union Agency for Cybersecurity *κ.ά.*, 2025).

6.2. Οργανωτική και Διοικητική Ετοιμότητα

Η εφαρμογή της Οδηγίας NIS2 εξαρτάται σε μεγάλο βαθμό από τη διοικητική και οργανωτική ετοιμότητα των οργανισμών που υπάγονται στο πεδίο εφαρμογής της. Η Οδηγία αντιμετωπίζει την κυβερνοασφάλεια ως ζήτημα ευθύνης της διοίκησης και όχι αποκλειστικά ως τεχνικό αντικείμενο των τμημάτων πληροφορικής. Η προσέγγιση αυτή προϋποθέτει ουσιαστική συμμετοχή της ανώτατης διοίκησης στην έγκριση των μέτρων, στην εποπτεία της εφαρμογής τους και στον συνολικό προσανατολισμό της διαχείρισης του κυβερνοκινδύνου.

Στην πράξη, όμως, η εμπλοκή αυτή δεν παρατηρείται πάντοτε στον ίδιο βαθμό. Η περιορισμένη συμμετοχή της διοίκησης δυσχεραίνει τη λήψη αποφάσεων, την ιεράρχηση των αναγκαίων παρεμβάσεων και την ενσωμάτωση της κυβερνοασφάλειας στη συνολική λειτουργία του οργανισμού. Στην εικόνα 12 φαίνεται ότι η έλλειψη υποστήριξης και προτεραιοποίησης από τη διοίκηση συγκαταλέγεται στα σημαντικότερα εμπόδια για την υλοποίηση των μέτρων της NIS2, τόσο στις μεγάλες όσο και στις μικρομεσαίες επιχειρήσεις της ΕΕ:



Εικόνα 12 - Βασικότερες δυσκολίες στην αποτελεσματική εφαρμογή των μέτρων της NIS2, σε μεγάλες και μικρομεσαίες επιχειρήσεις (European Union Agency for Cybersecurity κ.ά., 2025)

Η διαπίστωση αυτή επιβεβαιώνεται και από τομεακά ευρήματα, σύμφωνα με τα οποία, ακόμη και σε περιπτώσεις όπου η ηγεσία εγκρίνει μέτρα διαχείρισης κυβερνοκινδύνου, παραμένει αισθητό χάσμα ανάμεσα στην αυτοαξιολόγηση των οργανισμών και στην αξιολόγηση των αρμόδιων αρχών ως προς το πραγματικό επίπεδο ετοιμότητας. Παράλληλα, η αποτελεσματική εφαρμογή της NIS2 προϋποθέτει σαφή κατανομή ρόλων και αρμοδιοτήτων, καθώς και συντονισμό μεταξύ διαφορετικών τμημάτων και λειτουργιών, όπως η πληροφορική, η ασφάλεια, το νομικό τμήμα, η κανονιστική συμμόρφωση και οι επιχειρησιακές μονάδες. Όταν ο συντονισμός αυτός είναι ελλιπής, αυξάνεται ο κίνδυνος καθυστερήσεων, επικαλύψεων ή οργανωτικών κενών.

Η οργανωτική ετοιμότητα δεν περιορίζεται σε μια τυπική ανάθεση ευθυνών. Απαιτεί προσαρμογή διαδικασιών, ενίσχυση της εσωτερικής συνεργασίας και, σε αρκετές περιπτώσεις, αλλαγή στον τρόπο με τον οποίο ο οργανισμός εντάσσει την κυβερνοασφάλεια στη συνολική λειτουργία του. Η ανάγκη αυτή αποτυπώνεται και στη χαμηλή συμμετοχή πολλών οργανισμών σε μηχανισμούς συνεργασίας και ανταλλαγής πληροφοριών, γεγονός

που αναδεικνύει τη σημασία της ενεργότερης ένταξης των φορέων σε ευρύτερα σχήματα συντονισμού.

Η ανάπτυξη νέων διαδικασιών διαχείρισης κινδύνων, η ενσωμάτωση της ασφάλειας στις καθημερινές λειτουργίες και η υπέρβαση της αντίστασης στην αλλαγή συγκαταλέγονται στις βασικές οργανωτικές δυσκολίες. Η έγκαιρη επικοινωνία με τις αρμόδιες εθνικές αρχές μπορεί να διευκολύνει την ερμηνεία και εφαρμογή των απαιτήσεων, χωρίς ωστόσο να αντιμετωπίζει από μόνη της τις εσωτερικές αδυναμίες οργάνωσης και διακυβέρνησης. Οι τομείς με υψηλότερο επίπεδο ωριμότητας φαίνεται να ωφελούνται από σαφέστερη καθοδήγηση, ισχυρότερη εποπτική υποστήριξη, μεγαλύτερη συνεργασία και πιο ανεπτυγμένη επιχειρησιακή ετοιμότητα (Βασιλειάδης Δημήτριος, 2025; European Cyber Security Organisation, 2025; European Union Agency for Cybersecurity., 2025; European Union Agency for Cybersecurity κ.ά., 2025).

