EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ΕΘΝΙΚΟ ΠΛΑΙΣΙΟ ΑΞΙΟΛΟΓΗΣΗΣ ΙΚΑΝΟΤΗΤΩΝ

ΔΕΚΕΜΒΡΙΟΣ 2020

ΠΛΗΡΟΦΟΡΙΕΣ ΓΙΑ ΤΟΝ ENISA

Ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια, ο ENISA, είναι ο οργανισμός της Ένωσης που αποσκοπεί να διασφαλίσει υψηλό, κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ευρώπη. Ο Οργανισμός της ΕΕ για την Κυβερνοασφάλεια, που ιδρύθηκε το 2004 και ενισχύθηκε από την Πράξη της ΕΕ για την ασφάλεια στον κυβερνοχώρο, συμβάλλει στη χάραξη της πολιτικής της ΕΕ στον τομέα του κυβερνοχώρου, ενισχύει την αξιοπιστία των προϊόντων, υπηρεσιών και διαδικασιών ΤΠΕ με συστήματα πιστοποίησης της κυβερνοασφάλειας, συνεργάζεται με κράτη μέλη και φορείς της ΕΕ και βοηθά την Ευρώπη να προετοιμαστεί για τις μελλοντικές προκλήσεις στον κυβερνοχώρο. Μέσω της ανταλλαγής γνώσεων, της δημιουργίας ικανοτήτων και της ευαισθητοποίησης, ο Οργανισμός συνεργάζεται με τους βασικούς ενδιαφερόμενους φορείς για την ενίσχυση της εμπιστοσύνης στη συνδεδεμένη οικονομία, την υποστήριξη της ανθεκτικότητας των υποδομών της Ένωσης και, τελικά, τη διατήρηση της ψηφιακής ασφάλειας για την κοινωνία και τους πολίτες της Ευρώπης. Για περισσότερες πληροφορίες επισκεφθείτε τη διεύθυνση www.enisa.europa.eu.

ΕΠΙΚΟΙΝΩΝΙΑ

Για να επικοινωνήσετε με τους συντάκτες παρακαλούμε χρησιμοποιήστε τη διεύθυνση team@enisa.europa.eu.
Για πληροφορίες σχετικά με το παρόν έγγραφο, ανατρέξτε στη διεύθυνση press@enisa.europa.eu.

ΣΥΝΤΑΚΤΕΣ

Άννα Σαρρή, Πηνελόπη Κυρανούδη – Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA)
Aude Thirriot, Federico Charelli, Yang Dominique - Wavestone

ΕΥΧΑΡΙΣΤΙΕΣ

Ο ENISA θα ήθελε να ευχαριστήσει και να αναγνωρίσει τη συμβολή όλων των εμπειρογνωμόνων που συμμετείχαν και παρείχαν πολύτιμες πληροφορίες για την παρούσα έκθεση και ιδιαίτερα τους ακόλουθους, με αλφαβητική σειρά:

Διοικητική αρχή ασφάλειας των πληροφοριών (δημοκρατία της Σλοβενίας), Marjan Kavčič

Εθνική Αρχή Ασφαλείας (Σλοβακία)

Εθνική υπηρεσία για την ασφάλεια στον κυβερνοχώρο και την ασφάλεια των πληροφοριών (Τσεχική Δημοκρατία), Veronika Netolická

Εθνικό κέντρο της Πορτογαλίας για την ασφάλεια στον κυβερνοχώρο (Πορτογαλία), Alexandre Leite και Pedro Matos

Ευρωπαϊκό Κέντρο για τα εγκλήματα στον κυβερνοχώρο - EC3, Adrian-Ionut Bobeica

Ευρωπαϊκό Κέντρο για τα εγκλήματα στον κυβερνοχώρο - EC3, Alzofra Martinez Alvaro

Ιταλική κυβέρνηση (Ιταλία)

Κεντρική κρατική υπηρεσία για την Ανάπτυξη της Ψηφιακής Κοινωνίας (Ουγγαρία), Marin Ante Pivcevic

Κέντρο για την ασφάλεια στον κυβερνοχώρο (Βέλγιο)

Κέντρο Κυβερνοασφάλειας (CFCS – Center for Cybersikkerhed) (Δανία), Thomas Wulff

Ομοσπονδιακό Υπουργείο Εσωτερικών (Γερμανία), Sascha-Alexander Lettgen

Πανεπιστήμιο της Οξφόρδης - Παγκόσμιο Κέντρο Ικανοτήτων για την ασφάλεια στον κυβερνοχώρο, Carolin Weisser Harris

Τμήμα Εθνικής Ασφάλειας (Ισπανία), Maria Mar Lopez Gil

Τμήμα πολιτικής για την ασφάλεια στον κυβερνοχώρο, Τμήμα Περιβάλλοντος, Κλίματος και Επικοινωνιών (Ιρλανδία), James Caffrey

Υπηρεσία τεχνολογίας πληροφοριών Μάλτας (Μάλτα) Katia Bonello και Martin Camilleri

Υπουργείο Δικαιοσύνης και Ασφάλειας, NCTV (Κάτω Χώρες)

Υπουργείο Δικαιοσύνης και Δημόσιας Ασφάλειας (Νορβηγία), Robin Bakke

Υπουργείο Οικονομικών Υποθέσεων και Επικοινωνιών (Εσθονία), Anna-Liisa Pärnalaas

Υπουργείο Ψηφιακής Πολιτικής (Ελλάδα), Γιώργος Δρίβας, Νέστορας Χουλιάρας, Ευγενία Τσαπράλη και Σωτήρης Βασίλειος

Ο ENISA θα ήθελε επίσης να ευχαριστήσει όλους τους εμπειρογνώμονες που παρείχαν πληροφορίες και συνέβαλαν στην παρούσα μελέτη, αλλά προτίμησαν να παραμείνουν ανώνυμοι.

ΝΟΜΙΚΗ ΓΝΩΣΤΟΠΟΙΗΣΗ

ΔΗΛΩΣΗ ΠΕΡΙ ΠΝΕΥΜΑΤΙΚΗΣ ΙΔΙΟΚΤΗΣΙΑΣ

ISBN: 978-92-9204-474-9

DOI: 10.2824/562580

ΚΑΤΑΛΟΓΟΣ: TP-02-21-253-EL-N

1. ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΓΛΩΣΣΑΡΙΟ ΟΡΩΝ

ΑΚΡΩΝΥΜΙΟ	ΟΡΙΣΜΟΣ
C2M2	Μοντέλο ωριμότητας ικανοτήτων ασφάλειας στον κυβερνοχώρο
CCRA	Συμφωνία για την αναγνώριση κοινών κριτηρίων
CCSMM	Το κοινοτικό μοντέλο ωριμότητας ασφάλειας στον κυβερνοχώρο
CMM	Εθνικό μοντέλο ωριμότητας ικανοτήτων ασφάλειας στον κυβερνοχώρο
CMMC	Πιστοποίηση μοντέλου ωριμότητας ασφάλειας στον κυβερνοχώρο
CPI	Δείκτης ισχύος κυβερνοχώρου
CSIRT	Ομάδες παρέμβασης για συμβάντα που αφορούν την ασφάλεια υπολογιστών
CVD	Συντονισμένη δημοσιοποίηση τρωτών σημείων
ECCG	Ευρωπαϊκή ομάδα πιστοποίησης ασφάλειας στον κυβερνοχώρο
ECSM	Ευρωπαϊκός Μήνας για την Ασφάλεια στον Κυβερνοχώρο
ECSO	Ευρωπαϊκός Οργανισμός για την Ασφάλεια στον Κυβερνοχώρο
GCI	Παγκόσμιος δείκτης ασφάλειας στον κυβερνοχώρο
GDS	Κρατική ψηφιακή υπηρεσία
IA-CM	Μοντέλο μονάδας εσωτερικού ελέγχου για τον δημόσιο τομέα
ISMM	Μοντέλο ωριμότητας ασφάλειας των πληροφοριών για το πλαίσιο ασφάλειας στον κυβερνοχώρο του NIST
NIST	Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας
NLO	Εθνικοί υπάλληλοι-σύνδεσμοι
PIMS:	Σύστημα διαχείρισης πληροφοριών ιδιωτικής ζωής
Q-C2M2	Πρότυπο ωριμότητας δυνατοτήτων του Κατάρ για την ασφάλεια στον κυβερνοχώρο
SOG-IS MRA	Ομάδα Ανώτερων Υπαλλήλων για την Ασφάλεια των Συστημάτων Πληροφοριών, Συμφωνία Αμοιβαίας Αναγνώρισης
ΑΔΠ	Ασφάλεια δικτύων και πληροφοριών
ΓΚΠΔ	Γενικός κανονισμός για την προστασία δεδομένων
ΔΕΤ	Διεθνής Ένωση Τηλεπικοινωνιών
Ε&Α	Έρευνα και ανάπτυξη
ΕΕ	Ευρωπαϊκή Ένωση
ΕΖΕΣ	Ευρωπαϊκή Ζώνη Ελεύθερων Συναλλαγών

ΕΠΕΠ	Ευρωπαϊκό πλαίσιο επαγγελματικών προσόντων
ΕΣΑΚ	Εθνικές στρατηγικές για την ασφάλεια στον κυβερνοχώρο
ΕΣΔΙΤ	Εταιρικές σχέσεις δημοσίου-ιδιωτικού τομέα
ΚΜ	Κράτος μέλος
ΜΜΕ	Μικρομεσαίες επιχειρήσεις
ΝΠΔ	Νόμος περί προστασίας των δεδομένων
ΟΕΝ:	Οργανισμός επιβολής του νόμου
ΤΒΙ	Τεχνολογίες για τη Βελτίωση της προστασίας της Ιδιωτικότητας
ΤΛ	Τεχνολογία λειτουργιών
ΤΝ	Τεχνητή νοημοσύνη
ΤΠΕ	Τεχνολογίες πληροφοριών και επικοινωνιών
ΥΖΣ	Υποδομή πληροφοριών ζωτικής σημασίας
ΦΕΒΠ	Φορείς εκμετάλλευσης βασικών πληροφοριών
ΨΕΑ	Ψηφιακή ενιαία αγορά

ΣΥΝΟΠΤΙΚΗ ΠΑΡΟΥΣΙΑΣΗ

Το τρέχον τοπίο των κυβερνοαπειλών εξακολουθεί να διευρύνεται και οι κυβερνοεπιθέσεις εξακολουθούν να αυξάνονται σε ένταση και αριθμό. Συνεπώς, τα κράτη μέλη της ΕΕ πρέπει να ανταποκριθούν αποτελεσματικά αναπτύσσοντας περαιτέρω και προσαρμόζοντας τις εθνικές στρατηγικές τους για την ασφάλεια στον κυβερνοχώρο (ΕΣΑΚ). Από τη στιγμή της δημοσίευσης των πρώτων μελετών του ENISA σχετικά με τις ΕΣΑΚ το 2012, τα κράτη μέλη της ΕΕ και οι χώρες της ΕΖΕΣ έχουν σημειώσει σημαντική πρόοδο στην ανάπτυξη και την εφαρμογή των στρατηγικών τους.

Η παρούσα έκθεση παρουσιάζει το έργο του ENISA για τη δημιουργία ενός εθνικού πλαισίου αξιολόγησης ικανοτήτων (ΕΠΑΙ).

Στόχος είναι να παρασχεθεί στα κράτη μέλη ένα πλαίσιο για την αυτοαξιολόγηση του επιπέδου ωριμότητάς τους, μέσω της αξιολόγησης των στόχων των ΕΣΑΚ, που θα τα βοηθήσει να ενισχύσουν και να αξιοποιήσουν τις ικανότητες στον τομέα της ασφάλειας στον κυβερνοχώρο τόσο σε στρατηγικό όσο και σε επιχειρησιακό επίπεδο.

Το πλαίσιο παρουσιάζει μια απλή αντιπροσωπευτική εικόνα του επιπέδου ωριμότητας των κρατών μελών όσον αφορά την ασφάλεια στον κυβερνοχώρο. Το ΕΠΑΙ είναι ένα εργαλείο που βοηθάει τα κράτη μέλη:

- να παράσχουν χρήσιμες πληροφορίες για την ανάπτυξη μιας μακροπρόθεσμης στρατηγικής (π.χ. ορθές πρακτικές, κατευθυντήριες γραμμές)·
- να συμβάλλουν στον εντοπισμό ελλειπόντων στοιχείων των ΕΣΑΚ·
- να συμβάλουν στην περαιτέρω δημιουργία των ικανοτήτων ασφάλειας στον κυβερνοχώρο·
- να υποστηρίξουν τη λογοδοσία στο πλαίσιο των πολιτικών δράσεων·
- να παρέχουν αξιοπιστία στο ευρύ κοινό και τους διεθνείς εταίρους·
- να υποστηρίζουν την ενημέρωση και να βελτιώνουν τη δημόσια εικόνα ως διαφανούς οργανισμού·
- να συμβάλλουν στην πρόβλεψη των μελλοντικών ζητημάτων·
- να συμβάλλουν στον προσδιορισμό των αντληθέντων διδαγμάτων και των βέλτιστων πρακτικών·
- να παράσχουν ένα βασικό επίπεδο όσον αφορά τις ικανότητες για την ασφάλεια στον κυβερνοχώρο σε ολόκληρη την ΕΕ για τη διευκόλυνση των συζητήσεων· και
- να συμβάλλουν στην αξιολόγηση των εθνικών ικανοτήτων όσον αφορά την ασφάλεια στον κυβερνοχώρο.

Το παρόν πλαίσιο σχεδιάστηκε με την υποστήριξη των εμπειρογνωμόνων του ENISA και εκπροσώπων από 19 κράτη μέλη και χώρες της ΕΖΕΣ[1]. Το κοινό-στόχος της παρούσας έκθεσης είναι οι υπεύθυνοι χάραξης πολιτικής, οι εμπειρογνώμονες και οι κυβερνητικοί αξιωματούχοι που είναι υπεύθυνοι ή συμμετέχουν στον σχεδιασμό, την εφαρμογή και την αξιολόγηση μιας ΕΣΑΚ και, σε ευρύτερο επίπεδο, των ικανοτήτων ασφάλειας στον κυβερνοχώρο.

Το εθνικό πλαίσιο αξιολόγησης ικανοτήτων καλύπτει 17 στρατηγικούς στόχους και διαρθρώνεται γύρω από τέσσερις κύριες δέσμες:

- Δέσμη #1: Διακυβέρνηση και πρότυπα ασφάλειας στον κυβερνοχώρο
  1. Ανάπτυξη ενός εθνικού σχεδίου έκτακτης ανάγκης για την ασφάλεια στον κυβερνοχώρο
  2. Θέσπιση βασικών μέτρων ασφαλείας
  3. Εξασφάλιση της ψηφιακής ταυτότητας και οικοδόμηση εμπιστοσύνης στις ψηφιακές δημόσιες υπηρεσίες

- Δέσμη #2: Δημιουργία ικανοτήτων και ευαισθητοποίηση
  4. Διοργάνωση ασκήσεων για την ασφάλεια στον κυβερνοχώρο
  5. Δημιουργία ικανότητας απόκρισης σε περιστατικά στον κυβερνοχώρο
  6. Ευαισθητοποίηση των χρηστών
  7. Ενίσχυση των προγραμμάτων κατάρτισης και εκπαίδευσης
  8. Ενίσχυση Ε&Α
  9. Παροχή κινήτρων στον ιδιωτικό τομέα ώστε να επενδύει σε μέτρα ασφαλείας
  10. Βελτίωση της κυβερνοασφάλειας στην αλυσίδα εφοδιασμού

- Δέσμη #3: Νομοθετικό και ρυθμιστικό πλαίσιο
  11. Προστασία υποδομής πληροφοριών ζωτικής σημασίας, ΦΕΒΠ και ΠΨΥ
  12. Αντιμετώπιση εγκλήματος στον κυβερνοχώρο
  13. Θέσπιση μηχανισμών αναφοράς περιστατικών
  14. Ενίσχυση της προστασίας της ιδιωτικής ζωής και των δεδομένων

- Δέσμη #4: Συνεργασία
  15. Δημιουργία εταιρικής σχέσης δημοσίου-ιδιωτικού τομέα
  16. Θεσμοθέτηση της συνεργασίας μεταξύ δημόσιων οργανισμών
  17. Συμμετοχή σε διεθνή συνεργασία

[1] Ελήφθησαν συνεντεύξεις από τα ακόλουθα κράτη μέλη και χώρες της ΕΖΕΣ: Βέλγιο, Γερμανία, Δανία, Ελλάδα, Εσθονία, Ιρλανδία, Ισπανία, Ιταλία, Κάτω Χώρες, Κροατία, Λιχτενστάιν, Μάλτα, Νορβηγία, Ουγγαρία, Πορτογαλία, Σλοβακία, Σλοβενία, Σουηδία και Τσεχική Δημοκρατία.

1. ΕΙΣΑΓΩΓΗ

Η οδηγία για την ασφάλεια δικτύων και πληροφοριών σε ολόκληρη την Ένωση (οδηγία ΑΔΠ) που δημοσιεύθηκε τον Ιούλιο του 2016, απαιτεί από τα κράτη μέλη της ΕΕ να εγκρίνουν μια εθνική στρατηγική για την ασφάλεια των συστημάτων δικτύου και πληροφοριών, η οποία αναφέρεται επίσης ως ΕΣΑΚ (Εθνική στρατηγική για την ασφάλεια στον κυβερνοχώρο), όπως ορίζεται στα άρθρα 1 και 7. Σε αυτό το πλαίσιο, μια ΕΣΑΚ ορίζεται ως ένα πλαίσιο που καθορίζει στρατηγικές αρχές, κατευθυντήριες γραμμές, στρατηγικούς στόχους, προτεραιότητες, κατάλληλες πολιτικές και κανονιστικά μέτρα. Ο προβλεπόμενος στόχος μιας ΕΣΑΚ είναι η επίτευξη και η διατήρηση υψηλού επιπέδου ασφάλειας συστημάτων δικτύου και πληροφοριών, επιτρέποντας έτσι στα κράτη μέλη να περιορίσουν τις ενδεχόμενες απειλές. Επιπλέον, η ΕΣΑΚ μπορεί επίσης να αποτελέσει καταλύτη για τη βιομηχανική ανάπτυξη και την οικονομική και κοινωνική πρόοδο.

Η πράξη της ΕΕ για την ασφάλεια στον κυβερνοχώρο ορίζει ότι ο ENISA προωθεί τη διάδοση βέλτιστων πρακτικών για τον καθορισμό και την εφαρμογή μιας ΕΣΑΚ, υποστηρίζοντας τα κράτη μέλη κατά την έγκριση της οδηγίας ΑΔΠ και συλλέγοντας πολύτιμα σχόλια σχετικά με τις εμπειρίες τους. Για τον σκοπό αυτό, ο ENISA ανέπτυξε διάφορα εργαλεία για να βοηθήσει τα κράτη μέλη να χαράξουν, να εφαρμόσουν και να αξιολογήσουν τις εθνικές στρατηγικές τους για την ασφάλεια στον κυβερνοχώρο (ΕΣΑΚ).

Στο πλαίσιο της εντολής του, ο ENISA στοχεύει στην ανάπτυξη ενός εθνικού πλαισίου αυτοαξιολόγησης ικανοτήτων για τη μέτρηση του επιπέδου ωριμότητας των διαφόρων ΕΣΑΚ. Στόχος της παρούσας έκθεσης είναι να παρουσιάσει τη μελέτη που διενεργήθηκε κατά τον καθορισμό του πλαισίου αυτοαξιολόγησης.

1.1 ΑΝΤΙΚΕΙΜΕΝΟ ΚΑΙ ΣΤΟΧΟΙ ΤΗΣ ΜΕΛΕΤΗΣ

Ο κύριος στόχος της παρούσας μελέτης είναι να δημιουργήσει ένα εθνικό πλαίσιο αυτοαξιολόγησης ικανοτήτων, το οποίο αναφέρεται παρακάτω ως ΕΠΑΙ, για τη μέτρηση του επιπέδου ωριμότητας των κρατών μελών όσον αφορά τις ικανότητες ασφάλειας στον κυβερνοχώρο. Ειδικότερα, το πλαίσιο θα πρέπει να παρέχει στα κράτη μέλη τη δυνατότητα:

- να διενεργούν την αξιολόγηση των εθνικών τους ικανοτήτων ασφάλειας στον κυβερνοχώρο·
- να ενισχύουν την ευαισθητοποίηση όσον αφορά το επίπεδο ωριμότητας της χώρας·
- να εντοπίζουν τομείς που επιδέχονται βελτίωση· και
- να οικοδομούν ικανότητες ασφάλειας στον κυβερνοχώρο·

Το παρόν πλαίσιο θα πρέπει να βοηθήσει τα κράτη μέλη, και ιδίως τους εθνικούς υπεύθυνους χάραξης πολιτικής, να πραγματοποιήσουν μια άσκηση αυτοαξιολόγησης με στόχο τη βελτίωση των εθνικών ικανοτήτων ασφάλειας στον κυβερνοχώρο.

1.2 ΜΕΘΟΔΟΛΟΓΙΚΗ ΠΡΟΣΕΓΓΙΣΗ

Η μεθοδολογική προσέγγιση που χρησιμοποιείται για την ανάπτυξη του εθνικού πλαισίου αυτοαξιολόγησης ικανοτήτων βασίζεται σε τέσσερα βασικά βήματα:

1. **Δευτερογενής έρευνα τεκμηρίωσης**: Το πρώτο βήμα περιελάμβανε τη διεξαγωγή εκτεταμένης βιβλιογραφικής επισκόπησης για τη συλλογή βέλτιστων πρακτικών σχετικά με την ανάπτυξη ενός πλαισίου αξιολόγησης ωριμότητας για τις εθνικές στρατηγικές ασφάλειας στον κυβερνοχώρο. Η δευτερογενής έρευνα τεκμηρίωσης

επικεντρώθηκε σε μια συστηματική ανάλυση των σχετικών εγγράφων σχετικά με τη δημιουργία ικανοτήτων στον τομέα της ασφάλειας στον κυβερνοχώρο και τον καθορισμό πολιτικής, στις υφιστάμενες ΕΣΑΚ των κρατών μελών και σε μια σύγκριση των υφιστάμενων μοντέλων ωριμότητας ασφάλειας στον κυβερνοχώρο. Διενεργήθηκε συγκριτική αξιολόγηση των επιδόσεων για τα υπάρχοντα μοντέλα ωριμότητας μέσω της υιοθέτησης ενός πλαισίου ανάλυσης που αναπτύχθηκε για τον σκοπό της παρούσας μελέτης. Το πλαίσιο ανάλυσης βασίζεται στη μεθοδολογία Becker[2] για την ανάπτυξη μοντέλων ωριμότητας η οποία καθορίζει ένα γενικό και ενοποιημένο διαδικαστικό μοντέλο για τον σχεδιασμό μοντέλων ωριμότητας και παρέχει σαφείς απαιτήσεις για την ανάπτυξη μοντέλων ωριμότητας. Το πλαίσιο ανάλυσης προσαρμόστηκε περαιτέρω για να καλύψει τις ανάγκες της παρούσας μελέτης.

2. **Συλλογή απόψεων εμπειρογνωμόνων και ενδιαφερομένων**: Με βάση τα δεδομένα που συγκεντρώθηκαν μέσω της δευτερογενούς έρευνας τεκμηρίωσης και των σχετικών προκαταρκτικών ευρημάτων της ανάλυσης, αυτή η φάση περιλάμβανε τον εντοπισμό και την πρόσκληση αναγνωρισμένων εμπειρογνωμόνων που έχουν εμπειρία στην ανάπτυξη και εφαρμογή ΕΣΑΚ ή μοντέλων ωριμότητας για τη διεξαγωγή συνεντεύξεων. Ο ENISA επικοινώνησε με την Ομάδα εμπειρογνωμόνων για τις εθνικές στρατηγικές ασφάλειας στον κυβερνοχώρο και τους Εθνικούς υπαλλήλους-συνδέσμους (NLO) προκειμένου να βρει τους σχετικούς εμπειρογνώμονες σε κάθε κράτος μέλος. Επιπλέον, πραγματοποιήθηκαν συνεντεύξεις με ορισμένους εμπειρογνώμονες που συμμετείχαν στην ανάπτυξη μοντέλων ωριμότητας. Συνολικά, πραγματοποιήθηκαν 22 συνεντεύξεις, από τις οποίες οι 19 διεξήχθησαν με εκπροσώπους οργανισμών για την ασφάλεια στον κυβερνοχώρο σε διαφορετικά κράτη μέλη (και χώρες της ΕΖΕΣ).
3. **Ανάλυση πληροφοριών αξιολόγησης:** Τα δεδομένα που συλλέχθηκαν μέσω της δευτερογενούς έρευνας τεκμηρίωσης και των συνεντεύξεων αναλύθηκαν στη συνέχεια προκειμένου να προσδιοριστούν οι βέλτιστες πρακτικές κατά τον σχεδιασμό του πλαισίου αυτοαξιολόγησης με σκοπό τη μέτρηση της ωριμότητας των ΕΣΑΚ, την κατανόηση των αναγκών των κρατών μελών και τον προσδιορισμό των δεδομένων που μπορούν να συλλεχθούν στις διάφορες ευρωπαϊκές χώρες[3]. Αυτή η ανάλυση κατέστησε δυνατή την τελική διαμόρφωση του προκαταρκτικού μοντέλου που αναπτύχθηκε στα προηγούμενα βήματα και τη βελτίωση του συνόλου των δεικτών που περιλαμβάνονται στο μοντέλο, των επιπέδων ωριμότητας και των διαστάσεών του.
4. **Οριστικοποίηση του μοντέλου:** Στη συνέχεια, εξετάστηκε η επικαιροποιημένη έκδοση του εθνικού πλαισίου αυτοαξιολόγησης ικανοτήτων από τους εμπειρογνώμονες του ENISA και επικυρώθηκε περαιτέρω από εμπειρογνώμονες μέσω ενός εργαστηρίου που πραγματοποιήθηκε τον Οκτώβριο του 2020 πριν από τη δημοσίευση.

1.3 ΚΟΙΝΟ-ΣΤΟΧΟΣ

Το κοινό-στόχος της παρούσας έκθεσης είναι οι υπεύθυνοι χάραξης πολιτικής, οι εμπειρογνώμονες και οι κυβερνητικοί αξιωματούχοι που είναι υπεύθυνοι ή συμμετέχουν στον σχεδιασμό, την εφαρμογή και την αξιολόγηση των ΕΣΑΚ και, σε ευρύτερο επίπεδο, των ικανοτήτων ασφάλειας στον κυβερνοχώρο. Επιπλέον, τα ευρήματα που επισημοποιούνται σε αυτό το έγγραφο μπορεί να φανούν χρήσιμα στους εμπειρογνώμονες και τους ερευνητές των πολιτικών στον τομέα της ασφάλειας στον κυβερνοχώρο σε εθνικό ή ευρωπαϊκό επίπεδο.

[2] J. Becker, R. Knackstedt, και J. Pöppelbuß, «Developing Maturity Models for IT Management: A Procedure Model and its Application,» (Ανάπτυξη μοντέλων ωριμότητας για τη διαχείριση ΤΠ: Ένα διαδικαστικό μοντέλο και η εφαρμογή του) Business & Information Systems Engineering, τόμος 1, αριθ. 3, σελ. 213–222, Ιούνιος 2009.
[3] Για τον σκοπό αυτής της έρευνας, οι «ευρωπαϊκές χώρες» που αναφέρονται στην παρούσα έκθεση περιλαμβάνουν τα 27 κράτη μέλη της ΕΕ.

2. ΙΣΤΟΡΙΚΟ

2.1 ΠΡΟΗΓΟΥΜΕΝΟ ΕΡΓΟ ΣΧΕΤΙΚΑ ΜΕ ΤΟΝ ΚΥΚΛΟ ΖΩΗΣ ΤΩΝ ΕΣΑΚ

Όπως αναφέρεται στην Πράξη της ΕΕ για την ασφάλεια στον κυβερνοχώρο, ένας από τους κύριους στόχους του ENISA είναι η υποστήριξη των κρατών μελών στην ανάπτυξη εθνικών στρατηγικών για την ασφάλεια των συστημάτων δικτύου και πληροφοριών, η προώθηση της διάδοσης των εν λόγω στρατηγικών και η παρακολούθηση της εφαρμογής τους. Στο πλαίσιο της εντολής του, ο ENISA συνέταξε διάφορα έγγραφα σχετικά με αυτό το θέμα προκειμένου να προωθήσει την ανταλλαγή ορθών πρακτικών και να υποστηρίξει την εφαρμογή των ΕΣΑΚ σε ολόκληρη την ΕΕ:

- Το έγγραφο «Practical guide on the development and execution phase of NCSS» (Πρακτικός οδηγός για το στάδιο ανάπτυξης και εκτέλεσης των ΕΣΑΚ)[4] που δημοσιεύθηκε το 2012
- Το έγγραφο «Setting the course for national efforts to strengthen security in cyberspace»[5] (Χάραξη πορείας εθνικών προσπαθειών για την ενίσχυση της ασφάλειας στον κυβερνοχώρο), που δημοσιεύθηκε το 2012
- Το πρώτο πλαίσιο του ENISA για την αξιολόγηση της ΕΣΑΚ ενός κράτους μέλους που δημοσιεύθηκε[6] το 2014.
- Τον «Διαδικτυακό διαδραστικό χάρτη ΕΣΑΚ»[7] που δημοσιεύθηκε το 2014.
- Το έγγραφο “NCSS Good Practice Guide” (Οδηγός ορθών πρακτικών ΕΣΑΚ)[8] που δημοσιεύθηκε το 2016.
- Το «National Cybersecurity Strategies Evaluation Tool» (Εργαλείο αξιολόγησης εθνικών στρατηγικών ασφάλειας στον κυβερνοχώρο)[9] το οποίο δημοσιεύθηκε το 2018.
- Το έγγραφο «Good practices in innovation on Cybersecurity under the NCSS» (Ορθές πρακτικές για την καινοτομία στον τομέα της ασφάλειας στον κυβερνοχώρο στο πλαίσιο της ΕΣΑΚ)[10] το οποίο δημοσιεύθηκε το 2019.

[4] NCSS: Practical Guide on Development and Execution (ENISA, 2012)
https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide
[5] NCSS: Setting the course for national efforts to strengthen security in cyberspace (Χάραξη πορείας εθνικών προσπαθειών για την ενίσχυση της ασφάλειας στον κυβερνοχώρο), (ENISA, 2012)
https://www.enisa.europa.eu/publications/cyber-security-strategies-paper
[6] Ένα πλαίσιο αξιολόγησης για τις ΕΣΑΚ (ENISA, 2014)
https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies
[7] Εθνικές Στρατηγικές για την Ασφάλεια στον Κυβερνοχώρο - Διαδραστικός Χάρτης (ENISA, 2014, επικαιροποιήθηκε το 2019)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
[8] Αυτό το έγγραφο επικαιροποιεί τον οδηγό του 2012: NCSS Good Practice Guide: Designing and Implementing National Cybersecurity Strategies (Οδηγός ορθών πρακτικών ΕΣΑΚ: Σχεδιασμός και εφαρμογή εθνικών στρατηγικών για την ασφάλεια στον κυβερνοχώρο), (ENISA, 2016)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide
[9] National Cybersecurity Strategies Evaluation Tool (2018)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
[10] https://www.enisa.europa.eu/publications/good-practices-in-innovation-on-cybersecurity-under-the-ncss-1
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

Το ΠΑΡΑΡΤΗΜΑ Α παρέχει μια σύντομη περίληψη των κύριων δημοσιεύσεων του ENISA σχετικά με αυτό το θέμα.

Οι προαναφερθέντες οδηγοί και τα έγγραφα μελετήθηκαν στο πλαίσιο της δευτερογενούς έρευνας τεκμηρίωσης. Συγκεκριμένα, το «Εργαλείο αξιολόγησης εθνικών στρατηγικών ασφάλειας στον κυβερνοχώρο»[11] είναι ένα θεμελιώδες στοιχείο του ΕΠΑΙ. Το ΕΠΑΙ βασίζεται στους στόχους που καλύπτονται στο διαδικτυακό εργαλείο αξιολόγησης ΕΣΑΚ.

2.2 ΚΟΙΝΟΙ ΣΤΟΧΟΙ ΠΟΥ ΠΡΟΣΔΙΟΡΙΖΟΝΤΑΙ ΣΤΙΣ ΕΥΡΩΠΑΪΚΕΣ ΕΣΑΚ

Η ανισότητα μεταξύ των διάφορων κρατών μελών καθιστά δύσκολο τον εντοπισμό κοινών δραστηριοτήτων ή σχεδίων δράσης μεταξύ διαφορετικών εθνικών πλαισίων, νομικών πλαισίων και πολιτικών θεματολογίων. Ωστόσο, οι ΕΣΑΚ των κρατών μελών έχουν συχνά στρατηγικούς στόχους που διαρθρώνονται γύρω από τα ίδια θέματα. Έτσι, με βάση το προηγούμενο έργο του ENISA και την ανάλυση των ΕΣΑΚ των κρατών μελών, προσδιορίστηκαν 22 στρατηγικοί στόχοι. 15 από τους εν λόγω στρατηγικούς στόχους είχαν ήδη προσδιοριστεί στις προηγούμενες εργασίες του ENISA, 2 προστέθηκαν πρόσφατα σε αυτή τη μελέτη και 5 στόχοι προσδιορίστηκαν για μελλοντική εξέταση.

2.2.1 Κοινοί στρατηγικοί στόχοι που καλύπτονται από τα κράτη μέλη

Με βάση τις προηγούμενες εργασίες του ENISA, συγκεκριμένα το Εργαλείο αξιολόγησης στρατηγικών ασφάλειας στον κυβερνοχώρο[12], στον παρακάτω πίνακα παρουσιάζεται το προαναφερθέν σύνολο 15 στρατηγικών στόχων που καλύπτονται συνήθως στις ΕΣΑΚ των κρατών μελών. Οι στόχοι περιγράφουν τον πυρήνα της συνολικής «εθνικής φιλοσοφίας» σχετικά με το θέμα. Για πρόσθετες πληροφορίες σχετικά με τους στόχους που περιγράφονται κατωτέρω, ανατρέξτε στην έκθεση του ENISA «NCSS Good Practice Guide» (Οδηγός ορθών πρακτικών ΕΣΑΚ)[13].

Πίνακας 1: Κοινοί στρατηγικοί στόχοι που καλύπτονται από τα κράτη μέλη στις ΕΣΑΚ τους

Αριθ.	Στρατηγικοί στόχοι ΕΣΑΚ	Στόχοι
1	**Ανάπτυξη εθνικών σχεδίων έκτακτης ανάγκης για την ασφάλεια στον κυβερνοχώρο**	▶ Παρουσίαση και εξήγηση των κριτηρίων που θα πρέπει να χρησιμοποιούνται για τον χαρακτηρισμό μιας κατάστασης ως κατάστασης κρίσης· ▶ Καθορισμός βασικών διαδικασιών και δράσεων για τη διαχείριση της κρίσης· και ▶ Σαφής καθορισμός των ρόλων και των ευθυνών των διάφορων ενδιαφερομένων κατά τη διάρκεια μιας κρίσης στον κυβερνοχώρο. ▶ Παρουσίαση και εξήγηση των κριτηρίων λήξης μιας κρίσης ή/και ποιος έχει την εξουσία να κηρύξει τη λήξη της.
2	**Θέσπιση βασικών μέτρων ασφαλείας**	▶ Εναρμόνιση των διαφορετικών πρακτικών που ακολουθούν οι οργανισμοί τόσο του δημόσιου όσο και του ιδιωτικού τομέα· ▶ Δημιουργία κοινής γλώσσας μεταξύ των αρμόδιων δημόσιων αρχών και των οργανισμών και άνοιγμα ασφαλών διαύλων επικοινωνίας· ▶ Παροχή δυνατότητας στους διάφορους ενδιαφερόμενους φορείς να ελέγχουν και να συγκρίνουν τις ικανότητές τους όσον αφορά την ασφάλεια στον κυβερνοχώρο.

[11] National Cybersecurity Strategies Evaluation Tool (2018)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
[12] National Cybersecurity Strategies Evaluation Tool (2018)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
[13] Αυτό το έγγραφο επικαιροποιεί τον οδηγό του 2012: NCSS Good Practice Guide: Designing and Implementing National Cybersecurity Strategies (Οδηγός ορθών πρακτικών ΕΣΑΚ: Σχεδιασμός και εφαρμογή εθνικών στρατηγικών για την ασφάλεια στον κυβερνοχώρο), (ENISA, 2016)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide

Αριθ.	Στρατηγικοί στόχοι ΕΣΑΚ	Στόχοι
		▶ Ανταλλαγή πληροφοριών σχετικά με τις ορθές πρακτικές ασφάλειας στον κυβερνοχώρο σε κάθε βιομηχανικό κλάδο· και ▶ Παροχή βοήθειας στους ενδιαφερόμενους φορείς ώστε να δίνουν προτεραιότητα σε επενδύσεις που αφορούν την ασφάλεια.
3	**Διοργάνωση ασκήσεων για την ασφάλεια στον κυβερνοχώρο**	▶ Προσδιορισμός του τι πρέπει να υποβληθεί σε δοκιμές (σχέδια και διαδικασίες, άτομα, υποδομή, ικανότητες απόκρισης, ικανότητες συνεργασίας, επικοινωνία, κ.λπ.)· ▶ Σύσταση εθνικής ομάδας προγραμματισμού ασκήσεων στον κυβερνοχώρο, με σαφή εντολή· και ▶ Ενσωμάτωση των ασκήσεων στον κυβερνοχώρο στο πλαίσιο του κύκλου ζωής της εθνικής στρατηγικής για την ασφάλεια στον κυβερνοχώρο ή του εθνικού σχεδίου έκτακτης ανάγκης για την ασφάλεια στον κυβερνοχώρο.
4	**Δημιουργία ικανότητας απόκρισης σε περιστατικά στον κυβερνοχώρο**	▶ Εντολή – σχετίζεται με τις εξουσίες, τους ρόλους και τις ευθύνες που πρέπει να ανατεθούν στην αρμόδια ομάδα από την αντίστοιχη κυβέρνηση· ▶ Χαρτοφυλάκιο υπηρεσιών – αυτό καλύπτει τις υπηρεσίες που παρέχει μια ομάδα στην περιφέρειά της ή χρησιμοποιεί για τη δική της εσωτερική λειτουργία· ▶ Επιχειρησιακές ικανότητες – αυτές αφορούν τις τεχνικές και επιχειρησιακές απαιτήσεις που πρέπει να πληροί μια ομάδα· και ▶ Ικανότητες συνεργασίας – αυτές περιλαμβάνουν απαιτήσεις σχετικά με την ανταλλαγή πληροφοριών με άλλες ομάδες που δεν καλύπτονται από τις προηγούμενες τρεις κατηγορίες, π.χ. υπεύθυνοι χάραξης πολιτικής, στρατιωτικές αρχές, ρυθμιστικές αρχές, φορείς εκμετάλλευσης (υποδομών πληροφοριών κρίσιμης σημασίας), αρχές επιβολής του νόμου.
5	**Ευαισθητοποίηση των χρηστών**	▶ Εντοπισμός κενών στις γνώσεις σχετικά με την ασφάλεια στον κυβερνοχώρο ή θέματα ασφάλειας των πληροφοριών· και ▶ Κάλυψη των κενών, μέσω αύξησης της ευαισθητοποίησης ή ανάπτυξης/ενίσχυσης του υπόβαθρου γνώσεων.
6	**Ενίσχυση των προγραμμάτων κατάρτισης και εκπαίδευσης**	▶ Ενίσχυση των επιχειρησιακών ικανοτήτων του υπάρχοντος εργατικού δυναμικού ασφάλειας των συστημάτων πληροφοριών· ▶ Ενθάρρυνση συμμετοχής των σπουδαστών και στη συνέχεια προετοιμασία τους ώστε να εξοικειωθούν με τον τομέα της ασφάλειας στον κυβερνοχώρο· ▶ Προώθηση και ενθάρρυνση των σχέσεων μεταξύ ακαδημαϊκών περιβαλλόντων ασφάλειας πληροφοριών και του κλάδου ασφάλειας πληροφοριών· και ▶ Ευθυγράμμιση της κατάρτισης για την ασφάλεια στον κυβερνοχώρο με τις επιχειρηματικές ανάγκες.
7	**Ενίσχυση Ε&Α**	▶ Προσδιορισμός των πραγματικών αιτιών των τρωτών σημείων αντί της αντιμετώπισης των επιπτώσεών τους· ▶ Συνεργασία μεταξύ επιστημόνων διαφορετικών κλάδων για την παροχή λύσεων σε πολυδιάστατα και περίπλοκα προβλήματα, όπως οι φυσικές απειλές και οι κυβερνοαπειλές· ▶ Συγκέντρωση των αναγκών του κλάδου και των ευρημάτων έρευνας, διευκολύνοντας με αυτόν τον τρόπο τη μετάβαση από τη θεωρία στην πράξη· και ▶ Αναζήτηση τρόπων όχι μόνο για τη διατήρηση αλλά και για την αύξηση του επιπέδου ασφάλειας στον κυβερνοχώρο για προϊόντα και υπηρεσίες που υποστηρίζουν υπάρχουσες υποδομές στον κυβερνοχώρο.
8	**Παροχή κινήτρων στον ιδιωτικό τομέα ώστε να επενδύει σε μέτρα ασφαλείας**	▶ Προσδιορισμός πιθανών κινήτρων για ιδιωτικές εταιρείες ώστε να επενδύσουν σε μέτρα ασφαλείας· και ▶ Παροχή κινήτρων σε εταιρείες για την ενθάρρυνση επενδύσεων για την ασφάλεια.
9	**Προστασία υποδομής πληροφοριών ζωτικής σημασίας, ΦΕΒΠ και ΠΨΥ (ΥΖΣ)**	▶ Προσδιορισμός υποδομών πληροφοριών ζωτικής σημασίας· και ▶ Προσδιορισμός και περιορισμός σχετικών κινδύνων για τις υποδομές πληροφοριών ζωτικής σημασίας.
10	**Αντιμετώπιση εγκλήματος στον κυβερνοχώρο**	▶ Θέσπιση νόμων στον τομέα του εγκλήματος στον κυβερνοχώρο· και ▶ Αύξηση της αποτελεσματικότητας των υπηρεσιών επιβολής του νόμου.