6.3. Πόροι, Κόστος και Ανθρώπινο Δυναμικό

Η εφαρμογή της Οδηγίας NIS2 απαιτεί σημαντικούς οικονομικούς και ανθρώπινους πόρους. Η υιοθέτηση νέων μέτρων κυβερνοασφάλειας, η αναβάθμιση υφιστάμενων διαδικασιών και η ανάπτυξη πιο ώριμων μηχανισμών διαχείρισης κινδύνου αυξάνουν το κόστος για τους οργανισμούς που υπάγονται στο πεδίο εφαρμογής της. Πρόσφατα ευρήματα δείχνουν ότι οι δαπάνες κυβερνοασφάλειας παραμένουν περίπου στο 9% των συνολικών δαπανών πληροφορικής, με διάμεση ετήσια δαπάνη περίπου 1,5 εκατ. ευρώ, ενώ η επενδυτική έμφαση μετατοπίζεται ολοένα περισσότερο προς την τεχνολογία και την εξωτερική ανάθεση υπηρεσιών, αντί προς την ενίσχυση των εσωτερικών ομάδων κυβερνοασφάλειας. Η επιβάρυνση αυτή δεν κατανέμεται ομοιόμορφα. Οι μεσαίου μεγέθους οργανισμοί, καθώς και οι οντότητες που εντάσσονται για πρώτη φορά στο κανονιστικό πεδίο της NIS2, καλούνται συχνά να αναπτύξουν βασικές δυνατότητες χωρίς να διαθέτουν ήδη αντίστοιχες δομές, την οικονομική ευχέρεια ή την οργανωτική υποστήριξη που χαρακτηρίζουν συνήθως τους μεγαλύτερους οργανισμούς. Όπως αποτυπώνεται στις εικόνες 11 και 12, η έλλειψη εξειδικευμένου προσωπικού και τεχνογνωσίας στους οργανισμούς αποτελούν ορισμένα από τα κορυφαία εμπόδια κατά την εφαρμογή της NIS2. Την ίδια στιγμή, σημαντικό ποσοστό οργανισμών δεν φαίνεται να έχει προβλέψει ειδικό προϋπολογισμό για την εφαρμογή της Οδηγίας, γεγονός που ενισχύει τον κίνδυνο αποσπασματικής ή καθυστερημένης υλοποίησης.

Η δυσκολία αυτή επιβεβαιώνεται και σε επίπεδο Ένωσης, όπου οι οργανισμοί συνεχίζουν να αντιμετωπίζουν έντονα προβλήματα προσέλκυσης (76%) και διατήρησης (71%) επαγγελματιών κυβερνοασφάλειας, κυρίως λόγω της έλλειψης υποψηφίων με τις απαιτούμενες δεξιότητες και του αυξημένου ανταγωνισμού για περιορισμένο ανθρώπινο δυναμικό. Η πίεση αυτή είναι ακόμη εντονότερη στις μικρομεσαίες επιχειρήσεις, οι οποίες αναφέρουν σε ακόμη μεγαλύτερο βαθμό δυσκολίες τόσο στην προσέλκυση όσο και στη διατήρηση κατάλληλου προσωπικού. Η εφαρμογή της NIS2 απαιτεί, πέρα από τεχνολογικές επενδύσεις, και στελέχη με επαρκή γνώση σε τομείς όπως η διαχείριση κινδύνων, η απόκριση σε περιστατικά, η παρακολούθηση συστημάτων και η κανονιστική προσαρμογή. Σε αρκετές περιπτώσεις, οι οργανισμοί δεν διαθέτουν το απαραίτητο εσωτερικό προσωπικό και αναγκάζονται είτε να επιβαρύνουν το ήδη υπάρχον προσωπικό είτε να προσφύγουν σε εξωτερικούς συμβούλους. Η δυσχέρεια αυτή γίνεται εντονότερη σε οργανισμούς με χαμηλότερο επίπεδο κυβερνοωριμότητας, όπου η εφαρμογή της Οδηγίας δεν στηρίζεται σε ήδη εδραιωμένες δομές και πρακτικές. Αντίστοιχες πιέσεις παρατηρούνται και στις αρμόδιες αρχές, οι οποίες χρειάζονται πρόσθετους πόρους και προσωπικό για να ανταποκριθούν στα αυξημένα καθήκοντα εποπτείας και υποστήριξης. Η τάση αυτή αποτυπώνεται και στη στελέχωση, καθώς το ανθρώπινο δυναμικό κυβερνοασφάλειας αντιστοιχεί πλέον μόλις στο 10,6% του συνολικού ανθρώπινου δυναμικού πληροφορικής.

Σημαντική διάσταση του προβλήματος αποτελεί και η εκπαίδευση. Η ουσιαστική εφαρμογή της NIS2 προϋποθέτει ανάπτυξη δεξιοτήτων, καλλιέργεια κατάλληλης κουλτούρας και συνεχή κατάρτιση του προσωπικού. Όταν δεν υπάρχουν επαρκή προγράμματα εκπαίδευσης και ευαισθητοποίησης, η έλλειψη τεχνογνωσίας διαιωνίζεται και η εφαρμογή των απαιτήσεων παραμένει τυπική ή αποσπασματική. Αντίστοιχα, σε επίπεδο τομέων και αρχών, η ενίσχυση της ωριμότητας συνδέεται και με την ανάγκη για περαιτέρω αναβάθμιση δεξιοτήτων και στοχευμένη υποστήριξη (Alkiviadis Giannakoulias, 2023; European Cyber Security Organisation, 2025; European Union Agency for Cybersecurity *κ.ά.*, 2025).

6.4. Τεχνική και Επιχειρησιακή Προσαρμογή

Η εφαρμογή της Οδηγίας NIS2 απαιτεί σημαντική τεχνική και επιχειρησιακή προσαρμογή από τους οργανισμούς που εμπίπτουν στο πεδίο εφαρμογής της. Η διαδικασία αυτή δεν εξελίσσεται υπό τις ίδιες συνθήκες για όλους. Ορισμένοι τομείς και οργανισμοί διαθέτουν

ήδη ώριμες δομές κυβερνοασφάλειας, ενώ άλλοι καλούνται να αναπτύξουν σε σύντομο χρονικό διάστημα δυνατότητες που μέχρι σήμερα δεν είχαν αναπτύξει συστηματικά. Η δυσκολία είναι εντονότερη σε τομείς με χαμηλότερο επίπεδο κυβερνοωριμότητας και σε οντότητες που εντάσσονται για πρώτη φορά στο κανονιστικό πεδίο της NIS2, χωρίς προηγούμενη εμπειρία από αντίστοιχες υποχρεώσεις.

Η τεχνική αυτή μετάβαση πραγματοποιείται συχνά πάνω σε υφιστάμενα πληροφοριακά και επιχειρησιακά περιβάλλοντα που χαρακτηρίζονται από πολυπλοκότητα, ετερογένεια και εξάρτηση από παλαιά ή παρωχημένα συστήματα (legacy systems), καθώς και τεχνολογίες που δεν σχεδιάστηκαν με σύγχρονες απαιτήσεις κυβερνοασφάλειας. Σε τέτοιες περιπτώσεις, η ενσωμάτωση νέων μέτρων ξεπερνά την απλή προσθήκη τεχνικών λύσεων και απαιτεί αναθεώρηση πρακτικών, αναπροσαρμογή διαδικασιών και συνεχή επιχειρησιακή υποστήριξη.

Η πρακτική αυτή δυσκολία επιβεβαιώνεται και από πρόσφατα ευρήματα, σύμφωνα με τα οποία οι μεγαλύτερες δυσκολίες στην εφαρμογή της NIS2 εντοπίζονται στη διαχείριση ευπαθειών και ενημερώσεων ασφαλείας, καθώς και στην επιχειρησιακή συνέχεια και αποκατάσταση μετά από καταστροφή. Παράλληλα, ως βασικό εμπόδιο αναφέρονται οι επιχειρησιακοί περιορισμοί που συνδέονται με παλαιότερα ή παρωχωμένα συστήματα και με τεχνολογίες επιχειρησιακής λειτουργίας (Operational Technology - OT), τα οποία δεν μπορούν εύκολα να ενημερωθούν ή να τεθούν εκτός λειτουργίας χωρίς να επηρεαστούν κρίσιμες λειτουργίες. Το ίδιο πρόβλημα εμφανίζεται και στην έγκαιρη εφαρμογή ενημερώσεων ασφάλειας (patching), καθώς και στις δοκιμές ασφάλειας. Σχεδόν το ένα τρίτο των οργανισμών δηλώνει ότι δεν έχει πραγματοποιήσει καμία μορφή αξιολόγησης ή δοκιμών κυβερνοασφάλειας κατά το προηγούμενο δωδεκάμηνο. Παράλληλα, σχεδόν τα δύο τρίτα χρειάζονται τουλάχιστον έναν μήνα για την εφαρμογή κρίσιμων ενημερώσεων ασφαλείας, ενώ περισσότερο από το ένα τέταρτο χρειάζεται πάνω από τρεις μήνες.

Η δυσκολία γίνεται ακόμη μεγαλύτερη σε τομείς με αυξημένη λειτουργική κρισιμότητα ή με αυστηρότερα επιχειρησιακά όρια. Σε ορισμένα περιβάλλοντα, όπως εκείνα που διέπονται ήδη από ειδικά τεχνικά ή τομεακά καθεστώτα, η εφαρμογή νέων μέτρων πρέπει να ευθυγραμμιστεί με προϋπάρχουσες απαιτήσεις ασφάλειας, επιχειρησιακής συνέχειας και κανονιστικής συμμόρφωσης. Η δυσκολία αυτή είναι ιδιαίτερα εμφανής στον τομέα της υγείας, όπου η μεγάλη ετερογένεια των φορέων, η εξάρτηση από παλαιά ή παρωχημένα συστήματα και η χρήση ιατρικών συσκευών με ανεπαρκή επίπεδα ασφάλειας δυσχεραίνουν την υιοθέτηση και αποτελεσματική εφαρμογή σύγχρονων μέτρων κυβερνοασφάλειας. Στον

ίδιο τομέα, έχουν επίσης επισημανθεί ασυνέπειες ως προς την επιχειρησιακή ετοιμότητα. Αυτό σημαίνει ότι οι οργανισμοί δεν καλούνται μόνο να υιοθετήσουν νέα μέτρα, αλλά και να τα εντάξουν σε σύνθετα λειτουργικά περιβάλλοντα χωρίς να διαταράξουν κρίσιμες λειτουργίες.

Η τεχνική και επιχειρησιακή προσαρμογή αποτελεί μία από τις βασικές δυσκολίες εφαρμογής της NIS2. Η αποτελεσματική υλοποίηση εξαρτάται όχι μόνο από την ύπαρξη τεχνικών μέτρων, αλλά και από τη δυνατότητα του οργανισμού να τα ενσωματώσει σταθερά στην καθημερινή του λειτουργία, έτσι ώστε να ανταποκρίνεται στις ιδιαίτερες τεχνολογικές και επιχειρησιακές συνθήκες κάθε τομέα (Alkiviadis Giannakoulias, 2023; European Cyber Security Organisation, 2025; European Union Agency for Cybersecurity., 2025; European Union Agency for Cybersecurity *κ.ά.*, 2025).