Αριθ.	Στρατηγικοί στόχοι ΕΣΑΚ	Στόχοι
11	**Θέσπιση μηχανισμών αναφοράς περιστατικών**	▶ Απόκτηση γνώσεων όσον αφορά το συνολικό περιβάλλον απειλών· ▶ Αξιολόγηση των επιπτώσεων των συμβάντων (π.χ. παραβιάσεις ασφαλείας, αποτυχίες δικτύου, διακοπές υπηρεσίας)· ▶ Απόκτηση γνώσεων όσον αφορά υπάρχοντα και νέα τρωτά σημεία και τύπους επιθέσεων· ▶ Ανάλογη επικαιροποίηση μέτρων ασφαλείας· και ▶ Εφαρμογή διατάξεων της οδηγίας ΑΔΠ σχετικά με την αναφορά συμβάντων.
12	**Ενίσχυση της προστασίας της ιδιωτικής ζωής και των δεδομένων**	▶ Συμβολή στην ενίσχυση των θεμελιωδών δικαιωμάτων όσον αφορά την προστασία της ιδιωτικής ζωής και των δεδομένων.
13	**Δημιουργία εταιρικής σχέσης δημοσίου-ιδιωτικού τομέα (ΕΣΔΙΤ)**	▶ Αποτροπή (αποτροπή δραστών επιθέσεων)· ▶ Προστασία (με βάση την έρευνα για νέες απειλές ασφαλείας)· ▶ Ανίχνευση (κοινή χρήση πληροφοριών για την αντιμετώπιση νέων απειλών)· ▶ Ανταπόκριση (για την υλοποίηση της ικανότητας αντιμετώπισης του αρχικού αντικτύπου ενός περιστατικού)· και ▶ Ανάκαμψη (για την υλοποίηση της ικανότητας αντιμετώπισης του αρχικού αντικτύπου ενός περιστατικού)· και
14	**Θεσμοθέτηση της συνεργασίας μεταξύ δημόσιων οργανισμών**	▶ Αύξηση της συνεργασίας μεταξύ δημόσιων φορέων με αρμοδιότητες και ικανότητες που σχετίζονται με την ασφάλεια στον κυβερνοχώρο· ▶ Αποφυγή επικάλυψης αρμοδιοτήτων και πόρων μεταξύ δημόσιων υπηρεσιών· και ▶ Βελτίωση και θεσμοθέτηση της συνεργασίας μεταξύ δημόσιων υπηρεσιών σε διάφορους τομείς της ασφάλειας στον κυβερνοχώρο.
15	**Συμμετοχή σε διεθνή συνεργασία (όχι μόνο με τα κράτη μέλη της ΕΕ)**	▶ Οφέλη από τη δημιουργία κοινής βάσης γνώσεων μεταξύ των κρατών μελών της ΕΕ· ▶ Δημιουργία αποτελεσμάτων συνεργειών μεταξύ των εθνικών αρχών ασφάλειας στον κυβερνοχώρο· και ▶ Αποτελεσματική και ενισχυμένη καταπολέμηση του διακρατικού εγκλήματος.

2.2.2 Πρόσθετοι στρατηγικοί στόχοι

Με βάση τη δευτερογενή έρευνα τεκμηρίωσης που πραγματοποιήθηκε, καθώς και τις συνεντεύξεις που διεξήγαγε ο ENISA, προσδιορίστηκαν πρόσθετοι στρατηγικοί στόχοι. Τα κράτη μέλη αντιμετωπίζουν ολοένα και περισσότερο τα εν λόγω θέματα στις ΕΣΑΚ τους ή προσδιορίζουν σχέδια δράσης για το ίδιο ζήτημα. Παρέχονται επίσης παραδείγματα δραστηριοτήτων που εφαρμόζονται από τα κράτη μέλη. Εάν ένα παράδειγμα προέρχεται από δημόσια διαθέσιμη πηγή, παρέχεται παραπομπή. Σε περιπτώσεις όπου τα παραδείγματα βασίζονται σε εμπιστευτικές συνεντεύξεις με υπαλλήλους των κρατών μελών της ΕΕ, δεν παρέχονται παραπομπές.

Προσδιορίστηκαν οι ακόλουθοι πρόσθετοι στρατηγικοί στόχοι:

- Βελτίωση της κυβερνοασφάλειας στην αλυσίδα εφοδιασμού· και
- Εξασφάλιση της ψηφιακής ταυτότητας και οικοδόμηση εμπιστοσύνης στις ψηφιακές δημόσιες υπηρεσίες.

Βελτίωση της κυβερνοασφάλειας στην αλυσίδα εφοδιασμού

Οι μικρομεσαίες επιχειρήσεις (ΜΜΕ) αποτελούν τη ραχοκοκαλιά της ευρωπαϊκής οικονομίας. Αντιπροσωπεύουν το 99 % όλων των επιχειρήσεων στην ΕΕ[14] και το 2015, εκτιμήθηκε ότι οι ΜΜΕ δημιούργησαν περίπου το 85 % των νέων θέσεων εργασίας και παρείχαν τα δύο τρίτα της συνολικής απασχόλησης στον ιδιωτικό τομέα στην ΕΕ. Επιπλέον, δεδομένου ότι οι ΜΜΕ παρέχουν υπηρεσίες σε μεγάλες εταιρείες και συνεργάζονται όλο και περισσότερο με τις δημόσιες διοικήσεις[15], πρέπει να σημειωθεί ότι στο σημερινό διασυνδεδεμένο πλαίσιο, οι ΜΜΕ αποτελούν τον αδύναμο κρίκο για κυβερνοεπιθέσεις. Πράγματι, οι ΜΜΕ είναι οι πιο εκτεθειμένες σε κυβερνοεπιθέσεις, αλλά συχνά δεν μπορούν να επενδύσουν επαρκώς στην ασφάλεια στον κυβερνοχώρο[16]. Η βελτίωση της ασφάλειας στον κυβερνοχώρο της αλυσίδας εφοδιασμού θα πρέπει επομένως να πραγματοποιηθεί εστιάζοντας στις ΜΜΕ.

Εκτός από αυτήν τη συστημική προσέγγιση, τα κράτη μέλη μπορούν επίσης να δώσουν έμφαση στις προσπάθειες για την ασφάλεια στον κυβερνοχώρο, όσον αφορά συγκεκριμένες υπηρεσίες και προϊόντα ΤΠΕ που θεωρούνται ουσιώδη: τεχνολογίες ΤΠΕ που χρησιμοποιούνται σε υποδομές πληροφοριών ζωτικής σημασίας, μηχανισμοί ασφαλείας που επιβάλλονται στον τομέα των τηλεπικοινωνιών (έλεγχοι σε επίπεδο παρόχων υπηρεσιών διαδικτύου), υπηρεσίες εμπιστοσύνης όπως ορίζονται στον κανονισμό σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης (eIDAS), και παροχείς υπηρεσιών υπολογιστικού νέφους. Για παράδειγμα, στην εθνική στρατηγική της για την ασφάλεια στον κυβερνοχώρο για την περίοδο 2019-2024[17], η Πολωνία δεσμεύτηκε να αναπτύξει ένα εθνικό σχήμα αξιολόγησης και πιστοποίησης της κυβερνοασφάλειας ως μηχανισμό διασφάλισης ποιότητας στην αλυσίδα εφοδιασμού. Το εν λόγω σχήμα πιστοποίησης θα ευθυγραμμιστεί με το πλαίσιο πιστοποίησης της ΕΕ για ψηφιακά προϊόντα, υπηρεσίες και διαδικασίες ΤΠΕ που θεσπίστηκε με την πράξη της ΕΕ για την κυβερνοασφάλεια (2019/881).

Η βελτίωση της κυβερνοασφάλειας στην αλυσίδα εφοδιασμού είναι επομένως υψίστης σημασίας. Ο στόχος αυτός μπορεί να επιτευχθεί με τη θέσπιση ισχυρών πολιτικών για την προώθηση των ΜΜΕ, την παροχή κατευθυντήριων γραμμών για τις απαιτήσεις κυβερνοασφάλειας στις διαδικασίες δημοσίων συμβάσεων, την προαγωγή της συνεργασίας στον ιδιωτικό τομέα, τη δημιουργία ΕΣΔΙΤ, την προώθηση μηχανισμών συντονισμένης δημοσιοποίησης τρωτών σημείων (CVD)[18], τον σχεδιασμό του σχήματος πιστοποίησης προϊόντων, τη συμπερίληψη στοιχείων κυβερνοασφάλειας σε ψηφιακές πρωτοβουλίες για τις ΜΜΕ, και τη χρηματοδότηση ανάπτυξης δεξιοτήτων, μεταξύ άλλων.

Εξασφάλιση της ψηφιακής ταυτότητας και οικοδόμηση εμπιστοσύνης στις ψηφιακές δημόσιες υπηρεσίες

Τον Φεβρουάριο του 2020, η Επιτροπή παρουσίασε το όραμά της για τον ψηφιακό μετασχηματισμό της ΕΕ στην ανακοίνωση «Διαμόρφωση του ψηφιακού μέλλοντος της Ευρώπης»[19], με στόχο την παροχή τεχνολογιών χωρίς αποκλεισμούς που λειτουργούν για τους ανθρώπους και σέβονται τις θεμελιώδεις αξίες της ΕΕ. Ειδικότερα, στην ανακοίνωση αναφέρεται ότι η προώθηση του ψηφιακού μετασχηματισμού των δημόσιων διοικήσεων σε ολόκληρη την Ευρώπη είναι ζωτικής σημασίας. Υπό αυτήν την έννοια, η δημιουργία εμπιστοσύνης στην κυβέρνηση σε σχέση με την ψηφιακή ταυτότητα, καθώς και στις δημόσιες υπηρεσίες είναι υψίστης σημασίας. Αυτό είναι ακόμη πιο σημαντικό αν ληφθεί υπόψη το γεγονός ότι οι

[14] https://ec.europa.eu/growth/smes/
[15] https://www.oecd.org/fr/publications/smes-in-public-procurement-9789264307476-en.htm
[16] https://www.eesc.europa.eu/en/news-media/news/european-companies-especially-smes-face-growing-risk-cyber-attacks-study
[17] http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf
[18] https://english.ncsc.nl/publications/publications/2019/juni/01/coordinated-vulnerability-disclosure-the-guideline
[19] Διαμόρφωση του ψηφιακού μέλλοντος της Ευρώπης, COM(2020) 67 final: https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_3.pdf

συναλλαγές του δημόσιου τομέα και οι ανταλλαγές δεδομένων είναι συχνά ευαίσθητου χαρακτήρα.

Πολλές χώρες έχουν εκφράσει την πρόθεσή τους να εξετάσουν αυτό το θέμα στις ΕΣΑΚ τους, όπως: Γαλλία, Δανία, Εσθονία, Ισπανία, Κάτω Χώρες, Λουξεμβούργο, Μάλτα και Ηνωμένο Βασίλειο. Μεταξύ των εν λόγω χωρών, ορισμένες έχουν επίσης αναφέρει ότι αυτός ο στρατηγικός στόχος μπορεί να επιδιωχθεί στο πλαίσιο ενός ευρύτερου σχεδίου:

- Η Εσθονία συνδέει το σχέδιο δράσης της σχετικά με την ασφάλεια της ηλεκτρονικής ταυτότητας και την ικανότητα ηλεκτρονικού ελέγχου ταυτότητας με την ευρύτερη ψηφιακή ατζέντα του 2020 για την Εσθονία.
- Η ΕΣΑΚ της Γαλλίας αναφέρει ότι ο Υφυπουργός αρμόδιος για την Ψηφιακή Τεχνολογία επιβλέπει τη δημιουργία ενός χάρτη πορείας «για την προστασία της ψηφιακής ζωής, της ιδιωτικής ζωής και των δεδομένων προσωπικού χαρακτήρα του γαλλικού λαού».
- Η ΕΣΑΚ των Κάτω Χωρών αναφέρει ότι η ασφάλεια στον κυβερνοχώρο στις δημόσιες διοικήσεις, καθώς και οι δημόσιες υπηρεσίες που παρέχονται στους πολίτες και τις επιχειρήσεις συζητούνται λεπτομερέστερα στο ευρύ θεματολόγιο για την ψηφιακή διακυβέρνηση (Broad Agenda for Digital Government).
- Δεδομένου ότι η κυβέρνηση του Ηνωμένου Βασιλείου συνεχίζει να μεταφέρει περισσότερες από τις υπηρεσίες της στο διαδίκτυο, έχει συστήσει την Κυβερνητική ψηφιακή υπηρεσία (GDS) για να διασφαλίσει ότι όλες οι νέες ψηφιακές υπηρεσίες τις οποίες δημιουργεί ή προμηθεύεται η κυβέρνηση είναι επίσης «ασφαλείς εξ ορισμού», με την υποστήριξη του Εθνικού Κέντρου για την ασφάλεια στον κυβερνοχώρο (NCSC).

2.2.3 Άλλοι στρατηγικοί στόχοι που λαμβάνονται υπόψη

Κατά τη διάρκεια του σταδίου της δευτερογενούς έρευνας τεκμηρίωσης και στο πλαίσιο των συνεντεύξεων που πραγματοποιήθηκαν από τον ENISA, μελετήθηκαν άλλοι στρατηγικοί στόχοι. Ωστόσο, αποφασίστηκε ότι οι εν λόγω στόχοι δεν θα αποτελούσαν μέρος του πλαισίου αυτοαξιολόγησης. Το ΠΑΡΑΡΤΗΜΑ Γ – Άλλοι στόχοι που εξετάστηκαν

παρέχει ορισμούς για καθέναν από τους εν λόγω στόχους που μπορούν να χρησιμοποιηθούν για την τεκμηρίωση των μελλοντικών συζητήσεων σχετικά με πιθανές βελτιώσεις των ΕΣΑΚ.

Οι ακόλουθοι στρατηγικοί στόχοι μελετήθηκαν στο πλαίσιο του μελλοντικού σχεδιασμού:

- Ανάπτυξη ειδικών τομεακών στρατηγικών ασφάλειας στον κυβερνοχώρο.
- Καταπολέμηση των εκστρατειών παραπληροφόρησης.
- Διασφάλιση τεχνολογιών αιχμής (5G, TN, κβαντική υπολογιστική...)·
- Διασφάλιση της κυριαρχίας των δεδομένων· και
- Παροχή κινήτρων για την ανάπτυξη του τομέα της ασφάλισης στον κυβερνοχώρο.

2.3 ΒΑΣΙΚΑ ΣΥΜΠΕΡΑΣΜΑΤΑ ΑΠΟ ΤΗ ΣΥΓΚΡΙΤΙΚΗ ΑΞΙΟΛΟΓΗΣΗ ΕΠΙΔΟΣΕΩΝ

Η δευτερογενής έρευνα τεκμηρίωσης για υπάρχοντα μοντέλα ωριμότητας που σχετίζονται με την ασφάλεια στον κυβερνοχώρο διενεργήθηκε με σκοπό τη συλλογή πληροφοριών και αποδεικτικών στοιχείων για την υποστήριξη του σχεδιασμού του πλαισίου αυτοαξιολόγησης των εθνικών ικανοτήτων στον τομέα των ΕΣΑΚ. Σε αυτό το πλαίσιο, πραγματοποιήθηκε εκτεταμένη βιβλιογραφική ανασκόπηση των υπαρχόντων μοντέλων ώστε να συμπληρωθούν τα ευρήματα από την αρχική έρευνα αξιολόγησης επιπτώσεων για τα μοντέλα ωριμότητας για την κυβερνοασφάλεια και τις υπάρχουσες ΕΣΑΚ, που αναπτύσσονται στις ενότητες 2.1 και 2.2. Η εν

λόγω συστηματική ανασκόπηση υποστηρίζει την επιλογή και αιτιολόγηση των επιπέδων ωριμότητας του πλαισίου αξιολόγησης και τον ορισμό των διαφόρων διαστάσεων και δεικτών.

Στο πλαίσιο της συστηματικής ανασκόπησης των μοντέλων ωριμότητας, 10 μοντέλα εξετάστηκαν και αναλύθηκαν με βάση τα κύρια χαρακτηριστικά τους. Η συνολική επισκόπηση των κύριων χαρακτηριστικών για κάθε μοντέλο που εξετάζεται στο πλαίσιο της παρούσας μελέτης είναι διαθέσιμη στον πίνακα 2 και μια πιο λεπτομερής ανάλυση περιλαμβάνεται στο ΠΑΡΑΡΤΗΜΑ Α.

Πίνακας 2: Επισκόπηση των μοντέλων ωριμότητας που αναλύθηκαν

Όνομα μοντέλου	# επιπέδων ωριμότητας	# χαρακτηριστικών γνωρισμάτων	Μέθοδος αξιολόγησης	Απεικόνιση αποτελεσμάτων
Εθνικό μοντέλο ωριμότητας ικανοτήτων για την ασφάλεια στον κυβερνοχώρο (CMM)	5	5 βασικές διαστάσεις	Συνεργασία με τοπικό οργανισμό για την τελειοποίηση του μοντέλου πριν από την εφαρμογή του σε εθνικό πλαίσιο	Ραντάρ πέντε τμημάτων
Μοντέλο ωριμότητας ικανοτήτων ασφάλειας στον κυβερνοχώρο (C2M2)	4	10 βασικοί τομείς	Μεθοδολογία αυτοαξιολόγησης και εργαλειοθήκη	Πίνακας αποτελεσμάτων με κυκλικά διαγράμματα
Πλαίσιο για τη βελτίωση της κρίσιμης υποδομής για την ασφάλεια στον κυβερνοχώρο	δ/υ (4 Βαθμίδες)	5 βασικές λειτουργίες	Αυτοαξιολόγηση	δ/υ
Μοντέλο ωριμότητας ικανοτήτων του Κατάρ για την ασφάλεια στον κυβερνοχώρο (Q-C2M2)	5	5 βασικοί τομείς	δ/υ	δ/υ
Πιστοποίηση του μοντέλου ωριμότητας ασφάλειας στον κυβερνοχώρο (CMMC)	5	17 βασικοί τομείς	Αξιολόγηση από εξωτερικούς ελεγκτές	δ/υ
Το κοινοτικό μοντέλο ωριμότητας ασφάλειας στον κυβερνοχώρο (CCSMM)	5	6 βασικές διαστάσεις	Αξιολόγηση στο πλαίσιο των κοινοτήτων με πληροφορίες από κρατικές και ομοσπονδιακές υπηρεσίες επιβολής του νόμου	δ/υ
Μοντέλο ωριμότητας ασφάλειας των πληροφοριών για το πλαίσιο κυβερνοασφάλειας του NIST (ISMM)	5	23 τομείς που αξιολογήθηκαν	δ/υ	δ/υ
Μοντέλο Μονάδας Εσωτερικού Ελέγχου (MMEE) για τον δημόσιο τομέα	5	6 στοιχεία	Αυτοαξιολόγηση	δ/υ
Ο παγκόσμιος δείκτης ασφάλειας στον κυβερνοχώρο (GCI)	Δ/Υ	5 πυλώνες	Αυτοαξιολόγηση	Πίνακας κατάταξης
Ο Δείκτης Ισχύος Κυβερνοχώρου (CPI)	Δ/Υ	4 κατηγορίες	Συγκριτική αξιολόγηση από τη μονάδα πληροφοριών του Economist (Economist Intelligence Unit)	Πίνακας κατάταξης

Αυτή η συστηματική ανασκόπηση κατέστησε δυνατή την εξαγωγή συμπερασμάτων σχετικά με τις βέλτιστες πρακτικές που υιοθετήθηκαν σε υπάρχοντα μοντέλα προκειμένου να υποστηριχθεί η ανάπτυξη του εννοιολογικού μοντέλου για το τρέχον μοντέλο ωριμότητας. Συγκεκριμένα, η συγκριτική αξιολόγηση επιδόσεων υποστήριξε τον ορισμό των επιπέδων ωριμότητας, τη δημιουργία δεσμών διαστάσεων και την επιλογή δεικτών, καθώς και μια κατάλληλη μεθοδολογία οπτικοποίησης για τα αποτελέσματα του μοντέλου. Τα πιο σχετικά ευρήματα για καθένα από τα εν λόγω στοιχεία περιγράφονται λεπτομερώς στον Πίνακα 3.

Πίνακας 3: Βασικά συμπεράσματα από τη συγκριτική αξιολόγηση επιδόσεων

Χαρακτηριστικό	Βασικό συμπέρασμα
Επίπεδα ωριμότητας	▶ Μια κλίμακα ωριμότητας πέντε επιπέδων για τα πλαίσια αξιολόγησης όσον αφορά τις ικανότητες ασφάλειας στον κυβερνοχώρο είναι κοινώς αποδεκτή και μπορεί να παράσχει αναλυτικά αποτελέσματα αξιολόγησης (βλ. πίνακα 6 για μια διεξοδική εικόνα του ορισμού των επιπέδων ωριμότητας για κάθε μοντέλο)· ▶ Όλα τα μοντέλα παρέχουν έναν ορισμό υψηλού επιπέδου για κάθε επίπεδο ωριμότητας που στη συνέχεια προσαρμόζεται στις διαφορετικές διαστάσεις ή δέσμες διαστάσεων. ▶ Δύο κύριες πτυχές αξιολογούνται συνήθως κατά τη μέτρηση της ωριμότητας των ικανοτήτων ασφάλειας στον κυβερνοχώρο: η ωριμότητα των στρατηγικών και η ωριμότητα των διαδικασιών που θεσπίζονται για την εφαρμογή στρατηγικών.
Χαρακτηριστικά γνωρίσματα	▶ Από τη συγκριτική ανάλυση των χαρακτηριστικών των υπαρχόντων μοντέλων ωριμότητας προκύπτουν ετερογενή αποτελέσματα με μέσο αριθμό χαρακτηριστικών ανά μοντέλο από τέσσερα έως πέντε· ▶ Ένα μοντέλο που βασίζεται σε περίπου τέσσερα ή πέντε χαρακτηριστικά, παρέχει στις χώρες το σωστό επίπεδο λεπτομέρειας δεδομένων ομαδοποιώντας τις σχετικές διαστάσεις και διασφαλίζοντας την αναγνωσιμότητα των αποτελεσμάτων (βλ. πίνακα 7 για μια περιγραφή των χαρακτηριστικών για κάθε μοντέλο)· ▶ Η βασική αρχή που υιοθετείται από όλα τα μοντέλα κατά τον ορισμό των δεσμών βασίζεται στη συνοχή των στοιχείων που ομαδοποιούνται εντός κάθε δέσμης.
Μέθοδος αξιολόγησης	▶ Οι μέθοδοι αξιολόγησης που χρησιμοποιούνται στα διάφορα μοντέλα που αναλύονται διαφέρουν μεταξύ τους· ▶ Η πιο κοινή μέθοδος αξιολόγησης βασίζεται στην αυτοαξιολόγηση.
Απεικόνιση αποτελεσμάτων	▶ Είναι σημαντικό να παρουσιάζονται τα αποτελέσματα σε διαφορετικό επίπεδο λεπτομέρειας· ▶ Η μεθοδολογία οπτικοποίησης πρέπει να είναι επεξηγηματική και ευανάγνωστη.

Το εννοιολογικό μοντέλο δημιουργήθηκε με βάση τη συγκριτική αξιολόγηση επιδόσεων των διαφόρων μοντέλων ωριμότητας καθώς και σε προηγούμενες εργασίες του ENISA. Επίσης, αποφασίστηκε να αξιοποιηθεί το *διαδικτυακό διαδραστικό εργαλείο του ENISA* για την ανάπτυξη δεικτών ωριμότητας που χρησιμοποιούνται για κάθε χαρακτηριστικό.

2.4 ΠΡΟΚΛΗΣΕΙΣ ΤΗΣ ΑΞΙΟΛΟΓΗΣΗΣ ΤΩΝ ΕΣΑΚ

Τα κράτη μέλη αντιμετωπίζουν πολλές προκλήσεις κατά τη δημιουργία ικανοτήτων ασφάλειας στον κυβερνοχώρο και πιο συγκεκριμένα, κατά τη διασφάλιση ότι οι ικανότητες τους συμβαδίζουν πάντα με τις τελευταίες εξελίξεις. Ακολουθεί μια σύνοψη των προκλήσεων που προσδιορίστηκαν και συζητήθηκαν με τα κράτη μέλη στο πλαίσιο της παρούσας μελέτης:

- **Δυσκολίες συντονισμού και συνεργασίας:** Ο συντονισμός των προσπαθειών για την ασφάλεια στον κυβερνοχώρο σε εθνικό επίπεδο προκειμένου να υπάρξει

αποτελεσματική αντιμετώπιση θεμάτων ασφάλειας στον κυβερνοχώρο μπορεί να αποδειχθεί ότι αποτελεί πρόκληση λόγω του μεγάλου αριθμού των ενδιαφερομένων.

- **Έλλειψη πόρων για την εκτέλεση της αξιολόγησης:** Ανάλογα με το τοπικό πλαίσιο και τις εθνικές δομές διακυβέρνησης για την ασφάλεια στον κυβερνοχώρο, η αξιολόγηση της ΕΣΑΚ και των στόχων της μπορεί να διαρκέσει έως και πάνω από 15 ανθρωποημέρες.
- **Έλλειψη υποστήριξης για την ανάπτυξη ικανοτήτων ασφάλειας στον κυβερνοχώρο:** Ορισμένα κράτη μέλη ανέφεραν ότι για να υπερασπιστούν έναν προϋπολογισμό και να λάβουν υποστήριξη για την ανάπτυξη ικανοτήτων ασφάλειας στον κυβερνοχώρο, πρέπει πρώτα να πραγματοποιήσουν μια φάση αξιολόγησης για τον προσδιορισμό κενών και περιορισμών.
- **Δυσκολίες στην απόδοση επιτυχιών ή αλλαγών στη στρατηγική:** Δεδομένου ότι οι απειλές εξελίσσονται καθημερινά και η τεχνολογία βελτιώνεται, τα σχέδια δράσης πρέπει ως εκ τούτου να προσαρμόζονται συνεχώς. Ωστόσο, η αξιολόγηση μιας ΕΣΑΚ και η απόδοση των αλλαγών στην ίδια τη στρατηγική παραμένει δύσκολο έργο. Αυτό με τη σειρά του καθιστά δύσκολο τον προσδιορισμό των περιορισμών και των ελλείψεων της ΕΣΑΚ.
- **Δυσκολίες μέτρησης της αποτελεσματικότητας της ΕΣΑΚ:** Μπορούν να συλλεχθούν δείκτες για τη μέτρηση διαφορετικών τομέων όπως πρόοδος, εφαρμογή, ωριμότητα και αποτελεσματικότητα. Ενώ η μέτρηση της προόδου και της εφαρμογής είναι σχετικά εύκολη σε σύγκριση με τη μέτρηση της αποτελεσματικότητας, η τελευταία παραμένει πιο σημαντική για την αξιολόγηση των αποτελεσμάτων και των επιπτώσεων μιας ΕΣΑΚ. Με βάση τις συνεντεύξεις που διεξήγαγε ο ENISA, πολλά κράτη μέλη δήλωσαν ότι η ποσοτική μέτρηση της αποτελεσματικότητας μιας ΕΣΑΚ είναι σημαντική, αλλά αποτελεί επίσης ένα εξαιρετικά απαιτητικό έργο που είναι σχεδόν αδύνατο σε ορισμένες περιπτώσεις.
- **Δυσκολία υιοθέτησης ενός κοινού πλαισίου:** Τα κράτη μέλη της ΕΕ λειτουργούν σε διαφορετικά πλαίσια όσον αφορά την πολιτική, τους οργανισμούς, τον πολιτισμό, τη δομή της κοινωνίας και την ωριμότητα της ΕΣΑΚ. Ορισμένα κράτη μέλη από τα οποία ελήφθησαν συνεντεύξεις στο πλαίσιο αυτής της μελέτης ανέφεραν ότι μπορεί να αποδειχθεί δύσκολο να υπερασπιστούν και να χρησιμοποιήσουν ένα ενιαίο πλαίσιο αυτοαξιολόγησης για όλους.

2.5 ΟΦΕΛΗ ΜΙΑΣ ΕΘΝΙΚΗΣ ΑΞΙΟΛΟΓΗΣΗΣ ΙΚΑΝΟΤΗΤΩΝ

Από το 2017, όλα τα κράτη μέλη της ΕΕ διαθέτουν ΕΣΑΚ[20]. Ενώ πρόκειται για θετική εξέλιξη, είναι επίσης σημαντικό τα κράτη μέλη να είναι σε θέση να αξιολογούν σωστά αυτές τις ΕΣΑΚ, προσφέροντας έτσι προστιθέμενη αξία στον στρατηγικό σχεδιασμό και την εφαρμογή τους.

Ένας από τους στόχους του εθνικού πλαισίου αξιολόγησης ικανοτήτων είναι η αξιολόγηση των ικανοτήτων ασφάλειας στον κυβερνοχώρο με βάση τις προτεραιότητες που καθορίζονται στις διάφορες ΕΣΑΚ. Κατά βάση, το πλαίσιο αξιολογεί το επίπεδο ωριμότητας των ικανοτήτων ασφάλειας στον κυβερνοχώρο των κρατών μελών στους τομείς που καθορίζονται από τους στόχους των ΕΣΑΚ. Ως εκ τούτου, τα αποτελέσματα του πλαισίου υποστηρίζουν τους υπεύθυνους χάραξης πολιτικής των κρατών μελών στον καθορισμό της εθνικής στρατηγικής για την ασφάλεια στον κυβερνοχώρο, παρέχοντάς τους πληροφορίες των χωρών σχετικά με την τρέχουσα κατάσταση[21]. Το ΕΠΑΙ προορίζεται τελικά να βοηθήσει τα κράτη μέλη να προσδιορίσουν τομείς βελτίωσης και να αναπτύξουν ικανότητες.

[20] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
[21] Weiss, C.H. (1999). The interface between evaluation and public policy. Evaluation, (Η διεπαφή μεταξύ αξιολόγησης και δημόσιας πολιτικής. Αξιολόγηση) 5(4), 468-486.

Το πλαίσιο έχει ως στόχο να παράσχει στα κράτη μέλη αυτοαξιολόγηση του επιπέδου ωριμότητάς τους, μέσω της αξιολόγησης των στόχων των ΕΣΑΚ, που θα τα βοηθήσει να ενισχύσουν και να αξιοποιήσουν τις ικανότητες στον τομέα της ασφάλειας στον κυβερνοχώρο τόσο σε στρατηγικό όσο και σε επιχειρησιακό επίπεδο.

Στο πλαίσιο μιας πιο πρακτικής προσέγγισης, με βάση τις συνεντεύξεις που διεξήγαγε ο ENISA με διάφορους οργανισμούς που είναι υπεύθυνοι για τον τομέα της ασφάλειας στον κυβερνοχώρο σε διάφορα κράτη μέλη, προσδιορίστηκαν και υπογραμμίστηκαν τα ακόλουθα οφέλη του εθνικού πλαισίου αξιολόγησης ικανοτήτων:

- να παράσχουν χρήσιμες πληροφορίες για την ανάπτυξη μιας μακροπρόθεσμης στρατηγικής (π.χ. ορθές πρακτικές, κατευθυντήριες γραμμές)·
- να συμβάλλουν στον εντοπισμό ελλειπόντων στοιχείων των ΕΣΑΚ·
- να συμβάλουν στην περαιτέρω δημιουργία των ικανοτήτων ασφάλειας στον κυβερνοχώρο·
- να υποστηρίξουν τη λογοδοσία στο πλαίσιο των πολιτικών δράσεων·
- να παρέχουν αξιοπιστία στο ευρύ κοινό και τους διεθνείς εταίρους·
- να υποστηρίζουν την ενημέρωση και να βελτιώνουν τη δημόσια εικόνα ως διαφανούς οργανισμού·
- να συμβάλλουν στην πρόβλεψη των μελλοντικών ζητημάτων·
- να συμβάλλουν στον προσδιορισμό των αντληθέντων διδαγμάτων και των βέλτιστων πρακτικών·
- να παράσχουν μια γραμμή βάσης όσον αφορά τις ικανότητες για την ασφάλεια στον κυβερνοχώρο σε ολόκληρη την ΕΕ για τη διευκόλυνση των συζητήσεων· και
- να συμβάλλουν στην αξιολόγηση των εθνικών ικανοτήτων όσον αφορά την ασφάλεια στον κυβερνοχώρο.

3. ΜΕΘΟΔΟΛΟΓΙΑ ΤΟΥ ΕΘΝΙΚΟΥ ΠΛΑΙΣΙΟΥ ΑΞΙΟΛΟΓΗΣΗΣ ΙΚΑΝΟΤΗΤΩΝ

3.1 ΓΕΝΙΚΟΣ ΣΚΟΠΟΣ

Ο **κύριος στόχος** του ΕΠΑΙ είναι να μετρήσει το επίπεδο ωριμότητας των ικανοτήτων ασφάλειας στον κυβερνοχώρο των **κρατών μελών** για να τα υποστηρίξει στη διεξαγωγή αξιολόγησης των εθνικών τους ικανοτήτων ασφάλειας στον κυβερνοχώρο, ενισχύοντας την ευαισθητοποίηση της χώρας όσον αφορά το επίπεδο ωριμότητας, προσδιορίζοντας τομείς βελτίωσης και δημιουργώντας ικανότητες ασφάλειας στον κυβερνοχώρο.

3.2 ΕΠΙΠΕΔΑ ΩΡΙΜΟΤΗΤΑΣ

Το πλαίσιο βασίζεται σε **πέντε επίπεδα ωριμότητας** που καθορίζουν τα στάδια που περνούν τα κράτη μέλη κατά τη δημιουργία ικανοτήτων ασφάλειας στον κυβερνοχώρο στον τομέα που καλύπτεται από κάθε στόχο των ΕΣΑΚ. Τα επίπεδα απεικονίζουν αυξανόμενα επίπεδα ωριμότητας, ξεκινώντας από το αρχικό **Επίπεδο 1**, σύμφωνα με το οποίο τα κράτη μέλη δεν διαθέτουν σαφώς καθορισμένη προσέγγιση για τη δημιουργία ικανοτήτων στον κυβερνοχώρο στους τομείς που καλύπτονται από τους στόχους των ΕΣΑΚ και καταλήγοντας στο **Επίπεδο 5**, σύμφωνα με το οποίο η στρατηγική οικοδόμησης ικανοτήτων ασφάλειας στον κυβερνοχώρο είναι δυναμική και προσαρμόσιμη στις περιβαλλοντικές εξελίξεις. Ο Πίνακας 4 δείχνει την κλίμακα επιπέδου ωριμότητας με περιγραφή κάθε επιπέδου ωριμότητας.

Πίνακας 4: Η κλίμακα ωριμότητας πέντε επιπέδων του Εθνικού Πλαισίου Αξιολόγησης Ικανοτήτων του ENISA

ΕΠΙΠΕΔΟ 1 - ΑΡΧΙΚΟ/AD HOC ΣΤΑΔΙΟ	ΕΠΙΠΕΔΟ 2 - ΕΓΚΑΙΡΟΣ ΚΑΘΟΡΙΣΜΟΣ	ΕΠΙΠΕΔΟ 3 - ΕΦΑΡΜΟΓΗ	ΕΠΙΠΕΔΟ 4 - ΒΕΛΤΙΣΤΟΠΟΙΗΣΗ	ΕΠΙΠΕΔΟ 5 - ΠΡΟΣΑΡΜΟΓΗ
Το κράτος μέλος δεν έχει σαφώς καθορισμένη προσέγγιση για τη δημιουργία ικανοτήτων ασφάλειας στον κυβερνοχώρο στους τομείς που καλύπτονται από τους στόχους της ΕΣΑΚ. Ωστόσο, η χώρα μπορεί να εφαρμόζει κάποιους γενικούς στόχους και να έχει διενεργήσει ορισμένες μελέτες (τεχνικές, πολιτικές) για τη βελτίωση των εθνικών ικανοτήτων.	Ορίστηκε η εθνική προσέγγιση για τη δημιουργία ικανοτήτων στον τομέα που καλύπτεται από τους στόχους της ΕΣΑΚ. Τα σχέδια δράσης ή οι δραστηριότητες για την επίτευξη των αποτελεσμάτων εφαρμόζονται, αλλά βρίσκονται σε πρώιμο στάδιο. Επιπλέον, ενδέχεται να έχουν προσδιοριστεί ή/και δεσμευτεί ενεργά συμμετέχοντες ενδιαφερόμενοι.	Το σχέδιο δράσης για τη δημιουργία ικανοτήτων στον τομέα που καλύπτεται από τους στόχους της ΕΣΑΚ ορίζεται σαφώς και υποστηρίζεται από τους σχετικούς ενδιαφερόμενους φορείς. Οι πρακτικές και οι δραστηριότητες επιβάλλονται και εφαρμόζονται ομοιόμορφα σε εθνικό επίπεδο. Οι δραστηριότητες καθορίζονται και τεκμηριώνονται με σαφή κατανομή πόρων και διακυβέρνηση, καθώς και με ένα σύνολο προθεσμιών.	Το σχέδιο δράσης αξιολογείται σε τακτική βάση: θέτει προτεραιότητες, είναι βελτιστοποιημένο και βιώσιμο. Οι επιδόσεις των δραστηριοτήτων δημιουργίας ικανοτήτων στον κυβερνοχώρο μετράται τακτικά. Προσδιορίζονται παράγοντες επιτυχίας, προκλήσεις και κενά στην υλοποίηση των δραστηριοτήτων.	Η στρατηγική δημιουργίας ικανοτήτων στον κυβερνοχώρο είναι δυναμική και προσαρμόσιμη. Η συνεχής προσοχή στις περιβαλλοντικές εξελίξεις (τεχνολογικές εξελίξεις, παγκόσμιες συγκρούσεις, νέες απειλές…) ενισχύει την ικανότητα ταχείας λήψης αποφάσεων και την ικανότητα ταχείας δράσης για βελτίωση.