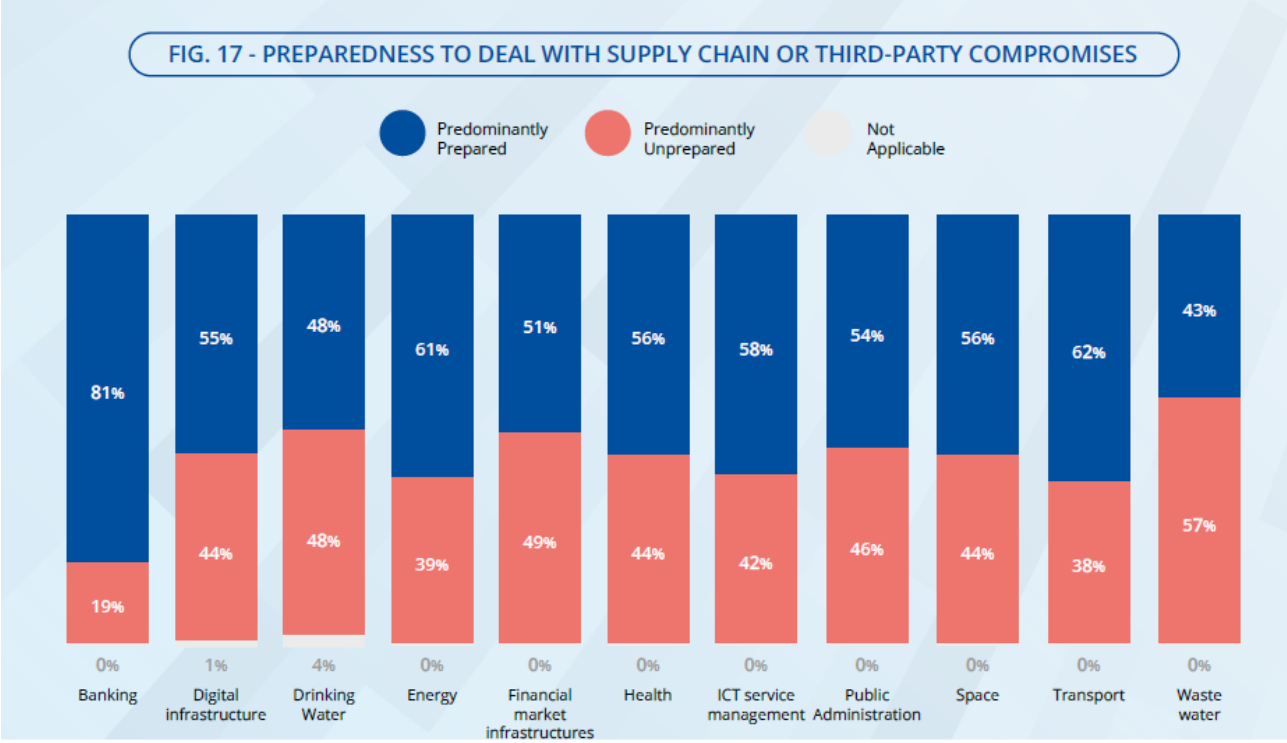
6.5. Εφοδιαστική Αλυσίδα και Τρίτα Μέρη

Η ασφάλεια της εφοδιαστικής αλυσίδας αποτελεί μία από τις πιο σύνθετες προκλήσεις εφαρμογής της Οδηγίας NIS2. Η δυσκολία δεν περιορίζεται στην υιοθέτηση εσωτερικών μέτρων από τον ίδιο τον οργανισμό, αλλά επεκτείνεται και στην ανάγκη αξιολόγησης της ασφάλειας προμηθευτών, παρόχων υπηρεσιών και λοιπών τρίτων μερών από τα οποία αυτός εξαρτάται. Στην πράξη, οι οργανισμοί καλούνται να διασφαλίσουν ότι οι συνεργάτες τους τηρούν επαρκές επίπεδο κυβερνοασφάλειας, χωρίς όμως να είναι πάντοτε σαφές μέχρι ποιο σημείο εκτείνεται η ευθύνη και η δυνατότητα ελέγχου του ίδιου του οργανισμού. Η αβεβαιότητα αυτή εντείνεται από την πολυπλοκότητα των σύγχρονων αλυσίδων εφοδιασμού, από την περιορισμένη ορατότητα στους υπεργολάβους ή προμηθευτές και από τη δυσκολία ουσιαστικής επαλήθευσης των σχετικών πρακτικών ασφάλειας.

Παρά τις δυσχέρειες αυτές, πολλοί οργανισμοί επιχειρούν να ενισχύσουν τον έλεγχο της εφοδιαστικής αλυσίδας μέσω απαιτήσεων συμμόρφωσης με πρότυπα ασφάλειας, αξιολογήσεων ή ελέγχων προμηθευτών και συμβατικών ρητρών κυβερνοασφάλειας. Ωστόσο, η αυξανόμενη εξάρτηση από εξωτερικές υπηρεσίες ΤΠΕ και από εξειδικευμένους παρόχους κυβερνοασφάλειας δημιουργεί νέα επίπεδα εξάρτησης και νέες πηγές έκθεσης σε κινδύνους. Οι δυσκολίες γίνονται ακόμη μεγαλύτερες όταν στην αλυσίδα συμμετέχουν μικρότεροι πάροχοι ή επιχειρήσεις με περιορισμένους πόρους, καθώς οι οργανισμοί που υπάγονται στην NIS2 μπορεί να επιβάλλουν σε αυτούς αυξημένες απαιτήσεις ασφάλειας, ακόμη και όταν οι ίδιοι δεν υπάγονται άμεσα στο πεδίο εφαρμογής της Οδηγίας. Ιδιαίτερη

προσοχή απαιτείται και στην περίπτωση παρόχων διαχειριζόμενων υπηρεσιών (Managed Service Providers – MSPs) και διαχειριζόμενων υπηρεσιών ασφάλειας (Managed Security Service Providers – MSSPs), οι οποίοι λειτουργούν συχνά ως κρίσιμοι τρίτοι πάροχοι για πολλούς οργανισμούς ταυτόχρονα.

Η άνιση αυτή ετοιμότητα αποτυπώνεται και στην εικόνα 13, όπου φαίνεται ότι η ικανότητα αντιμετώπισης περιστατικών που σχετίζονται με την εφοδιαστική αλυσίδα και με παραβιάσεις προμηθευτών ή τρίτων παρόχων διαφέρει αισθητά μεταξύ των τομέων:



Εικόνα 13 - Ετοιμότητα αντιμετώπισης περιστατικών εφοδιαστικής αλυσίδας και παραβιάσεων τρίτων παρόχων (European Union Agency for Cybersecurity κ.ά., 2025)

Η εικόνα αυτή δείχνει ότι, παρά τη σταδιακή ενίσχυση των σχετικών ελέγχων, η οργανωτική και επιχειρησιακή ετοιμότητα παραμένει άνιση. Σε αρκετούς τομείς, σημαντικό ποσοστό οργανισμών δηλώνει ότι δεν θεωρείται επαρκώς προετοιμασμένο για την αντιμετώπιση περιστατικών που προέρχονται από την εφοδιαστική αλυσίδα ή από τρίτα μέρη(European Cyber Security Organisation, 2025; European Union Agency for Cybersecurity., 2025; European Union Agency for Cybersecurity *κ.ά.*, 2025).