3.3 ΔΕΣΜΕΣ ΚΑΙ ΕΝΙΑΙΑ ΔΟΜΗ ΤΟΥ ΠΛΑΙΣΙΟΥ ΑΥΤΟΑΞΙΟΛΟΓΗΣΗΣ

Το πλαίσιο αυτοαξιολόγησης χαρακτηρίζεται από**τέσσερις δέσμες**: (I) Διακυβέρνηση και πρότυπα ασφάλειας στον κυβερνοχώρο, (II) Δημιουργία ικανοτήτων και ευαισθητοποίηση, (III) Νομοθετικό και ρυθμιστικό πλαίσιο και (IV) Συνεργασία. Κάθε μία από τις εν λόγω δέσμες καλύπτει έναν βασικό θεματικό τομέα για τη δημιουργία της ικανότητας ασφάλειας στον κυβερνοχώρο σε μια χώρα και περιέχει ένα σύνολο διαφορετικών στόχων που τα κράτη μέλη θα μπορούσαν να συμπεριλάβουν στις ΕΣΑΚ τους. Ειδικότερα:

- **(I) Διακυβέρνηση και πρότυπα ασφάλειας στον κυβερνοχώρο**: αυτή η δέσμη μετρά την ικανότητα των κρατών μελών να θεσπίζουν σωστή διακυβέρνηση, πρότυπα και ορθές πρακτικές στον τομέα της ασφάλειας στον κυβερνοχώρο. Αυτή η διάσταση λαμβάνει υπόψη διαφορετικές πτυχές της άμυνας στον κυβερνοχώρο και της ανθεκτικότητας, ενώ υποστηρίζει την ανάπτυξη του εθνικού κλάδου ασφάλειας στον κυβερνοχώρο και την οικοδόμηση εμπιστοσύνης στις κυβερνήσεις·
- **(II) Δημιουργία ικανοτήτων και ευαισθητοποίηση**: αυτή η δέσμη αξιολογεί την ικανότητα των κρατών μελών να μεριμνούν για την ευαισθητοποίηση σχετικά με τους κινδύνους και τις απειλές σχετικά με την ασφάλεια στον κυβερνοχώρο και τον τρόπο αντιμετώπισής τους. Επιπλέον, η εν λόγω διάσταση μετρά την ικανότητα της χώρας να δημιουργεί συνεχώς ικανότητες ασφάλειας στον κυβερνοχώρο και να αυξάνει το συνολικό επίπεδο γνώσεων και δεξιοτήτων σε αυτόν τον τομέα. Εξετάζει την ανάπτυξη της αγοράς της ασφάλειας στον κυβερνοχώρο και τις εξελίξεις της Ε&Α στον τομέα της ασφάλειας στον κυβερνοχώρο. Αυτή η δέσμη συγκεντρώνει όλους τους στόχους που θέτουν τις βάσεις για την ενίσχυση της ανάπτυξης ικανοτήτων·
- **(III) Νομοθετικό και ρυθμιστικό πλαίσιο**: η δέσμη αυτή μετρά την ικανότητα των κρατών μελών να εφαρμόζουν τα απαραίτητα νομικά και ρυθμιστικά μέσα για την αντιμετώπιση και την καταπολέμηση της αύξησης του εγκλήματος στον κυβερνοχώρο και των σχετικών περιστατικών στον κυβερνοχώρο, και να προστατεύουν την υποδομή

πληροφοριών κρίσιμης σημασίας. Επιπλέον, αυτή η διάσταση αξιολογεί επίσης την ικανότητα των κρατών μελών να δημιουργήσουν ένα νομικό πλαίσιο για την προστασία των πολιτών και των επιχειρήσεων, όπως για παράδειγμα στην περίπτωση της εξισορρόπησης της ασφάλειας και της ιδιωτικής ζωής.

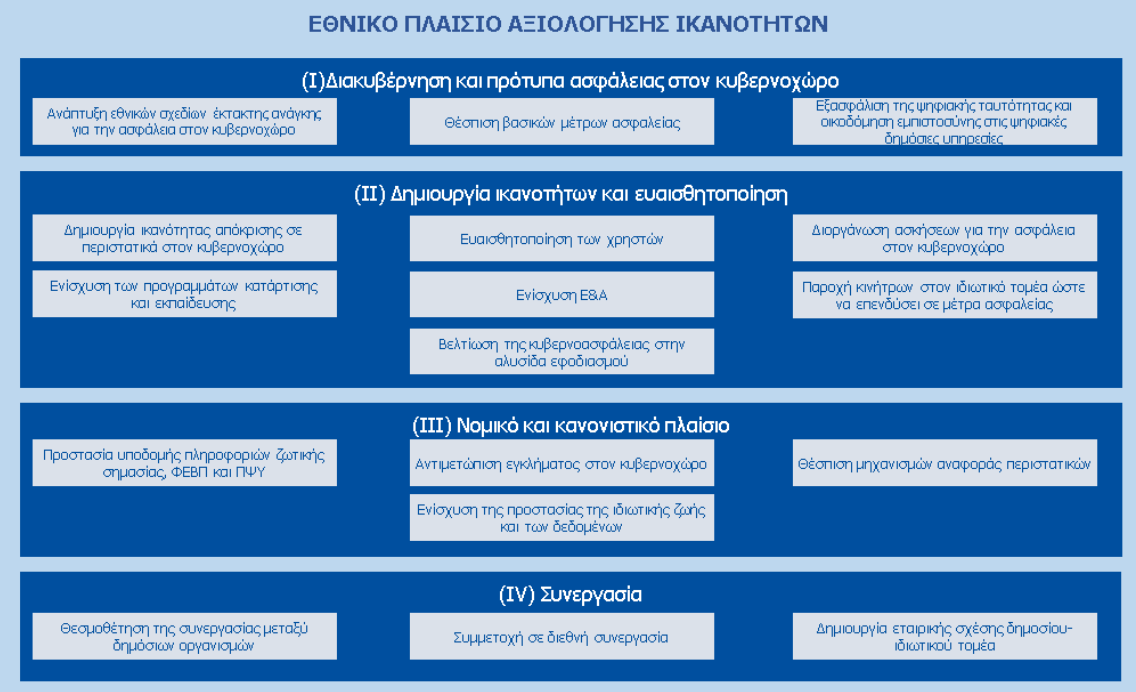
- **(IV) Συνεργασία:** η δέσμη αυτή αξιολογεί τη συνεργασία και την ανταλλαγή πληροφοριών μεταξύ διαφορετικών ομάδων ενδιαφερομένων σε εθνικό και διεθνές επίπεδο ως σημαντικό εργαλείο για την καλύτερη κατανόηση και ανταπόκριση σε ένα συνεχώς μεταβαλλόμενο περιβάλλον απειλών.

Οι στόχοι που συμπεριλήφθηκαν στο μοντέλο είναι αυτοί που συνήθως εγκρίνονται από τα κράτη μέλη και έχουν επιλεγεί μεταξύ των στόχων που αναφέρονται στην ενότητα 2.2. Συγκεκριμένα, το μοντέλο αξιολογεί τους ακόλουθους στόχους:

- 1. Ανάπτυξη εθνικών σχεδίων έκτακτης ανάγκης για την ασφάλεια στον κυβερνοχώρο (I)
- 2. Θέσπιση βασικών μέτρων ασφαλείας (I)
- 3. Εξασφάλιση της ψηφιακής ταυτότητας και οικοδόμηση εμπιστοσύνης στις ψηφιακές δημόσιες υπηρεσίες (I)
- 4. Δημιουργία ικανότητας απόκρισης σε περιστατικά στον κυβερνοχώρο (II)
- 5. Ευαισθητοποίηση των χρηστών (II)
- 6. Διοργάνωση ασκήσεων για την ασφάλεια στον κυβερνοχώρο (II)
- 7. Ενίσχυση των προγραμμάτων κατάρτισης και εκπαίδευσης (II)
- 8. Ενίσχυση E&A (II)
- 9. Παροχή κινήτρων στον ιδιωτικό τομέα ώστε να επενδύσει σε μέτρα ασφαλείας (II)
- 10. Βελτίωση της κυβερνοασφάλειας στην αλυσίδα εφοδιασμού (II)
- 11. Προστασία υποδομής πληροφοριών ζωτικής σημασίας, ΦΕΒΠ και ΠΨΥ (III)
- 12. Αντιμετώπιση εγκλήματος στον κυβερνοχώρο (III)
- 13. Θέσπιση μηχανισμών αναφοράς περιστατικών (III)
- 14. Ενίσχυση της προστασίας της ιδιωτικής ζωής και των δεδομένων (III)
- 15. Θεσμοθέτηση της συνεργασίας μεταξύ δημόσιων οργανισμών (IV)
- 16. Συμμετοχή σε διεθνή συνεργασία (IV)
- 17. Δημιουργία σύμπραξης δημόσιου και ιδιωτικού τομέα (IV)

Οι τέσσερις δέσμες και οι υποκείμενοι στόχοι συνδυάζονται στο μοντέλο για να υπάρξει μια ολοκληρωμένη εικόνα της ωριμότητας των ικανοτήτων ασφάλειας στον κυβερνοχώρο των κρατών μελών. Η Εικόνα 1 παρουσιάζει τη γενική δομή του πλαισίου αυτοαξιολόγησης και δείχνει πώς τα εν λόγω στοιχεία, συγκεκριμένα, οι στόχοι, οι δέσμες και το πλαίσιο αυτοαξιολόγησης, συνδέονται με την αξιολόγηση των επιδόσεων μιας χώρας.

Εικόνα 1: Δομή πλαισίου αυτοαξιολόγησης



Για κάθε στόχο που περιλαμβάνεται στο πλαίσιο αυτοαξιολόγησης, υπάρχει μια σειρά δεικτών που κατανέμονται μεταξύ των πέντε επιπέδων ωριμότητας. Κάθε δείκτης βασίζεται σε μια διχοτομική (ναι/όχι) ερώτηση. Ο δείκτης μπορεί να είναι απαιτούμενος ή μη απαιτούμενος.

3.4 ΜΗΧΑΝΙΣΜΟΣ ΒΑΘΜΟΛΟΓΗΣΗΣ

Ο **μηχανισμός βαθμολόγησης** του πλαισίου αυτοαξιολόγησης λαμβάνει υπόψη τα προαναφερθέντα στοιχεία και τις αρχές που απαριθμούνται στην ενότητα 3.5. Στην πραγματικότητα, το μοντέλο παρέχει μια βαθμολογία με βάση την τιμή δύο παραμέτρων, του **επιπέδου ωριμότητας** και του **λόγου κάλυψης**. Κάθε μία από αυτές τις παραμέτρους μπορεί να υπολογιστεί σε διαφορετικά επίπεδα: ανά στόχο, (ii) ανά ομάδα στόχων ή (iii) συνολικά.

Βαθμολογίες σε αντικειμενικό επίπεδο

Η **βαθμολογία του επιπέδου ωριμότητας** παρέχει μια επισκόπηση του επιπέδου ωριμότητας δείχνοντας ποιες ικανότητες και πρακτικές εφαρμόστηκαν. Η βαθμολογία του επιπέδου ωριμότητας υπολογίζεται ως το υψηλότερο επίπεδο για το οποίο ο ερωτώμενος ικανοποίησε όλες τις προϋποθέσεις (*δηλαδή* απάντηση ΝΑΙ σε όλες τις απαιτούμενες ερωτήσεις), εκτός από το ότι πληρούσε όλες τις προϋποθέσεις των προηγούμενων επιπέδων ωριμότητας.

Ο **λόγος κάλυψης** δείχνει την έκταση κάλυψης όλων των δεικτών για τους οποίους η απάντηση είναι θετική, ανεξάρτητα από το επίπεδό τους. Πρόκειται για μια συμπληρωματική τιμή που λαμβάνει υπόψη όλους τους δείκτες που μετρούν έναν στόχο. Ο λόγος κάλυψης υπολογίζεται ως η αναλογία μεταξύ του συνολικού αριθμού ερωτήσεων εντός του στόχου και του αριθμού ερωτήσεων για τις οποίες η απάντηση είναι θετική.

Είναι σημαντικό να διευκρινιστεί ότι για το υπόλοιπο έγγραφο, η ***βαθμολογία*** λέξεων χρησιμοποιείται για να αναφέρεται τόσο στις τιμές του επιπέδου ωριμότητας όσο και στον λόγο κάλυψης.

Εικόνα 2 - Ο μηχανισμός βαθμολόγησης ανά στόχο παρέχει μια απεικόνιση του μηχανισμού αξιολόγησης που περιγράφεται στην ενότητα 3.1 και αναλύεται στη συνέχεια.

Εικόνα 2: Μηχανισμός βαθμολόγησης ανά στόχο

Η Εικόνα 2 δείχνει ένα παράδειγμα του τρόπου υπολογισμού του επιπέδου ωριμότητας ανά στόχο. Αξίζει να σημειωθεί ότι ο ερωτώμενος πληρούσε όλες τις προϋποθέσεις των τριών πρώτων επιπέδων ωριμότητας και πληρούσε μόνο εν μέρει εκείνες του επιπέδου 4. Ως εκ τούτου, η βαθμολογία δείχνει ότι το ***επίπεδο ωριμότητας του ερωτώμενου είναι Επίπεδο 3 για τον σκοπό «Οργάνωση της άσκησης κυβερνοασφάλειας»****.*

Ωστόσο, στο παράδειγμα που απεικονίζεται στην Εικόνα 2, το επίπεδο ωριμότητας του στόχου δεν είναι σε θέση να καταγράψει τις πληροφορίες που παρέχονται από τους δείκτες που έχουν θετική βαθμολογία και αφορούν ανώτερο επίπεδο ωριμότητας από το Επίπεδο ωριμότητας 3. Σε αυτήν την περίπτωση, ο λόγος κάλυψης μπορεί να παράσχει μια επισκόπηση όλων των στοιχείων που ο ερωτώμενος εφάρμοσε προκειμένου να επιτύχει τον εν λόγω στόχο, ανεξαρτήτως του υφιστάμενου επιπέδου ωριμότητάς του. Σε αυτήν την περίπτωση, ο λόγος κάλυψης μεταξύ του συνολικού αριθμού ερωτήσεων εντός του στόχου και του αριθμού ερωτήσεων για τις οποίες η απάντηση είναι θετική ισούται με 19/27, δηλαδή ***η τιμή του λόγου κάλυψης είναι 70 %.***

Επιπλέον, για να προσαρμοστεί στις ιδιαιτερότητες των κρατών μελών, επιτρέποντας ταυτόχρονα μια συνεπή επισκόπηση, η βαθμολογία υπολογίζεται από δύο διαφορετικά δείγματα σε επίπεδο δέσμης και σε συνολικό επίπεδο:

- **Γενικές βαθμολογίες:** ένα πλήρες δείγμα που καλύπτει όλους τους στόχους που περιλαμβάνονται στη δέσμη ή στο συνολικό πλαίσιο (από ένα έως 17)·
- **Ειδικές βαθμολογίες:** ένα συγκεκριμένο δείγμα που καλύπτει μόνο τους στόχους που επιλέγει το κράτος μέλος (που συνήθως αντιστοιχούν στους στόχους που περιλαμβάνονται στην ΕΣΑΚ της συγκεκριμένης χώρας) εντός της δέσμης ή εντός του γενικού πλαισίου.

Βαθμολογίες σε επίπεδο δέσμης

Το **γενικό επίπεδο ωριμότητας κάθε δέσμης** υπολογίζεται ως ο αριθμητικός μέσος όρος του επιπέδου ωριμότητας όλων των στόχων εντός της εν λόγω δέσμης.

Το **ειδικό επίπεδο ωριμότητας κάθε δέσμης** υπολογίζεται ως ο αριθμητικός μέσος όρος του επιπέδου ωριμότητας των στόχων εντός αυτής της δέσμης που το κράτος μέλος επέλεξε να αξιολογήσει (συνήθως αντιστοιχεί στους στόχους της ΕΣΑΚ της συγκεκριμένης χώρας).

Για παράδειγμα, η Εικόνα 1 δείχνει ότι η δέσμη (Ι) Διακυβέρνηση και πρότυπα ασφάλειας στον κυβερνοχώρο αποτελείται από τρεις στόχους. Εάν υποθέσουμε ότι ο ερωτώμενος επέλεξε να αξιολογήσει μόνο τους δύο πρώτους στόχους, αλλά όχι τον τρίτο, και ότι οι δύο πρώτοι στόχοι παρουσιάζουν αντίστοιχα ένα επίπεδο ωριμότητας 2 και 4, τότε το επίπεδο ωριμότητας της δέσμης λαμβάνοντας υπόψη όλους τους στόχους είναι Επίπεδο 2 (γενικό επίπεδο ωριμότητας Δέσμης (Ι) = (2 + 4)/3), ενώ το επίπεδο ωριμότητας της δέσμης λαμβάνοντας υπόψη μόνο τους συγκεκριμένους στόχους που επιλέγει ο αξιολογητής είναι το Επίπεδο 3 (ειδικό επίπεδο ωριμότητας Δέσμης (Ι) = (2 +4)/2).

Ο **γενικός λόγος κάλυψης κάθε δέσμης** υπολογίζεται ως η αναλογία μεταξύ του συνολικού αριθμού ερωτήσεων εντός της δέσμης και του αριθμού ερωτήσεων για τις οποίες η απάντηση είναι θετική.

Ο **ειδικός λόγος κάλυψης κάθε δέσμης** υπολογίζεται ως η αναλογία μεταξύ του συνολικού αριθμού ερωτήσεων εντός της δέσμης σε σχέση με τους στόχους που το κράτος μέλος επέλεξε να αξιολογήσει (συνήθως αντιστοιχεί στους στόχους της ΕΣΑΚ της συγκεκριμένης χώρας) και του αριθμού των ερωτήσεων για τις οποίες η απάντηση είναι θετική.

Βαθμολογίες σε συνολικό επίπεδο

Το **συνολικόγενικό επίπεδο ωριμότητας μιας χώρας** υπολογίζεται ως ο αριθμητικός μέσος όρος του επιπέδου ωριμότητας όλων των στόχων εντός του πλαισίου, από ένα έως 17.

Το **συνολικό ειδικό επίπεδο ωριμότητας κάθε δέσμης** υπολογίζεται ως ο αριθμητικός μέσος όρος του επιπέδου ωριμότητας των στόχων εντός του πλαισίου που το κράτος μέλος επέλεξε να αξιολογήσει (συνήθως αντιστοιχεί στους στόχους της ΕΣΑΚ της συγκεκριμένης χώρας).

Ο **συνολικός γενικός λόγος κάλυψης μιας χώρας** υπολογίζεται ως η αναλογία μεταξύ του συνολικού αριθμού ερωτήσεων εντός του πλαισίου (από ένα έως 17) και του αριθμού ερωτήσεων για τις οποίες η απάντηση είναι θετική.

Ο **συνολικός ειδικός λόγος κάλυψης** μιας χώρας **υπολογίζεται ως η αναλογία μεταξύ του συνολικού αριθμού ερωτήσεων εντός των στόχων στο πλαίσιο που το κράτος μέλος επέλεξε να αξιολογήσει (συνήθως αντιστοιχεί στους στόχους της ΕΣΑΚ της συγκεκριμένης χώρας) και του αριθμού των ερωτήσεων για τις οποίες η απάντηση είναι θετική.**

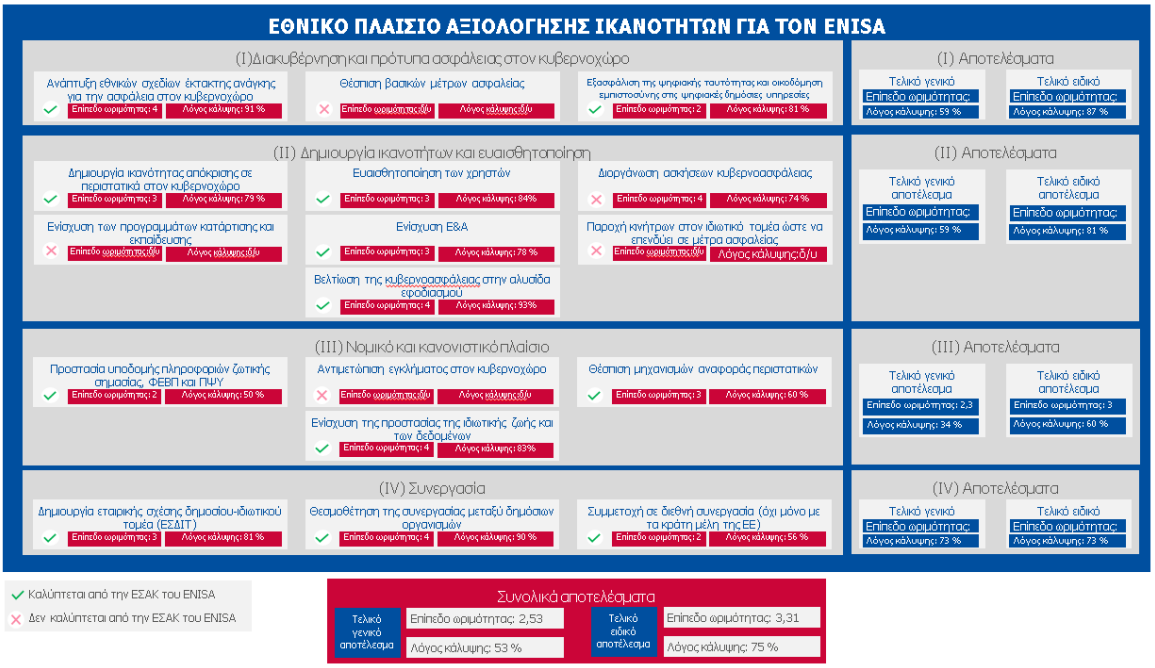
Για κάθε δείκτη, οι ερωτηθέντες μπορούν να επιλέξουν μια τρίτη επιλογή «δεν ξέρω/δεν ισχύει» για την απάντησή τους. Σε αυτήν την περίπτωση, ο δείκτης εξαιρείται από τον συνολικό υπολογισμό των αποτελεσμάτων.

Τα επίπεδα ωριμότητας σε επίπεδο δέσμης και σε συνολικό επίπεδο υπολογίζονται με έναν αριθμητικό μέσο όρο προκειμένου να παρουσιαστεί η πρόοδος μεταξύ δύο αξιολογήσεων. Πράγματι, η εναλλακτική λύση που συνίσταται στον υπολογισμό του επιπέδου ωριμότητας της δέσμης και του συνολικού επιπέδου ωριμότητας ως του επιπέδου ωριμότητας του λιγότερο ανεπτυγμένου στόχου – αν και είναι χρήσιμη από άποψη ωριμότητας – δεν μπορεί να εξηγήσει την πρόοδο που έχει σημειωθεί σε τομείς που καλύπτονται από άλλους στόχους.

Δεδομένου ότι το επίπεδο δέσμης και το συνολικό επίπεδο ενοποιούνται για σκοπούς αναφοράς, έχει γίνει η επιλογή να χρησιμοποιηθεί ο αριθμητικός μέσος όρος. Για περισσότερη ακρίβεια, χρησιμοποιήστε τις βαθμολογίες σε επίπεδο στόχου για σκοπούς αναφοράς.

Η εικόνα 3 κατωτέρω συνοψίζει τους μηχανισμούς βαθμολόγησης σε όλα τα διαφορετικά επίπεδα του μοντέλου (στόχος, δέσμη, σύνολο).

Εικόνα 3: Συνολικός μηχανισμός βαθμολόγησης



3.5 ΑΠΑΙΤΗΣΕΙΣ ΓΙΑ ΤΟ ΠΛΑΙΣΙΟ ΑΥΤΟΑΞΙΟΛΟΓΗΣΗΣ

Το εθνικό πλαίσιο αξιολόγησης ικανοτήτων που παρουσιάζεται σε αυτό το τμήμα βασίζεται στις ανάγκες που επισημαίνονται από τα κράτη μέλη και βασίζεται σε ένα σύνολο απαιτήσεων που αναφέρονται στη συνέχεια:

- Το ΕΠΑΙ αναπτύσσεται σε εθελοντική βάση από το κράτος μέλος ως πλαίσιο αυτοαξιολόγησης·
- Το ΕΠΑΙ αποσκοπεί στη μέτρηση των ικανοτήτων ασφάλειας στον κυβερνοχώρο των κρατών μελών σε σχέση με τους 17 στόχους. Ωστόσο, το κράτος μέλος μπορεί να επιλέξει τους στόχους που θέλει να αξιολογήσει και να αξιολογήσει μόνο ένα υποσύνολο των 17 στόχων.
- Το πλαίσιο αυτοαξιολόγησης αποσκοπεί στη μέτρηση του επιπέδου ωριμότητας των ικανοτήτων ασφάλειας στον κυβερνοχώρο του κράτους μέλους·
- Τα αποτελέσματα της αξιολόγησης δεν δημοσιεύονται εκτός εάν το κράτος μέλος αποφασίσει να το πράξει με δική του πρωτοβουλία·

- Το κράτος μέλος μπορεί να αναφέρει τα αποτελέσματα της αξιολόγησης παρουσιάζοντας το επίπεδο ωριμότητας των ικανοτήτων ασφάλειας στον κυβερνοχώρο της χώρας, μιας δέσμης στόχων ή ακόμη και ενός μοναδικού στόχου·
- Όλοι οι αξιολογηθέντες στόχοι είναι εξίσου συναφείς με το πλαίσιο αξιολόγησης, επομένως έχουν την ίδια σημασία. Το ίδιο ισχύει και για τους δείκτες που χρησιμοποιούνται σε αυτό· και
- Το κράτος μέλος μπορεί να παρακολουθεί την πρόοδό του σε βάθος χρόνου.

Το πλαίσιο αυτοαξιολόγησης στοχεύει στη στήριξη των κρατών μελών κατά τη δημιουργία ικανοτήτων ασφάλειας στον κυβερνοχώρο. Ως εκ τούτου, περιλαμβάνει επίσης ένα σύνολο συστάσεων ή κατευθυντήριων γραμμών για την καθοδήγηση των ευρωπαϊκών χωρών στη βελτίωση του επιπέδου ωριμότητάς τους.

Σημείωση: οι εν λόγω συστάσεις ή οδηγίες είναι γενικές βάσει δημοσιεύσεων του ENISA και διδαγμάτων που έχουν αντληθεί από άλλες χώρες και θα βασίζονται στο αποτέλεσμα της αυτοαξιολόγησης.

4. ΔΕΙΚΤΕΣ ΕΠΑΙ

4.1 ΔΕΙΚΤΕΣ ΠΛΑΙΣΙΟΥ

Το παρόν τμήμα παρουσιάζει τους δείκτες του Εθνικού Πλαισίου Αξιολόγησης Ικανοτήτων του ENISA. Τα ακόλουθα τμήματα οργανώνονται ανά δέσμη.

Για κάθε δέσμη, ένας πίνακας παρουσιάζει το πλήρες σύνολο δεικτών με τη μορφή ερωτήσεων που είναι αντιπροσωπευτικές ενός δεδομένου επιπέδου ωριμότητας. Το ερωτηματολόγιο είναι το κύριο μέσο για την αυτοαξιολόγηση. Για κάθε στόχο, υπάρχουν δύο σειρές δεικτών που πρέπει να σημειωθούν:

- Μια σειρά γενικών στρατηγικών ερωτήσεων ωριμότητας (9 γενικές ερωτήσεις), οι οποίες σημειώνονται από το α) έως το γ) για κάθε επίπεδο ωριμότητας και επαναλαμβάνονται για κάθε στόχο· και
- Μια σειρά ερωτήσεων σχετικά με τις ικανότητες ασφάλειας στον κυβερνοχώρο (319 ερωτήσεις ικανοτήτων ασφάλειας στον κυβερνοχώρο), που αριθμούνται από το «1» έως το «10» για κάθε επίπεδο ωριμότητας, και αφορούν τον τομέα που καλύπτεται από τον στόχο.

Κάθε ερώτηση παρουσιάζεται με μια ετικέτα (0-1) που δείχνει εάν η ερώτηση αποτελεί απαιτούμενο δείκτη (1) ή μη απαιτούμενο δείκτη (0) για το επίπεδο ωριμότητας.

Κάθε ερώτηση μπορεί να αναγνωριστεί από έναν αριθμό αναγνώρισης που αποτελείται από:

- Τον αριθμό στόχου·
- Το επίπεδο ωριμότητας· και
- Τον αριθμό ερώτησης.

Για παράδειγμα, η ερώτηση με αναγνωριστικό αριθμό 1.2.4 είναι το τέταρτο ερώτημα στο επίπεδο ωριμότητας 2 του στρατηγικού στόχου (I) «Ανάπτυξη εθνικών σχεδίων έκτακτης ανάγκης για την ασφάλεια στον κυβερνοχώρο».

Πρέπει να σημειωθεί ότι στο ερωτηματολόγιο, το αντικείμενο των ερωτήσεων είναι σε εθνικό επίπεδο εκτός εάν αναφέρεται διαφορετικά. Σε όλες τις ερωτήσεις, η αντωνυμία «Εσείς» αναφέρεται στο κράτος μέλος με γενικό τρόπο και δεν αναφέρεται στο άτομο ή στον κυβερνητικό φορέα που διενεργεί την αξιολόγηση.

Ο ορισμός κάθε στόχου βρίσκεται στο κεφάλαιο 2.2 - Κοινοί στόχοι που προσδιορίζονται στις ευρωπαϊκές ΕΣΑΚ.

4.1.1 Δέσμη #1: Διακυβέρνηση και πρότυπα ασφάλειας στον κυβερνοχώρο

Στόχος ΕΣΑΚ	#	Επίπεδο 1	R	Επίπεδο 2	R	Επίπεδο 3	R	Επίπεδο 4	R	Επίπεδο 5	R
1 – Ανάπτυξη εθνικών σχεδίων έκτακτης ανάγκης για την ασφάλεια στον κυβερνοχώρο	α	Έχετε συμπεριλάβει τον στόχο στην τρέχουσα ΕΣΑΚ, ή σκοπεύετε να τον συμπεριλάβετε στην επόμενη έκδοση;	1	Υπάρχουν άτυπες πρακτικές ή δραστηριότητες που συμβάλλουν στην επίτευξη του στόχου με μη συντεταγμένο τρόπο;	1	Διαθέτετε επίσημα καθορισμένο και τεκμηριωμένο σχέδιο δράσης;	1	Επανεξετάζετε το σχέδιο δράσης σας ως προς τον στόχο του για να ελέγξετε την απόδοσή του;	1	Έχετε θεσπίσει μηχανισμούς για να διασφαλίσετε ότι το σχέδιο δράσης προσαρμόζεται με δυναμικό τρόπο στις περιβαλλοντικές εξελίξεις;	1
	β			Ορίσατε τα επιδιωκόμενα αποτελέσματα, τις κατευθυντήριες αρχές ή τις βασικές δραστηριότητες του σχεδίου δράσης σας;	1	Διαθέτετε σχέδιο δράσης με σαφή κατανομή πόρων και διακυβέρνηση;	1	Επανεξετάζετε το σχέδιο δράσης σας ως προς τον στόχο του για να διασφαλίσετε ότι οι προτεραιότητες είναι σωστά ιεραρχημένες και ότι το σχέδιο σας έχει βελτιστοποιηθεί;	1		
	γ			Κατά περίπτωση, το σχέδιο δράσης σας υλοποιείται και είναι ήδη αποτελεσματικό σε περιορισμένο πεδίο εφαρμογής;	0						
	1	Ξεκινήσατε να εργάζεστε για τη δημιουργία εθνικών σχεδίων έκτακτης ανάγκης για την ασφάλεια στον κυβερνοχώρο; *π.χ.*καθορίζοντας τους γενικούς στόχους, το αντικείμενο ή/και τις αρχές των σχεδίων έκτακτης ανάγκης...	1	Διαθέτετε κάποιο δόγμα/εθνική στρατηγική που περιλαμβάνει την ασφάλεια στον κυβερνοχώρο ως παράγοντα κρίσης (δηλαδή ένα σχέδιο στρατηγικής, μια πολιτική, κ.λπ.);	1	Έχετε κάποιο εθνικό σχέδιο διαχείρισης κρίσεων στον κυβερνοχώρο;	1	Είστε ικανοποιημένοι με τον αριθμό ή το ποσοστό των τομέων κρίσιμης σημασίας που περιλαμβάνονται στο εθνικό σχέδιο έκτακτης ανάγκης για την ασφάλεια κυβερνοχώρο;	1	Εφαρμόζετε κάποια διαδικασία άντλησης διδαγμάτων μετά από ασκήσεις για την ασφάλεια στον κυβερνοχώρο ή πραγματικές κρίσεις σε εθνικό επίπεδο;	1
	2	Είναι γενικά κατανοητό ότι τα περιστατικά στον κυβερνοχώρο αποτελούν παράγοντα κρίσης που θα μπορούσε να απειλήσει την εθνική ασφάλεια;	0	Διαθέτετε κάποια κεντρική βάση δεδομένων για την απόκτηση πληροφοριών και την ενημέρωση των υπευθύνων λήψης αποφάσεων; *δηλ.* τυχόν μεθόδους, πλατφόρμες ή τοποθεσίες για να διασφαλίζεται ότι όλοι οι φορείς αντιμετώπισης κρίσεων μπορούν να έχουν πρόσβαση στις ίδιες πληροφορίες σε πραγματικό χρόνο σχετικά με την κρίση στον κυβερνοχώρο.	1	Εφαρμόζετε διαδικασίες σε εθνικό επίπεδο που αφορούν κρίσεις στον κυβερνοχώρο;	1	Οργανώνετε αρκετά συχνά δραστηριότητες (δηλαδή ασκήσεις) που σχετίζονται με τον εθνικό προγραμματισμό έκτακτης ανάγκης για την ασφάλεια στον κυβερνοχώρο;	1	Εφαρμόζετε κάποια διαδικασία τακτικού ελέγχου του εθνικού σχεδίου;	1
	3	Έχουν διενεργηθεί μελέτες (τεχνικές, επιχειρησιακές, πολιτικές) στον τομέα του σχεδιασμού έκτακτης ανάγκης για την ασφάλεια στον κυβερνοχώρο;	0	Διατίθενται οι σχετικοί πόροι για την εποπτεία της ανάπτυξης και της εκτέλεσης εθνικών σχεδίων έκτακτης ανάγκης για την ασφάλεια στον κυβερνοχώρο;	1	Διαθέτετε ομάδα επικοινωνίας ειδικά εκπαιδευμένη να ανταποκρίνεται σε κυβερνητικές κρίσεις και να ενημερώνει το κοινό;	1	Διαθέτετε επαρκές προσωπικό που ασχολείται με τον σχεδιασμό αντιμετώπισης κρίσεων, τη μελέτη των αντληθέντων διδαγμάτων και την υλοποίηση αλλαγών;	1	Διαθέτετε επαρκή εργαλεία και πλατφόρμες για καλύτερη αντίληψη της κατάστασης;	1

	4	-		Εφαρμόζετε μεθοδολογία αξιολόγησης κυβερνοαπειλών σε εθνικό επίπεδο που περιλαμβάνει διαδικασίες εκτίμησης επιπτώσεων;	0	Αξιοποιείτε όλους τους σχετικούς εθνικούς ενδιαφερόμενους φορείς (εθνική ασφάλεια, άμυνα, πολιτική προστασία, αρχές επιβολής του νόμου, υπουργεία, αρχές κ.λπ.)	1	Διαθέτετε επαρκές εκπαιδευμένο προσωπικό για την αντιμετώπιση κρίσεων στον κυβερνοχώρο σε εθνικό επίπεδο;	1	Εφαρμόζετε συγκεκριμένο μοντέλο ωριμότητας για την παρακολούθηση και βελτίωση του σχεδίου έκτακτης ανάγκης για την ασφάλεια στον κυβερνοχώρο;	0
	5	-		-		Διαθέτετε επαρκείς εγκαταστάσεις διαχείρισης κρίσεων και κέντρα επιχειρήσεων;	1	-		Διαθέτετε πόρους που είτε ειδικεύονται στην πρόβλεψη απειλών είτε εκτελούν προγνωστικό έργο για την ασφάλεια στον κυβερνοχώρο ώστε να αντιμετωπίσετε κάποια μελλοντική κρίση ή προκλήσεις του αύριο;	0
	6	-		-		Συνεργάζεστε με διεθνείς ενδιαφερόμενους φορείς στην ΕΕ εάν απαιτείται;	0	-		-	
	7	-		-		Συνεργάζεστε με διεθνείς ενδιαφερόμενους φορείς σε χώρες εκτός της ΕΕ εάν απαιτείται;	0	-		-	

Στόχος ΕΣΑΚ	#	Επίπεδο 1	R	Επίπεδο 2	R	Επίπεδο 3	R	Επίπεδο 4	R	Επίπεδο 5	R
2 – Θέσπιση βασικών μέτρων ασφαλείας	α	Έχετε συμπεριλάβει τον στόχο στην τρέχουσα ΕΣΑΚ, ή σκοπεύετε να τον συμπεριλάβετε στην επόμενη έκδοση;	1	Υπάρχουν άτυπες πρακτικές ή δραστηριότητες που συμβάλλουν στην επίτευξη του στόχου με μη συντεταγμένο τρόπο;	1	Διαθέτετε επίσημα καθορισμένο και τεκμηριωμένο σχέδιο δράσης;	1	Επανεξετάζετε το σχέδιο δράσης σας ως προς τον στόχο του για να ελέγξετε την απόδοσή του;	1	Έχετε θεσπίσει μηχανισμούς για να διασφαλίσετε ότι το σχέδιο δράσης προσαρμόζεται με δυναμικό τρόπο στις περιβαλλοντικές εξελίξεις;	1
	β			Ορίσατε τα επιδιωκόμενα αποτελέσματα, τις κατευθυντήριες αρχές ή τις βασικές δραστηριότητες του σχεδίου δράσης σας;	1	Διαθέτετε σχέδιο δράσης με σαφή κατανομή πόρων και διακυβέρνηση;	1	Επανεξετάζετε το σχέδιο δράσης σας ως προς τον στόχο του για να διασφαλίσετε ότι οι προτεραιότητες είναι σωστά ιεραρχημένες και ότι το σχέδιο σας έχει βελτιστοποιηθεί;	1		
	γ			Κατά περίπτωση, το σχέδιο δράσης σας υλοποιείται και είναι ήδη αποτελεσματικό σε περιορισμένο πεδίο εφαρμογής;	0						
	1	Διενεργήσατε μελέτη για τον προσδιορισμό απαιτήσεων και ελλείψεων σε **δημόσιους** οργανισμούς βάσει διεθνώς αναγνωρισμένων προτύπων; *π.χ.* ISO27001, ISO27002, BS 15000, EN ISO27799, PCI-DSS, CobiT, ITIL, BSI IT-Grundschutz, IETF, IEEE, NIST, FIPS, ITU, ISA, IEC, CIS...	1	Τα μέτρα ασφαλείας λαμβάνονται σύμφωνα με διεθνή/εθνικά πρότυπα;	1	Τα βασικά μέτρα ασφαλείας είναι υποχρεωτικά;	1	Υπάρχει κάποια διαδικασία για τη συχνή επικαιροποίηση των βασικών μέτρων ασφαλείας;	1	Διαθέτετε διαδικασία αυστηροποίησης της ΤΠΕ όταν τα περιστατικά δεν αντιμετωπίζονται επιτυχώς;	1

	2	Διενεργήσατε μελέτη για τον προσδιορισμό απαιτήσεων και ελλείψεων σε **ιδιωτικούς** οργανισμούς βάσει διεθνώς αναγνωρισμένων προτύπων; π.χ. ISO27001, ISO27002, BS 15000, EN ISO27799, PCI-DSS, CobiT, ITIL, BSI IT-Grundschutz, IETF, IEEE, NIST, FIPS, ITU, ISA, IEC, CIS...	1	Ζητείται η γνώμη του ιδιωτικού τομέα και άλλων ενδιαφερομένων κατά τον καθορισμό των βασικών μέτρων ασφαλείας;	1	Εφαρμόζετε οριζόντια μέτρα ασφαλείας σε τομείς κρίσιμης σημασίας;	1	Εφαρμόζεται μηχανισμός παρακολούθησης για την εξέταση της εφαρμογής βασικών μέτρων ασφαλείας;	1	Αξιολογείτε τη συνάφεια των νέων προτύπων που αναπτύσσονται ως απάντηση στις τελευταίες εξελίξεις στο τοπίο απειλών;	1
	3	-		-		Εφαρμόζετε τομεακά μέτρα ασφαλείας σε τομείς κρίσιμης σημασίας;	1	Υπάρχει εθνική αρχή για τον έλεγχο της επιβολής των βασικών μέτρων ασφαλείας;	1	Έχετε ή προωθείτε εθνική διαδικασία συντονισμένης δημοσιοποίησης τρωτών σημείων (CVD);	1
	4	-				Τα βασικά μέτρα ασφαλείας συνάδουν με τα σχετικά συστήματα πιστοποίησης;	1	Εφαρμόζετε διαδικασία για τον εντοπισμό μη συμμορφούμενων οργανισμών εντός συγκεκριμένης χρονικής περιόδου;	1	-	
	5	-		-		Εφαρμόζετε διαδικασία αυτοαξιολόγησης κινδύνων για τα βασικά μέτρα ασφαλείας;	1	Εφαρμόζετε διαδικασία ελέγχου για τη διασφάλιση της ορθής εφαρμογής των μέτρων ασφαλείας;	1	-	
Στόχος ΕΣΑΚ	**#**	**Επίπεδο 1**	**R**	**Επίπεδο 2**	**R**	**Επίπεδο 3**	**R**	**Επίπεδο 4**	**R**	**Επίπεδο 5**	**R**
2 – Θέσπιση βασικών μέτρων ασφαλείας	6	-		-		Εξετάζετε υποχρεωτικά βασικά μέτρα ασφαλείας στις διαδικασίες δημοσίων συμβάσεων κυβερνητικών φορέων;	0	Ορίζετε ή ενθαρρύνετε ενεργά την υιοθέτηση ασφαλών προτύπων για την ανάπτυξη προϊόντων ΤΠ/ΕΤ (ιατρικός εξοπλισμός, συνδεδεμένα και αυτόνομα οχήματα, επαγγελματικό ραδιόφωνο, εξοπλισμός βαριάς βιομηχανίας...);	0	-	