6.6. Αναφορά Περιστατικών και Λειτουργική Συνέπεια

Η αναφορά περιστατικών αποτελεί μία από τις πιο απαιτητικές πτυχές της εφαρμογής της Οδηγίας NIS2, όχι μόνο λόγω της κανονιστικής της βαρύτητας, αλλά και λόγω της επιχειρησιακής ετοιμότητας που προϋποθέτει. Στην πράξη, οι οργανισμοί δεν καλούνται απλώς να τηρήσουν συγκεκριμένες προθεσμίες, αλλά να αναγνωρίζουν έγκαιρα ένα περιστατικό, να αξιολογούν τη σοβαρότητά του και να ενεργοποιούν αξιόπιστα εσωτερικές διαδικασίες αναφοράς και κλιμάκωσης. Η δυσκολία αυτή εντείνεται από τις αποκλίσεις που παρατηρούνται μεταξύ κρατών ως προς τα χρονοδιαγράμματα, τα κριτήρια ενεργοποίησης της υποχρέωσης αναφοράς και το εύρος των περιστατικών που θεωρούνται αναφερόμενα, γεγονός που καθιστά την ομοιόμορφη εφαρμογή ιδιαίτερα απαιτητική, ιδίως για οργανισμούς με διασυνοριακή παρουσία.

Η λειτουργική αυτή δυσκολία συνδέεται άμεσα με τον εσωτερικό συντονισμό του οργανισμού. Η έγκαιρη και συνεπής αναφορά ενός περιστατικού απαιτεί συνεργασία μεταξύ πληροφορικής, ασφάλειας, νομικού τμήματος και επιχειρησιακών μονάδων, ώστε να υπάρχει κοινή κατανόηση του συμβάντος, επαρκής συλλογή πληροφοριών και σαφής κατανομή αρμοδιοτήτων. Όταν ο συντονισμός αυτός είναι ελλιπής, αυξάνεται ο κίνδυνος καθυστέρησης, ελλιπούς αξιολόγησης ή ασυνέπειας μεταξύ εσωτερικής διαχείρισης και εξωτερικής αναφοράς. Η δυσκολία αυτή επιβεβαιώνεται και από ευρύτερα ευρήματα, σύμφωνα με τα οποία ο χειρισμός περιστατικών εξακολουθεί να συγκαταλέγεται στις δυσκολότερες απαιτήσεις εφαρμογής. Την ίδια στιγμή, περιορισμένος αριθμός οργανισμών αναφέρει βελτίωση στην ταχύτερη ανίχνευση ή στην ενίσχυση των δυνατοτήτων απόκρισης και ανάκαμψης.

Η αποτελεσματικότητα της αναφοράς περιστατικών εξαρτάται, όμως, και από την επάρκεια των αρμόδιων δομών που τη δέχονται και τη διαχειρίζονται. Η διεύρυνση του πεδίου εφαρμογής της NIS2 και η αύξηση των υποχρεώσεων αναφοράς δημιουργούν πρόσθετες απαιτήσεις για τις αρμόδιες αρχές και τα CSIRTs, τόσο σε ανθρώπινους πόρους όσο και σε τεχνικές δυνατότητες. Έχει εκτιμηθεί, μάλιστα, ότι μόνο για τη διαχείριση της αναφοράς περιστατικών απαιτείται αισθητή ενίσχυση του προσωπικού των αρμόδιων αρχών, ενώ η ευρύτητα της ίδιας της έννοιας του «περιστατικού» καθιστά αναγκαία τη χρήση συστημάτων ταξινόμησης, τυποποιημένων διαδικασιών και σταθερών μηχανισμών ανταλλαγής πληροφοριών. Υπό αυτή την έννοια, η λειτουργική συνέπεια στην αναφορά περιστατικών δεν εξαρτάται μόνο από τις υποχρεώσεις των οργανισμών, αλλά και από το

κατά πόσο το ευρύτερο οικοσύστημα απόκρισης διαθέτει επαρκή οργάνωση, κοινές πρακτικές και σαφείς διαύλους επικοινωνίας.

Το πρόβλημα αυτό γίνεται ακόμη πιο εμφανές σε τομείς που βρίσκονται σε πρώιμο στάδιο ωρίμανσης. Στον δημόσιο τομέα, για παράδειγμα, παρότι η ψηφιοποίηση έχει ενισχυθεί και οι επενδύσεις στην ασφάλεια είναι αξιοσημείωτες, μόνο ένα μέρος των φορέων αναπτύσσει ενεργά σχέδια, πολιτικές, διαδικασίες και εκπαιδεύσεις που ενισχύουν την ετοιμότητα, ενώ η συμμετοχή σε εθνικές ασκήσεις κυβερνοασφάλειας παραμένει χαμηλή. Απαιτούνται δοκιμασμένες διαδικασίες, ασκήσεις, σαφέστερη καθοδήγηση και ισχυρότεροι μηχανισμοί συνεργασίας και ανταλλαγής πληροφοριών (Alkiviadis Giannakoulias, 2023; European Cyber Security Organisation, 2025; European Union Agency for Cybersecurity., 2025; European Union Agency for Cybersecurity *κ.ά.*, 2025).

7. ΣΥΜΠΕΡΑΣΜΑΤΑ

Η παρούσα εργασία εξέτασε την Οδηγία NIS2 ως πλαίσιο εφαρμογής, ελέγχων και συμμόρφωσης σε επίπεδο οργανισμού. Η συνολική ανάλυση έδειξε ότι η Οδηγία εισάγει ένα απαιτητικό και πολυεπίπεδο σύνολο υποχρεώσεων, το οποίο επηρεάζει τη διακυβέρνηση, τη διαχείριση κινδύνων, την οργανωτική προετοιμασία και τη λειτουργική ετοιμότητα των οργανισμών. Η συμμόρφωση με τη NIS2 συνδέεται άμεσα με την ικανότητα κάθε οργανισμού να μεταφέρει τις κανονιστικές απαιτήσεις σε σαφείς διαδικασίες, τεκμηριωμένες πρακτικές και σταθερούς μηχανισμούς παρακολούθησης.