Στόχος ΕΣΑΚ	**#**	**Επίπεδο 1**	**R**	**Επίπεδο 2**	**R**	**Επίπεδο 3**	**R**	**Επίπεδο 4**	**R**	**Επίπεδο 5**	**R**
3 – Εξασφάλιση της ψηφιακής ταυτότητας και οικοδόμηση εμπιστοσύνης στις ψηφιακές δημόσιες υπηρεσίες	α	Έχετε συμπεριλάβει τον στόχο στην τρέχουσα ΕΣΑΚ, ή σκοπεύετε να τον συμπεριλάβετε στην επόμενη έκδοση;	1	Υπάρχουν άτυπες πρακτικές ή δραστηριότητες που συμβάλλουν στην επίτευξη του στόχου με μη συντεταγμένο τρόπο;	1	Διαθέτετε επίσημα καθορισμένο και τεκμηριωμένο σχέδιο δράσης;	1	Επανεξετάζετε το σχέδιο δράσης σας ως προς τον στόχο του για να ελέγξετε την απόδοσή του;	1	Έχετε θεσπίσει μηχανισμούς για να διασφαλίσετε ότι το σχέδιο δράσης προσαρμόζεται με δυναμικό τρόπο στις περιβαλλοντικές εξελίξεις;	1
	β			Ορίσατε τα επιδιωκόμενα αποτελέσματα, τις κατευθυντήριες αρχές ή τις βασικές δραστηριότητες του σχεδίου δράσης σας;	1	Διαθέτετε σχέδιο δράσης με σαφή κατανομή πόρων και διακυβέρνηση;	1	Επανεξετάζετε το σχέδιο δράσης σας ως προς τον στόχο του για να διασφαλίσετε ότι οι προτεραιότητες είναι σωστά ιεραρχημένες και ότι το σχέδιο σας έχει βελτιστοποιηθεί;	1		

	γ			Κατά περίπτωση, το σχέδιο δράσης σας υλοποιείται και είναι ήδη αποτελεσματικό σε περιορισμένο πεδίο εφαρμογής;	0						
	1	Έχετε πραγματοποιήσει μελέτες ή αναλύσεις των ελλείψεων για να προσδιορίσετε τις ανάγκες εξασφάλισης ψηφιακών δημόσιων υπηρεσιών σε πολίτες και επιχειρήσεις;	1	Πραγματοποιείτε αναλύσεις κινδύνου για να προσδιορίσετε το προφίλ κινδύνου περιουσιακών στοιχείων ή υπηρεσιών προτού τα μεταφέρετε στο υπολογιστικό νέφος (cloud) ή για να συμμετέχετε σε έργα ψηφιακού μετασχηματισμού;	1	Προωθείτε τις μεθοδολογίες προστασίας της ιδιωτικής ζωής ήδη από τον σχεδιασμό σε όλα τα έργα ηλεκτρονικής διακυβέρνησης;	1	Συλλέγετε δείκτες για περιστατικά στον κυβερνοχώρο που συνεπάγονται παραβίαση ψηφιακών δημόσιων υπηρεσιών;	1	Συμμετέχετε σε ευρωπαϊκές ομάδες εργασίας για τη διατήρηση προτύπων ή/και τον σχεδιασμό νέων απαιτήσεων για ηλεκτρονικές υπηρεσίες εμπιστοσύνης (ηλεκτρονικές υπογραφές, ηλεκτρονικές σφραγίδες, υπηρεσίες παράδοσης ηλεκτρονικού μητρώου, χρονοσφράγιση, επαλήθευση ταυτότητας ιστοτόπου); π.χ. ETSI/CEN/CENELEC, ISO, IETF, NIST, ITU ...	1
	2	-		Εφαρμόζετε στρατηγική για να δημιουργήσετε ή να προωθήσετε ασφαλή εθνικά συστήματα ηλεκτρονικής ταυτοποίησης (eID) για πολίτες και επιχειρήσεις;	1	Συμπεριλαμβάνετε ιδιωτικούς φορείς στον σχεδιασμό και στην παροχή ασφαλών ψηφιακών δημόσιων υπηρεσιών;	1	Έχετε εφαρμόσει την αμοιβαία αναγνώριση μέσων ηλεκτρονικής ταυτοποίησης με άλλα κράτη μέλη;	1	Συμμετέχετε ενεργά σε αξιολογήσεις από ομοτίμους στο πλαίσιο κοινοποίησης συστημάτων ηλεκτρονικής ταυτοποίησης (eID) στην Ευρωπαϊκή Επιτροπή;	1
	3	-		Εφαρμόζετε κάποια στρατηγική για τη δημιουργία ή την προώθηση ασφαλών εθνικών ηλεκτρονικών υπηρεσιών εμπιστοσύνης (ηλεκτρονικές υπογραφές, ηλεκτρονικές σφραγίδες, υπηρεσίες παράδοσης ηλεκτρονικού μητρώου, χρονοσφράγιση, επαλήθευση ταυτότητας ιστοτόπου) για πολίτες και επιχειρήσεις;	1	Εφαρμόζετε ελάχιστο βασικό επίπεδο ασφαλείας για όλες τις ψηφιακές δημόσιες υπηρεσίες;	1	-		-	

Στόχος ΕΣΑΚ	#	Επίπεδο 1	R	Επίπεδο 2	R	Επίπεδο 3	R	Επίπεδο 4	R	Επίπεδο 5	R
3 – Εξασφάλιση της ψηφιακής ταυτότητας και οικοδόμηση εμπιστοσύνης στις ψηφιακές δημόσιες υπηρεσίες	4	-		Έχετε μια στρατηγική για το κυβερνητικό υπολογιστικό νέφος (μια στρατηγική υπολογιστικού νέφους που επικεντρώνεται στην κυβέρνηση και στους δημόσιους φορείς όπως υπουργεία, κυβερνητικές υπηρεσίες και δημόσιες διοικήσεις...) που λαμβάνει υπόψη τις επιπτώσεις στην ασφάλεια;	0	Υπάρχουν διαθέσιμα συστήματα ηλεκτρονικής αναγνώρισης για πολίτες και επιχειρήσεις με ουσιαστικό ή υψηλό επίπεδο διασφάλισης όπως ορίζεται στο παράρτημα του κανονισμού eIDAS (ΕΕ) αριθ. 910/2014;	1	-		-	

	5	-		-		Διαθέτετε ψηφιακές δημόσιες υπηρεσίες που απαιτούν συστήματα ηλεκτρονικής ταυτοποίησης με ουσιαστικό ή υψηλό επίπεδο διασφάλισης όπως ορίζεται στο παράρτημα του κανονισμού eIDAS (ΕΕ) αριθ. 910/2014;	1	-		-	
	6	-		-		Διαθέτετε παρόχους υπηρεσιών εμπιστοσύνης για πολίτες και επιχειρήσεις (ηλεκτρονικές υπογραφές, ηλεκτρονικές σφραγίδες, υπηρεσίες παράδοσης ηλεκτρονικού μητρώου, χρονοσφράγιση, επαλήθευση ταυτότητας ιστοτόπου);	1	-		-	
	7	-		-		Προωθείτε την υιοθέτηση βασικών μέτρων ασφαλείας για όλα τα μοντέλα ανάπτυξης υπολογιστικού νέφους (π.χ. Ιδιωτικό, Δημόσιο, Υβριδικό) υποδομή ως υπηρεσία (IaaS), πλατφόρμα ως υπηρεσία (PaaS), λογισμικό ως υπηρεσία (SaaS);	0	-		-	

4.1.2 Δέσμη #2: Δημιουργία ικανοτήτων και ευαισθητοποίηση

Στόχος ΕΣΑΚ	#	Επίπεδο 1	R	Επίπεδο 2	R	Επίπεδο 3	R	Επίπεδο 4	R	Επίπεδο 5	R
4 – Δημιουργία ικανότητας απόκρισης σε περιστατικά στον κυβερνοχώρο	α	Έχετε συμπεριλάβει τον στόχο στην τρέχουσα ΕΣΑΚ, ή σκοπεύετε να τον συμπεριλάβετε στην επόμενη έκδοση;	1	Υπάρχουν άτυπες πρακτικές ή δραστηριότητες που συμβάλλουν στην επίτευξη του στόχου με μη συντεταγμένο τρόπο;	1	Διαθέτετε επίσημα καθορισμένο και τεκμηριωμένο σχέδιο δράσης;	1	Επανεξετάζετε το σχέδιο δράσης σας ως προς τον στόχο του για να ελέγξετε την απόδοσή του;	1	Έχετε θεσπίσει μηχανισμούς για να διασφαλίσετε ότι το σχέδιο δράσης προσαρμόζεται με δυναμικό τρόπο στις περιβαλλοντικές εξελίξεις;	1
	β			Ορίσατε τα επιδιωκόμενα αποτελέσματα, τις κατευθυντήριες αρχές ή τις βασικές δραστηριότητες του σχεδίου δράσης σας;	1	Διαθέτετε σχέδιο δράσης με σαφή κατανομή πόρων και διακυβέρνηση;	1	Επανεξετάζετε το σχέδιο δράσης σας ως προς τον στόχο του για να διασφαλίσετε ότι οι προτεραιότητες είναι σωστά ιεραρχημένες και ότι το σχέδιο σας έχει βελτιστοποιηθεί;	1		
	γ			Κατά περίπτωση, το σχέδιο δράσης σας υλοποιείται και είναι ήδη αποτελεσματικό σε περιορισμένο πεδίο εφαρμογής;	0						
	1	Διαθέτετε τη δυνατότητα άτυπης απόκρισης σε περιστατικά εντός ή μεταξύ δημόσιου και ιδιωτικού τομέα;	1	Έχετε τουλάχιστον μια επίσημη εθνική ομάδα παρέμβασης για συμβάντα που αφορούν την ασφάλεια υπολογιστών (CSIRT);	1	Έχετε την ικανότητα απόκρισης σε περιστατικά για τους τομείς που αναφέρονται στο παράρτημα ΙΙ της οδηγίας ΑΔΠ;	1	Έχετε καθορίσει και προωθήσει τυποποιημένες πρακτικές για διαδικασίες απόκρισης σε συμβάντα και συστήματα ταξινόμησης συμβάντων;	1	Διαθέτετε μηχανισμούς για την έγκαιρη ανίχνευση, τον εντοπισμό, την πρόληψη, την απόκριση και τον μετριασμό των τρωτών σημείων «ημέρας μηδέν»;	1
	2	-		Η/Οι εθνική(-ές) σας CSIRT έχει(-ουν) σαφώς καθορισμένο αντικείμενο παρέμβασης; *π.χ.* ανάλογα με τον στοχευμένο τομέα, τα είδη των συμβάντων, τις επιπτώσεις	1	Υπάρχει μηχανισμός συνεργασίας CSIRT στη χώρα σας για την απόκριση σε περιστατικά;	1	Αξιολογείτε την ικανότητα απόκρισής σας σε περιστατικά για να βεβαιωθείτε ότι διαθέτετε τους κατάλληλους πόρους και δεξιότητες για την εκτέλεση των καθηκόντων που ορίζονται στο σημείο 2) του παραρτήματος Ι της οδηγίας ΑΔΠ;	1	-	
	3	-		Η/Οι εθνική(-ές) σας CSIRT έχει(-ουν) σαφώς καθορισμένες σχέσεις με άλλους εθνικούς ενδιαφερόμενους σχετικά με το εθνικό τοπίο ασφάλειας στον κυβερνοχώρο και την πρακτική απόκρισης σε περιστατικά (π.χ. υπηρεσίες επιβολής του νόμου, στρατιωτικές αρχές, πάροχοι υπηρεσιών διαδικτύου, εθνικό κέντρο για την ασφάλεια στον κυβερνοχώρο);	0	Η/Οι εθνική(-ές) σας CSIRT έχει(-ουν) την ικανότητα απόκρισης σε περιστατικά σύμφωνα με το παράρτημα Ι της οδηγίας ΑΔΠ; *π.χ.* διαθεσιμότητα, φυσική ασφάλεια, επιχειρησιακή συνέχεια, διεθνής συνεργασία, παρακολούθηση περιστατικών, ικανότητα έγκαιρης προειδοποίησης και συναγερμού, απόκριση σε περιστατικά, ανάλυση κινδύνου και επίγνωση κατάστασης, συνεργασία με τον ιδιωτικό τομέα, τυποποιημένες πρακτικές...	1	-		-	

	4	-			Υπάρχει μηχανισμός συνεργασίας με άλλες γειτονικές χώρες σχετικά με περιστατικά;	1	-		-	
	5	-		-	Έχετε ορίσει επισήμως σαφείς πολιτικές και διαδικασίες χειρισμού περιστατικών;	1	-		-	
Στόχος ΕΣΑΚ	**#**	**Επίπεδο 1**	**R**	**Επίπεδο 2**	**R**	**Επίπεδο 3**	**R**	**Επίπεδο 4**	**R**	**Επίπεδο 5**	**R**
4 – Δημιουργία ικανότητας απόκρισης σε περιστατικά στον κυβερνοχώρο	6	-		-		Συμμετέχει(-ουν) η/οι εθνική(-ές) σας CSIRT σε ασκήσεις κυβερνοασφάλειας σε εθνικό και σε διεθνές επίπεδο;	1	-		-	
	7	-		-		Η/Οι εθνική(-οί) σας CSIRT συνδέονται με το FIRST (Φόρουμ για την απόκριση σε συμβάντα και ομάδες ασφαλείας);	0	-		-	

Στόχος ΕΣΑΚ	**#**	**Επίπεδο 1**	**R**	**Επίπεδο 2**	**R**	**Επίπεδο 3**	**R**	**Επίπεδο 4**	**R**	**Επίπεδο 5**	**R**
5 – Ευαισθητοποίηση των χρηστών	α	Έχετε συμπεριλάβει τον στόχο στην τρέχουσα ΕΣΑΚ, ή σκοπεύετε να τον συμπεριλάβετε στην επόμενη έκδοση;	1	Υπάρχουν άτυπες πρακτικές ή δραστηριότητες που συμβάλλουν στην επίτευξη του στόχου με μη συντεταγμένο τρόπο;	1	Διαθέτετε επίσημα καθορισμένο και τεκμηριωμένο σχέδιο δράσης;	1	Επανεξετάζετε το σχέδιο δράσης σας ως προς τον στόχο του για να ελέγξετε την απόδοσή του;	1	Έχετε θεσπίσει μηχανισμούς για να διασφαλίσετε ότι το σχέδιο δράσης προσαρμόζεται με δυναμικό τρόπο στις περιβαλλοντικές εξελίξεις;	1
	β			Ορίσατε τα επιδιωκόμενα αποτελέσματα, τις κατευθυντήριες αρχές ή τις βασικές δραστηριότητες του σχεδίου δράσης σας;	1	Διαθέτετε σχέδιο δράσης με σαφή κατανομή πόρων και διακυβέρνηση;	1	Επανεξετάζετε το σχέδιο δράσης σας ως προς τον στόχο του για να διασφαλίσετε ότι οι προτεραιότητες είναι σωστά ιεραρχημένες και ότι το σχέδιο σας έχει βελτιστοποιηθεί;	1		
	γ			Κατά περίπτωση, το σχέδιο δράσης σας υλοποιείται και είναι ήδη αποτελεσματικό σε περιορισμένο πεδίο εφαρμογής;	0						
	1	Υπάρχει ελάχιστη αναγνώριση από την κυβέρνηση, τον ιδιωτικό τομέα ή τους γενικούς χρήστες, ότι είναι αναγκαίο να καλλιεργηθεί η ευαισθητοποίηση για θέματα ασφάλειας στον κυβερνοχώρο και προστασίας της ιδιωτικής ζωής;	1	Έχετε προσδιορίσει ένα συγκεκριμένο κοινό-στόχο για την ευαισθητοποίηση των χρηστών; *π.χ.* γενικοί χρήστες, νέοι, επιχειρηματικοί χρήστες (που μπορούν να αναλυθούν περαιτέρω: ΜΜΕ, φορείς εκμετάλλευσης βασικών υπηρεσιών, πάροχοι ψηφιακών υπηρεσιών κ.λπ.)	1	Έχετε αναπτύξει σχέδια επικοινωνίας/στρατηγική για τις εκστρατείες;	1	Πραγματοποιείτε μετρήσεις για την αξιολόγηση της εκστρατείας σας κατά το στάδιο του προγραμματισμού;	1	Εφαρμόζετε μηχανισμούς για να διασφαλίσετε ότι οι εκστρατείες ευαισθητοποίησης συμβαδίζουν συνεχώς με την τεχνολογική πρόοδο, τις αλλαγές στο τοπίο απειλών, τους νομικούς κανονισμούς και τις οδηγίες εθνικής ασφάλειας;	1

	2	Οι δημόσιες υπηρεσίες διεξάγουν εκστρατείες ευαισθητοποίησης όσον αφορά τον κυβερνοχώρο εντός του οργανισμού τους σε ad-hoc βάση; π.χ. μετά από ένα περιστατικό στον κυβερνοχώρο.	0	Καταρτίζετε σχεδιασμό έργου για την ευαισθητοποίηση σχετικά με θέματα ασφάλειας πληροφοριών και απορρήτου;	1	Διαθέτετε διαδικασία δημιουργίας περιεχομένου σε κυβερνητικό επίπεδο;	1	Αξιολογείτε τις εκστρατείες σας μετά την εκτέλεση;	1	Προβαίνετε σε αξιολόγηση σε τακτά χρονικά διαστήματα για να μετρήσετε τη μετατόπιση στάσης ή τις αλλαγές συμπεριφοράς σχετικά με θέματα ασφάλειας στον κυβερνοχώρο και προστασίας της ιδιωτικής ζωής στον ιδιωτικό και στον δημόσιο τομέα;	1
Στόχος ΕΣΑΚ	**#**	**Επίπεδο 1**	**R**	**Επίπεδο 2**	**R**	**Επίπεδο 3**	**R**	**Επίπεδο 4**	**R**	**Επίπεδο 5**	**R**
5 – Ευαισθητοποίηση των χρηστών	3	Οι δημόσιες υπηρεσίες διεξάγουν εκστρατείες ευαισθητοποίησης στον κυβερνοχώρο για το ευρύ κοινό σε ad-hoc βάση; *π.χ.* μετά από ένα περιστατικό στον κυβερνοχώρο.	0	Διαθέτετε πόρους διαθέσιμους και εύκολα προσδιορίσιμους (*π.χ.* μια διαδικτυακή πύλη, πακέτο εργαλείων ευαισθητοποίησης) για οποιονδήποτε χρήστη επιδιώκει να εκπαιδευτεί στον τομέα των πληροφοριών σχετικά με θέματα ασφάλειας στον κυβερνοχώρο και θέματα απορρήτου;	1	Διαθέτετε μηχανισμούς για τον προσδιορισμό περιοχών στόχων για την ευαισθητοποίηση (π.χ. τοπίο απειλών του ENISA, εθνικά τοπία, διεθνή τοπία, σχόλια από εθνικά κέντρα εγκλήματος στον κυβερνοχώρο κ.λπ.);	1	Διαθέτετε μηχανισμούς για την αναγνώριση του πιο σχετικού μέσου ή του διαύλου επικοινωνίας ανάλογα με το κοινό-στόχο για τη μεγιστοποίηση της προσέγγισης και της αφοσίωσης; *π.χ.* διαφορετικοί τύποι ψηφιακών μέσων, φυλλάδια, μηνύματα ηλεκτρονικού ταχυδρομείου, διδακτικό υλικό, αφίσες σε πολυσύχναστες περιοχές, τηλεόραση, ραδιόφωνο…	1	Συμβουλεύεστε εμπειρογνώμονες συμπεριφοράς για να προσαρμόσετε την εκστρατεία σας στο κοινό-στόχο;	1
	4	-		-		Συγκεντρώνετε ενδιαφερόμενους, εμπειρογνώμονες και ομάδες επικοινωνίας για τη δημιουργία περιεχομένου;	1			-	
	5	-		-		Διασφαλίζετε τη συμμετοχή και τη δέσμευση του ιδιωτικού τομέα στις προσπάθειες ευαισθητοποίησης για την προώθηση και τη διάδοση των μηνυμάτων σε ευρύτερο κοινό;	1	-		-	
	6	-		-		Αναλαμβάνετε συγκεκριμένες πρωτοβουλίες ευαισθητοποίησης για στελέχη του δημόσιου, ιδιωτικού και ακαδημαϊκού τομέα ή του τομέα της κοινωνίας των πολιτών;	1	-		-	
	7	-		-		Συμμετέχετε στην εκστρατεία του ENISA «Ευρωπαϊκός Μήνας για την Ασφάλεια στον Κυβερνοχώρο» (ECSM);	0	-		-	

Στόχος ΕΣΑΚ	#	Επίπεδο 1	R	Επίπεδο 2	R	Επίπεδο 3	R	Επίπεδο 4	R	Επίπεδο 5	R
6 – Διοργάνωση ασκήσεων κυβερνοασφάλειας	α	Έχετε συμπεριλάβει τον στόχο στην τρέχουσα ΕΣΑΚ, ή σκοπεύετε να τον συμπεριλάβετε στην επόμενη έκδοση;	1	Υπάρχουν άτυπες πρακτικές ή δραστηριότητες που συμβάλλουν στην επίτευξη του στόχου με μη συντεταγμένο τρόπο;	1	Διαθέτετε επίσημα καθορισμένο και τεκμηριωμένο σχέδιο δράσης;	1	Επανεξετάζετε το σχέδιο δράσης σας ως προς τον στόχο του για να ελέγξετε την απόδοσή του;	1	Έχετε θεσπίσει μηχανισμούς για να διασφαλίσετε ότι το σχέδιο δράσης προσαρμόζεται με δυναμικό τρόπο στις περιβαλλοντικές εξελίξεις;	1
	β			Ορίσατε τα επιδιωκόμενα αποτελέσματα, τις κατευθυντήριες αρχές ή τις βασικές δραστηριότητες του σχεδίου δράσης σας;	1	Διαθέτετε σχέδιο δράσης με σαφή κατανομή πόρων και διακυβέρνηση;	1	Επανεξετάζετε το σχέδιο δράσης σας ως προς τον στόχο του για να διασφαλίσετε ότι οι προτεραιότητες είναι σωστά ιεραρχημένες και ότι το σχέδιο σας έχει βελτιστοποιηθεί;	1		
	γ			Κατά περίπτωση, το σχέδιο δράσης σας υλοποιείται και είναι ήδη αποτελεσματικό σε περιορισμένο πεδίο εφαρμογής;	0						
6 – Διοργάνωση ασκήσεων για την ασφάλεια στον κυβερνοχώρο	1	Διεξάγετε ασκήσεις διαχείρισης κρίσεων σε άλλους τομείς (εκτός της ασφάλειας στον κυβερνοχώρο) σε εθνικό ή πανευρωπαϊκό επίπεδο;	1	Διαθέτετε κάποιο πρόγραμμα ασκήσεων κυβερνοασφάλειας σε εθνικό επίπεδο;	1	Διασφαλίζετε τη συμμετοχή όλων των αρμόδιων αρχών δημόσιας διοίκησης; (ακόμα και αν το σενάριο αφορά συγκεκριμένο τομέα)	1	Συντάσσετε εκ των υστέρων εκθέσεις ενεργειών/εκθέσεις αξιολόγησης;	1	Έχετε ικανότητες ανάλυσης αντληθέντων διδαγμάτων στον τομέα ασφάλειας στον κυβερνοχώρο (διαδικασίες αναφορών, ανάλυση, μετριασμός);	1
	2	Διαθέτετε πόρους για τον σχεδιασμό και τον προγραμματισμό ασκήσεων διαχείρισης κρίσεων;	1	Διενεργείτε ή δίνετε προτεραιότητα σε ασκήσεις διαχείρισης κρίσεων στον κυβερνοχώρο σε ζωτικής σημασίας κοινωνικές λειτουργίες και κρίσιμης σημασίας υποδομές;	1	Διασφαλίζετε τη συμμετοχή του ιδιωτικού τομέα στον σχεδιασμό και στην εκτέλεση των ασκήσεων;	1	Δοκιμάζετε τα σχέδια και τις διαδικασίες που πραγματοποιούνται σε εθνικό επίπεδο;	1	Εφαρμόζετε καθιερωμένη διαδικασία αντληθέντων διδαγμάτων;	1
	3	-		Έχετε προσδιορίσει έναν οργανισμό συντονισμού υπεύθυνο για την επίβλεψη του σχεδιασμού και του προγραμματισμού ασκήσεων κυβερνοασφάλειας (δημόσιο φορέα, φορέα παροχής συμβουλών...);	0	Διοργανώνετε ασκήσεις ανά τομέα σε εθνικό ή/και διεθνές επίπεδο;	1	Συμμετέχετε σε ασκήσεις κυβερνοασφάλειας σε πανευρωπαϊκό επίπεδο;	1	Προσαρμόζετε τα σενάρια ασκήσεων ανάλογα με τις τελευταίες εξελίξεις (τεχνολογικές εξελίξεις, παγκόσμιες συγκρούσεις, τοπίο απειλών...);	1
	4	-		-		Διοργανώνετε ασκήσεις σε όλους τους τομείς κρίσιμης σημασίας που αναφέρονται στο παράρτημα II της οδηγίας ΑΔΠ;	1	-		Ευθυγραμμίζετε τις διαδικασίες διαχείρισης κρίσεων με άλλα κράτη μέλη για να διασφαλίσετε την αποτελεσματική πανευρωπαϊκή διαχείριση κρίσεων;	1
	5	-		-		Διοργανώνετε διατομεακές ασκήσεις κυβερνοασφάλειας;	1	-		Διαθέτετε μηχανισμό ταχείας προσαρμογής στη στρατηγική, τα σχέδια και τις διαδικασίες από τα αντληθέντα διδάγματα κατά τη διάρκεια των ασκήσεων;	0

	6	-		-		Διοργανώνετε ασκήσεις κυβερνοασφάλειας ιδιάζουσες σε διάφορα επίπεδα; (τεχνικό και επιχειρησιακό επίπεδο, επίπεδο διαδικασιών, επίπεδο λήψης αποφάσεων, πολιτικό επίπεδο...)	0	-		-	

Στόχος ΕΣΑΚ	#	Level 1	R	Επίπεδο 2	R	Επίπεδο 3	R	Επίπεδο 4	R	Επίπεδο 5	R
7 – Ενίσχυση των προγραμμάτων κατάρτισης και εκπαίδευσης	α	Έχετε συμπεριλάβει τον στόχο στην τρέχουσα ΕΣΑΚ, ή σκοπεύετε να τον συμπεριλάβετε στην επόμενη έκδοση;	1	Υπάρχουν άτυπες πρακτικές ή δραστηριότητες που συμβάλλουν στην επίτευξη του στόχου με μη συντεταγμένο τρόπο;	1	Διαθέτετε επίσημα καθορισμένο και τεκμηριωμένο σχέδιο δράσης;	1	Επανεξετάζετε το σχέδιο δράσης σας ως προς τον στόχο του για να ελέγξετε την απόδοσή του;	1	Έχετε θεσπίσει μηχανισμούς για να διασφαλίσετε ότι το σχέδιο δράσης προσαρμόζεται με δυναμικό τρόπο στις περιβαλλοντικές εξελίξεις;	1
	β			Ορίσατε τα επιδιωκόμενα αποτελέσματα, τις κατευθυντήριες αρχές ή τις βασικές δραστηριότητες του σχεδίου δράσης σας;	1	Διαθέτετε σχέδιο δράσης με σαφή κατανομή πόρων και διακυβέρνηση;	1	Επανεξετάζετε το σχέδιο δράσης σας ως προς τον στόχο του για να διασφαλίσετε ότι οι προτεραιότητες είναι σωστά ιεραρχημένες και ότι το σχέδιο σας έχει βελτιστοποιηθεί;	1		
	γ			Κατά περίπτωση, το σχέδιο δράσης σας υλοποιείται και είναι ήδη αποτελεσματικό σε περιορισμένο πεδίο εφαρμογής;	0						
	1	Σκέφτεστε να αναπτύξετε προγράμματα κατάρτισης και εκπαίδευσης σχετικά με την ασφάλεια κυβερνοχώρο;	1	Έχετε καθιερώσει μαθήματα που αφορούν την ασφάλεια στον κυβερνοχώρο;	1	Η χώρα σας εμπεριέχει την κουλτούρα της ασφάλειας στον κυβερνοχώρο στο αρχικό στάδιο της εκπαιδευτικής πορείας των μαθητών; Για παράδειγμα, προτιμάτε τη διεξαγωγή μαθημάτων για την ασφάλεια στον κυβερνοχώρο στο γυμνάσιο και στο λύκειο;	1	Προτρέπετε το προσωπικό του ιδιωτικού και του δημόσιου τομέα να είναι διαπιστευμένο ή πιστοποιημένο;	1	Εφαρμόζετε μηχανισμούς για να διασφαλίσετε ότι η κατάρτιση και τα εκπαιδευτικά προγράμματα συμβαδίζουν συνεχώς με τις τρέχουσες και αναδυόμενες τεχνολογικές εξελίξεις, τις αλλαγές στο τοπίο απειλών, τους νομικούς κανονισμούς και τις οδηγίες εθνικής ασφάλειας;	1
	2	-		Τα πανεπιστήμια της χώρας σας προσφέρουν διδακτορικούς τίτλους για την ασφάλεια στον κυβερνοχώρο ως ανεξάρτητο επιστημονικό τομέα και όχι ως μάθημα της επιστήμης των υπολογιστών;	1	Διαθέτετε εθνικά ερευνητικά εργαστήρια και εκπαιδευτικά ιδρύματα που ειδικεύονται στην ασφάλεια στον κυβερνοχώρο;	1	Έχει αναπτύξει η χώρα σας προγράμματα κατάρτισης για την ασφάλεια στον κυβερνοχώρο ή προγράμματα καθοδήγησης για να υποστηρίξει τις εθνικές νεοσύστατες επιχειρήσεις και τις ΜΜΕ;	1	Δημιουργείτε ακαδημαϊκά κέντρα αριστείας για την ασφάλεια στον κυβερνοχώρο τα οποία θα λειτουργούν ως κόμβοι έρευνας και εκπαίδευσης;	1
	3	-		Προτίθεστε να εκπαιδεύσετε εκπαιδευτικούς, ανεξαρτήτως του τομέα τους, σε θέματα ασφάλειας πληροφοριών και απορρήτου; *π.χ.*διαδικτυακή ασφάλεια, προστασία δεδομένων προσωπικού χαρακτήρα, εκφοβισμός στον κυβερνοχώρο.	1	Ενθαρρύνετε/χρηματοδοτείτε ειδικά μαθήματα για την ασφάλεια στον κυβερνοχώρο και προγράμματα κατάρτισης για τους υπαλλήλους των κρατών μελών;	1	Προωθείτε ενεργά την προσθήκη μαθημάτων ασφάλειας πληροφοριών στην τριτοβάθμια εκπαίδευση όχι μόνο για φοιτητές πληροφορικής αλλά και για οποιαδήποτε άλλη επαγγελματική ειδικότητα; *π.χ.* μαθήματα προσαρμοσμένα στις ανάγκες αυτού του επαγγέλματος.	1	Συμμετέχουν ακαδημαϊκά ιδρύματα σε κορυφαίες συζητήσεις στον τομέα της εκπαίδευσης και της έρευνας για την ασφάλεια στον κυβερνοχώρο διεθνώς;	0

	4	-		-		Έχετε μαθήματα κυβερνοασφάλειας ή/και εξειδικευμένο πρόγραμμα σπουδών για το επίπεδο 5 έως 8 του ΕΠΠ (Ευρωπαϊκό Πλαίσιο Προσόντων);	1	Αξιολογείτε το χάσμα δεξιοτήτων (έλλειψη εργατικού δυναμικού στον τομέα της ασφάλειας στον κυβερνοχώρο) στον τομέα της ασφάλειας πληροφοριών σε τακτική βάση;	1	-	
	5	-		-		Ενθαρρύνετε ή/και υποστηρίζετε πρωτοβουλίες για να συμπεριλάβετε μαθήματα διαδικτυακής ασφάλειας στην πρωτοβάθμια και δευτεροβάθμια εκπαίδευση;	1	Ενθαρρύνετε τη δικτύωση και την ανταλλαγή πληροφοριών μεταξύ ακαδημαϊκών ιδρυμάτων σε εθνικό και σε διεθνές επίπεδο;	1		
Στόχος ΕΣΑΚ	**#**	**Επίπεδο 1**	**R**	**Επίπεδο 2**	**R**	**Επίπεδο 3**	**R**	**Επίπεδο 4**	**R**	**Επίπεδο 5**	**R**
7 - Ενίσχυση των προγραμμάτων κατάρτισης και εκπαίδευσης	6	-		-		Χρηματοδοτείτε ή προσφέρετε στους πολίτες δωρεάν βασική εκπαίδευση για την ασφάλεια στον κυβερνοχώρο;	0	Διασφαλίζετε τη συμμετοχή του ιδιωτικού τομέα σε οποιαδήποτε μορφή σε πρωτοβουλίες εκπαίδευσης για την ασφάλεια ; π.χ. σχεδιασμός και πραγματοποίηση μαθημάτων, πρακτική άσκηση, τοποθέτηση σε θέση εργασίας...	1	-	
	7	-		-		Διοργανώνετε ετήσιες εκδηλώσεις ασφαλείας πληροφοριών (π.χ. διαγωνισμοί δικτυοπαραβίασης ή μαραθώνιοι ανάπτυξης εφαρμογών);	0	Εφαρμόζετε μηχανισμούς χρηματοδότησης για να ενθαρρύνετε την απόκτηση τίτλων σπουδών στον τομέα της ασφάλειας στον κυβερνοχώρο; *π.χ.* υποτροφίες, εγγυημένη μαθητεία/πρακτική άσκηση, εγγυημένες θέσεις εργασίας σε συγκεκριμένο κλάδο ή ρόλοι στον δημόσιο τομέα	0	-	

Στόχος ΕΣΑΚ	#	Επίπεδο 1	R	Επίπεδο 2	R	Επίπεδο 3	R	Επίπεδο 4	R	Επίπεδο 5	R
8 – Ενίσχυση Ε&Α	α	Έχετε συμπεριλάβει τον στόχο στην τρέχουσα ΕΣΑΚ, ή σκοπεύετε να τον συμπεριλάβετε στην επόμενη έκδοση;	1	Υπάρχουν άτυπες πρακτικές ή δραστηριότητες που συμβάλλουν στην επίτευξη του στόχου με μη συντεταγμένο τρόπο;	1	Διαθέτετε επίσημα καθορισμένο και τεκμηριωμένο σχέδιο δράσης;	1	Επανεξετάζετε το σχέδιο δράσης σας ως προς τον στόχο του για να ελέγξετε την απόδοσή του;	1	Έχετε θεσπίσει μηχανισμούς για να διασφαλίσετε ότι το σχέδιο δράσης προσαρμόζεται με δυναμικό τρόπο στις περιβαλλοντικές εξελίξεις;	1
	β			Ορίσατε τα επιδιωκόμενα αποτελέσματα, τις κατευθυντήριες αρχές ή τις βασικές δραστηριότητες του σχεδίου δράσης σας;	1	Διαθέτετε σχέδιο δράσης με σαφή κατανομή πόρων και διακυβέρνηση;	1	Επανεξετάζετε το σχέδιο δράσης σας ως προς τον στόχο του για να διασφαλίσετε ότι οι προτεραιότητες είναι σωστά ιεραρχημένες και ότι το σχέδιο σας έχει βελτιστοποιηθεί;	1		
	γ			Κατά περίπτωση, το σχέδιο δράσης σας υλοποιείται και είναι ήδη αποτελεσματικό σε περιορισμένο πεδίο εφαρμογής;	0						
	1	Έχετε πραγματοποιήσει μελέτες ή αναλύσεις για τον προσδιορισμό προτεραιοτήτων Ε&Α στον τομέα της ασφάλειας στον κυβερνοχώρο;	1	Εφαρμόζετε διαδικασία καθορισμού προτεραιοτήτων Ε&Α (π.χ. αναδυόμενα θέματα για την αποτροπή, την προστασία, τον εντοπισμό και την προσαρμογή σε νέα είδη κυβερνοεπιθέσεων);	1	Υπάρχει σχέδιο σύνδεσης των πρωτοβουλιών Ε&Α με την πραγματική οικονομία;	1	Ευθυγραμμίζονται οι πρωτοβουλίες Ε&Α στον τομέα της ασφάλειας στον κυβερνοχώρο με σχετικούς στρατηγικούς στόχους, π.χ. ΨΕΑ, Η2020, Ψηφιακή Ευρώπη, στρατηγική της ΕΕ για την ασφάλεια στον κυβερνοχώρο;	1	Συνεχίζετε σε εθνικό επίπεδο συνεργασία με διεθνείς πρωτοβουλίες Ε&Α που σχετίζονται με την ασφάλεια στον κυβερνοχώρο;	1
	2	-		Συμμετέχει ο ιδιωτικός τομέας στον καθορισμό προτεραιοτήτων Ε&Α;	1	Υπάρχουν εθνικά έργα που σχετίζονται με την ασφάλεια στον κυβερνοχώρο;	1	Υπάρχει κάποιο σύστημα αξιολόγησης για πρωτοβουλίες Ε&Α;	1	Ευθυγραμμίζονται οι προτεραιότητες Ε&Α με τον ισχύοντα ή τον επερχόμενο κανονισμό (σε εθνικό επίπεδο);	1

Στόχος ΕΣΑΚ	#	Επίπεδο 1	R	Επίπεδο 2	R	Επίπεδο 3	R	Επίπεδο 4	R	Επίπεδο 5	R
8 – Ενίσχυση Ε&Α	3	-		Συμμετέχει ο ακαδημαϊκός τομέας στον καθορισμό προτεραιοτήτων Ε&Α;	1	Διαθέτετε τοπικά/περιφερειακά οικοσυστήματα νεοσύστατων εταιρειών και άλλα κανάλια δικτύωσης (π.χ. τεχνολογικά πάρκα, συμπλέγματα καινοτομίας, εκδηλώσεις/πλατφόρμες δικτύωσης) για την προώθηση της καινοτομίας (συμπεριλαμβανομένων των νεοσύστατων επιχειρήσεων ασφάλειας στον κυβερνοχώρο);	1	Υπάρχουν συμφωνίες συνεργασίας με πανεπιστήμια και άλλες ερευνητικές εγκαταστάσεις;	1	Συμμετέχετε σε κορυφαίες συζητήσεις σε ένα ή πολλά θέματα Ε&Α αιχμής σε διεθνές επίπεδο;	0
	4	-		Υπάρχουν εθνικές πρωτοβουλίες Ε&Α που σχετίζονται με την ασφάλεια στον κυβερνοχώρο;	0	Υπάρχουν επενδύσεις σε προγράμματα Ε&Α για την ασφάλεια στον κυβερνοχώρο στον ακαδημαϊκό και στον ιδιωτικό τομέα;	1	Υπάρχει αναγνωρισμένος θεσμικός φορέας που επιβλέπει τις δραστηριότητες Ε&Α στον τομέα της ασφάλειας στον κυβερνοχώρο;	0	-	
	5	-		-		Διαθέτετε έδρα βιομηχανικής έρευνας σε πανεπιστήμια για τη σύνδεση ερευνητικών θεμάτων με τις ανάγκες της αγοράς;	1	-		-	
	6	-		-		Διαθέτετε προγράμματα χρηματοδότησης Ε&Α για την ασφάλεια στον κυβερνοχώρο;	0	-		-	

Στόχος ΕΣΑΚ	#	Level 1	R	Επίπεδο 2	R	Επίπεδο 3	R	Επίπεδο 4	R	Επίπεδο 5	R
9 – Παροχή κινήτρων στον ιδιωτικό τομέα ώστε να επενδύσει σε μέτρα ασφαλείας	α	Έχετε συμπεριλάβει τον στόχο στην τρέχουσα ΕΣΑΚ, ή σκοπεύετε να τον συμπεριλάβετε στην επόμενη έκδοση;	1	Υπάρχουν άτυπες πρακτικές ή δραστηριότητες που συμβάλλουν στην επίτευξη του στόχου με μη συντεταγμένο τρόπο;	1	Διαθέτετε επίσημα καθορισμένο και τεκμηριωμένο σχέδιο δράσης;	1	Επανεξετάζετε το σχέδιο δράσης σας ως προς τον στόχο του για να ελέγξετε την απόδοσή του;	1	Έχετε θεσπίσει μηχανισμούς για να διασφαλίσετε ότι το σχέδιο δράσης προσαρμόζεται με δυναμικό τρόπο στις περιβαλλοντικές εξελίξεις;	1
	β			Ορίσατε τα επιδιωκόμενα αποτελέσματα, τις κατευθυντήριες αρχές ή τις βασικές δραστηριότητες του σχεδίου δράσης σας;	1	Διαθέτετε σχέδιο δράσης με σαφή κατανομή πόρων και διακυβέρνηση;	1	Επανεξετάζετε το σχέδιο δράσης σας ως προς τον στόχο του για να διασφαλίσετε ότι οι προτεραιότητες είναι σωστά ιεραρχημένες και ότι το σχέδιο σας έχει βελτιστοποιηθεί;	1		