Αρχικά, η εξέταση του νομικού και ρυθμιστικού πλαισίου ανέδειξε ότι η θέσπιση της Οδηγίας NIS2 συνδέεται άμεσα με τις αδυναμίες που εμφάνισε η εφαρμογή της προηγούμενης Οδηγίας NIS, ιδίως ως προς τον κατακερματισμό του πεδίου εφαρμογής και την ανομοιομορφία των εθνικών προσεγγίσεων. Η NIS2 επιδίωξε να περιορίσει αυτά τα κενά μέσω ενός σαφέστερου και αυστηρότερου κανονιστικού πλαισίου, με διευρυμένο πεδίο εφαρμογής, νέα κατηγοριοποίηση των οντοτήτων σε βασικές και σημαντικές, ενισχυμένες απαιτήσεις θεσμικής διακυβέρνησης και πιο οργανωμένους μηχανισμούς εποπτείας και επιβολής. Από την ανάλυση αυτή προκύπτει ότι το νέο πλαίσιο αποδίδει στην κυβερνοασφάλεια σταθερή θέση στη λειτουργία και στη διοίκηση των οργανισμών, συνδέοντάς την με ζητήματα ευθύνης, ετοιμότητας και θεσμικού συντονισμού.

Στη συνέχεια, η εξέταση του πλαισίου εφαρμογής ανέδειξε ότι η προσαρμογή στις απαιτήσεις της NIS2 ακολουθεί μια διαρκή διαδικασία. Η διαδικασία αυτή περιλαμβάνει προετοιμασία, διαμόρφωση πολιτικών ασφάλειας, αποτίμηση κινδύνων, επιλογή και υλοποίηση μέτρων, καθώς και συνεχή παρακολούθηση της αποτελεσματικότητάς τους. Έγινε επίσης σαφές ότι η εφαρμογή της Οδηγίας βασίζεται στη λογική της διαχείρισης κινδύνων, αφού τα μέτρα προσδιορίζονται με βάση τις ανάγκες, τις αδυναμίες και το επίπεδο έκθεσης κάθε οργανισμού. Η συμμετοχή της διοίκησης έχει ιδιαίτερη βαρύτητα σε όλα τα στάδια αυτής της πορείας.

Η ανάλυση του πλαισίου ελέγχων και συμμόρφωσης ανέδειξε επίσης τη σημασία του ελέγχου ως βασικού στοιχείου της συνολικής εφαρμογής της NIS2. Οι έλεγχοι συμβάλλουν στην αποτίμηση του βαθμού ετοιμότητας, στην αναγνώριση αδυναμιών, στην αξιολόγηση του επιπέδου συμμόρφωσης και στον σχεδιασμό διορθωτικών ενεργειών. Η σύνδεση της NIS2 με πρότυπα όπως το ISO/IEC 27001 ανέδειξε τη χρησιμότητα υφιστάμενων μεθοδολογικών εργαλείων για την οργάνωση των σχετικών διαδικασιών. Ταυτόχρονα, έγινε

σαφές ότι η αξιοποίηση του συγκεκριμένου προτύπου μπορεί να υποστηρίξει τη συμμόρφωση με τη NIS2, παρότι δεν την καλύπτει πλήρως. Η επένδυση στην κυβερνοασφάλεια συνδέεται με βελτίωση των διαδικασιών διαχείρισης κινδύνων, πιο έγκαιρη ανίχνευση περιστατικών και ενίσχυση των δυνατοτήτων απόκρισης και αποκατάστασης.

Ιδιαίτερη σημασία είχαν και τα συμπεράσματα που προέκυψαν από την εξέταση των προκλήσεων εφαρμογής. Η κανονιστική και ερμηνευτική αβεβαιότητα, οι διαφορές στην οργανωτική και διοικητική ετοιμότητα, οι περιορισμοί σε πόρους και ανθρώπινο δυναμικό, οι απαιτήσεις τεχνικής και επιχειρησιακής προσαρμογής, καθώς και οι εξαρτήσεις από την εφοδιαστική αλυσίδα και τα τρίτα μέρη, συγκροτούν ένα σύνθετο περιβάλλον συμμόρφωσης. Η εφαρμογή της NIS2 συνδέεται έτσι με τον βαθμό οργανωτικής ωρίμανσης κάθε φορέα, με την ποιότητα του εσωτερικού συντονισμού και με τη δυνατότητα σταθερής προσαρμογής σε εξελισσόμενους κινδύνους.

ΣΥΝΤΟΜΕΥΣΕΙΣ – ΑΡΚΤΙΚΟΛΕΞΑ – ΑΚΡΩΝΥΜΙΑ

CER	Critical Entities Resilience
CSIRT	Computer Security Incident Response Team
DCMS	Department for Digital, Culture, Media & Sport
DNS	Domain Name System
DORA	Digital Operational Resilience Act
EE	European Union
eIDAS	electronic Identification, Authentication and Trust Services
GDPR	General Data Protection Regulation
IEC	International Electrotechnical Commission
ISMS	Information Security Management System
ISO	International Organization for Standardization
MSP	Managed Service Provider
MSSP	Managed Secyrity Service Provider
NCSA	National Cybersecurity Authority
NIS	Network and Information Systems
OT	Operational Technology
SPOC	Single Point of Contact
TLD	Top-Level Domain
ΕΑΚ	Εθνική Αρχή Κυβερνοασφάλειας
ΕΕ	Ευρωπαϊκή Ένωση
ΜμΕ	Πολύ μικρές, μικρές και μεσαίες επιχειρήσεις
ΣΕΒ	Σύνδεσμος Επιχειρήσεων και Βιομηχανιών
ΤΠΕ	Τεχνολογίες Πληροφορικής και Επικοινωνιών

ΒΙΒΛΙΟΓΡΑΦΙΚΕΣ ΑΝΑΦΟΡΕΣ

[1] Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης (2016) *Οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 6ης Ιουλίου 2016, σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση*, *OJ L 194*. Διαθέσιμο στο: http://data.europa.eu/eli/dir/2016/1148/oj.

[2] Αθήνα: Εθνικό Τυπογραφείο (2018) *Ν. 4577/2018 Ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας 2016/1148/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση και άλλες διατάξεις.*, *ΦΕΚ 199/Α/03-12-2018*. Διαθέσιμο στο: https://www.mindigital.gr/wp-content/uploads/2019/09/N.4577_2018.pdf.