	γ			Κατά περίπτωση, το σχέδιο δράσης σας υλοποιείται και είναι ήδη αποτελεσματικό σε περιορισμένο πεδίο εφαρμογής;	0						
	1	Υπάρχει βιομηχανική πολιτική ή πολιτική βούληση για την ενθάρρυνση της ανάπτυξης του κλάδου ασφάλειας στον κυβερνοχώρο;	1	Συμμετέχει ο ιδιωτικός τομέας στον σχεδιασμό προτεραιοτήτων;	1	Εφαρμόζονται οικονομικά/ρυθμιστικά ή άλλα είδη κινήτρων για την προαγωγή επενδύσεων στον τομέα της ασφάλειας στον κυβερνοχώρο;	1	Υπάρχουν ιδιωτικοί φορείς που ανταποκρίνονται σε κίνητρα επενδύοντας σε μέτρα ασφαλείας; *π.χ.* επενδυτές ειδικευμένοι στον τομέα της ασφάλειας στον κυβερνοχώρο και μη εξειδικευμένοι επενδυτές	1	Εστιάζετε τα κίνητρα σε θέματα ασφάλειας στον κυβερνοχώρο ανάλογα με τις τελευταίες εξελίξεις στον τομέα των απειλών;	1
Στόχος ΕΣΑΚ	**#**	**Επίπεδο 1**	**R**	**Επίπεδο 2**	**R**	**Επίπεδο 3**	**R**	**Επίπεδο 4**	**R**	**Επίπεδο 5**	**R**
9 – Παροχή κινήτρων στον ιδιωτικό τομέα ώστε να επενδύσει σε μέτρα ασφαλείας	2	-		Εχετε προσδιορίσει συγκεκριμένα θέματα ασφάλειας στον κυβερνοχώρο τα οποία πρόκειται να αναπτυχθούν;*π.χ.* κρυπτογραφία, απόρρητο, νέα μορφή ταυτοποίησης, ΤΝ για την ασφάλεια στον κυβερνοχώρο...	0	Παρέχετε υποστήριξη (π.χ. φορολογικά κίνητρα) για νεοσύστατες επιχειρήσεις και ΜΜΕ του τομέα της ασφάλειας στον κυβερνοχώρο;	1	Παρέχετε κίνητρα στον ιδιωτικό τομέα ώστε να επικεντρωθεί στην ασφάλεια των τεχνολογιών αιχμής; *π.χ.* 5G, τεχνητή νοημοσύνη, ΔτΠ, κβαντική υπολογιστική...	1	-	
	3	-		-		Παρέχετε φορολογικά κίνητρα ή άλλα οικονομικά κίνητρα για επενδυτές του ιδιωτικού τομέα σε νεοσύστατες επιχειρήσεις του τομέα της ασφάλειας στον κυβερνοχώρο;	1	-		-	
	4	-		-		Διευκολύνετε την πρόσβαση για νεοσύστατες επιχειρήσεις και ΜΜΕ του τομέα ασφάλειας στον κυβερνοχώρο στις διαδικασίες δημοσίων συμβάσεων;	0	-		-	
	5	-		-		Υπάρχει διαθέσιμος προϋπολογισμός για την παροχή κινήτρων στον ιδιωτικό τομέα;	0	-		-	

Στόχος ΕΣΑΚ	#	Επίπεδο 1	R	Επίπεδο 2	R	Επίπεδο 3	R	Επίπεδο 4	R	Επίπεδο 5	R
10 – Βελτίωση της κυβερνοασφάλειας στην αλυσίδα εφοδιασμού	α	Έχετε συμπεριλάβει τον στόχο στην τρέχουσα ΕΣΑΚ, ή σκοπεύετε να τον συμπεριλάβετε στην επόμενη έκδοση;	1	Υπάρχουν άτυπες πρακτικές ή δραστηριότητες που συμβάλλουν στην επίτευξη του στόχου με μη συντεταγμένο τρόπο;	1	Διαθέτετε επίσημα καθορισμένο και τεκμηριωμένο σχέδιο δράσης;	1	Επανεξετάζετε το σχέδιο δράσης σας ως προς τον στόχο του για να ελέγξετε την απόδοσή του;	1	Έχετε θεσπίσει μηχανισμούς για να διασφαλίσετε ότι το σχέδιο δράσης προσαρμόζεται με δυναμικό τρόπο στις περιβαλλοντικές εξελίξεις;	1
	β			Ορίσατε τα επιδιωκόμενα αποτελέσματα, τις κατευθυντήριες αρχές ή τις βασικές δραστηριότητες του σχεδίου δράσης σας;	1	Διαθέτετε σχέδιο δράσης με σαφή κατανομή πόρων και διακυβέρνηση;	1	Επανεξετάζετε το σχέδιο δράσης σας ως προς τον στόχο του για να διασφαλίσετε ότι οι προτεραιότητες είναι σωστά ιεραρχημένες και ότι το σχέδιο σας έχει βελτιστοποιηθεί;	1		
	γ			Κατά περίπτωση, το σχέδιο δράσης σας υλοποιείται και είναι ήδη αποτελεσματικό σε περιορισμένο πεδίο εφαρμογής;	0						
	1	Έχετε πραγματοποιήσει μελέτη σχετικά με τις ορθές πρακτικές ασφαλείας για τη διαχείριση της εφοδιαστικής αλυσίδας που χρησιμοποιούνται στον τομέα των δημοσίων συμβάσεων σε διάφορα τμήματα του κλάδου ή/και στον δημόσιο τομέα;	1	Διενεργείτε αξιολογήσεις ασφάλειας στον κυβερνοχώρο στην αλυσίδα εφοδιασμού υπηρεσιών και προϊόντων ΤΠΕ σε τομείς κρίσιμης σημασίας (όπως προσδιορίζεται στο παράρτημα ΙΙ της οδηγίας 2016/1148 για την ασφάλεια δικτύων και πληροφοριών);	1	Χρησιμοποιείτε σύστημα πιστοποίησης ασφαλείας για προϊόντα και υπηρεσίες που βασίζονται σε ΤΠΕ; *π.χ.* SOG-IS MRA στην Ευρώπη (Ομάδα Ανώτερων Υπαλλήλων για την Ασφάλεια των Συστημάτων Πληροφοριών, Συμφωνία Αμοιβαίας Αναγνώρισης), Συμφωνία για την αναγνώριση κοινών κριτηρίων (CCRA), εθνικές πρωτοβουλίες, τομεακές πρωτοβουλίες…	1	Εφαρμόζετε κάποια διαδικασία για την επικαιροποίηση των αξιολογήσεων ασφάλειας στον κυβερνοχώρο της αλυσίδας εφοδιασμού υπηρεσιών και προϊόντων ΤΠΕ σε τομείς κρίσιμης σημασίας (όπως προσδιορίζεται στο παράρτημα ΙΙ της οδηγίας 2016/1148 για την ασφάλεια δικτύων και πληροφοριών);	1	Διαθέτετε αισθητήρες ανίχνευσης σε βασικά στοιχεία της αλυσίδας εφοδιασμού για τον εντοπισμό κάποιας πρώιμης ένδειξης συμβιβασμού; *π.χ.* έλεγχοι ασφάλειας σε επίπεδο παρόχων υπηρεσιών διαδικτύου, αισθητήρες ασφαλείας σε σημαντικά στοιχεία υποδομής...-	1

Στόχος ΕΣΑΚ	#	Επίπεδο 1	R	Επίπεδο 2	R	Επίπεδο 3	R	Επίπεδο 4	R	Επίπεδο 5	R
10 – Βελτίωση της κυβερνοασφάλειας στην αλυσίδα εφοδιασμού	2	-		Εφαρμόζετε πρότυπα στις πολιτικές δημοσίων συμβάσεων των δημόσιων διοικήσεων για να διασφαλίσετε ότι οι πάροχοι προϊόντων ή υπηρεσιών ΤΠΕ πληρούν τις βασικές απαιτήσεις ασφάλειας των πληροφοριών; *π.χ.* ISO/IEC 27001 και 27002, ISO/IEC 27036…	1	Προωθείτε ενεργά την ασφάλεια και το απόρρητο σχεδιάζοντας βέλτιστες πρακτικές στην ανάπτυξη προϊόντων και υπηρεσιών ΤΠΕ; *π.χ.* κύκλος ζωής ασφαλούς ανάπτυξης λογισμικού, κύκλος ζωής ΔτΠ	1	Εφαρμόζετε κάποια διαδικασία για τον προσδιορισμό αδύναμων κρίκων του τομέα στης ασφάλειας στον κυβερνοχώρο στην αλυσίδα εφοδιασμού υπηρεσιών και προϊόντων ΤΠΕ σε τομείς κρίσιμης σημασίας (όπως προσδιορίζεται στο παράρτημα ΙΙ της οδηγίας 2016/1148 για την ασφάλεια δικτύων και πληροφοριών);	1	-	
	3	-		-		Αναπτύσσετε και παρέχετε κεντρικούς καταλόγους με εκτεταμένες πληροφορίες υπαρχόντων προτύπων ασφάλειας και απορρήτου πληροφοριών που είναι κλιμακούμενες και εφαρμόζονται από τις ΜΜΕ;	1	Διαθέτετε μηχανισμούς οι οποίοι να διασφαλίζουν ότι τα προϊόντα και οι υπηρεσίες ΤΠΕ που είναι κρίσιμης σημασίας για τους ΦΕΒΠ είναι ανθεκτικοί όσον αφορά την ασφάλεια κυβερνοχώρο (*δηλ.* τη δυνατότητα διατήρησης της διαθεσιμότητας και της ασφάλειας έναντι ενός περιστατικού στον κυβερνοχώρο); *π.χ.* μέσω δοκιμών, τακτικών αξιολογήσεων, ανίχνευσης παραβιασμένων στοιχείων…	1	-	
	4	-				Συμμετέχετε ενεργά στο σχεδιασμό ενός πλαισίου πιστοποίησης της ΕΕ για ψηφιακά προϊόντα, υπηρεσίες και διαδικασίες ΤΠΕ, όπως ορίζεται στην πράξη της ΕΕ για την ασφάλεια στον κυβερνοχώρο (κανονισμός (ΕΕ) 2019/881); *π.χ.* συμμετοχή στην ευρωπαϊκή ομάδα πιστοποίησης της ασφάλειας στον κυβερνοχώρο (ECCG), προώθηση τεχνικών προτύπων και διαδικασιών για την ασφάλεια προϊόντων/υπηρεσιών ΤΠΕ	0	Προωθείτε την ανάπτυξη συστημάτων πιστοποίησης που απευθύνονται σε ΜΜΕ για την ενίσχυση της υιοθέτησης προτύπων ασφάλειας και απορρήτου πληροφοριών;	0	-	

	5	-		-		Παρέχετε οποιοδήποτε είδος κινήτρων στις ΜΜΕ για την υιοθέτηση προτύπων ασφάλειας και απορρήτου;	0	Εφαρμόζετε διατάξεις για να ενθαρρύνετε μεγάλες εταιρείες να αυξήσουν την ασφάλεια στον κυβερνοχώρο των μικρών επιχειρήσεων στις αλυσίδες εφοδιασμού τους; *π.χ.* κόμβος ασφάλειας στον κυβερνοχώρο, εκστρατείες εκπαίδευσης και ευαισθητοποίησης...	0	-	
	6	-		-		Ενθαρρύνετε τους προμηθευτές λογισμικού να υποστηρίζουν τις ΜΜΕ διασφαλίζοντας ασφαλείς προκαθορισμένες ρυθμίσεις σε προϊόντα που απευθύνονται σε μικρούς οργανισμούς;	0	-		-	

4.1.3 Δέσμη #3: Νομοθετικό και ρυθμιστικό πλαίσιο

Στόχος ΕΣΑΚ	#	Επίπεδο 1	R	Επίπεδο 2	R	Επίπεδο 3	R	Επίπεδο 4	R	Επίπεδο 5	R
11 – Προστασία υποδομής πληροφοριών ζωτικής σημασίας, ΦΕΒΠ και ΠΨΥ	α	Έχετε συμπεριλάβει τον στόχο στην τρέχουσα ΕΣΑΚ, ή σκοπεύετε να τον συμπεριλάβετε στην επόμενη έκδοση;	1	Υπάρχουν άτυπες πρακτικές ή δραστηριότητες που συμβάλλουν στην επίτευξη του στόχου με μη συντεταγμένο τρόπο;	1	Διαθέτετε επίσημα καθορισμένο και τεκμηριωμένο σχέδιο δράσης;	1	Επανεξετάζετε το σχέδιο δράσης σας ως προς τον στόχο του για να ελέγξετε την απόδοσή του;	1	Έχετε θεσπίσει μηχανισμούς για να διασφαλίσετε ότι το σχέδιο δράσης προσαρμόζεται με δυναμικό τρόπο στις περιβαλλοντικές εξελίξεις;	1
	β			Ορίσατε τα επιδιωκόμενα αποτελέσματα, τις κατευθυντήριες αρχές ή τις βασικές δραστηριότητες του σχεδίου δράσης σας;	1	Διαθέτετε σχέδιο δράσης με σαφή κατανομή πόρων και διακυβέρνηση;	1	Επανεξετάζετε το σχέδιο δράσης σας ως προς τον στόχο του για να διασφαλίσετε ότι οι προτεραιότητες είναι σωστά ιεραρχημένες και ότι το σχέδιο σας έχει βελτιστοποιηθεί;	1		
	γ			Κατά περίπτωση, το σχέδιο δράσης σας υλοποιείται και είναι ήδη αποτελεσματικό σε περιορισμένο πεδίο εφαρμογής;	0						
	1	Υπάρχει γενική αντίληψη ότι οι φορείς εκμετάλλευσης ΥΖΣ συμβάλλουν στην εθνική ασφάλεια;	1	Διαθέτετε μεθοδολογία για τον προσδιορισμό βασικών υπηρεσιών;	1	Εφαρμόζετε την οδηγία ΑΔΠ (2016/1148);	1	Διαθέτετε διαδικασία επικαιροποίησης του μητρώου κινδύνων;	1	Δημιουργείτε και επικαιροποιείτε αναφορές τοπίου απειλών;	1
	2	-		Διαθέτετε μεθοδολογία για τον προσδιορισμό των ΥΖΣ;	1	Εφαρμόζετε την οδηγία ευρωπαϊκών υποδομών ζωτικής σημασίας-ΕΥΖΣ (2008/114) σχετικά με τον προσδιορισμό και τον χαρακτηρισμό των ΕΥΖΣ και την αξιολόγηση της ανάγκης βελτίωσης της προστασίας τους;	1	Εφαρμόζετε άλλους μηχανισμούς για να εκτιμήσετε εάν τα τεχνικά και οργανωτικά μέτρα που εφαρμόζει ο ΦΕΒΠ είναι κατάλληλα για τη διαχείριση των κινδύνων για την ασφάλεια των δικτύων και των συστημάτων πληροφοριών; π.χ. τακτικοί έλεγχοι ασφάλειας στον κυβερνοχώρο, εθνικό πλαίσιο για την εφαρμογή τυποποιημένων μέτρων, τεχνικά εργαλεία που παρέχονται από την κυβέρνηση, όπως αισθητήρες ανίχνευσης ή αναθεώρηση διαμόρφωσης για συγκεκριμένο σύστημα...	1	Ανάλογα με τις τελευταίες εξελίξεις στο τοπίο απειλών, μπορείτε να εντάξετε έναν νέο τομέα στο σχέδιο δράσης σας για την προστασία των ΥΖΣ (CIIP);	1
	3	-		Διαθέτετε μεθοδολογία για τον προσδιορισμό ΦΕΒΠ;	1	Διαθέτετε εθνικό μητρώο για αναγνωρισμένο ΦΕΒΠ ανά τομέα κρίσιμης σημασίας;	1	Ελέγχετε και, συνεπώς, επικαιροποιείτε τον κατάλογο των αναγνωρισμένων ΦΕΒΠ τουλάχιστον ανά διετία;	1	Ανάλογα με τις τελευταίες εξελίξεις στο τοπίο απειλών, μπορείτε να προσαρμόσετε νέες απαιτήσεις στο σχέδιο δράσης σας για την προστασία των ΥΖΣ (CIIP);	1

Στόχος ΕΣΑΚ	#										
11 – Προστασία υποδομής πληροφοριών ζωτικής σημασίας, ΦΕΒΠ και ΠΨΥ	4	-		Διαθέτετε μεθοδολογία για τον προσδιορισμό παρόχων ψηφιακών υπηρεσιών;	1	Διαθέτετε εθνικό μητρώο για τους προσδιορισθέντες παρόχους ψηφιακών υπηρεσιών;	1	Εφαρμόζετε άλλους μηχανισμούς για να εκτιμήσετε εάν τα τεχνικά και οργανωτικά μέτρα που εφαρμόζουν οι πάροχοι ψηφιακών υπηρεσιών είναι κατάλληλα για τη διαχείριση των κινδύνων για την ασφάλεια των συστημάτων δικτύου και πληροφοριών; π.χ. τακτικοί έλεγχοι ασφάλειας στον κυβερνοχώρο, εθνικό πλαίσιο για την εφαρμογή τυποποιημένων μέτρων, τεχνικά εργαλεία που παρέχονται από την κυβέρνηση, όπως αισθητήρες ανίχνευσης ή αναθεώρηση διαμόρφωσης για συγκεκριμένο σύστημα...	1	-	
	5	-		Έχετε μία ή περισσότερες εθνικές αρχές που παρέχουν εποπτεία σχετικά με την προστασία υποδομής πληροφοριών ζωτικής σημασίας και την ασφάλεια συστημάτων δικτύου και πληροφοριών; π.χ. όπως απαιτείται από την οδηγία ΑΔΠ (2016/1148)	1	Διαθέτετε εθνικό μητρώο κινδύνων για προσδιορισθέντες ή γνωστούς κινδύνους;	1	Ελέγχετε και, συνεπώς, επικαιροποιείτε τον κατάλογο των προσδιορισθέντων παρόχων ψηφιακών υπηρεσιών τουλάχιστον ανά διετία;	1	-	
	6	-		Αναπτύσσετε ειδικά τομεακά προγράμματα προστασίας; π.χ. που συμπεριλαμβάνουν βασικά μέτρα ασφάλειας στον κυβερνοχώρο (υποχρεωτικά ή κατευθυντήριες γραμμές)	0	Διαθέτετε μεθοδολογία για τη χαρτογράφηση εξαρτήσεων ΥΖΣ;	1	Χρησιμοποιείτε σύστημα πιστοποίησης ασφάλειας (εθνικό ή διεθνές) για να βοηθήσετε τους ΦΕΒΠ και τους παρόχους ψηφιακών υπηρεσιών να εντοπίζουν ασφαλή προϊόντα ΤΠΕ; π.χ. συμφωνία αμοιβαίας αναγνώρισης της SOG-IS στην Ευρώπη, εθνικές πρωτοβουλίες...	1	-	

	7	-		-		Χρησιμοποιείτε πρακτικές διαχείρισης κινδύνων για τον εντοπισμό, την ποσοτικοποίηση και τη διαχείριση κινδύνων που σχετίζονται με ΥΖΣ σε εθνικό επίπεδο;	1	Χρησιμοποιείτε σύστημα πιστοποίησης ασφαλείας ή μια διαδικασία προεπιλογής για να αξιολογήσετε τους παρόχους υπηρεσιών που συνεργάζονται με ΦΕΒΠ; π.χ. πάροχοι υπηρεσιών στον τομέα της ανίχνευσης περιστατικών, της απόκρισης σε περιστατικά, του ελέγχου ασφάλειας στον κυβερνοχώρο, των υπηρεσιών υπολογιστικού νέφους, των έξυπνων καρτών…	1	-	
	8	-		-		Συμμετέχετε σε διαδικασία διαβούλευσης για τον προσδιορισμό διασυνοριακών εξαρτήσεων;	1	Εφαρμόζετε μηχανισμούς για τη μέτρηση του επιπέδου συμμόρφωσης των ΦΕΒΠ και των παρόχων ψηφιακών υπηρεσιών με τα βασικά μέτρα ασφάλειας στον κυβερνοχώρο;	0	-	
Στόχος ΕΣΑΚ	**#**	**Επίπεδο 1**	**R**	**Επίπεδο 2**	**R**	**Επίπεδο 3**	**R**	**Επίπεδο 4**	**R**	**Επίπεδο 5**	**R**
11 – Προστασία υποδομής πληροφοριών ζωτικής σημασίας, ΦΕΒΠ και ΠΨΥ	9					Διαθέτετε ενιαίο σημείο επαφής που είναι αρμόδιο για τον συντονισμό θεμάτων που σχετίζονται με την ασφάλεια των συστημάτων δικτύου και πληροφοριών σε εθνικό επίπεδο και τη διασυνοριακή συνεργασία σε επίπεδο Ένωσης;	1	Εφαρμόζετε διατάξεις προκειμένου να διασφαλίσετε τη συνέχεια των υπηρεσιών που παρέχονται από υποδομές πληροφοριών ζωτικής σημασίας; π.χ. πρόβλεψη κρίσεων, διαδικασίες για την αναδιαμόρφωση συστημάτων πληροφοριών ζωτικής σημασίας, επιχειρηματική συνέχεια χωρίς ΤΠ, διαδικασίες αντιγράφων ασφαλείας αποσυνδεδεμένου δικτύου (air gap)...	0		
	10					Ορίζετε βασικά μέτρα ασφάλειας στον κυβερνοχώρο (υποχρεωτικά ή κατευθυντήριες γραμμές) για παρόχους ψηφιακών υπηρεσιών και όλους τους τομείς που προσδιορίζονται στο παράρτημα ΙΙ της οδηγίας ΑΔΠ (2016/1148);	1				
	11	-		-		Παρέχετε εργαλεία ή μεθοδολογίες για τον εντοπισμό περιστατικών στον κυβερνοχώρο;	1	-		-	

Στόχος ΕΣΑΚ	#	Επίπεδο 1	R	Επίπεδο 2	R	Επίπεδο 3	R	Επίπεδο 4	R	Επίπεδο 5	R
12 – Αντιμετώπιση εγκλήματος στον κυβερνοχώρο	α	Έχετε συμπεριλάβει τον στόχο στην τρέχουσα ΕΣΑΚ, ή σκοπεύετε να τον συμπεριλάβετε στην επόμενη έκδοση;	1	Υπάρχουν άτυπες πρακτικές ή δραστηριότητες που συμβάλλουν στην επίτευξη του στόχου με μη συντεταγμένο τρόπο;	1	Διαθέτετε επίσημα καθορισμένο και τεκμηριωμένο σχέδιο δράσης;	1	Επανεξετάζετε το σχέδιο δράσης σας ως προς τον στόχο του για να ελέγξετε την απόδοσή του;	1	Έχετε θεσπίσει μηχανισμούς για να διασφαλίσετε ότι το σχέδιο δράσης προσαρμόζεται με δυναμικό τρόπο στις περιβαλλοντικές εξελίξεις;	1
	β			Ορίσατε τα επιδιωκόμενα αποτελέσματα, τις κατευθυντήριες αρχές ή τις βασικές δραστηριότητες του σχεδίου δράσης σας;	1	Διαθέτετε σχέδιο δράσης με σαφή κατανομή πόρων και διακυβέρνηση;	1	Επανεξετάζετε το σχέδιο δράσης σας ως προς τον στόχο του για να διασφαλίσετε ότι οι προτεραιότητες είναι σωστά ιεραρχημένες και ότι το σχέδιο σας έχει βελτιστοποιηθεί;	1		
	γ			Κατά περίπτωση, το σχέδιο δράσης σας υλοποιείται και είναι ήδη αποτελεσματικό σε περιορισμένο πεδίο εφαρμογής;	0						
	1	Έχετε πραγματοποιήσει μελέτη για το προσδιορισμό των απαιτήσεων επιβολής του νόμου (νομική βάση, πόροι, δεξιότητες…) για την αποτελεσματική αντιμετώπιση του εγκλήματος στον κυβερνοχώρο;	1	Το εθνικό νομικό σας πλαίσιο συμμορφώνεται πλήρως με το σχετικό νομικό πλαίσιο της ΕΕ, συμπεριλαμβανομένης της οδηγίας 2013/40/ΕΕ για τις επιθέσεις κατά συστημάτων πληροφοριών; π.χ. παράνομη πρόσβαση σε συστήματα πληροφοριών, παράνομη παρεμβολή σε σύστημα, παράνομη παρεμβολή σε δεδομένα, παράνομη παρακολούθηση, εργαλεία που χρησιμοποιούνται για διάπραξη αδικημάτων...	1	Διαθέτετε μονάδες για την αντιμετώπιση του εγκλήματος στον κυβερνοχώρο στις εισαγγελικές υπηρεσίες;	1	Συλλέγετε στατιστικά στοιχεία σύμφωνα με τις διατάξεις του άρθρου 14 παράγραφος 1 της οδηγίας 2013/40/ΕΕ (οδηγία για τις επιθέσεις κατά συστημάτων πληροφοριών);	1	Διαθέτετε διοργανική κατάρτιση ή εργαστήρια κατάρτισης για υπηρεσίες επιβολής του νόμου, δικαστές, εισαγγελείς και εθνικές/κυβερνητικές CSIRT σε εθνικό ή/και σε πολυεθνικό επίπεδο;	1
	2	Έχετε πραγματοποιήσει μελέτη για το προσδιορισμό των εισαγγελέων και των δικαστών (νομική βάση, πόροι, δεξιότητες…) για την αποτελεσματική αντιμετώπιση του εγκλήματος στον κυβερνοχώρο;	1	Διαθέτετε νομική διάταξη που να αφορά τη διαδικτυακή κλοπή ταυτότητας και την κλοπή δεδομένων προσωπικού χαρακτήρα;	1	Διαθέτετε ειδικό προϋπολογισμό για μονάδες εγκλήματος στον κυβερνοχώρο;	1	Συλλέγετε ξεχωριστά στατιστικά στοιχεία για το έγκλημα στον κυβερνοχώρο; π.χ. επιχειρησιακά στατιστικά στοιχεία, στατιστικά στοιχεία για τις τάσεις στον κυβερνοχώρο, στατιστικά στοιχεία για τα έσοδα από εγκλήματα στον κυβερνοχώρο και προκληθείσες ζημίες…	1	Συμμετέχετε σε συντονισμένες δράσεις σε διεθνές επίπεδο για την παρεμπόδιση εγκληματικών δραστηριοτήτων; π.χ. διείσδυση φόρουμ εγκληματικής πειρατείας, οργανωμένες ομάδες εγκλήματος στον κυβερνοχώρο, αγορές αόρατου ιστού και αφαίρεση δικτύων μολυσμένων υπολογιστών (botnet)...	1

	3	Έχει υπογράψει η χώρα σας τη Σύμβαση της Βουδαπέστης του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο;	1	Διαθέτετε νομική διάταξη που να αφορά διαδικτυακές παραβιάσεις διανοητικής ιδιοκτησίας και πνευματικών δικαιωμάτων;	1	Έχετε δημιουργήσει κεντρικό φορέα/οντότητα για τον συντονισμό των δραστηριοτήτων στον τομέα της καταπολέμησης του εγκλήματος στον κυβερνοχώρο;	1	Αξιολογείτε την επάρκεια της εκπαίδευσης που παρέχεται στις υπηρεσίες επιβολής του νόμου, στο δικαστικό σώμα και στο εθνικό προσωπικό CSIRT για την αντιμετώπιση του εγκλήματος στον κυβερνοχώρο;	1	Υπάρχει σαφής διαχωρισμός καθηκόντων μεταξύ CSIRT, υπηρεσιών επιβολής του νόμου και δικαστικού σώματος (εισαγγελείς και δικαστές) όταν συνεργάζονται για την αντιμετώπιση εγκλημάτων στον κυβερνοχώρο;	1
	4			Διαθέτετε νομική διάταξη που να αφορά τη διαδικτυακή παρενόχληση ή τον εκφοβισμό στον κυβερνοχώρο;	1	Έχετε συστήσει μηχανισμούς συνεργασίας μεταξύ των αρμόδιων εθνικών φορέων που συμμετέχουν στην καταπολέμηση του εγκλήματος στον κυβερνοχώρο, συμπεριλαμβανομένων των εθνικών φορέων επιβολής του νόμου CSIRT;	1	Διεξάγετε τακτικές αξιολογήσεις για να διασφαλίσετε ότι διαθέτετε επαρκείς πόρους (ανθρώπινο δυναμικό, προϋπολογισμό και εργαλεία) για τις μονάδες εγκλήματος στον κυβερνοχώρο εντός των αρχών επιβολής του νόμου;	1	Το ρυθμιστικό σας πλαίσιο διευκολύνει τη συνεργασία μεταξύ CSIRT/αρχών επιβολής του νόμου και δικαστικού σώματος (εισαγγελείς και δικαστές);	1
Στόχος ΕΣΑΚ	**#**	**Επίπεδο 1**	**R**	**Επίπεδο 2**	**R**	**Επίπεδο 3**	**R**	**Επίπεδο 4**	**R**	**Επίπεδο 5**	**R**
12 – Αντιμετώπιση εγκλήματος στον κυβερνοχώρο	5			Διαθέτετε νομική διάταξη για την αντιμετώπιση της απάτης μέσω ηλεκτρονικών υπολογιστών; π.χ. συμμόρφωση με τις διατάξεις της Σύμβασης της Βουδαπέστης του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο	1	Συνεργάζεστε και ανταλλάσσετε πληροφορίες με άλλα κράτη μέλη στον τομέα της καταπολέμησης του εγκλήματος στον κυβερνοχώρο;	1	Διεξάγετε τακτικές αξιολογήσεις για να διασφαλίσετε ότι διαθέτετε επαρκείς πόρους (ανθρώπινο δυναμικό, προϋπολογισμό και εργαλεία) για τις μονάδες εγκλήματος στον κυβερνοχώρο εντός των διωκτικών αρχών;	1	Συμμετέχετε στη δημιουργία και τη διατήρηση τυποποιημένων εργαλείων και μεθοδολογιών, εντύπων και διαδικασιών που θα κοινοποιούνται στους ενδιαφερόμενους φορείς της ΕΕ (αρχές επιβολής του νόμου, CSIRT, ENISA, Ευρωπαϊκό Κέντρο για τα Εγκλήματα στον Κυβερνοχώρο (EC3) της Ευρωπόλ...);	1
	6	-		Διαθέτετε νομική διάταξη για την προστασία των παιδιών στο επιγραμμικό περιβάλλον; π.χ. συμμόρφωση με τις διατάξεις της οδηγίας 2011/93/ΕΕ και της Σύμβασης της Βουδαπέστης του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο...	1	Συνεργάζεστε και ανταλλάσσετε πληροφορίες με οργανισμούς της ΕΕ (π.χ. Ευρωπαϊκό Κέντρο για τα Εγκλήματα στον Κυβερνοχώρο της Ευρωπόλ, Eurojust, ENISA) στον τομέα της καταπολέμησης του εγκλήματος στον κυβερνοχώρο;	1	Διαθέτετε μονάδες ειδικών δικαστηρίων ή εξειδικευμένους δικαστές για τη διαχείριση υποθέσεων εγκλήματος στον κυβερνοχώρο;	1	Διαθέτετε προηγμένους μηχανισμούς για να αποτρέπετε την προσέλκυση ή τη συμμετοχή ατόμων σε εγκλήματα στον κυβερνοχώρο;	0

	7	-		Έχετε προσδιορίσει κάποιο επιχειρησιακό εθνικό σημείο επαφής για την ανταλλαγή πληροφοριών και την ανταπόκριση σε επείγοντα αιτήματα παροχής πληροφοριών από άλλα κράτη μέλη σχετικά με αδικήματα που ορίζονται στην οδηγία 2013/40/ΕΕ (οδηγία για τις επιθέσεις κατά συστημάτων πληροφοριών);	1	Διαθέτετε τα κατάλληλα εργαλεία για την αντιμετώπιση του εγκλήματος στον κυβερνοχώρο; π.χ. ταξινομία και ταξινόμηση του εγκλήματος στον κυβερνοχώρο, εργαλεία συλλογής ηλεκτρονικών αποδεικτικών στοιχείων, ψηφιακά εγκληματολογικά εργαλεία, αξιόπιστες πλατφόρμες διαμοιρασμού...	1	Εφαρμόζετε διατάξεις για την παροχή υποστήριξης και βοήθειας σε θύματα εγκλημάτων στον κυβερνοχώρο (γενικοί χρήστες, ΜΜΕ, μεγάλες εταιρείες);	1	Χρησιμοποιεί η χώρα σας σχέδιο στρατηγικής της ΕΕ ή/και το Πρωτόκολλο επιβολής του νόμου της ΕΕ για την αντιμετώπιση καταστάσεων έκτακτης ανάγκης (EU LE ERP) για την αποτελεσματική ανταπόκριση σε μεγάλης κλίμακας περιστατικά στον κυβερνοχώρο;	0
	8			Η υπηρεσία επιβολής του νόμου που διαθέτετε περιλαμβάνει ειδική μονάδα εγκλήματος στον κυβερνοχώρο;	1	Διαθέτετε τυποποιημένες επιχειρησιακές διαδικασίες για τη διαχείριση ηλεκτρονικών αποδεικτικών στοιχείων;	1	Έχετε θεσπίσει διοργανικό πλαίσιο και μηχανισμούς συνεργασίας μεταξύ όλων των αρμόδιων ενδιαφερόμενων φορέων (π.χ. αρχές επιβολής του νόμου, εθνικές CSIRT, δικαστικές κοινότητες), συμπεριλαμβανομένου του ιδιωτικού τομέα (π.χ. φορείς εκμετάλλευσης βασικών υπηρεσιών, πάροχοι υπηρεσιών), κατά περίπτωση, για την αντιμετώπιση κυβερνοεπιθέσεων;	1	-	
	9			Έχετε ορίσει, σύμφωνα με το άρθρο 35 της σύμβασης της Βουδαπέστης, σημείο επαφής σε 24ωρη βάση και 7 ημέρες την εβδομάδα;	1	Συμμετέχει η χώρα σας σε ευκαιρίες κατάρτισης που προσφέρονται ή/και υποστηρίζονται από οργανισμούς της ΕΕ (π.χ. Ευρωπόλ, Eurojust, OLAF, Cepol, ENISA);	0	Το ρυθμιστικό σας πλαίσιο διευκολύνει τη συνεργασία μεταξύ CSIRT και αρχών επιβολής του νόμου;	1	-	
Στόχος ΕΣΑΚ	**#**	**Επίπεδο 1**	**R**	**Επίπεδο 2**	**R**	**Επίπεδο 3**	**R**	**Επίπεδο 4**	**R**	**Επίπεδο 5**	**R**	
12 – Αντιμετώπιση εγκλήματος στον κυβερνοχώρο	10	-		Έχετε ορίσει εθνικό σημείο επαφής που λειτουργεί σε 24ωρη βάση και 7 ημέρες την εβδομάδα για το πρωτόκολλο επιβολής του νόμου της ΕΕ για την αντιμετώπιση καταστάσεων έκτακτης ανάγκης (EU LE ERP) για την αντιμετώπιση σοβαρών κυβερνοεπιθέσεων;	1	Σκοπεύει η χώρα σας να εγκρίνει το 2ο πρόσθετο πρωτόκολλο του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο;	0	Διαθέτετε μηχανισμούς (π.χ. εργαλεία, διαδικασίες) για τη διευκόλυνση της ανταλλαγής πληροφοριών και της συνεργασίας μεταξύ CSIRT/αρχών επιβολής του νόμου και πιθανώς του δικαστικού σώματος (εισαγγελείς και δικαστές) στον τομέα της καταπολέμησης του εγκλήματος στον κυβερνοχώρο;	1	-	

	11			Παρέχετε εξειδικευμένη εκπαίδευση σε ενδιαφερόμενους που ασχολούνται με την αντιμετώπιση του εγκλήματος στον κυβερνοχώρο (αρχές επιβολής του νόμου, δικαστικό σώμα, CSIRT) σε τακτική βάση; π.χ. εκπαιδευτικές συνεδρίες σχετικά με την αρχειοθέτηση/δίωξη εγκλημάτων στον κυβερνοχώρο, εκπαίδευση σχετικά με τη συλλογή ηλεκτρονικών αποδεικτικών στοιχείων και τη διασφάλιση της ακεραιότητας στο σύνολο της ψηφιακής αλυσίδας φύλαξης και ψηφιακής εγκληματολογίας, μεταξύ άλλων	1						
	12			Έχει επικυρώσει/προσχωρήσει η χώρα σας (σ)τη Σύμβαση της Βουδαπέστης του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο;	1			-	-	-	
	13	-		Έχει υπογράψει και επικυρώσει η χώρα σας το πρόσθετο πρωτόκολλο (ποινικοποίηση πράξεων ρατσιστικού και ξενοφοβικού χαρακτήρα που διαπράττονται μέσω συστημάτων ηλεκτρονικών υπολογιστών) στη Σύμβαση της Βουδαπέστης του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο;	0	-	-	-		-	

Στόχος ΕΣΑΚ	#	Επίπεδο 1	R	Επίπεδο 2	R	Επίπεδο 3	R	Επίπεδο 4	R	Επίπεδο 5	R
13 – Θέσπιση μηχανισμών αναφοράς περιστατικών	α	Έχετε συμπεριλάβει τον στόχο στην τρέχουσα ΕΣΑΚ, ή σκοπεύετε να τον συμπεριλάβετε στην επόμενη έκδοση;	1	Υπάρχουν άτυπες πρακτικές ή δραστηριότητες που συμβάλλουν στην επίτευξη του στόχου με μη συντεταγμένο τρόπο;	1	Διαθέτετε επίσημα καθορισμένο και τεκμηριωμένο σχέδιο δράσης;	1	Επανεξετάζετε το σχέδιο δράσης σας ως προς τον στόχο του για να ελέγξετε την απόδοσή του;	1	Έχετε θεσπίσει μηχανισμούς για να διασφαλίσετε ότι το σχέδιο δράσης προσαρμόζεται με δυναμικό τρόπο στις περιβαλλοντικές εξελίξεις;	1
	β			Ορίσατε τα επιδιωκόμενα αποτελέσματα, τις κατευθυντήριες αρχές ή τις βασικές δραστηριότητες του σχεδίου δράσης σας;	1	Διαθέτετε σχέδιο δράσης με σαφή κατανομή πόρων και διακυβέρνηση;	1	Επανεξετάζετε το σχέδιο δράσης σας ως προς τον στόχο του για να διασφαλίσετε ότι οι προτεραιότητες είναι σωστά ιεραρχημένες και ότι το σχέδιο σας έχει βελτιστοποιηθεί;	1		
	γ			Κατά περίπτωση, το σχέδιο δράσης σας υλοποιείται και είναι ήδη αποτελεσματικό σε περιορισμένο πεδίο εφαρμογής;	0						
	1	Διαθέτετε ανεπίσημους μηχανισμούς ανταλλαγής πληροφοριών σχετικά με περιστατικά στον κυβερνοχώρο μεταξύ ιδιωτικών οργανισμών και εθνικών αρχών;	1	Διαθέτετε σύστημα αναφοράς περιστατικών για όλους τους τομείς του παραρτήματος ΙΙ της οδηγίας ΑΔΠ;	1	Διαθέτετε υποχρεωτικό σύστημα αναφοράς περιστατικών το οποίο να λειτουργεί στην πράξη;	1	Διαθέτετε εναρμονισμένη διαδικασία για τομεακά συστήματα αναφοράς περιστατικών;	1	Δημιουργείτε ετήσια αναφορά περιστατικών;	1
	2	-		Εφαρμόζετε τις απαιτήσεις κοινοποίησης για παρόχους τηλεπικοινωνιακών υπηρεσιών σύμφωνα με το άρθρο 40 της οδηγίας (ΕΕ) 2018/1972; Η οδηγία ορίζει ότι τα κράτη μέλη μεριμνούν ώστε οι πάροχοι δημόσιων δικτύων ηλεκτρονικών επικοινωνιών ή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών να κοινοποιούν χωρίς αδικαιολόγητη καθυστέρηση στην αρμόδια εθνική αρχή κάθε περιστατικό ασφάλειας το οποίο είχε σημαντικό αντίκτυπο στη λειτουργία δικτύων ή υπηρεσιών.	1	Υφίσταται μηχανισμός συντονισμού/συνεργασίας για υποχρεώσεις αναφοράς περιστατικών σχετικά με τον ΓΚΠΔ, την οδηγία σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση, το άρθρο 40 (πρώην άρθρο 13α) και τον κανονισμό eIDAS;	1	Διαθέτετε σύστημα αναφοράς περιστατικών για τομείς πλην εκείνων που αναφέρονται στην οδηγία ΑΔΠ;	1	Υφίστανται αναφορές όσον αφορά το τοπίο ασφάλειας στον κυβερνοχώρο ή άλλα είδη ανάλυσης που εκπονούνται από την οντότητα που λαμβάνει τις αναφορές περιστατικών;	1

Στόχος ΕΣΑΚ	#	Επίπεδο 1	R	Επίπεδο 2	R	Επίπεδο 3	R	Επίπεδο 4	R	Επίπεδο 5	R
13 – Θέσπιση μηχανισμών αναφοράς περιστατικών	3	-		Εφαρμόζετε τις απαιτήσεις κοινοποίησης για παρόχους υπηρεσιών εμπιστοσύνης σύμφωνα με το άρθρο 19 του κανονισμού eIDAS [κανονισμός (ΕΕ) 910/2014]; Το άρθρο 19 απαιτεί, μεταξύ άλλων, από τους παρόχους υπηρεσιών εμπιστοσύνης να ενημερώνουν τον εποπτικό φορέα για σημαντικά περιστατικά/παραβιάσεις.	1	Διαθέτετε τα κατάλληλα εργαλεία για να διασφαλίσετε την εμπιστευτικότητα και την ακεραιότητα των πληροφοριών που κοινοποιούνται μέσω των διαφόρων διαύλων αναφοράς;	1	Μετράτε την αποτελεσματικότητα των διαδικασιών αναφοράς περιστατικών; *π.χ.* δείκτες για περιστατικά που έχουν αναφερθεί μέσω των κατάλληλων διαύλων, χρόνος υποβολής της αναφοράς περιστατικού...	1	-	
	4	-		Εφαρμόζετε τις απαιτήσεις κοινοποίησης για παρόχους ψηφιακών υπηρεσιών σύμφωνα με το άρθρο 16 της οδηγίας ΑΔΠ; Το άρθρο 16 απαιτεί από τους παρόχους ψηφιακών υπηρεσιών να κοινοποιούν στην αρμόδια αρχή ή την CSIRT χωρίς αδικαιολόγητη καθυστέρηση κάθε περιστατικό που έχει σημαντικό αντίκτυπο στην παροχή της υπηρεσίας που προσφέρουν εντός της Ένωσης, όπως αναφέρεται στο παράρτημα ΙΙΙ.	1	Διαθέτετε πλατφόρμα/εργαλείο για τη διευκόλυνση της διαδικασίας υποβολής αναφοράς;	0	Διαθέτετε κοινή ταξινομία σε εθνικό επίπεδο για την ταξινόμηση περιστατικών και τις κατηγορίες βασικών αιτιών;	0	-	

Στόχος ΕΣΑΚ	#	Επίπεδο 1	R	Επίπεδο 2	R	Επίπεδο 3	R	Επίπεδο 4	R	Επίπεδο 5	R
14 – Ενίσχυση της προστασίας της ιδιωτικής ζωής και των δεδομένων	α	Έχετε συμπεριλάβει τον στόχο στην τρέχουσα ΕΣΑΚ, ή σκοπεύετε να τον συμπεριλάβετε στην επόμενη έκδοση;	1	Υπάρχουν άτυπες πρακτικές ή δραστηριότητες που συμβάλλουν στην επίτευξη του στόχου με μη συντεταγμένο τρόπο;	1	Διαθέτετε επίσημα καθορισμένο και τεκμηριωμένο σχέδιο δράσης;	1	Επανεξετάζετε το σχέδιο δράσης σας ως προς τον στόχο του για να ελέγξετε την απόδοσή του;	1	Έχετε θεσπίσει μηχανισμούς για να διασφαλίσετε ότι το σχέδιο δράσης προσαρμόζεται με δυναμικό τρόπο στις περιβαλλοντικές εξελίξεις;	1
	β			Ορίσατε τα επιδιωκόμενα αποτελέσματα, τις κατευθυντήριες αρχές ή τις βασικές δραστηριότητες του σχεδίου δράσης σας;	1	Διαθέτετε σχέδιο δράσης με σαφή κατανομή πόρων και διακυβέρνηση;	1	Επανεξετάζετε το σχέδιο δράσης σας ως προς τον στόχο του για να διασφαλίσετε ότι οι προτεραιότητες είναι σωστά ιεραρχημένες και ότι το σχέδιο σας έχει βελτιστοποιηθεί;	1		
	γ			Κατά περίπτωση, το σχέδιο δράσης σας υλοποιείται και είναι ήδη αποτελεσματικό σε περιορισμένο πεδίο εφαρμογής;	0						
	1	Έχετε διεξαγάγει μελέτες ή αναλύσεις για τον προσδιορισμό των σημείων προς βελτίωση για την καλύτερη προστασία των δικαιωμάτων ιδιωτικής ζωής των πολιτών;	1	Η εθνική αρχή προστασίας δεδομένων συμμετέχει σε τομείς που αφορούν την ασφάλεια στον κυβερνοχώρο (π.χ. κατάρτιση νέων νόμων και κανονισμών για την ασφάλεια στον κυβερνοχώρο, θέσπιση ελάχιστων μέτρων ασφαλείας);	1	Προωθείτε βέλτιστες πρακτικές για μέτρα ασφαλείας και προστασία των δεδομένων ήδη από τον σχεδιασμό για τον δημόσιο και/ή τον ιδιωτικό τομέα;	1	Διεξάγετε τακτικές αξιολογήσεις για να διασφαλίσετε ότι διαθέτετε επαρκείς πόρους (ανθρώπινο δυναμικό, προϋπολογισμό και εργαλεία) για την αρχή προστασίας δεδομένων;	1	Έχετε θεσπίσει μηχανισμούς για την παρακολούθηση των τελευταίων τεχνολογικών εξελίξεων με σκοπό την προσαρμογή των σχετικών κατευθυντήριων γραμμών και νομικών διατάξεων/υποχρεώσεων;	1
	2	Έχετε αναπτύξει νομική βάση σε εθνικό επίπεδο για την επιβολή του γενικού κανονισμού για την προστασία των δεδομένων (κανονισμός ΕΕ αριθ. 2016/679) π.χ. για τη διατήρηση ή θέσπιση πιο συγκεκριμένων διατάξεων ή περιορισμών για τους κανόνες του κανονισμού	0	-		Πραγματοποιείτε προγράμματα ευαισθητοποίησης και κατάρτισης σχετικά με αυτό το θέμα;	1	Ενθαρρύνετε τους οργανισμούς και τις επιχειρήσεις να λαμβάνουν πιστοποίηση ISO/IEC 27701:2019 για σύστημα διαχείρισης πληροφοριών ιδιωτικότητας (PIMS);	1	Συμμετέχετε/προωθείτε ενεργά πρωτοβουλίες E&A σχετικά με τις τεχνολογίες για τη βελτίωση της προστασίας της ιδιωτικότητας;	0
	3	-		-		Συντονίζετε διαδικασίες αναφοράς περιστατικών με την ΑΠΔ;	1	-		-	
	4	-		-		Προωθείτε και υποστηρίζετε την ανάπτυξη τεχνικών προτύπων για την ασφάλεια και την ιδιωτικότητα πληροφοριών; Είναι τα εν λόγω πρότυπα ειδικά προσαρμοσμένα σε μικρές και μεσαίες επιχειρήσεις (ΜΜΕ);	0	-		-	

	5	-		-		Παρέχετε πρακτικές και κλιμακούμενες κατευθυντήριες γραμμές για την υποστήριξη διαφορετικών ειδών υπεύθυνων επεξεργασίας δεδομένων όσον αφορά την τήρηση των νομικών απαιτήσεων και υποχρεώσεων για την ιδιωτική ζωή και την προστασία δεδομένων;	0	-		-	

4.1.4 Δέσμη #4: Συνεργασία

Στόχος ΕΣΑΚ	#	Επίπεδο 1	R	Επίπεδο 2	R	Επίπεδο 3	R	Επίπεδο 4	R	Επίπεδο 5	R
15 – Δημιουργία εταιρικής σχέσης δημοσίου-ιδιωτικού τομέα (ΕΣΔΙΤ)	α	Έχετε συμπεριλάβει τον στόχο στην τρέχουσα ΕΣΑΚ, ή σκοπεύετε να τον συμπεριλάβετε στην επόμενη έκδοση;	1	Υπάρχουν άτυπες πρακτικές ή δραστηριότητες που συμβάλλουν στην επίτευξη του στόχου με μη συντεταγμένο τρόπο;	1	Διαθέτετε επίσημα καθορισμένο και τεκμηριωμένο σχέδιο δράσης;	1	Επανεξετάζετε το σχέδιο δράσης σας ως προς τον στόχο του για να ελέγξετε την απόδοσή του;	1	Έχετε θεσπίσει μηχανισμούς για να διασφαλίσετε ότι το σχέδιο δράσης προσαρμόζεται με δυναμικό τρόπο στις περιβαλλοντικές εξελίξεις;	1
	β			Ορίσατε τα επιδιωκόμενα αποτελέσματα, τις κατευθυντήριες αρχές ή τις βασικές δραστηριότητες του σχεδίου δράσης σας;	1	Διαθέτετε σχέδιο δράσης με σαφή κατανομή πόρων και διακυβέρνηση;	1	Επανεξετάζετε το σχέδιο δράσης σας ως προς τον στόχο του για να διασφαλίσετε ότι οι προτεραιότητες είναι σωστά ιεραρχημένες και ότι το σχέδιο σας έχει βελτιστοποιηθεί;	1		
	γ			Κατά περίπτωση, το σχέδιο δράσης σας υλοποιείται και είναι ήδη αποτελεσματικό σε περιορισμένο πεδίο εφαρμογής;	0						
	1	Είναι γενικώς κατανοητό ότι οι εταιρικές σχέσεις δημοσίου-ιδιωτικού τομέα συμβάλλουν στην ενίσχυση του επιπέδου κυβερνοασφάλειας στη χώρα με διαφορετικά μέσα; *π.χ.* μέσω των κοινών συμφερόντων στην ανάπτυξη της βιομηχανίας της ασφάλειας στον κυβερνοχώρο, της συμμετοχής στην εκπόνηση ενός σχετικού ρυθμιστικού πλαισίου για την ασφάλεια στον κυβερνοχώρο, της ενθάρρυνσης της Ε&Α...	1	Διαθέτετε ένα εθνικό σχέδιο δράσης για τη δημιουργία εταιρικών σχέσεων δημοσίου-ιδιωτικού τομέα;	1	Έχετε δημιουργήσει εθνικές εταιρικές σχέσεις δημοσίου-ιδιωτικού τομέα;	1	Έχετε δημιουργήσει διατομεακές εταιρικές σχέσεις δημοσίου-ιδιωτικού τομέα;	1	Ανάλογα με τις τελευταίες τεχνολογικές και κανονιστικές εξελίξεις, έχετε προσαρμόσει ή δημιουργήσει εταιρικές σχέσεις δημοσίου-ιδιωτικού τομέα;	1
	2	-		Έχετε δημιουργήσει μια νομική ή συμβατική βάση (συγκεκριμένους νόμους, συμφωνίες διαφύλαξης απορρήτου, διανοητική ιδιοκτησία) για τις εταιρικές σχέσεις δημοσίου-ιδιωτικού τομέα;	1	Έχετε δημιουργήσει τομεακές εταιρικές σχέσεις δημοσίου-ιδιωτικού τομέα;	1	Στις εταιρικές σχέσεις δημοσίου-ιδιωτικού τομέα που έχετε δημιουργήσει, εστιάζετε και στη συνεργασία δημόσιου-δημόσιου φορέα και ιδιωτικού-ιδιωτικού φορέα;	1		
	3	-		-		Χρηματοδοτείτε τη δημιουργία εταιρικών σχέσεων δημοσίου-ιδιωτικού τομέα;	1	Προωθείτε εταιρικές σχέσεις δημοσίου-ιδιωτικού τομέα μεταξύ μικρών και μεσαίων επιχειρήσεων (ΜΜΕ);	1	-	

	4	-		-		Σε γενικές γραμμές, οι δημόσιοι οργανισμοί ηγούνται των εταιρικών σχέσεων δημοσίου-ιδιωτικού τομέα;*π.χ.* ένα ενιαίο σημείο επαφής από τον δημόσιο τομέα είναι αρμόδιο για τη διακυβέρνηση και τον συντονισμό της σύμπραξης, εκ των προτέρων συμφωνία των δημόσιων οργανισμών σχετικά με τα επιθυμητά επιτεύγματα, σαφείς κατευθυντήριες γραμμές από τις δημόσιες διοικητικές αρχές σχετικά με τις ανάγκες και τους περιορισμούς τους προς τον ιδιωτικό τομέα...	1	Μετράτε τα αποτελέσματα των εταιρικών σχέσεων δημοσίου-ιδιωτικού τομέα;	1	-	
	5	-		-		Είστε μέλος της συμβατικής εταιρικής σχέσης δημοσίου-ιδιωτικού τομέα του Ευρωπαϊκού Οργανισμού για την Ασφάλεια στον Κυβερνοχώρο (ECSO);	0	-		-	
Στόχος ΕΣΑΚ	**#**	**Επίπεδο 1**	**R**	**Επίπεδο 2**	**R**	**Επίπεδο 3**	**R**	**Επίπεδο 4**	**R**	**Επίπεδο 5**	**R**
15 – Δημιουργία εταιρικής σχέσης δημοσίου-ιδιωτικού τομέα	6	-		-		Διαθέτετε μία ή αρκετές εταιρικές σχέσεις δημοσίου-ιδιωτικού τομέα σχετικά με τις δραστηριότητες της CSIRT;	0	-		-	
	7					Διαθέτετε μία ή αρκετές εταιρικές σχέσεις δημοσίου-ιδιωτικού τομέα που ασχολείται με ζητήματα προστασίας των υποδομών πληροφοριών ζωτικής σημασίας;	0				
	8	-		-		Διαθέτετε μία ή αρκετές εταιρικές σχέσεις δημοσίου-ιδιωτικού τομέα που ασχολείται με την ευαισθητοποίηση ως προς την ασφάλεια στον κυβερνοχώρο και την ανάπτυξη δεξιοτήτων;	0	-		-	

Στόχος ΕΣΑΚ	#	Επίπεδο 1	R	Επίπεδο 2	R	Επίπεδο 3	R	Επίπεδο 4	R	Επίπεδο 5	R
16 – Θεσμοθέτηση της συνεργασίας μεταξύ δημόσιων οργανισμών	α	Έχετε συμπεριλάβει τον στόχο στην τρέχουσα ΕΣΑΚ, ή σκοπεύετε να τον συμπεριλάβετε στην επόμενη έκδοση;	1	Υπάρχουν άτυπες πρακτικές ή δραστηριότητες που συμβάλλουν στην επίτευξη του στόχου με μη συντεταγμένο τρόπο;	1	Διαθέτετε επίσημα καθορισμένο και τεκμηριωμένο σχέδιο δράσης;	1	Επανεξετάζετε το σχέδιο δράσης σας ως προς τον στόχο του για να ελέγξετε την απόδοσή του;	1	Έχετε θεσπίσει μηχανισμούς για να διασφαλίσετε ότι το σχέδιο δράσης προσαρμόζεται με δυναμικό τρόπο στις περιβαλλοντικές εξελίξεις;	1
	β			Ορίσατε τα επιδιωκόμενα αποτελέσματα, τις κατευθυντήριες αρχές ή τις βασικές δραστηριότητες του σχεδίου δράσης σας;	1	Διαθέτετε σχέδιο δράσης με σαφή κατανομή πόρων και διακυβέρνηση;	1	Επανεξετάζετε το σχέδιο δράσης σας ως προς τον στόχο του για να διασφαλίσετε ότι οι προτεραιότητες είναι σωστά ιεραρχημένες και ότι το σχέδιο σας έχει βελτιστοποιηθεί;	1		
	γ			Κατά περίπτωση, το σχέδιο δράσης σας υλοποιείται και είναι ήδη αποτελεσματικό σε περιορισμένο πεδίο εφαρμογής;	0						
	1	Διαθέτετε άτυπους διαύλους συνεργασίας μεταξύ δημόσιων φορέων;	1	Διαθέτετε ένα εθνικό πρόγραμμα συνεργασίας για την ασφάλεια στον κυβερνοχώρο; *π.χ.* συμβουλευτικά σώματα, ομάδες καθοδήγησης, φόρουμ, συμβούλια, κέντρα κυβερνοχώρου ή ομάδες εμπειρογνωμόνων	1	Συμμετέχουν οι δημόσιες αρχές στο πρόγραμμα συνεργασίας;	1	Διασφαλίζετε την ύπαρξη ειδικών διαύλων συνεργασίας για την ασφάλεια στον κυβερνοχώρο τουλάχιστον μεταξύ των ακόλουθων δημόσιων φορέων: υπηρεσίες πληροφοριών, εγχώριοι φορείς επιβολής του νόμου, διωκτικές αρχές, κυβερνητικοί φορείς, εθνική ομάδα παρέμβασης για συμβάντα που αφορούν την ασφάλεια των υπολογιστών και στρατός;	1	Παρέχετε στους δημόσιους οργανισμούς ενιαία ελάχιστη πληροφόρηση σχετικά με τις τελευταίες εξελίξεις του πεδίου των απειλών και της κατάστασης της ασφάλειας στον κυβερνοχώρο;	1
	2	-		-		Έχετε δημιουργήσει πλατφόρμες συνεργασίας για την ανταλλαγή πληροφοριών;	1	Μετράτε τις επιτυχίες και τα όρια των διαφόρων προγραμμάτων συνεργασίας όσον αφορά την προώθηση αποτελεσματικής συνεργασίας;	1	-	

Στόχος ΕΣΑΚ	#	Επίπεδο 1	R	Επίπεδο 2	R	Επίπεδο 3	R	Επίπεδο 4	R	Επίπεδο 5	R
16 – Θεσμοθέτηση της συνεργασίας μεταξύ δημόσιων οργανισμών	3	-		-		Έχετε προσδιορίσει το πεδίο εφαρμογής των πλατφορμών συνεργασίας (π.χ. καθήκοντα και υποχρεώσεις, αριθμός θεματικών τομέων);	1	-		-	
	4	-		-		Διοργανώνετε ετήσιες συνεδριάσεις;	1	-		-	

	5	-		-		Διαθέτετε μηχανισμούς συνεργασίας μεταξύ των αρμόδιων αρχών στις διάφορες γεωγραφικές περιφέρειες; *π.χ.* δίκτυο ανταποκριτών ασφαλείας ανά περιφέρεια, αξιωματικούς ασφάλειας στον κυβερνοχώρο στα περιφερειακά οικονομικά επιμελητήρια...	1	-		-	

Στόχος ΕΣΑΚ	#	Επίπεδο 1	R	Επίπεδο 2	R	Επίπεδο 3	R	Επίπεδο 4	R	Επίπεδο 5	R
17 – Συμμετοχή σε διεθνή συνεργασία (όχι μόνο με κράτη μέλη της ΕΕ)	α	Έχετε συμπεριλάβει τον στόχο στην τρέχουσα ΕΣΑΚ, ή σκοπεύετε να τον συμπεριλάβετε στην επόμενη έκδοση;	1	Υπάρχουν άτυπες πρακτικές ή δραστηριότητες που συμβάλλουν στην επίτευξη του στόχου με μη συντεταγμένο τρόπο;	1	Διαθέτετε επίσημα καθορισμένο και τεκμηριωμένο σχέδιο δράσης;	1	Επανεξετάζετε το σχέδιο δράσης σας ως προς τον στόχο του για να ελέγξετε την απόδοσή του;	1	Έχετε θεσπίσει μηχανισμούς για να διασφαλίσετε ότι το σχέδιο δράσης προσαρμόζεται με δυναμικό τρόπο στις περιβαλλοντικές εξελίξεις;	1
	β			Ορίσατε τα επιδιωκόμενα αποτελέσματα, τις κατευθυντήριες αρχές ή τις βασικές δραστηριότητες του σχεδίου δράσης σας;	1	Διαθέτετε σχέδιο δράσης με σαφή κατανομή πόρων και διακυβέρνηση;	1	Επανεξετάζετε το σχέδιο δράσης σας ως προς τον στόχο του για να διασφαλίσετε ότι οι προτεραιότητες είναι σωστά ιεραρχημένες και ότι το σχέδιο σας έχει βελτιστοποιηθεί;	1		
	γ			Κατά περίπτωση, το σχέδιο δράσης σας υλοποιείται και είναι ήδη αποτελεσματικό σε περιορισμένο πεδίο εφαρμογής;	0						
	1	Έχετε χαράξει μια διεθνή στρατηγική συμμετοχής;	1	Έχετε συνάψει συμφωνίες συνεργασίας με άλλες χώρες (διμερείς, πολυμερείς) ή με συνεργάτες σε άλλες χώρες; *π.χ.* ανταλλαγή πληροφοριών, δημιουργία ικανοτήτων, παροχή συνδρομής...	1	Προβαίνετε στην ανταλλαγή πληροφοριών σε στρατηγικό επίπεδο; *π.χ.* πολιτική υψηλού επιπέδου, αντίληψη κινδύνου...	1	Συμμετέχουν οι εθνικοί δημόσιοι φορείς ασφάλειας στον κυβερνοχώρο της χώρας σας σε προγράμματα διεθνούς συνεργασίας;	1	Πραγματοποιείτε συζητήσεις για ένα ή περισσότερα θέματα στο πλαίσιο πολυμερών συμφωνιών;	1
	2	Διαθέτετε άτυπους διαύλους συνεργασίας με άλλες χώρες;	1	Διαθέτετε ένα ενιαίο σημείο επαφής που μπορεί να λειτουργεί ως σύνδεσμος για να διασφαλίσει τη διασυνοριακή συνεργασία με τις αρχές των κρατών μελών (ομάδα συνεργασίας, δίκτυο ομάδων παρέμβασης για συμβάντα που αφορούν την ασφάλεια των υπολογιστών...);	1	Προβαίνετε στην ανταλλαγή πληροφοριών σε τακτικό επίπεδο; *π.χ.* δελτίο για παράγοντες απειλής, κέντρα ανταλλαγής και ανάλυσης πληροφοριών, τακτικές, τεχνικές και διαδικασίες...	1	Αξιολογείτε σε τακτική βάση τα αποτελέσματα των πρωτοβουλιών διεθνούς συνεργασίας;	1	Πραγματοποιείτε συζητήσεις για ένα ή περισσότερα θέματα στο πλαίσιο διεθνών συνθηκών ή συμβάσεων;	1

Στόχος ΕΣΑΚ	#	Επίπεδο 1	R	Επίπεδο 2	R	Επίπεδο 3	R	Επίπεδο 4	R	Επίπεδο 5	R
17 – Συμμετοχή σε διεθνή συνεργασία (όχι μόνο με κράτη μέλη της ΕΕ)	3	Έχει εκφράσει η κρατική ηγεσία την πρόθεσή της να συμμετάσχει σε διεθνή συνεργασία στον τομέα της ασφάλειας στον κυβερνοχώρο;	1	Υπάρχουν συγκεκριμένα άτομα που ασχολούνται με τη διεθνή συνεργασία;	1	Ανταλλάσσετε πληροφορίες σε επιχειρησιακό επίπεδο; *π.χ.* επιχειρησιακός συντονισμός πληροφοριών, εν εξελίξει περιστατικά, δείκτες έκθεσης σε κίνδυνο...	1	-		Πραγματοποιείτε συζητήσεις ή διαπραγματεύσεις για ένα ή περισσότερα θέματα με διεθνείς ομάδες εμπειρογνωμόνων; *π.χ.* Η Εθνική Επιτροπή για τη Σταθερότητα του Κυβερνοχώρου (GCSC), η ομάδα συνεργασίας για την ασφάλεια δικτύων και πληροφοριών του RNISA, η ομάδα κυβερνητικών εμπειρογνωμόνων για την ασφάλεια των πληροφοριών του ΟΗΕ (GGE)...	1
	4	-		-		Συμμετέχετε σε διεθνείς ασκήσεις κυβερνοασφάλειας;	1	-		-	
	5	-		-		Συμμετέχετε σε διεθνείς πρωτοβουλίες δημιουργίας ικανοτήτων; *π.χ.* κατάρτιση, ανάπτυξη δεξιοτήτων, κατάρτιση τυποποιημένων διαδικασιών...	0	-		-	
	6	-		-		Έχετε συνάψει συμφωνίες αμοιβαίας συνδρομής με άλλες χώρες;*π.χ.*δραστηριότητες αρχών επιβολής του νόμου, νομικές διαδικασίες, αμοιβαιότητα ικανοτήτων απόκρισης σε περιστατικά, ανταλλαγή πόρων κυβερνοασφάλειας...	0	-		-	
	7	-		-		Έχετε υπογράψει ή επικυρώσει διεθνείς συνθήκες ή συμβάσεις στον τομέα της ασφάλειας στον κυβερνοχώρο; *π.χ.* τον Διεθνή κώδικα δεοντολογίας για την ασφάλεια των πληροφοριών, τη Σύμβαση για το έγκλημα στον κυβερνοχώρο	0	-		-	

4.2 ΚΑΤΕΥΘΥΝΤΗΡΙΕΣ ΓΡΑΜΜΕΣ ΓΙΑ ΤΗ ΧΡΗΣΗ ΤΟΥ ΠΛΑΙΣΙΟΥ

Στόχος της παρούσας ενότητας είναι να παράσχει στα κράτη μέλη μερικές κατευθυντήριες γραμμές και συστάσεις για την ανάπτυξη του πλαισίου και τη συμπλήρωση του ερωτηματολογίου. Οι συστάσεις που απαριθμούνται παρακάτω προκύπτουν κυρίως από την ανατροφοδότηση από συνεντεύξεις με τους εκπροσώπους των κρατών μελών:

- **Προληπτικές ενέργειες συντονισμού για τη συγκέντρωση και την ενοποίηση δεδομένων.** Τα περισσότερα κράτη μέλη αναγνωρίζουν ότι η ολοκλήρωση αυτής της άσκησης αυτοαξιολόγησης απαιτεί περίπου 15 ανθρωποημέρες. Για τη διενέργεια της αυτοαξιολόγησης, θα πρέπει να ζητηθεί η γνώμη ενός ευρέος φάσματος ενδιαφερόμενων παραγόντων. Συνεπώς, συνιστάται η διάθεση χρόνου στο προπαρασκευαστικό στάδιο για τον εντοπισμό των σχετικών ενδιαφερόμενων παραγόντων εντός των κυβερνητικών οργανισμών, των δημόσιων υπηρεσιών και του ιδιωτικού τομέα.
- **Προσδιορισμός ενός κεντρικού οργανισμού αρμόδιου για την ολοκλήρωση της αυτοαξιολόγησης σε εθνικό επίπεδο.** Επειδή η συγκέντρωση υλικού για όλους τους δείκτες του ΕΠΑΙ μπορεί να πραγματοποιείται από πολλούς ενδιαφερόμενους φορείς, συνιστάται η ανάθεση της ολοκλήρωσης της αυτοαξιολόγησης σε έναν οργανισμό ή υπηρεσία που θα επικοινωνήσει με τους σχετικούς ενδιαφερόμενους φορείς και θα αναλάβει τον συντονισμό τους.
- **Χρήση της άσκησης αξιολόγησης ως τρόπου κοινοποίησης και επικοινωνίας θεμάτων που αφορούν την ασφάλεια στον κυβερνοχώρο.** Σύμφωνα με τα αντληθέντα διδάγματα που αντάλλαξαν τα κράτη μέλη, οι συζητήσεις (είτε υπό τη μορφή προσωπικών συνεντεύξεων είτε υπό τη μορφή συλλογικών εργαστηρίων) αποτελούν μια εξαιρετική ευκαιρία ανάπτυξης διαλόγου σχετικά με θέματα ασφάλειας στον κυβερνοχώρο και ανταλλαγής κοινών απόψεων και σημείων προς βελτίωση. Πέρα από την ανάδειξη των βασικών επιτευγμάτων, η ανταλλαγή αποτελεσμάτων μπορεί να συμβάλλει και στην προώθηση ζητημάτων ασφάλειας στον κυβερνοχώρο.
- **Αξιοποίηση της ΕΣΑΚ ως πεδίου για την επιλογή των στόχων που θα υποβληθούν σε αξιολόγηση.** Οι 17 στόχοι που στοιχειοθετούν το Εθνικό Πλαίσιο Αξιολόγησης Ικανοτήτων καταρτίστηκαν βάσει των στόχων που καλύπτονται συνήθως από τα κράτη μέλη στις οικείες ΕΣΑΚ. Οι στόχοι που καλύπτονται στο πλαίσιο της ΕΣΑΚ θα πρέπει να χρησιμοποιηθούν ως βάση της αξιολόγησης. Ωστόσο, η ΕΣΑΚ δεν θα πρέπει να περιορίσει την αξιολόγηση. Εφόσον η ΕΣΑΚ εστιάζεται, όπως είναι φυσικό, σε προτεραιότητες, ορισμένοι τομείς παραλείπονται σκοπίμως. Ωστόσο, αυτό δεν συνεπάγεται έλλειψη μιας δεδομένης ικανότητας. Για παράδειγμα, στην περίπτωση που ένας συγκεκριμένος στόχος παραλείπεται από την ΕΣΑΚ, αλλά η ενδιαφερόμενη χώρα διαθέτει ικανότητες ασφάλειας στον κυβερνοχώρο που σχετίζονται με τον εν λόγω στόχο, η αξιολόγησή του μπορεί να πραγματοποιηθεί.
- **Σε περιπτώσεις εξέλιξης του πεδίου εφαρμογής της ΕΣΑΚ, βεβαιωθείτε ότι η ερμηνεία της βαθμολογίας παραμένει συνεπής με την εξέλιξη της ΕΣΑΚ.** Ο κύκλος ζωής της ΕΣΑΚ είναι μια πολυετής διαδικασία. Οι ΕΣΑΚ ορισμένων κρατών μελών εφαρμόζονται συνήθως με έναν χάρτη πορείας 3 έως 5 ετών, και σημειώνονται οι αλλαγές στο πεδίο εφαρμογής μεταξύ δύο διαδοχικών εκδόσεων της ΕΣΑΚ. Εν προκειμένω, πρέπει να δοθεί ιδιαίτερη μέριμνα κατά την παρουσίαση των αποτελεσμάτων της αυτοαξιολόγησης μεταξύ των δύο εκδόσεων της ΕΣΑΚ: οι αλλαγές σε επίπεδο πεδίου εφαρμογής ενδέχεται πράγματι να επηρεάσουν την τελική βαθμολογία ωριμότητας. Συνιστάται η σύγκριση των βαθμολογιών στο πλήρες πεδίο εφαρμογής των στρατηγικών στόχων από το ένα έτος στο επόμενο (*δηλ.* Συνολική γενική βαθμολογία).

Υπενθύμιση για τον μηχανισμό βαθμολόγησης – παράδειγμα για τον λόγο κάλυψης
Ο μηχανισμός βαθμολόγησης περιλαμβάνει δύο επίπεδα βαθμολόγησης:
(i) έναν **συνολικό γενικό λόγο κάλυψης** βάσει του συνολικού καταλόγου στρατηγικών στόχων που περιλαμβάνονται στο πλαίσιο αυτοαξιολόγησης· και
(ii) **έναν συνολικό ειδικό λόγο κάλυψης** βάσει των στρατηγικών στόχων που επιλέγει το κράτος μέλος (που συνήθως αντιστοιχούν στους στόχους που περιλαμβάνονται στην ΕΣΑΚ της συγκεκριμένης χώρας).

Εκ σχεδιασμού (βλ. ενότητα 3.1 για τον μηχανισμό βαθμολόγησης), ο συνολικός ειδικός λόγος κάλυψης θα είναι ίσος ή μεγαλύτερος από τον συνολικό γενικό λόγο κάλυψης, διότι ο τελευταίος μπορεί να περιλαμβάνει στόχους που δεν καλύπτονται από το κράτος μέλος και που, κατά συνέπεια, μειώνουν τον συνολικό γενικό λόγο κάλυψης. Όταν ένα κράτος μέλος προσθέτει έναν νέο στόχο, ο συνολικός λόγος κάλυψης αυξάνεται (δηλ. καλύπτονται περισσότεροι δείκτες ωριμότητας), ενώ η συνολική ειδική ωριμότητα ενδέχεται να μειωθεί (σε περίπτωση που ο νέος στόχος βρίσκεται σε αρχικό στάδιο και παρουσιάζει, επομένως, χαμηλό επίπεδο ωριμότητας).

- **Κατά τη συμπλήρωση του ερωτηματολογίου αυτοαξιολόγησης, πρέπει να θυμάστε ότι ο πρωταρχικός στόχος είναι η υποστήριξη των κρατών μελών στην ανάπτυξη ικανοτήτων ασφάλειας στον κυβερνοχώρο.** Επομένως, κατά τη συμπλήρωση της αυτοαξιολόγησης, ακόμα και εάν είναι σε ορισμένες περιπτώσεις δύσκολο να απαντηθεί μια ερώτηση με οριστικό τρόπο, συνιστάται η επιλογή της γενικώς αποδεκτής απάντησης. Εάν, για παράδειγμα, η απάντηση σε μια ερώτηση είναι θετική σε ένα ορισμένο πεδίο εφαρμογής, και αρνητική σε ένα άλλο, τα κράτη μέλη θα πρέπει να θυμούνται ότι μια αρνητική απάντηση απαιτεί δράση: είτε ένα σχέδιο διόρθωσης είτε ένα σχέδιο δράσης για κάποιον τομέα που χρήζει βελτίωσης το οποίο θα πρέπει να ληφθεί υπόψη στις μελλοντικές εξελίξεις.

5. ΕΠΟΜΕΝΑ ΒΗΜΑΤΑ

5.1 ΜΕΛΛΟΝΤΙΚΕΣ ΒΕΛΤΙΩΣΕΙΣ

Κατά τη διάρκεια των συνεντεύξεων με τους εκπροσώπους των κρατών μελών και κατά τη διάρκεια του σταδίου της δευτερογενούς έρευνας τεκμηρίωσης, καταρτίστηκαν επίσης οι εξής συστάσεις για τη βελτίωση του τρέχοντος Πλαισίου Αξιολόγησης Εθνικών Ικανοτήτων ως πιθανές μελλοντικές εξελίξεις:

- **Ανάπτυξη του συστήματος βαθμολόγησης για περισσότερη ακρίβεια.** Για παράδειγμα, θα μπορούσε να εισαχθεί ένα ποσοστό κάλυψης αντί για το δυαδικό σύστημα απαντήσεων ΝΑΙ/ΟΧΙ το οποίο θα επιτρέπει την καλύτερη αποτύπωση της πολυπλοκότητας της εδραίωσης των ικανοτήτων σε εθνικό επίπεδο. Ως πρώτο βήμα, επελέγη μια απλή προσέγγιση με απαντήσεις τύπου ΝΑΙ/ΟΧΙ.
- **Εισαγωγή ποσοτικών δεικτών μέτρησης για τη μέτρηση της αποτελεσματικότητας της ΕΣΑΚ του κράτους μέλους.** Πράγματι, το Πλαίσιο Αξιολόγησης Εθνικών Ικανοτήτων εστιάζει στην αξιολόγηση του επιπέδου ωριμότητας των ικανοτήτων ασφάλειας στον κυβερνοχώρο των κρατών μελών. Συμπληρωματικά, θα μπορούσαν να αξιοποιηθούν δείκτες μέτρησης για τη μέτρηση της αποτελεσματικότητας των δραστηριοτήτων και των σχεδίων δράσης που εφαρμόζουν τα κράτη μέλη για την οικοδόμηση αυτών των ικανοτήτων. Δεν φαινόταν ρεαλιστική επιλογή η δημιουργία τέτοιων δεικτών μέτρησης στην παρούσα φάση, δεδομένου ότι υπάρχει ελάχιστη ανατροφοδότηση από το πεδίο, είναι δύσκολη η εύρεση ουσιαστικών δεικτών που συνδέουν το αποτέλεσμα με την υλοποίηση της ΕΣΑΚ, και είναι δύσκολη η δημιουργία ρεαλιστικών δεικτών που μπορούν στη συνέχεια να συλλεχθούν. Ωστόσο, αυτό το ζήτημα παραμένει ανοικτό προς συζήτηση στο μέλλον.
- **Μετάβαση από μια άσκηση αυτοαξιολόγησης σε μια προσέγγιση αξιολόγησης.** Μια πιθανή μελλοντική εξέλιξη του πλαισίου θα μπορούσε να περιλαμβάνει τη μετάβαση προς μια προσέγγιση αξιολόγησης της ωριμότητας των ικανοτήτων ασφάλειας στον κυβερνοχώρο των κρατών μελών με μεγαλύτερη συνέπεια. Η διεξαγωγή της αξιολόγησης από ένα τρίτο μέρος θα μπορούσε να ελαχιστοποιήσει την πιθανή μεροληψία.

ΠΑΡΑΡΤΗΜΑ Α – ΕΠΙΣΚΟΠΗΣΗ ΤΩΝ ΑΠΟΤΕΛΕΣΜΑΤΩΝ ΤΗΣ ΔΕΥΤΕΡΟΓΕΝΟΥΣ ΕΡΕΥΝΑΣ ΤΕΚΜΗΡΙΩΣΗΣ

Το Παράρτημα Α περιέχει μια σύνοψη του προηγούμενου έργου του ENISA για τις ΕΣΑΚ και μια ανασκόπηση των διαθέσιμων σχετικών μοντέλων ωριμότητας σχετικά με τις ικανότητες ασφάλειας στον κυβερνοχώρο. Οι παρακάτω υποθέσεις λαμβάνονται υπόψη για την επιλογή και ανασκόπηση των μοντέλων:

- Δεν βασίζονται όλα τα μοντέλα σε μια αυστηρή ερευνητική μεθοδολογία·
- Η δομή και τα αποτελέσματα των προτύπων δεν επεξηγούνται πάντα διεξοδικά με σαφή σύνδεση των διαφορετικών στοιχείων που χαρακτηρίζουν κάθε μοντέλο·
- Ορισμένα μοντέλα δεν παρέχουν λεπτομέρειες σχετικά με τη διαδικασία ανάπτυξης, τη δομή και τη μεθοδολογία αξιολόγησης·
- Άλλα μοντέλα και εργαλεία τα οποία βρήκαμε δεν παρέχουν καθόλου λεπτομέρειες σχετικά με τη δομή και το περιεχόμενο και, κατά συνέπεια, δεν περιλαμβάνονται στον κατάλογο· και
- Η επιλογή των μοντέλων προς εξέταση βασίζεται στη γεωγραφική κάλυψη. Θα δοθεί έμφαση κυρίως σε μοντέλα ωριμότητας για τις ικανότητες ασφάλειας στον κυβερνοχώρο τα οποία έχουν σχεδιαστεί για την αξιολόγηση της απόδοσης των ευρωπαϊκών χωρών. Ωστόσο, είναι σημαντικό να επεκταθεί η γεωγραφική κάλυψη για την ανάλυση ορθών πρακτικών δημιουργίας προτύπων ωριμότητας ανά τον κόσμο.

Αυτή η συστηματική ανασκόπηση των σχετικών δημόσια διαθέσιμων μοντέλων ωριμότητας για τις ικανότητες ασφάλειας στον κυβερνοχώρο διεξήχθη χρησιμοποιώντας ένα εξατομικευμένο πλαίσιο ανάλυσης που βασίζεται στη μεθοδολογία που ορίζει ο Becker για την ανάπτυξη μοντέλων ωριμότητα[22]. Για κάθε υφιστάμενο μοντέλο ωριμότητας αναλύθηκαν τα εξής στοιχεία:

- **Όνομα Μοντέλου Ωριμότητας:** Το όνομα του μοντέλου ωριμότητας και των βασικών σημείων αναφοράς:
- **Θεσμική πηγή:** Το ίδρυμα, είτε δημόσιο είτε ιδιωτικό, που είναι αρμόδιο για τον σχεδιασμό του μοντέλου·
- **Γενικός Σκοπός και Στόχος:** Το συνολικό πεδίο εφαρμογής του μοντέλου και οι επιθυμητοί στόχοι·
- **Αριθμός και ορισμός Επιπέδων:** Ο αριθμός επιπέδων ωριμότητας του μοντέλου, καθώς και η γενική περιγραφή τους·
- **Αριθμός και όνομα Χαρακτηριστικών Γνωρισμάτων:** Ο αριθμός και το όνομα των χαρακτηριστικών γνωρισμάτων που χρησιμοποιεί το μοντέλο ωριμότητας. Η ανάλυση των χαρακτηριστικών γνωρισμάτων έχει τριπλό στόχο:

[22] J. Becker, R. Knackstedt, and J. Pöppelbuß, “Developing Maturity Models for IT Management: A Procedure Model and its Application,» (Ανάπτυξη μοντέλων ωριμότητας για τη διαχείριση ΤΠ: Ένα διαδικαστικό μοντέλο και η εφαρμογή του) Business & Information Systems Engineering, τόμος 1, αριθ. 3, σελ. 213–222, Ιούνιος 2009.