[3] Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης (2022) *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, την τροποποίηση του κανονισμού (ΕΕ) αριθ. 910/2014 και της οδηγίας (ΕΕ) 2018/1972, και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148 (οδηγία NIS 2) (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ)*, *OJ L 333*. Διαθέσιμο στο: http://data.europa.eu/eli/dir/2022/2555/oj.

[4] Αθήνα: Εθνικό Τυπογραφείο (2024) *Ν. 5160/2024 Ενσωμάτωση της Οδηγίας (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, την τροποποίηση του Κανονισμού (ΕΕ) 910/2014 και της Οδηγίας (ΕΕ) 2018/1972, και την κατάργηση της Οδηγίας (ΕΕ) 2016/1148 (Οδηγία NIS 2) και άλλες διατάξεις.*, *ΦΕΚ 195/Α/27-11-2024*. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=NIM:202405334.

[5] Anna Zygierewicz (2020) *Directive on security of network and information systems (NIS Directive)*. Briefing. European Parliament. Διαθέσιμο στο: https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/654198/EPRS_BRI(2020)654198_EN.pdf.

[6] Αλεξάνδρα Εξάρχου (2024) *Ευρωπαϊκή Οδηγία (ΕΕ) NIS2 2022/2555*. Master Thesis. Πανεπιστήμιο Πειραιώς. Διαθέσιμο στο: https://dione.lib.unipi.gr/xmlui/handle/unipi/17947.

[7] Άννα Πέλλα (2025) *Πλαίσιο εφαρμογής της Οδηγίας (ΕΕ) NIS2 2022/2555*. Master Thesis. Πανεπιστήμιο Πειραιώς. Διαθέσιμο στο: https://dione.lib.unipi.gr/xmlui/handle/unipi/17868.

[8] Christos Venizelos (2022) *Security Controls and Security Standards: Correlations and Synergies*. Master Thesis. Πανεπιστήμιο Πειραιώς. Διαθέσιμο στο: https://dione.lib.unipi.gr/xmlui/handle/unipi/14555.

[9] European Commission (2018) *Directive on Security of Network and Information systems, the first EU-wide legislation on cybersecurity*, *European Commission - European Commission*. Διαθέσιμο στο: https://ec.europa.eu/commission/presscorner/detail/en/memo_18_3651.

[10] European Commission (2023) *Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) - FAQs | Shaping Europe's digital future*. Διαθέσιμο στο: https://digital-strategy.ec.europa.eu/en/faqs/directive-measures-high-common-level-cybersecurity-across-union-nis2-directive-faqs.

[11] ΣΕΒ σύνδεσμος επιχειρήσεων και βιομηχανιών - Τομέας Τεχνολογίας & Ψηφιακού Μετασχηματισμού (2025) 'ΟΔΗΓΟΣ για τη Συμμόρφωση των Επιχειρήσεων με τον Ν. 5160/2024 και την Οδηγία NIS2'. Διαθέσιμο στο: https://www.sev.org.gr/wp-content/uploads/2025/10/ODHGOS_KYBERNOASFALEIAS_FINAL_04.pdf.

[12] Puppet by Perforce (χ.χ.) *How to Use Policy as Code for Easier NIS2 Compliance at Enterprise Scale*. White Paper. Διαθέσιμο στο: https://www.puppet.com/resources/nis2-compliance-guide.

[13] Piggin, R. (2018) 'Securing Critical Services', *ITNOW*, 60(2), σελ. 58–61. Διαθέσιμο στο: https://doi.org/10.1093/itnow/bwy057.

[14] Καλαντζής, Π. (2024) 'NIS2 – Απαιτήσεις για συμμόρφωση, προκλήσεις και ευκαιρίες', Μάιος, σελ. 32–40.

[15] Εθνική Αρχή Κυβερνοασφάλειας (2025) 'Εθνική Στρατηγική Κυβερνοασφάλειας 2026 – 2030'. Διαθέσιμο στο: https://cyber.gov.gr/wp-content/uploads/2025/12/%CE%95%CE%A3%CE%9A-2026-2030.pdf.

[16] Εθνική Αρχή Κυβερνοασφάλειας (2024) 'Η Οδηγία NIS2 στην Ελλάδα'. Διαθέσιμο στο: https://cyber.gov.gr/wp-content/uploads/2025/03/250323_%CE%9F%CE%B4%CE%B7%CE%B3%CF%8C%CF%82-%CE%91%CE%BD%CE%B1%CF%86%CE%BF%CF%81%CE%AC%CF%82-%CE%9D.-5160_2024-1.pdf.

[17] Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης (2022) *Οδηγία (ΕΕ) 2022/2557 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 14ης Δεκεμβρίου 2022 για την ανθεκτικότητα των κρίσιμων οντοτήτων και την κατάργηση της οδηγίας 2008/114/ΕΚ του Συμβουλίου (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ)*, *OJ L*. Διαθέσιμο στο: http://data.europa.eu/eli/dir/2022/2557/oj.

[18] Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της Ευρωπαϊκής Ένωσης (2022) *Κανονισμός (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 14ης Δεκεμβρίου 2022 σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα και την τροποποίηση των κανονισμών (ΕΚ) αριθ. 1060/2009, (ΕΕ) αριθ. 648/2012, (ΕΕ) αριθ. 600/2014, (ΕΕ) αριθ. 909/2014 και (ΕΕ) 2016/1011 (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ)*, *OJ L*. Διαθέσιμο στο: http://data.europa.eu/eli/reg/2022/2554/oj.

[19] Ευρωπαϊκή Επιτροπή (2003) *Σύσταση της Επιτροπής, της 6ης Μαΐου 2003, σχετικά με τον ορισμό των πολύ μικρών, των μικρών και των μεσαίων επιχειρήσεων*, *32003H0361*. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/ALL/?uri=celex:32003H0361.

[20] National Cyber Security Centre (2025) 'NIS 2 Risk Management Measures Guidance'. Διαθέσιμο στο: https://www.ncsc.gov.ie/pdfs/NIS2_Draft_Risk_Management_Measures_Guidance.pdf.