- Ανάλυση του μοντέλου ωριμότητας σε ευκολονόητα τμήματα·
- Συγκέντρωση αρκετών χαρακτηριστικών γνωρισμάτων σε ομάδες χαρακτηριστικών γνωρισμάτων που πληρούν τον ίδιο στόχο· και
- Παροχή διαφορετικών οπτικών του υποκειμένου του επιπέδου ωριμότητας·

- **Μέθοδος αξιολόγησης:** Η μέθοδος αξιολόγησης του μοντέλου ωριμότητας·
- **Αναπαράσταση αποτελεσμάτων**: Ορισμός της μεθόδου οπτικοποίησης των αποτελεσμάτων του μοντέλου ωριμότητας. Η λογική πίσω από αυτό το βήμα είναι ότι τα μοντέλα ωριμότητας συνήθως αποτυγχάνουν εάν είναι υπερβολικά περίπλοκα και, συνεπώς, ο τρόπος αναπαράστασης πρέπει να πληροί πρακτικές ανάγκες.

Προηγούμενο έργο για την ΕΣΑΚ

Ο ENISA δημοσίευσε δύο έγγραφα σχετικά με τις ΕΣΑΚ το 2012 στο πλαίσιο των πρώιμων προσπαθειών του. Αρχικά, το έγγραφο «Practical guide on the development and execution phase of NCSS» («Πρακτικός οδηγός για το στάδιο ανάπτυξης και εκτέλεσης της ΕΣΑΚ»)[23] πρότεινε ένα σύνολο συγκεκριμένων δράσεων για την αποδοτική υλοποίηση μιας ΕΣΑΚ και παρουσιάζει τον κύκλο ζωής μιας ΕΣΑΚ σε τέσσερα στάδια: ανάπτυξη στρατηγικής, εκτέλεση στρατηγικής, αξιολόγηση στρατηγικής και συντήρηση στρατηγικής. Έπειτα, ένα έγγραφο με τίτλο «Setting the course for national efforts to strengthen security in cyberspace» («Προετοιμάζοντας το έδαφος για τις εθνικές προσπάθειες ενίσχυσης της ασφάλειας στον κυβερνοχώρο»)[24] παρουσίαζε την κατάσταση των στρατηγικών ασφάλειας στον κυβερνοχώρο εντός και εκτός της ΕΕ το 2012 και πρότεινε στα κράτη μέλη να προσδιορίσουν κοινές θεματικές και διαφορές μεταξύ των οικείων ΕΣΑΚ.

Το 2014, ο ENISA δημοσίευσε το πρώτο πλαίσιο για την αξιολόγηση της ΕΣΑΚ ενός κράτους μέλους[25]. Αυτό το πλαίσιο περιλαμβάνει συστάσεις και ορθές πρακτικές, καθώς και ένα σύνολο εργαλείων δημιουργίας ικανοτήτων για την αξιολόγηση μιας ΕΣΑΚ (*π.χ.* προσδιορισμένοι στόχοι, πληροφορίες, αποτελέσματα, βασικοί δείκτες επίδοσης...). Τα εν λόγω εργαλεία είναι προσαρμοσμένα στις ανάγκες των χωρών σε διαφορετικά επίπεδα ωριμότητας στο πλαίσιο του στρατηγικού σχεδιασμού τους. Το ίδιο έτος, ο ENISA δημοσίευσε τον «Διαδικτυακό Διαδραστικό Χάρτη ΕΣΑΚ»[26], ο οποίος επιτρέπει στους χρήστες να συμβουλεύονται γρήγορα τις ΕΣΑΚ όλων των κρατών μελών και των κρατών ΕΖΕΣ, συμπεριλαμβανομένων των στρατηγικών στόχων τους και ορθών παραδειγμάτων υλοποίησης. Ο Χάρτης δημιουργήθηκε ως η πρώτη βιβλιοθήκη ΕΣΑΚ (2014), επικαιροποιήθηκε με παραδείγματα υλοποίησης το 2018, και από το 2019 λειτουργεί πλέον ως *κόμβος πληροφοριών* για τη συγκέντρωση δεδομένων που παρέχονται από τα κράτη μέλη σχετικά με τις προσπάθειές τους να ενισχύσουν την εθνική ασφάλεια στον κυβερνοχώρο.

[23] NCSS: Practical Guide on Development and Execution (ENISA, 2012)
https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide
[24] NCSS: Setting the course for national efforts to strengthen security in cyberspace (Χάραξη πορείας εθνικών προσπαθειών για την ενίσχυση της ασφάλειας στον κυβερνοχώρο), (ENISA, 2012)
https://www.enisa.europa.eu/publications/cyber-security-strategies-paper
[25] Ένα πλαίσιο αξιολόγησης για τις ΕΣΑΚ (ENISA, 2014).
https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies
[26] Εθνικές Στρατηγικές για την Ασφάλεια στον Κυβερνοχώρο - Διαδραστικός Χάρτης (ENISA, 2014, επικαιροποιήθηκε το 2019)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

Το έγγραφο «NCSS Good Practice Guide» («Οδηγός ορθών πρακτικών ΕΣΑΚ»[27] δημοσιεύτηκε το 2016 και προσδιορίζει δεκαπέντε στρατηγικούς στόχους. Ο εν λόγω οδηγός αναλύει και την κατάσταση υλοποίησης της ΕΣΑΚ έκαστου κράτους μέλους και προσδιορίζει διάφορα κενά και προκλήσεις υλοποίησης.

Το 2018, ο ENISA δημοσίευσε το «Εργαλείο Αξιολόγησης Εθνικών Στρατηγικών ασφάλειας στον κυβερνοχώρο»[28], ένα διαδραστικό εργαλείο αυτοαξιολόγησης που βοηθά τα κράτη μέλη να αξιολογούν τις στρατηγικές προτεραιότητες και τους στόχους τους που σχετίζονται με την ΕΣΑΚ τους. Μέσα από ένα σύνολο απλών ερωτήσεων, αυτό το εργαλείο παρέχει στα κράτη μέλη συγκεκριμένες συστάσεις για την υλοποίηση κάθε στόχου. Τέλος, το έγγραφο «Good practices in innovation on Cybersecurity under the NCSS» («Ορθές πρακτικές στην καινοτομία για την ασφάλεια στον κυβερνοχώρο βάσει της ΕΣΑΚ»)[29] που δημοσιεύτηκε το 2019 παρουσιάζει το ζήτημα της καινοτομίας στην ασφάλεια στον κυβερνοχώρο βάσει της ΕΣΑΚ. Το έγγραφο καθορίζει τις προκλήσεις και τις ορθές πρακτικές στις διαφορετικές διαστάσεις καινοτομίας, όπως περιγράφονται από τους εμπειρογνώμονες του θέματος, προκειμένου να συμβάλει στη χάραξη μελλοντικών στρατηγικών στόχων καινοτομίας.

Α.1 Εθνικό μοντέλο ωριμότητας ικανοτήτων για την ασφάλεια στον κυβερνοχώρο (CMM)

Το Μοντέλο ωριμότητας ικανοτήτων ασφάλειας στον κυβερνοχώρο για Έθνη (CMM) έχει αναπτυχθεί από το Παγκόσμιο Κέντρο Ικανοτήτων Ασφάλειας στον Κυβερνοχώρο (Capacity Centre), που αποτελεί μέρος της Σχολής Oxford Martin του Πανεπιστημίου της Οξφόρδης. Στόχος του Κέντρου είναι η αύξηση της κλίμακας και της αποτελεσματικότητας της δημιουργίας ικανοτήτων ασφάλειας στον κυβερνοχώρο τόσο στο ΗΒ όσο και διεθνώς, μέσω της αξιοποίησης του Μοντέλου ωριμότητας ικανοτήτων ασφάλειας στον κυβερνοχώρο για Έθνη (CMM). Το CMM απευθύνεται απευθείας σε χώρες που επιθυμούν να ενισχύσουν τις οικείες εθνικές ικανότητες ασφάλειας στον κυβερνοχώρο. Το CMM χρησιμοποιήθηκε αρχικά το 2014 και αναθεωρήθηκε το 2016 αφού χρησιμοποιήθηκε για την ανασκόπηση 11 εθνικών ικανοτήτων ασφάλειας στον κυβερνοχώρο.

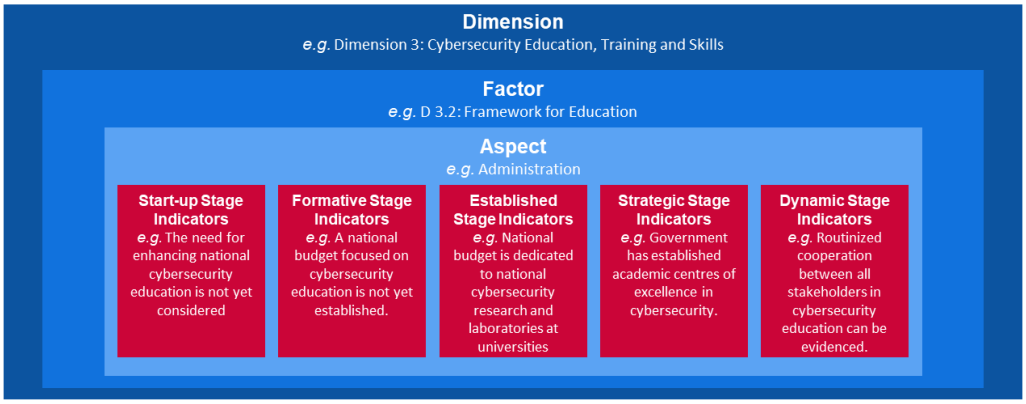
Χαρακτηριστικά Γνωρίσματα/ Διαστάσεις

Το CMM θεωρεί ότι οι ικανότητες ασφάλειας στον κυβερνοχώρο αποτελούνται από **πέντε διαστάσεις** που αντιπροσωπεύουν τις ομάδες ικανοτήτων ασφάλειας στον κυβερνοχώρο. Κάθε δέσμη αντιπροσωπεύει έναν διαφορετικό ερευνητικό «φακό» μέσω του οποίου μπορούν να μελετηθούν και να γίνουν κατανοητές οι ικανότητες ασφάλειας στον κυβερνοχώρο. Στις πέντε διαστάσεις, οι **παράγοντες** περιγράφουν αναλυτικά την κατοχή ικανοτήτων ασφάλειας στον κυβερνοχώρο. Αυτά τα λεπτομερή στοιχεία συμβάλλουν στη βελτίωση της ωριμότητας των ικανοτήτων ασφάλειας στον κυβερνοχώρο στο πλαίσιο κάθε διάστασης. Οι διάφορες συνιστώσες κάθε παράγοντα αντιπροσωπεύονται από αρκετές **πτυχές**. Οι πτυχές συνιστούν μια μέθοδο οργάνωσης για τη διαίρεση των δεικτών σε μικρότερες ομάδες που είναι πιο εύκολα κατανοητές. Στη συνέχεια, κάθε πτυχή αξιολογείται μέσω **δεικτών** για την περιγραφή των βημάτων, ενεργειών ή στοιχείων που είναι ενδεικτικά του συγκεκριμένου σταδίου ωριμότητας (που ορίζεται στην επόμενη ενότητα) στο πλαίσιο κάθε επιμέρους πτυχής, παράγοντα και διάστασης.

[27] Αυτό το έγγραφο επικαιροποιεί τον οδηγό του 2012: NCSS Good Practice Guide: Designing and Implementing National Cybersecurity Strategies (Οδηγός ορθών πρακτικών ΕΣΑΚ: Σχεδιασμός και εφαρμογή εθνικών στρατηγικών για την ασφάλεια στον κυβερνοχώρο), (ENISA, 2016)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide
[28] Εργαλείο Αξιολόγησης Εθνικών Στρατηγικών Ασφάλειας στον Κυβερνοχώρο (2018)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
[29] https://www.enisa.europa.eu/publications/good-practices-in-innovation-on-cybersecurity-under-the-ncss-1

Οι όροι που αναφέρονται ανωτέρω μπορούν να κατηγοριοποιηθούν όπως φαίνεται στην παρακάτω εικόνα.

Εικόνα 4: Κατάσταση δεικτώνCMM



Dimension e.g. Dimension 3: Cybersecurity Education, Training and Skills	Διάσταση π.χ. Διάσταση 3: Εκπαίδευση, Κατάρτιση και Δεξιότητες για την Ασφάλεια στον Κυβερνοχώρο
Factor e.g. D 3.2: Framework for Education	Παράγοντας π.χ. D 3.2: Πλαίσιο για την Εκπαίδευση
Aspect e.g. Administration	Πτυχή π.χ. Διοίκηση
Start-up Stage Indicators e.g. The for enhancing national cybersecurity education is not yet considered	Δείκτες Αρχικού Σταδίου π.χ. Δεν εξετάζεται ακόμα η βελτίωση της εθνικής εκπαίδευσης για την κυβερνοασφάλεια
Formative Stage Indictors e.g. A national budget focused on cybersecurity education is not yet established	Δείκτες Σταδίου Διαμόρφωσης π.χ. Δεν έχει προβλεφθεί ακόμα εθνικός προϋπολογισμός ειδικά για την εκπαίδευση για την κυβερνοασφάλεια
Established Stage Indicators e.g. National budget is dedicated to national cybersecurity research and laboratories at universities	Δείκτες Παγιωμένου Σταδίου π.χ. Εθνικός προϋπολογισμός αφιερωμένος στην έρευνα και τα πανεπιστημιακά εργαστήρια για την εθνική ασφάλεια στον κυβερνοχώρο
Strategic Stage Indicators e.g. Government has established academic center of excellence in cybersecurity education can be evidenced.	Δείκτες Στρατηγικού Σταδίου π.χ. Υπάρχουν αποδεικτικά στοιχεία ότι η κυβέρνηση έχει ιδρύσει ένα ακαδημαϊκό κέντρο αριστείας για την εκπαίδευση για την κυβερνοασφάλεια.
Dynamic Stage Indicators e.g. Routinized cooperation between all stakeholder	Δείκτες Δυναμικού Σταδίου π.χ. Συνεχής συνεργασία μεταξύ όλων των ενδιαφερόμενων μερών

Οι πέντε διαστάσεις αναλύονται παρακάτω:

i Χάραξη πολιτικής και στρατηγικής για την κυβερνοασφάλεια (6 παράγοντες)·
ii Ενθάρρυνση υπεύθυνης κουλτούρας κυβερνοασφάλειας στην κοινωνία (5 παράγοντες)·
iii Ανάπτυξη γνώσεων κυβερνοασφάλειας (3 παράγοντες)·
iv Θέσπιση αποτελεσματικών νομικών και κανονιστικών πλαισίων (3 παράγοντες)· και
v Έλεγχος κινδύνων μέσω προτύπων, οργανισμών και τεχνολογιών (7 παράγοντες).

Επίπεδα ωριμότητας

Το CMM χρησιμοποιεί **5 επίπεδα ωριμότητας** προκειμένου να καθορίσει τον βαθμό προόδου μιας χώρας σε σχέση με έναν συγκεκριμένο παράγοντα/πτυχή των ικανοτήτων ασφάλειας στον κυβερνοχώρο. Αυτά τα επίπεδα λειτουργούν ως γενική επισκόπηση των υφιστάμενων ικανοτήτων ασφάλειας στον κυβερνοχώρο:

- **Αρχικό Στάδιο**: Σε αυτό το στάδιο, είτε δεν υφίσταται ωριμότητα ασφάλειας στον κυβερνοχώρο, είτε βρίσκεται σε πολύ εμβρυϊκή φάση. Ενδέχεται να υπάρχουν αρχικές συζητήσεις για τη δημιουργία ικανοτήτων ασφάλειας στον κυβερνοχώρο, όμως δεν

έχουν αναληφθεί συγκεκριμένες δράσεις. Δεν υπάρχουν εμφανή αποδεικτικά στοιχεία στο παρόν στάδιο·

- **Στάδιο Διαμόρφωσης**: Ορισμένα χαρακτηριστικά των πτυχών έχουν αρχίσει να αναπτύσσονται και να διαμορφώνονται, όμως ενδέχεται να είναι ad-hoc, ανοργάνωτα, ασαφώς καθορισμένα ή απλώς «νέα». Ωστόσο, υπάρχουν εμφανή τα αποδεικτικά στοιχεία αυτής της δραστηριότητας.
- **Παγιωμένο Στάδιο**: Εφαρμόζονται αποτελεσματικά τα στοιχεία της πτυχής. Ωστόσο, δεν έχει σχεδιαστεί προσεκτικά η σχετική κατανομή των πόρων. Έχουν ληφθεί ελάχιστες συμβιβαστικές αποφάσεις αναφορικά με τις «σχετικές» επενδύσεις στα διάφορα στοιχεία της πτυχής. Ωστόσο, η πτυχή είναι λειτουργική και καθορισμένη·
- **Στρατηγικό Στάδιο**: Έχουν πραγματοποιηθεί επιλογές όσον αφορά ποια στοιχεία της πτυχής είναι πιο σημαντικά, και ποια είναι λιγότερο σημαντικά για τον συγκεκριμένο οργανισμό ή κράτος. Το στρατηγικό στάδιο αντανακλά το γεγονός ότι αυτές οι επιλογές έχουν ολοκληρωθεί, και εξαρτώνται από τις ιδιαίτερες συνθήκες της χώρας ή του οργανισμού· και
- **Δυναμικό Στάδιο**: Σε αυτό το στάδιο υφίστανται σαφείς μηχανισμοί για την μεταβολή της στρατηγικής ανάλογα με τις επικρατούσες συνθήκες όπως η τεχνολογία του περιβάλλοντος απειλών, οι συγκρούσεις σε παγκόσμιο επίπεδο ή μια σημαντική αλλαγή σε έναν τομέα ενδιαφέροντος (*π.χ.* κυβερνοέγκλημα ή ιδιωτική ζωή). Οι δυναμικοί οργανισμοί έχουν αναπτύξει μεθόδους για τη γρήγορη μεταβολή των στρατηγικών. Στα χαρακτηριστικά αυτού του σταδίου περιλαμβάνονται η ταχεία λήψη αποφάσεων, η ανακατανομή των πόρων, και η συνεχής παρακολούθηση του μεταβαλλόμενου περιβάλλοντος.

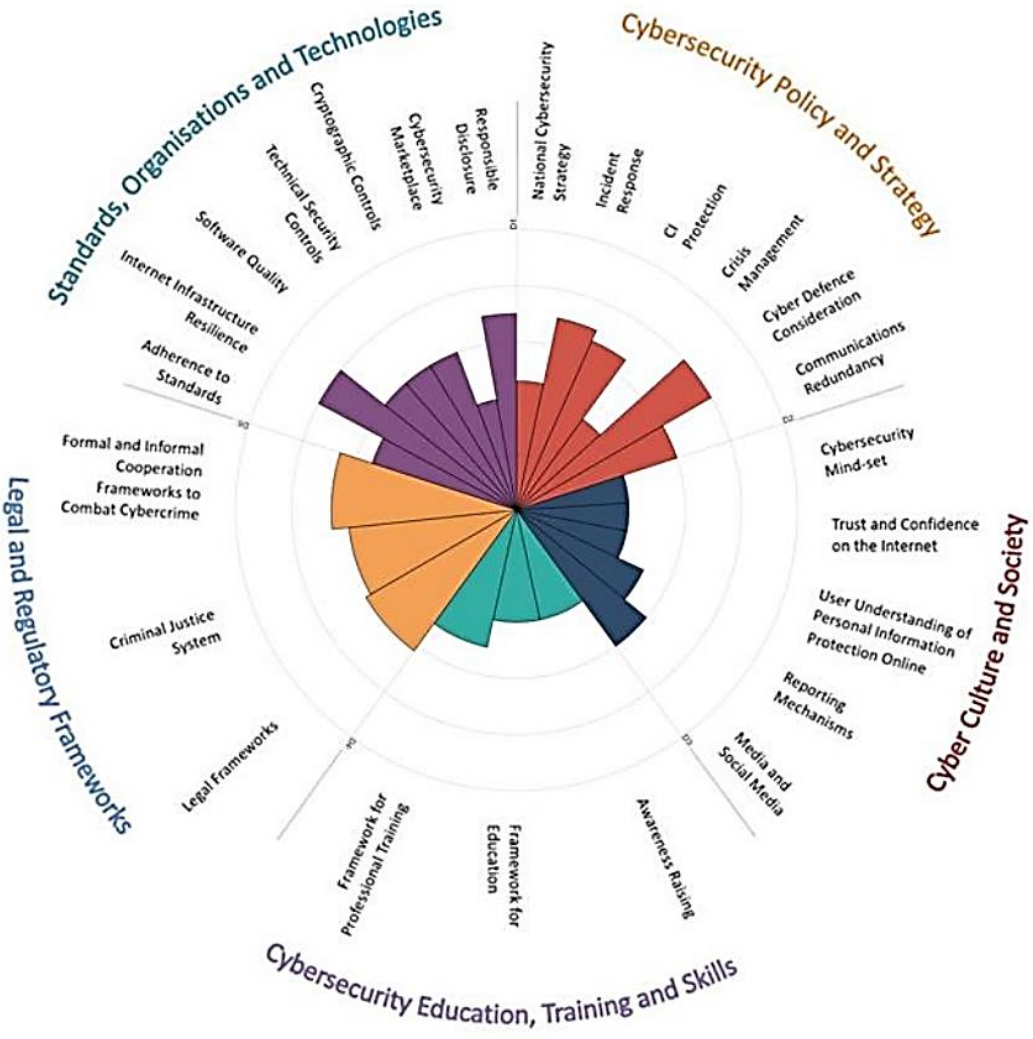
Μέθοδος αξιολόγησης

Επειδή το Κέντρο Ικανοτήτων δεν διαθέτει λεπτομερείς και εις βάθος γνώσεις για κάθε εθνικό πλαίσιο στο οποίο υλοποιείται το μοντέλο, συνεργάζεται με διεθνείς οργανισμούς, υπουργεία ή οργανισμούς υποδοχής στην αντίστοιχη χώρα για την εξέταση της ωριμότητας ικανοτήτων ασφάλειας στον κυβερνοχώρο. Για την αξιολόγηση του επιπέδου ωριμότητας των πέντε διαστάσεων που περιλαμβάνονται στο CMM, το Κέντρο Ικανοτήτων και ο οργανισμός υποδοχής συναντιούνται με τους σχετικούς εθνικούς ενδιαφερόμενους παράγοντες του δημόσιου και ιδιωτικού τομέα για 2 ή 3 ημέρες για την καθοδήγηση των ομάδων εστίασης σχετικά με τις διαστάσεις του CMM. Κάθε διάσταση συζητείται τουλάχιστον δύο φορές από διαφορετικές ομάδες ενδιαφερόμενων παραγόντων. Με αυτόν τον τρόπο διαμορφώνεται το προκαταρκτικό σύνολο δεδομένων για τη μεταγενέστερη αξιολόγηση.

Τρόπος αναπαράστασης των αποτελεσμάτων

Το CCM προσφέρει μια επισκόπηση του επιπέδου ωριμότητας κάθε χώρας μέσω ενός ραντάρ που αποτελείται από πέντε τμήματα, ένα για κάθε διάσταση. Κάθε διάσταση αντιπροσωπεύει το ένα πέμπτο της γραφικής παράστασης, και τα πέντε στάδια ωριμότητας για κάθε παράγοντα εκτείνονται πέρα από το κέντρο της γραφικής παράστασης· όπως φαίνεται στη συνέχεια, το «αρχικό στάδιο» βρίσκεται πιο κοντά στο κέντρο της γραφικής παράστασης και το «δυναμικό στάδιο» βρίσκεται στην περίμετρο.

Εικόνα 5 CMM: Επισκόπηση αποτελεσμάτων



Standards, Organisations and Technologies	Πρότυπα, οργανισμοί και τεχνολογίες
Legal Regulatory Frameworks	Νομοθετικά κανονιστικά πλαίσια
Cybersecurity Education, Training and Skills	Εκπαίδευση, Κατάρτιση και Δεξιότητες για την Ασφάλεια στον Κυβερνοχώρο
Cybersecurity Policy and Strategy	Πολιτική και στρατηγική για την ασφάλεια στον κυβερνοχώρο
Cyber Culture and Society	Κουλτούρα και κοινωνία στον κυβερνοχώρο
Responsible Disclosure	Υπεύθυνη γνωστοποίηση
Cybersecurity market place	Αγορά ασφάλειας στον κυβερνοχώρο
Technical Security Controls	Τεχνικοί έλεγχοι ασφάλειας
Cryptographic Controls	Κρυπτογραφικοί έλεγχοι
Software Quality	Ποιότητα λογισμικού
Internet Infrastructure Resilience	Ανθεκτικότητα υποδομής διαδικτύου
Adherence to Standards	Τήρηση προτύπων
Formal and Informal Cooperation Frameworks to Combat Cybercrime	Τυπικά και άτυπα πλαίσια συνεργασίας για την καταπολέμηση του κυβερνοεγκλήματος
Criminal Justice System	Σύστημα ποινικής δικαιοσύνης
Legal Frameworks	Νομικά πλαίσια
Framework for Professional Training	Πλαίσιο επαγγελματικής κατάρτισης
Framework for Education	Πλαίσιο για την Εκπαίδευση
Awareness Raising	Ευαισθητοποίηση
Media and Social Medai	Μέσα ενημέρωσης και μέσα κοινωνικής δικτύωσης
Reporting Mechanisms	Μηχανισμοί υποβολής αναφορών
User Understanding of Personal Information Protection Online	Κατανόηση της προστασίας πληροφοριών προσωπικού χαρακτήρα στο Διαδίκτυο από τον χρήστη
Trust and Confidence on the Internet	Πίστη και εμπιστοσύνη στο Διαδίκτυο
Cybersecurity Mind-set	Νοοτροπία ασφάλειας στον κυβερνοχώρο

Communications Redundancy	Μείωση επικοινωνιών
Cyber Defence Consideration	Συνεκτίμηση κυβερνοάμυνας
Crisis Management	Διαχείριση κρίσεων
CI Protection	Προστασία CI
Incident Response	Απόκριση σε περιστατικά
National Cybersecurity Strategy	Εθνική Στρατηγική για την Ασφάλεια στον Κυβερνοχώρο·

Παγκόσμιο Κέντρο Ικανοτήτων για την Ασφάλεια στον Κυβερνοχώρο, Πανεπιστήμιο της Οξφόρδης, 2017.

Α.2 Μοντέλο ωριμότητας ικανοτήτων ασφάλειας στον κυβερνοχώρο (C2M2)

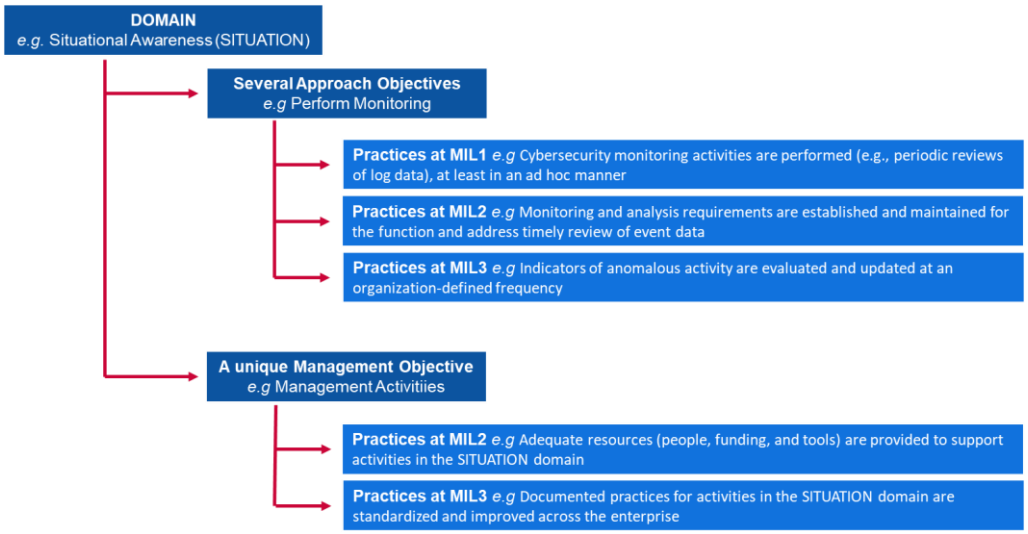
Το Μοντέλο ωριμότητας ικανοτήτων ασφάλειας στον κυβερνοχώρο (C2M2) έχει αναπτυχθεί από το Υπουργείο Ενέργειας των ΗΠΑ σε συνεργασία με εμπειρογνώμονες του ιδιωτικού και του δημόσιου τομέα. Στόχος του Κέντρου Δυνατοτήτων είναι να βοηθά οργανισμούς κάθε τομέα, είδους και μεγέθους στην αξιολόγηση και τη βελτίωση των οικείων προγραμμάτων ασφάλειας στον κυβερνοχώρο και την ενίσχυση της επιχειρησιακής ανθεκτικότητάς τους. Το C2M2 εστιάζει στην υλοποίηση και τη διαχείριση πρακτικών ασφάλειας στον κυβερνοχώρο που συνδέονται με στοιχεία πληροφοριών, τεχνολογίας πληροφοριών και επιχειρησιακής τεχνολογίας και με τα περιβάλλοντα στα οποία λειτουργούν. Το C2M2 ορίζει τα μοντέλα ωριμότητας ως: «ένα σύνολο χαρακτηριστικών, γνωρισμάτων, δεικτών ή μοτίβων που αντιπροσωπεύουν την ικανότητα και την πρόοδο σε έναν συγκεκριμένο τομέα». Το C2M2 χρησιμοποιήθηκε για πρώτη φορά το 2014 και αναθεωρήθηκε το 2019.

Χαρακτηριστικά Γνωρίσματα/ Διαστάσεις

Το C2M2 εξετάζει **δέκα τομείς** που αντιπροσωπεύουν μια λογική ομαδοποίηση των πρακτικών ασφάλειας στον κυβερνοχώρο. Κάθε σύνολο πρακτικών αντιπροσωπεύει τις δραστηριότητες στις οποίες μπορεί να προβεί ένας οργανισμός για την εδραίωση και την ωρίμανση της ικανότητας στον τομέα. Κάθε τομέας συνδέεται στη συνέχεια με έναν **μοναδικό στόχο διαχείρισης** και **αρκετούς στόχους προσέγγισης**. Τόσο στους στόχους προσέγγισης όσο και στον στόχο διαχείρισης, αναλύονται λεπτομερώς **αρκετές πρακτικές** για την περιγραφή θεσμοθετημένων δραστηριοτήτων.

Η σχέση μεταξύ αυτών των εννοιών συνοψίζεται παρακάτω:

Εικόνα 6: Κατάσταση δείκτη C2M2



Domain eg Situational Awareness (SITUATION)	**Τομέας** π.χ. Επίγνωση της κατάστασης (ΚΑΤΑΣΤΑΣΗ)
Several Approaches Objectives e.g. Perform Monitoring	**Αρκετοί Στόχοι Προσέγγισης** π.χ. Παρακολούθηση

Practices at MIL1 e.g Cybersecurity monitoring activities are performed (e.g., periodic reviews of log data), at least in an ad hoc manner	**Πρακτικές σε MIL1** π.χ. εκτελούνται δραστηριότητες παρακολούθησης της ασφάλειας στον κυβερνοχώρο (π.χ. περιοδικές επισκοπήσεις δεδομένων κορμού), τουλάχιστον με ad hoc τρόπο
Practices at MIL2 e.g Monitoring and analysis requirement are established and maintained for the function and adress timely review of event data	**Πρακτικές σε MIL2** π.χ. θεσπίζονται και διατηρούνται απαιτήσεις παρακολούθησης και ανάλυσης για τη λειτουργία και την έγκαιρη εξέταση των δεδομένων των περιστατικών
Practices at MIL3 e.g Indicators of anomalous activity are evaluated and updated at an organization-defined frequency	**Πρακτικές σε MIL3** π.χ. οι δείκτες ασυνήθους δραστηριότητας αξιολογούνται και επικαιροποιούνται με βάση τη συχνότητα που προβλέπεται από τον οργανισμό
A unique Management Objectve e.g. Management Activities	Ένας μοναδικός Στόχος Διαχείρισης π.χ. Δραστηριότητες Διαχείρισης
Practices at MIL2 e.g Adequate resources (people, funding, and tools) are provided to support activities in the SITUATION domain	**Πρακτικές σε MIL2** π.χ. παρέχονται επαρκείς πόροι (ανθρώπινο δυναμικό, χρηματοδότηση και εργαλεία) για την υποστήριξη δραστηριοτήτων στον τομέα της ΚΑΤΑΣΤΑΣΗΣ
Practices at MIL3 e.g Documented practices for activities in the SITUATION domain are standardized and improved across the entreprise	**Πρακτικές σε MIL3** π.χ. οι τεκμηριωμένες πρακτικές για δραστηριότητες στον τομέα της ΚΑΤΑΣΤΑΣΗΣ είναι τυποποιημένες και βελτιωμένες σε όλη την επιχείρηση

Οι δέκα τομείς αναλύονται παρακάτω:

i Διαχείριση κινδύνου (RISK, RM)·
ii Διαχείριση περιουσιακών στοιχείων, αλλαγής και διαμόρφωσης (ASSET, ACM)·
iii Διαχείριση ταυτότητας και πρόσβασης (ACCESS, IAM)·
iv Διαχείριση απειλών και τρωτών σημείων (THREAT, TVM)·
v Επίγνωση της κατάστασης (SITUATION, SA)·
vi Απόκριση σε συμβάντα και περιστατικά (RESPONSE, IR)·
vii Διαχείριση αλυσίδας εφοδιασμού και εξωτερικών εξαρτήσεων (DEPENDENCIES, EDM)·
viii Διαχείριση εργατικού δυναμικού (WORKFORCE, WF)·
ix Αρχιτεκτονική ασφάλειας στον κυβερνοχώρο (ARCHITECTURE)· και
x Διαχείριση προγράμματος ασφάλειας στον κυβερνοχώρο (PROGRAM, CPM).

Επίπεδα ωριμότητας

Το C2M2 χρησιμοποιεί **4 επίπεδα ωριμότητας** (τα οποία ονομάζονται Επίπεδα Δεικτών Ωριμότητας – MIL) για να προσδιορίσει μια διπλή πρόοδο ωριμότητας: την πρόοδο σε επίπεδο προσέγγισης και την πρόοδο σε επίπεδο διαχείρισης. Τα MIL κυμαίνονται από MIL0 έως MIL3 και εφαρμόζονται ανεξάρτητα το ένα από το άλλο σε κάθε τομέα.

- **MIL0**: Δεν εφαρμόζονται οι πρακτικές.
- **MIL1**: Εφαρμόζονται αρχικές πρακτικές, αλλά σε ad hoc βάση.
- **MIL2**: Χαρακτηριστικά διαχείρισης:
  - Οι πρακτικές είναι τεκμηριωμένες·
  - Παρέχονται επαρκείς πόροι για την υποστήριξη της διαδικασίας·
  - Το προσωπικό που εφαρμόζει τις πρακτικές έχει επαρκείς δεξιότητες και γνώσεις· και
  - Έχει ανατεθεί η ευθύνη και η αρμοδιότητα για την εφαρμογή των πρακτικών.

  Χαρακτηριστικό προσέγγισης:
  - Οι πρακτικές είναι πιο ολοκληρωμένες ή προχωρημένες σε σχέση με το MIL1.
- **MIL3**: Χαρακτηριστικά διαχείρισης:
  - Οι δραστηριότητες κατευθύνονται από πολιτικές (ή άλλες οργανωτικές οδηγίες)·
  - Καθορίζονται στόχοι απόδοσης για τις δραστηριότητες του τομέα οι οποίοι υπόκεινται σε εποπτεία για την παρακολούθηση της επίτευξής τους· και
  - Οι τεκμηριωμένες πρακτικές για δραστηριότητες του τομέα τυποποιούνται και βελτιώνονται σε όλη την επιχείρηση.

  Χαρακτηριστικό προσέγγισης:
  - Οι πρακτικές είναι πιο ολοκληρωμένες ή προχωρημένες σε σχέση με το MIL2.

Μέθοδος αξιολόγησης

Το C2M2 έχει σχεδιαστεί για να χρησιμοποιείται σε συνδυασμό με μια **μεθοδολογία αυτοαξιολόγησης** και μια εργαλειοθήκη (διαθέσιμη κατόπιν αιτήματος) προκειμένου να βοηθά τον οργανισμό να μετρά και να βελτιώνει το οικείο πρόγραμμα ασφάλειας στον κυβερνοχώρο.

Μια αυτοαξιολόγηση που χρησιμοποιεί την εργαλειοθήκη μπορεί να ολοκληρωθεί σε μία ημέρα, όμως η εργαλειοθήκη θα μπορούσε να προσαρμοστεί σε μια πιο αυστηρή προσπάθεια αξιολόγησης. Επιπλέον, το C2M2 μπορεί να χρησιμοποιηθεί για την καθοδήγηση της ανάπτυξης ενός νέου προγράμματος ασφάλειας στον κυβερνοχώρο.

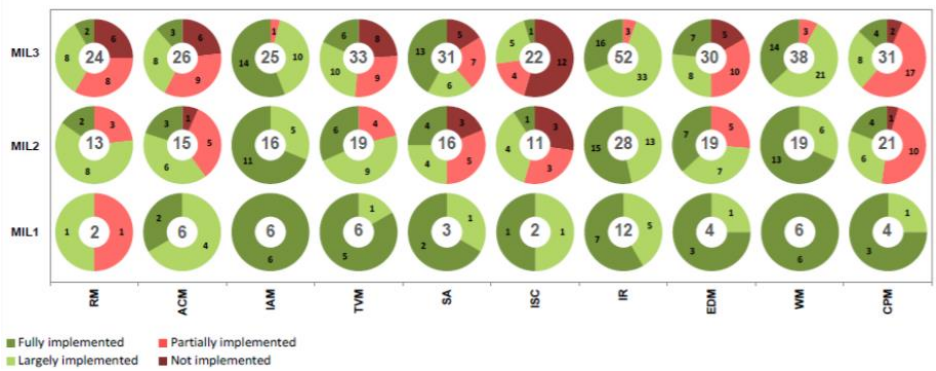
Το περιεχόμενο του μοντέλου παρουσιάζεται με πολύ αφηρημένο τρόπο προκειμένου να μπορεί να ερμηνευτεί από οργανισμούς διαφόρων ειδών, δομών, μεγεθών και τομέων. Η ευρεία χρήση του μοντέλου από έναν τομέα μπορεί να στηρίξει τη συγκριτική αξιολόγηση των ικανοτήτων ασφάλειας στον κυβερνοχώρο του εν λόγω τομέα.

Τρόπος αναπαράστασης των αποτελεσμάτων

Το C2M2 παρέχει μια Έκθεση Βαθμολογίας Αξιολόγησης, η οποία προκύπτει από τα αποτελέσματα της έρευνας. Η έκθεση παρουσιάζει τα αποτελέσματα από δύο οπτικές: την οπτική του Στόχου, η οποία παρουσιάζει απαντήσεις σε πρακτικά ερωτήματα για κάθε τομέα και τους στόχους του, και την οπτική του Τομέα, η οποία παρουσιάζει απαντήσεις από όλους τους τομείς και τα MIL. Και οι δύο οπτικές βασίζονται σε ένα σύστημα παράστασης που χαρακτηρίζεται από κυκλικά διαγράμματα (γνωστά και ως «doughnuts»), ένα ανά απάντηση, και σε έναν μηχανισμό βαθμολόγησης με σύστημα «φωτεινού σηματοδότη». Όπως φαίνεται στην Εικόνα 7, οι κόκκινοι τομείς σε ένα κυκλικό διάγραμμα παρουσιάζουν τον αριθμό των ερωτήσεων της έρευνας που έλαβαν απάντηση «Δεν έχει υλοποιηθεί» (σκούρο κόκκινο) ή «Υλοποιήθηκε μερικώς» (ανοιχτό κόκκινο). Οι πράσινοι τομείς αντιπροσωπεύουν τον αριθμό ερωτήσεων που έλαβαν ως απάντηση «Υλοποιήθηκε ευρέως» (ανοικτό πράσινο) ή «Υλοποιήθηκε πλήρως» (σκούρο πράσινο).