[21] Αρχή Ψηφιακής Ασφάλειας (2024) 'ΣΥΝΟΠΤΙΚΟΣ ΟΔΗΓΟΣ ΑΝΑΦΟΡΙΚΑ ΜΕΤΗΝ ΟΔΗΓΙΑ NIS2'. Διαθέσιμο στο: https://dsa.cy/images/pdf-upload/nis2-guide.pdf.

[22] European Union Agency for Cybersecurity. (2025) Technical implementation guidance on Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of NIS2 Directive as regards technical and methodological requirements of cybersecurity risk-management measures: June 2025, version 1.0. LU: Publications Office. Διαθέσιμο στο: https://data.europa.eu/doi/10.2824/2702548.

[23] Κωτσικοπούλου, Μ. (2025) 'Σε ισχύ το νέο Εργαλείο Αξιολόγησης Συμμόρφωσης Οντοτήτων με τον ν. 5160/2024 -Μ. Μπλέτσας «Θεσπίζουμε το κανονιστικό πλαίσιο ενίσχυσης της κυβερνοανθεκτικότητας»', Εθνική Αρχή Κυβερνοασφάλειας, 10 Σεπτέμβριος. Διαθέσιμο στο: https://cyber.gov.gr/se-ischy-to-neo-ergaleio-axiologisis-symmorfosis-ontotiton-me-ton-n-5160-2024-m-mpletsas-thespizoyme-to-kanonistiko-plaisio-enischysis-tis-kyvernoanthektikotitas/.

[24] Advisera (2024) 'NIS2 Gap Analysis [Free Tool] | Advisera', 4 Οκτώβριος. Διαθέσιμο στο: https://advisera.com/tools/nis-2-gap-analysis-tool/.

[25] Commugen (χ.χ.) 'A CISO's Essential NIS2 Guide'. Διαθέσιμο στο: https://cyber.commugen.com/submit-nis2.

[26] Kosutic, D. (2024) 'NIS2 compliance: 16 steps for cybersecurity risk management measures', 22 Ιανουάριος. Διαθέσιμο στο: https://advisera.com/articles/nis2-implementation-steps/.

[27] ISO/IEC (2022a) 'Information security, cybersecurity and privacy protection — Information security controls'. Διαθέσιμο στο: https://www.iso.org/standard/75652.html.

[28] ISO/IEC (2022b) 'Information security, cybersecurity and privacy protection — Information security management systems — Requirements'. Διαθέσιμο στο: https://www.iso.org/standard/27001.

[29] CYBERDAY (χ.χ.) *NIS2 ready with ISO 27001'S best practices*. Διαθέσιμο στο: https://www.cyberday.ai/guides/nis2-ebook.

[30] European Network and Information Security Agency . (2013) Schemes for auditing security measures: an overview. LU: Publications Office. Διαθέσιμο στο: https://data.europa.eu/doi/10.2824/23801.

[31] ISO/IEC (2018) 'Guidelines for auditing management systems'. Διαθέσιμο στο: https://www.iso.org/standard/27001.

[32] Advisera (χ.χ.) 'Κατευθυντήριες Οδηγίες εφαρμογής της Οδηγίας NIS 2 2022/2555 και του Ν. 5160/2024'.

[33] BSI group (χ.χ.) 'NIS2 to ISO/IEC 27001 Mapping Tool'. Διαθέσιμο στο: https://www.bsigroup.com/globalassets/localfiles/de-de/isoiec-27001/ressourcen/bsi-ce-nis2-mapping-tool-de-de-en.pdf.

[34] Jessica Marban (2025) From ISO 27001:2022 to NIS2 - Identifying Gaps and Overlaps. Master Thesis. University of Applied Sciences FH Campus Wien. Διαθέσιμο στο: https://pub.hcw.ac.at/obvfcwhsacc/content/titleinfo/12164753/full.pdf.

[35] Yli-Karro, V. (2025) Ensuring NIS 2 compliance in an ISO/IEC 27001 certified organization: Master Thesis. Tampere University. Διαθέσιμο στο: https://trepo.tuni.fi/bitstream/handle/10024/205043/Yli-KarroValtteri.pdf.

[36] Andrew Bowo (2025) Adapting Cybersecurity Frameworks for NIS2 Compliance. Master Thesis. University of Turku. Διαθέσιμο στο: https://www.utupub.fi/bitstream/handle/10024/181351/Bowo_Andrew_Thesis.pdf.

[37] TXOne Networks (2023) 'Mastering the NIS2 Directive: Achieving Cybersecurity Compliance'. Διαθέσιμο στο: https://www.txone.com/white-papers/mastering-nis2-directive/.

[38] European Cyber Security Organisation (2025) 'NIS2 Implementation: Challenges and Priorities'. Διαθέσιμο στο: https://ecs-org.eu/?publications=white-paper-nis2-implementation-challenges-and-priorities.

[39] Βασιλειάδης Δημήτριος (2025) Η Οδηγία NIS2: Η Περίπτωση των Περιφερειακών Αυτοδιοικήσεων. Master Thesis. Πανεπιστήμιο Δυτικής Αττικής. Διαθέσιμο στο: https://polynoe.lib.uniwa.gr/xmlui/handle/11400/9317.

[40] Alkiviadis Giannakoulias (2023) NIS 2 Directive: Implications for System and Infrastructure Security. Master Thesis. University of Piraeus. Διαθέσιμο στο: https://dione.lib.unipi.gr/xmlui/handle/unipi/15207.

[41] European Union Agency for Cybersecurity. (2025) ENISA NIS360 2024: ENISA cybersecurity maturity & criticality assessment of NIS2 sectors. LU: Publications Office. Διαθέσιμο στο: https://doi.org/10.2824/1378797.

[42] European Union Agency for Cybersecurity κ.ά. (2025) NIS investments 2025. GR: European Union Agency for Cybersecurity (NIS investments). Διαθέσιμο στο: https://doi.org/10.2824/7442427.