Η Εικόνα 7 που ακολουθεί είναι ένα παράδειγμα κάρτας βαθμολογίας στο τέλος μιας αξιολόγησης ωριμότητας. Στον άξονα X, υπάρχουν 10 τομείς του C2M2 και στον άξονα Ψ περιλαμβάνονται τα επίπεδα ωριμότητας (MIL). Κατά την εξέταση του τομέα Διαχείρισης κινδύνου (RM) της γραφικής παράστασης, παρατηρούνται τρία κυκλικά διαγράμματα, το καθένα από τα οποία αντιστοιχεί σε κάθε επίπεδο ωριμότητας ML1, ML2 και ML3. Για τον τομέα RM, στη γραφική παράσταση επισημαίνεται ότι υπάρχουν δύο στοιχεία προς αξιολόγηση για την επίτευξη του πρώτου επιπέδου ωριμότητας, ML1. Σε αυτή την περίπτωση, ένα στοιχείο έλαβε βαθμολογία «Υλοποιήθηκε ευρέως» και ένα άλλο βαθμολογία «Υλοποιήθηκε μερικώς». Για το δεύτερο επίπεδο ωριμότητας, ML2, το μοντέλο προβλέπει την αξιολόγηση 13 στοιχείων. Δύο εξ αυτών των 13 στοιχείων ανήκουν στο πρώτο επίπεδο, ML1, και 11 στο δεύτερο επίπεδο, ML2. Το ίδιο ισχύει και για το τρίτο επίπεδο, ML3.

Εικόνα 7: C2M2 – Παράδειγμα οπτικής τομέα



Fully implemented	Υλοποιήθηκε πλήρως
Largely implemented	Υλοποιήθηκε ευρέως
Partially implemented	Υλοποιήθηκε μερικώς
Not implemented	Δεν έχει υλοποιηθεί
MIL1	MIL1
MIL2	MIL2
MIL3	MIL3
RM	RM

ACM	ACM
IAM	IAM
TVM	TVM
SA	SA
ISC	ISC
IR	IR
EDM	EDM
WM	WM
CPM	CPM

Πηγή: Υπουργείο Ενέργειας των ΗΠΑ, Office of electricity delivery and energy reliability (Υπηρεσία παράδοσης ηλεκτρικής ενέργειας και αξιοπιστίας εφοδιασμού ενέργειας), 2015.

A.3 Πλαίσιο για τη βελτίωση της κρίσιμης υποδομής για την ασφάλεια στον κυβερνοχώρο

Το Πλαίσιο για τη βελτίωση της κρίσιμης υποδομής για την ασφάλεια στον κυβερνοχώρο έχει αναπτυχθεί από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογιών (NIST) των ΗΠΑ. Εστιάζει στην καθοδήγηση των δραστηριοτήτων για την ασφάλεια στον κυβερνοχώρο και τη διαχείριση των κινδύνων στο εσωτερικό ενός οργανισμού. Απευθύνεται σε όλα τα είδη οργανισμών ανεξαρτήτως μεγέθους, βαθμού κινδύνου ασφάλειας στον κυβερνοχώρο ή πολυπλοκότητας της ασφάλειας στον κυβερνοχώρο. Εφόσον πρόκειται για πλαίσιο και όχι για μοντέλο, ο σχεδιασμός του διαφέρει από αυτόν των μοντέλων που αναλύονται παραπάνω.

Το Πλαίσιο αποτελείται από τρία μέρη: τον Πυρήνα του Πλαισίου, τις Βαθμίδες Υλοποίησης και τα Προφίλ του Πλαισίου:

- Ο **Πυρήνας του Πλαισίου** είναι ένα σύνολο δραστηριοτήτων ασφάλειας στον κυβερνοχώρο, επιθυμητών αποτελεσμάτων και εφαρμόσιμων αναφορών που είναι κοινά σε τομείς κρίσιμης υποδομής. Αυτά είναι παρόμοια με τα χαρακτηριστικά γνωρίσματα ή τις διαστάσεις των μοντέλων ωριμότητας των ικανοτήτων ασφάλειας στον κυβερνοχώρο.
- Οι **Βαθμίδες Υλοποίησης του Πλαισίου** («Βαθμίδες») προσφέρουν ένα πλαίσιο σχετικά με το πώς ένας οργανισμός αντιμετωπίζει τον κίνδυνο ασφάλειας στον κυβερνοχώρο και με τις διεργασίες που εφαρμόζονται για τη διαχείριση του εν λόγω κινδύνου. Οι Βαθμίδες κυμαίνονται από Μερική (Βαθμίδα 1) σε Προσαρμοστική (Βαθμίδα 4) και περιγράφουν τον αυξανόμενο βαθμό αυστηρότητας και πολυπλοκότητας των πρακτικών διαχείρισης του κινδύνου ασφάλειας στον κυβερνοχώρο. Οι Βαθμίδες δεν αντιπροσωπεύουν επίπεδα ωριμότητας, αλλά αποσκοπούν στην υποστήριξη της λήψης των αποφάσεων από τον οργανισμό σχετικά με τον τρόπο διαχείρισης κινδύνων ασφάλειας στον κυβερνοχώρο, καθώς και σχετικά με το ποιες διαστάσεις του οργανισμού έχουν μεγαλύτερη προτεραιότητα και θα μπορούσαν να λάβουν επιπρόσθετους πόρους.
- Το **Προφίλ του Πλαισίου** («Προφίλ») αναπαριστά τα αποτελέσματα βάσει των επιχειρησιακών αναγκών που έχει επιλέξει ένας οργανισμός από τις Κατηγορίες και τις Υποκατηγορίες του Πλαισίου. Το Προφίλ μπορεί να χαρακτηριστεί ως προς την ευθυγράμμιση των προτύπων, των κατευθυντήριων γραμμών και των πρακτικών με τον Πυρήνα του Πλαισίου σε ένα συγκεκριμένο σενάριο υλοποίησης. Τα Προφίλ μπορούν να χρησιμοποιηθούν για τον προσδιορισμό ευκαιριών για τη βελτίωση της στάσης ασφάλειας στον κυβερνοχώρο μέσω της σύγκρισης ενός «Τρέχοντος» προφίλ (της κατάστασης «ως έχει») με ένα προφίλ «Στόχος» (τη «μελλοντική» κατάσταση).

Ο Πυρήνας του Πλαισίου

Ο Πυρήνας του Πλαισίου αποτελείται από πέντε **Λειτουργίες**. Όταν εξετάζονται από κοινού, αυτές οι Λειτουργίες προσφέρουν μια υψηλού επιπέδου στρατηγική οπτική του κύκλου ζωής της διαχείρισης του κινδύνου ασφάλειας στον κυβερνοχώρο ενός οργανισμού. Στη συνέχεια, ο Πυρήνας του Πλαισίου προσδιορίζει τις υποκείμενες βασικές **Κατηγορίες** και **Υποκατηγορίες**

για κάθε Λειτουργία και τις αντιστοιχίζει με παραδείγματα Ενημερωτικών Αναφορών όπως υφιστάμενα πρότυπα, κατευθυντήριες γραμμές και πρακτικές για κάθε Υποκατηγορία.

Οι Λειτουργίες και οι Κατηγορίες αναλύονται παρακάτω:

i **Προσδιορισμός**: Ανάπτυξη της κατανόησης του οργανισμού σχετικά με τον τρόπο διαχείρισης των κινδύνων ασφάλειας στον κυβερνοχώρο για τα συστήματα, τα άτομα, τα περιουσιακά στοιχεία, τα δεδομένα και τις ικανότητες.
   - Υποκατηγορίες: Διαχείριση Περιουσιακών Στοιχείων· Επιχειρηματικό Περιβάλλον· Διακυβέρνηση· Διαχείριση Κινδύνου· και Στρατηγική Διαχείρισης Κινδύνου

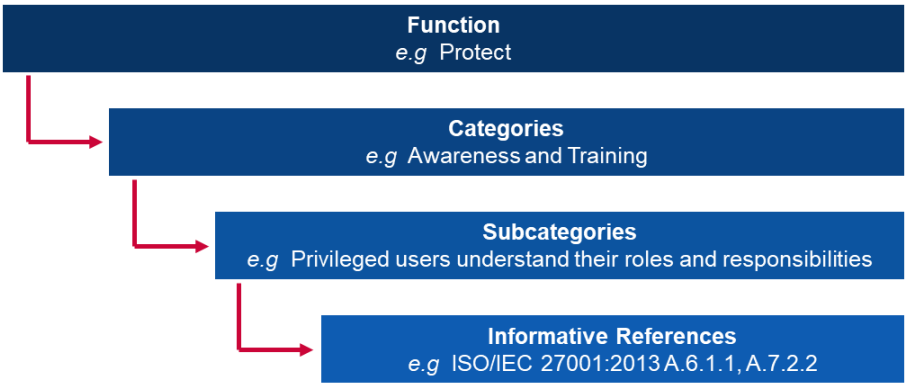
ii **Προστασία**: Ανάπτυξη και υλοποίηση κατάλληλων διασφαλίσεων για τη διασφάλιση της παράδοσης κρίσιμων υπηρεσιών.
   - Υποκατηγορίες: Διαχείριση Ταυτότητας και Έλεγχος Πρόσβασης· Ευαισθητοποίηση και Κατάρτιση· Ασφάλεια Δεδομένων· Διεργασίες και Διαδικασίες Προστασίας Πληροφοριών· Διατήρηση· και Τεχνολογία Προστασίας

iii **Εντοπισμός**: Ανάπτυξη και υλοποίηση κατάλληλων δραστηριοτήτων για τον προσδιορισμό ενός περιστατικού στον κυβερνοχώρο.
   - Υποκατηγορίες: Ανωμαλίες και Περιστατικά· Συνεχής Παρακολούθηση Ασφαλείας· και Διαδικασίες Εντοπισμού.

iv **Απάντηση**: Ανάπτυξη και υλοποίηση κατάλληλων δραστηριοτήτων για την ανάληψη δράσης σχετικά με ένα εντοπισμένο περιστατικό στον κυβερνοχώρο.
   - Υποκατηγορίες: Σχεδιασμός Απόκρισης· Επικοινωνίες· Ανάλυση· Μετριασμός· και Βελτιώσεις.

v **Ανάκαμψη**: Ανάπτυξη και υλοποίηση κατάλληλων δραστηριοτήτων για τη διατήρηση σχεδίων για την ανθεκτικότητα και την αποκατάσταση οποιωνδήποτε ικανοτήτων ή υπηρεσιών απομειώθηκαν λόγω ενός περιστατικού στον κυβερνοχώρο.
   - Υποκατηγορίες: Σχεδιασμός Ανάκαμψης· Βελτιώσεις και Επικοινωνίες

Εικόνα 8: Κατάσταση του Πλαισίου για τη βελτίωση της κρίσιμης υποδομής για την ασφάλεια στον κυβερνοχώρο



Function e.g Project	**Λειτουργία** π.χ. Έργο
Categories e.g Awarness and Training	**Κατηγορίες** π.χ. Ευαισθητοποίηση και Κατάρτιση
Subcategories e.g Privileged useres understand their roles and responsibilities	**Υποκατηγορίες** π.χ. Οι προνομιούχοι χρήστες κατανοούν τους ρόλους και τις ευθύνες τους
Informative References e.g ISO/IEC 27001:2013 A.6.1.1,A.7.2.2	**Ενημερωτικές Αναφορές**π.χ. ISO/IEC 27001:2013 A.6.1.1,A.7.2.2

Βαθμίδες

Το Πλαίσιο για τη βελτίωση της κρίσιμης υποδομής για την ασφάλεια στον κυβερνοχώρο βασίζεται σε **4 Βαθμίδες**, καθεμία από τις οποίες προσδιορίζεται βάσει τριών αξόνων: Διαδικασία Διαχείρισης Κινδύνου, Πρόγραμμα Ολοκληρωμένης Διαχείρισης Κινδύνου και Εξωτερική Συμμετοχή. Οι Βαθμίδες δεν θεωρούνται επίπεδα ωριμότητας αλλά πλαίσιο το οποίο παρέχει στους οργανισμούς ένα πλαίσιο των απόψεών τους για τον κίνδυνο για την ασφάλεια στον κυβερνοχώρο και τις διεργασίες που εφαρμόζονται για τη διαχείριση του εν λόγω κινδύνου.

- **Βαθμίδα 1: Μερική**
  - **Διαδικασία Διαχείρισης Κινδύνου**: οι πρακτικές διαχείρισης κινδύνου του οργανισμού δεν είναι τυποποιημένες, και η διαχείριση κινδύνου γίνεται σε ad hoc βάση και ενίοτε με αντιδραστικό τρόπο·
  - **Πρόγραμμα Ολοκληρωμένης Διαχείρισης Κινδύνου**: υπάρχει περιορισμένη ευαισθητοποίηση για τον κίνδυνο για την ασφάλεια στον κυβερνοχώρο σε επίπεδο οργανισμού. Ο οργανισμός εφαρμόζει τη διαχείριση του κινδύνου για την ασφάλεια στον κυβερνοχώρο σε μη τακτική βάση και κατά περίπτωση, και μπορεί να μη διαθέτει διεργασίες που επιτρέπουν την ανταλλαγή των πληροφοριών για την ασφάλεια στον κυβερνοχώρο εντός του οργανισμού·
  - **Εξωτερική Συμμετοχή**: ο οργανισμός δεν κατανοεί τον ρόλο του στο ευρύτερο οικοσύστημα ούτε σε σχέση με αυτούς από τους οποίους εξαρτάται ούτε σε σχέση με αυτούς που εξαρτώνται από αυτόν. Σε γενικές γραμμές, ο οργανισμός δεν γνωρίζει τους κινδύνους της αλυσίδας εφοδιασμού στον κυβερνοχώρο για τα προϊόντα και τις υπηρεσίες που παρέχει και χρησιμοποιεί·
- **Βαθμίδα 2: Με κριτήριο την επικινδυνότητα**
  - **Διαδικασία Διαχείρισης Κινδύνου**: οι πρακτικές διαχείρισης κινδύνου εγκρίνονται από τη διοίκηση, όμως μπορεί να μην είναι παγιωμένες ως πολιτική του οργανισμού·
  - **Πρόγραμμα Ολοκληρωμένης Διαχείρισης Κινδύνου**: υπάρχει ευαισθητοποίηση για τον κίνδυνο για την ασφάλεια στον κυβερνοχώρο σε επίπεδο οργανισμού, όμως δεν έχει θεσπιστεί μια προσέγγιση για τη διαχείριση του κινδύνου για την ασφάλεια στον κυβερνοχώρο για όλον τον οργανισμό. Πραγματοποιείται η αξιολόγηση του κινδύνου ασφάλειας στον κυβερνοχώρο των περιουσιακών στοιχείων του οργανισμού και των εξωτερικών περιουσιακών στοιχείων, όμως συνήθως δεν είναι επαναλαμβανόμενη.
  - **Εξωτερική Συμμετοχή**: σε γενικές γραμμές ο οργανισμός κατανοεί τον ρόλο του στο ευρύτερο οικοσύστημα σε σχέση είτε με αυτούς από τους οποίους εξαρτάται είτε με αυτούς που εξαρτώνται από αυτόν, αλλά όχι και με τους δύο. Επιπλέον, ο οργανισμός έχει επίγνωση των κινδύνων της αλυσίδας εφοδιασμού στον κυβερνοχώρο οι οποίοι σχετίζονται με τα προϊόντα και τις υπηρεσίες που παρέχει και χρησιμοποιεί, αλλά δεν ενεργεί με συνεπή ή επίσημο τρόπο ενάντια σε αυτούς τους κινδύνους·
- **Βαθμίδα 3: Επαναλαμβανόμενη**
  - **Διαδικασία Διαχείρισης Κινδύνου**: οι πρακτικές διαχείρισης κινδύνου του οργανισμού έχουν εγκριθεί επίσημα και εκφράζονται ως πολιτική. Οι πρακτικές ασφάλειας στον κυβερνοχώρο του οργανισμού επικαιροποιούνται τακτικά βάσει της εφαρμογής διαδικασιών διαχείρισης κινδύνου σε αλλαγές ως προς τις επιχειρηματικές απαιτήσεις/απαιτήσεις αποστολής και βάσει ενός μεταβαλλόμενου τοπίου απειλών και τεχνολογίας·
  - **Πρόγραμμα Ολοκληρωμένης Διαχείρισης Κινδύνου**: υφίσταται προσέγγιση για τη διαχείριση του κινδύνου ασφάλειας στον κυβερνοχώρο για όλον τον οργανισμό. Οι πολιτικές, διεργασίες και διαδικασίες με κριτήριο την επικινδυνότητα ορίζονται, υλοποιούνται, όπως προβλέπεται, και αναθεωρούνται. Τα ανώτερα στελέχη διασφαλίζουν τη συνεκτίμηση της ασφάλειας στον κυβερνοχώρο σε όλες τις γραμμές λειτουργίας του οργανισμού·
  - **Εξωτερική Συμμετοχή**: ο οργανισμός κατανοεί τον ρόλο του, τις εξαρτήσεις του, και όσους εξαρτώνται από αυτόν στο ευρύτερο οικοσύστημα και μπορεί να συμβάλλει στην ευρύτερη κατανόηση των κινδύνων από την κοινότητα. Ο οργανισμός έχει επίγνωση των κινδύνων της αλυσίδας εφοδιασμού στον κυβερνοχώρο που σχετίζονται με τα προϊόντα και τις υπηρεσίες που παρέχει και χρησιμοποιεί·
- **Βαθμίδα 4: Προσαρμοστική**
  - **Διαδικασία Διαχείρισης Κινδύνου**: ο οργανισμός προσαρμόζει τις οικείες πρακτικές ασφάλειας στον κυβερνοχώρο βάσει προηγούμενων και υφιστάμενων δραστηριοτήτων ασφάλειας στον κυβερνοχώρο, συμπεριλαμβανομένων αντληθέντων διδαγμάτων και προγνωστικών δεικτών·
  - **Πρόγραμμα Ολοκληρωμένης Διαχείρισης Κινδύνου**: υφίσταται μια προσέγγιση για τη διαχείριση του κινδύνου ασφάλειας στον κυβερνοχώρο για όλον τον οργανισμό που χρησιμοποιεί πολιτικές, διεργασίες και διαδικασίες με κριτήριο την

επικινδυνότητα για την αντιμετώπιση πιθανών περιστατικών στον κυβερνοχώρο· και

- **Εξωτερική Συμμετοχή**: ο οργανισμός κατανοεί τον ρόλο του, τις εξαρτήσεις του, και όσους εξαρτώνται από αυτόν στο ευρύτερο οικοσύστημα και συμβάλλει στην ευρύτερη κατανόηση των κινδύνων από την κοινότητα.

Μέθοδος αξιολόγησης

Στόχος του Πλαισίου για τη βελτίωση της κρίσιμης υποδομής για την ασφάλεια στον κυβερνοχώρο είναι να βοηθήσει τους οργανισμούς να αξιολογούν τον κίνδυνό τους για να καταστήσουν την προσέγγιση και τις επενδύσεις τους για την ασφάλεια στον κυβερνοχώρο πιο ορθολογικές, αποτελεσματικές και αξιόλογες. Για να εξετάσει την αποτελεσματικότητα των επενδύσεων, ένας οργανισμός πρέπει αρχικά να έχει κατανοήσει σαφώς τους οργανωτικούς στόχους του, τη σχέση μεταξύ αυτών των στόχων και των υποστηρικτικών αποτελεσμάτων για την ασφάλεια στον κυβερνοχώρο. Τα αποτελέσματα για την ασφάλεια στον κυβερνοχώρο του Πυρήνα του Πλαισίου υποστηρίζουν την αυτοαξιολόγηση της αποτελεσματικότητας των επενδύσεων και των δραστηριοτήτων ασφάλειας στον κυβερνοχώρο.

A.4 Μοντέλο ωριμότητας ικανοτήτων του Κατάρ για την ασφάλεια στον κυβερνοχώρο (Q-C2M2)

Το Μοντέλο ωριμότητας ικανοτήτων του Κατάρ για την ασφάλεια στον κυβερνοχώρο (Q-C2M2) αναπτύχθηκε από τη Σχολή της Νομικής του Πανεπιστημίου του Κατάρ το 2018. Το Q-C2M2 βασίζεται σε διάφορα υφιστάμενα μοντέλα για τη θέσπιση μιας ολοκληρωμένης μεθοδολογίας αξιολόγησης για την ενίσχυση του πλαισίου του Κατάρ για την ασφάλεια στον κυβερνοχώρο.

Χαρακτηριστικά Γνωρίσματα/ Διαστάσεις

Το Q-C2M2 υιοθετεί την προσέγγιση του Εθνικού Ινστιτούτου Προτύπων και Τεχνολογίας (NIST) αξιοποιώντας πέντε βασικές λειτουργίες ως κύριους τομείς. Οι πέντε βασικές λειτουργίες είναι εφαρμόσιμες στο πλαίσιο του Κατάρ διότι είναι συνήθεις στους τομείς βασικής υποδομής, οι οποίοι αποτελούν ένα σημαντικό στοιχείο για το πλαίσιο ασφάλειας στον κυβερνοχώρο του Κατάρ. Το Q-C2M2 βασίζεται σε **πέντε τομείς**, καθένας εκ των οποίων διαιρείται σε αρκετούς **υποτομείς** ώστε να καλύπτεται ολόκληρο το φάσμα της ωριμότητας των ικανοτήτων ασφάλειας στον κυβερνοχώρο.

Οι πέντε τομείς αναλύονται παρακάτω:

i. Ο **τομέας Κατανόηση** περιλαμβάνει τέσσερις υποτομείς: Διακυβέρνηση στον κυβερνοχώρο, περιουσιακά στοιχεία, κίνδυνοι και κατάρτιση·
ii. Οι υποτομείς του **τομέα Ασφάλεια** περιλαμβάνουν την Ασφάλεια Δεδομένων, την Τεχνολογική Ασφάλεια, την Ασφάλεια του Ελέγχου Πρόσβασης, την Ασφάλεια των Επικοινωνιών και την Ασφάλεια Προσωπικού·
iii. Ο **τομέας Έκθεση** περιλαμβάνει τους υποτομείς της Παρακολούθησης, της Διαχείρισης Περιστατικών, του Εντοπισμού, της Ανάλυσης και της Έκθεσης·
iv. Ο **τομέας Απόκριση** περιλαμβάνει τον Σχεδιασμό της Απόκρισης, τον Μετριασμό και την Επικοινωνία της Απόκρισης· και
v. Ο **τομέας Συντήρηση** περιλαμβάνει τον Σχεδιασμό της Ανάκαμψης, τη Διαχείριση της Συνέχειας, τη Βελτίωση και τις Εξωτερικές Εξαρτήσεις.

Επίπεδα ωριμότητας

Το Q-C2M2 χρησιμοποιεί **5 επίπεδα ωριμότητας** και μετρά την ωριμότητα των ικανοτήτων μιας κρατικής οντότητας ή ενός μη κρατικού οργανισμού στο επίπεδο των βασικών λειτουργιών. Στόχος αυτών των επιπέδων είναι η αξιολόγηση της ωριμότητας των πέντε τομέων που αναλύονται στην παραπάνω ενότητα.

- **Εκκίνηση**: Εφαρμόζονται ad-hoc πρακτικές και διεργασίες ασφάλειας στον κυβερνοχώρο σε μερικούς τομείς·

- **Υλοποίηση**: Έχουν υιοθετηθεί πολιτικές για την υλοποίηση όλων των δραστηριοτήτων ασφάλειας στον κυβερνοχώρο στους τομείς με στόχο την ολοκλήρωση της υλοποίησης σε έναν ορισμένο χρόνο·
- **Ανάπτυξη**: Έχουν υλοποιηθεί πολιτικές και πρακτικές για την ανάπτυξη και τη βελτίωση των δραστηριοτήτων ασφάλειας στον κυβερνοχώρο στους τομείς με στόχο την πρόταση νέων δραστηριοτήτων προς υλοποίηση·
- **Προσαρμογή**: Πραγματοποιείται αναθεώρηση και επανεξέταση των δραστηριοτήτων ασφάλειας στον κυβερνοχώρο και υιοθετούνται πρακτικές βάσει των προγνωστικών δεικτών που προκύπτουν από προηγούμενες εμπειρίες και μέτρα· και
- **Ευελιξία**: Συνεχίζεται η εφαρμογή του σταδίου της προσαρμογής με επιπλέον έμφαση στην ευελιξία και την ταχύτητα κατά την υλοποίηση των δραστηριοτήτων στους τομείς.

Μέθοδος αξιολόγησης

Το Q-C2M2 βρίσκεται σε ένα πρώιμο στάδιο έρευνας και δεν είναι ακόμα έτοιμο προς εφαρμογή. Πρόκειται για ένα πλαίσιο που θα μπορούσε να χρησιμοποιηθεί για τη χρήση ενός λεπτομερούς μοντέλου αξιολόγησης για τους οργανισμούς του Κατάρ στο μέλλον.

A.5 Πιστοποίηση του μοντέλου ωριμότητας ασφάλειας στον κυβερνοχώρο (CMMC)

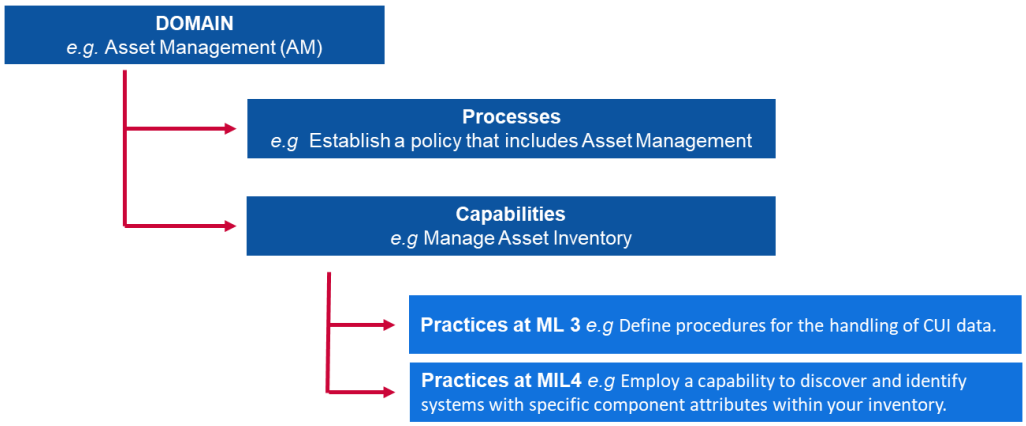
Η πιστοποίηση του μοντέλου ωριμότητας της ασφάλειας στον κυβερνοχώρο (CMMC) σχεδιάστηκε από το Υπουργείο Άμυνας των ΗΠΑ σε συνεργασία με το Πανεπιστήμιο Carnegie Mellon και το Εργαστήριο Εφαρμοσμένης Φυσικής του Πανεπιστημίου John Hopkins. Κατά τον σχεδιασμό αυτού του μοντέλου, ο βασικός στόχος του Υπουργείου Άμυνας ήταν η προστασία πληροφοριών από τον τομέα της Βιομηχανικής Βάσης Άμυνας (DIB). Οι πληροφορίες τις οποίες στοχεύει το CMMC είναι διαβαθμισμένες είτε ως «Ομοσπονδιακές Συμβατικές Πληροφορίες», δηλαδή πληροφορίες που παρέχονται από την Κυβέρνηση ή παράγονται για την Κυβέρνηση βάσει σύμβασης και δεν προορίζονται για δημοσίευση, είτε ως «Ελεγχόμενες Μη Διαβαθμισμένες Πληροφορίες», δηλαδή πληροφορίες που χρήζουν προστασίας ή ελέγχων διάδοσης σύμφωνα με τους νόμους, τους κανονισμούς και τις κυβερνητικές πολιτικές. Το CMMC μετρά την ωριμότητα ασφάλειας στον κυβερνοχώρο και προβλέπει βέλτιστες πρακτικές παράλληλα με ένα στοιχείο πιστοποίησης για τη διασφάλιση της εφαρμογής πρακτικών που συνδέονται με κάθε επίπεδο ωριμότητας. Η τελευταία έκδοση του CMMC δημοσιεύτηκε το 2020.

Χαρακτηριστικά Γνωρίσματα/ Διαστάσεις

Το CMMC εξετάζει **δεκαεπτά τομείς** που αντιπροσωπεύουν ομάδες διεργασιών και ικανοτήτων ασφάλειας στον κυβερνοχώρο. Κάθε τομέας αναλύεται σε πολλαπλές διεργασίες που είναι παρόμοιες σε όλους τους τομείς και αντιστοιχεί σε πολλές **ικανότητες** που εκτείνονται σε πέντε επίπεδα ωριμότητας. Στη συνέχεια, οι ικανότητες (ή η ικανότητα) εξειδικεύονται περαιτέρω σε **πρακτικές** για κάθε σχετικό επίπεδο ωριμότητας.

Η σχέση μεταξύ αυτών των εννοιών έχει ως εξής:

Εικόνα 9: Κατάσταση δεικτών CMM



DOMAIN e.g. Asset Management (AM)	**ΤΟΜΕΑΣ** π.χ. Διαχείριση περιουσιακών στοιχείων (AM)
Processes e.g Establish a policy that includes Asset Management	**Διεργασίες** π.χ. Θέσπιση πολιτικής που περιλαμβάνει τη διαχείριση περιουσιακών στοιχείων
Capabilities e.g Manage Asset Inventory	**Ικανότητες** π.χ. Διαχείριση καταλόγου απογραφής περιουσιακών στοιχείων
Practices at ML 3 e.g Define procedures for the handling of CUI data	**Πρακτικές στο ML 3** π.χ. Καθορισμός διαδικασιών για τη διαχείριση δεδομένων ελεγχόμενων μη διαβαθμισμένων πληροφοριών (CUI)
Practices at MIL4 e.g Employ a capability to discover and identify systems with specific component attributes within inventory	**Πρακτικές στο MIL4** π.χ. Χρήση μιας ικανότητας για την ανακάλυψη και τον προσδιορισμό συστημάτων με συγκεκριμένα γνωρίσματα στοιχείων στον κατάλογο απογραφής

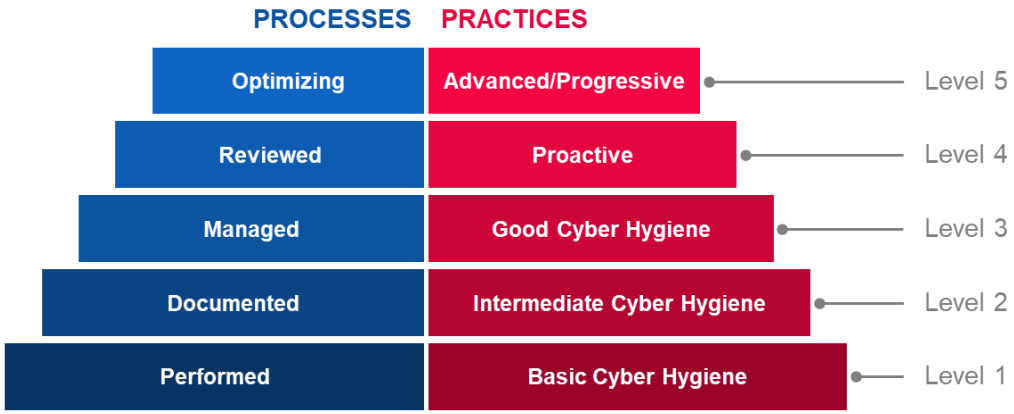
Οι δεκαεπτά τομείς αναλύονται στη συνέχεια:

i Έλεγχος πρόσβασης (AC)·
ii Διαχείριση περιουσιακών στοιχείων (AM)·
iii Λογιστικός έλεγχος και λογοδοσία (AU)·
iv Ενημέρωση και κατάρτιση (AT)·
v Διαχείριση διαμόρφωσης (CM)·
vi Ταυτοποίηση και επαλήθευση ταυτότητας (IA)·
vii Απόκριση σε περιστατικά (IR)·
viii Συντήρηση (MA)·
ix Προστασία μέσων (MP)·
x Ασφάλεια προσωπικού (PS)·
xi Φυσική προστασία(PE)·
xii Ανάκαμψη (RE)·
xiii Διαχείριση κινδύνων (RM)·
xiv Αξιολόγηση ασφάλειας (CA)·
xv Επίγνωση της κατάστασης (SA)·
xvi Προστασία συστήματος και επικοινωνιών (SC) ·και
xvii Ακεραιότητα συστήματος και πληροφοριών (SI).

Επίπεδα ωριμότητας

Το CMMC χρησιμοποιεί **5 επίπεδα ωριμότητας** τα οποία ορίζονται βάσει διεργασιών και πρακτικών. Για να φτάσει σε ένα ορισμένο επίπεδο ωριμότητας στο CMMC, ένας οργανισμός πρέπει να πληροί τις προϋποθέσεις για τις διεργασίες και τις πρακτικές για το εν λόγω επίπεδο. Αυτό συνεπάγεται, επίσης, ότι πληροί τις προϋποθέσεις όλων των προηγούμενων επιπέδων.

Εικόνα 10: Επίπεδα ωριμότητας CMMC



PROCESSES	ΔΙΕΡΓΑΣΙΕΣ
Optimizing	Βελτιστοποίησης
Reviewed	Αναθεωρημένες
Managed	Διαχειριζόμενες
Documented	Τεκμηριωμένες
Performed	Υλοποιούμενες
PRACTICES	ΠΡΑΚΤΙΚΕΣ
Advanced/Progressive	Προηγμένες/Προορατικές
Proactive	Προορατικές
Good Cyber Hygiene	Καλή Κυβερνοϋγιεινή
Intermediate Cyber Hygiene	Μέτρια Κυβερνοϋγιεινή
Basic Cyber Hygiene	Βασική Κυβερνοϋγιεινή
Level 5	Επίπεδο 5
Level 4	Επίπεδο 4
Level 3	Επίπεδο 3
Level 2	Επίπεδο 2
Level 1	Επίπεδο 1

- **Επίπεδο 1**
  - **Διεργασίες – Υλοποιούμενες**: διότι ο οργανισμός μπορεί να είναι σε θέση να υλοποιεί αυτές τις πρακτικές μόνο σε ad hoc βάση και μπορεί να βασίζεται σε τεκμηρίωση ή όχι. Η ωριμότητα της διεργασίας δεν αξιολογείται για το Επίπεδο 1·
  - **Πρακτικές – Βασική Κυβερνοϋγιεινή**: το επίπεδο 1 εστιάζει στην προστασία των FCI (Ομοσπονδιακές Συμβατικές Πληροφορίες) και αποτελείται μόνο από πρακτικές που αντιστοιχούν στις βασικές απαιτήσεις διασφάλισης·
- **Επίπεδο 2**
  - **Διεργασίες – Τεκμηριωμένες**: το επίπεδο 2 προϋποθέτει τη θέσπιση και τεκμηρίωση πρακτικών και πολιτικών που θα κατευθύνουν την υλοποίηση των προσπαθειών του CMMC. Η τεκμηρίωση δίνει τη δυνατότητα επαναλαμβανόμενης εφαρμογής των πρακτικών. Οι οργανισμοί αναπτύσσουν ώριμες ικανότητες τεκμηριώνοντας τις διεργασίες τους και εφαρμόζοντάς τις, στη συνέχεια, όπως είναι τεκμηριωμένες·
  - **Πρακτικές – Μέτρια Κυβερνοϋγιεινή**: το επίπεδο 2 λειτουργεί ως πρόοδος από το Επίπεδο 1 στο Επίπεδο 3 και αποτελείται από ένα υποσύνολο απαιτήσεων ασφαλείας που καθορίζονται στο NIST SP 800-171, καθώς και από πρακτικές από άλλα πρότυπα και σημεία αναφοράς·
- **Επίπεδο 3**
  - **Διεργασίες – Διαχειριζόμενες**: το επίπεδο 3 προϋποθέτει τη θέσπιση, συντήρηση και υποστήριξη ενός σχεδίου που παρουσιάζει τη διαχείριση δραστηριοτήτων για την εφαρμογή των πρακτικών. Το σχέδιο μπορεί να περιλαμβάνει πληροφορίες σχετικά με αποστολές, στόχους, σχέδια έργων,

πόρους, απαιτούμενη κατάρτιση και συμμετοχή σχετικών ενδιαφερόμενων παραγόντων·

- **Πρακτικές – Καλή Κυβερνοϋγιεινή**: το επίπεδο 3 επικεντρώνεται στην προστασία των CUI και περιλαμβάνει όλες τις απαιτήσεις ασφαλείας που προσδιορίζονται στο NIST SP 800-171, καθώς και επιπρόσθετες πρακτικές από άλλα πρότυπα και σημεία αναφοράς για τον μετριασμό των απειλών·

- **Επίπεδο 4**
  - **Διεργασίες – Αναθεωρημένες**: το επίπεδο 4 προϋποθέτει την αναθεώρηση και μέτρηση των πρακτικών για σκοπούς αποτελεσματικότητας. Πέρα από τη μέτρηση των πρακτικών ως προς την αποτελεσματικότητα, οι οργανισμοί σε αυτό το επίπεδο μπορούν να αναλαμβάνουν διορθωτικές ενέργειες όταν είναι απαραίτητο και να ενημερώνουν τα υψηλότερα επίπεδα διοίκησης για καταστάσεις ή ζητήματα σε επαναλαμβανόμενη βάση·
  - **Πρακτικές – Προορατικές**: το επίπεδο 4 επικεντρώνεται στην προστασία των CUI (Ελεγχόμενες Μη Διαβαθμισμένες Πληροφορίες) και περιλαμβάνει ένα υποσύνολο ενισχυμένων απαιτήσεων ασφαλείας. Αυτές οι πρακτικές βελτιώνουν τις ικανότητες εντοπισμού και απόκρισης ενός οργανισμού για την αντιμετώπιση των μεταβαλλόμενων τακτικών, τεχνικών και διεργασιών και την προσαρμογή σε αυτές·

- **Επίπεδο 5**
  - **Διεργασίες – Βελτιστοποίησης**: το επίπεδο 5 προϋποθέτει την τυποποίηση και βελτιστοποίηση της εφαρμογής διεργασιών σε ολόκληρο τον οργανισμό· και
  - **Πρακτικές – Προηγμένες/Προορατικές**: το επίπεδο 5 επικεντρώνεται στην προστασία των CUI. Οι επιπρόσθετες πρακτικές αυξάνουν το βάθος και την εξειδίκευση των ικανοτήτων ασφάλειας στον κυβερνοχώρο.

Μέθοδος αξιολόγησης

Το CMMC είναι ένα σχετικά πρόσφατο μοντέλο, που οριστικοποιήθηκε στο πρώτο τρίμηνο του 2020. Μέχρι σήμερα, δεν έχει αξιοποιηθεί από κάποιον οργανισμό. Ωστόσο, οι ανάδοχοι του Υπουργείου Άμυνας των ΗΠΑ αναμένουν να επικοινωνήσουν με πιστοποιημένους εξεταστές τρίτων μερών για τη διενέργεια λογιστικών ελέγχων. Το Υπουργείο Άμυνας των ΗΠΑ αναμένει από τους αναδόχους του να εφαρμόσουν βέλτιστες πρακτικές για την ανάπτυξη της ασφάλειας στον κυβερνοχώρο και την προστασία ευαίσθητων πληροφοριών.

Α.6 Το κοινοτικό μοντέλο ωριμότητας ασφάλειας στον κυβερνοχώρο (CCSMM)

Το κοινοτικό μοντέλο ωριμότητας ασφάλειας στον κυβερνοχώρο (CCSMM) αναπτύχθηκε από το Κέντρο για τη Διασφάλιση και την Ασφάλεια Υποδομών του Πανεπιστημίου του Τέξας. Στόχος του CCSMM είναι να καθορίσει με καλύτερο τρόπο μεθόδους για τον προσδιορισμό της τρέχουσας κατάστασης μιας κοινότητας ως προς την κυβερνοετοιμότητά της και να παράσχει έναν χάρτη πορείας που μπορούν να ακολουθούν οι κοινότητες στο πλαίσιο των προσπαθειών προετοιμασίας τους. Το CCSMM απευθύνεται κυρίως σε τοπικές ή πολιτειακές κυβερνήσεις. Σχεδιάστηκε το 2007.

Χαρακτηριστικά Γνωρίσματα/ Διαστάσεις

Καθορίζονται τα επίπεδα ωριμότητας βάσει **6 βασικών διαστάσεων** που καλύπτουν τις διαφορετικές πτυχές ασφάλειας στον κυβερνοχώρο στο εσωτερικό κοινοτήτων και οργανισμών. Αυτές οι διαστάσεις καθορίζονται με σαφήνεια για κάθε επίπεδο ωριμότητας (αναλύονται λεπτομερώς στην Εικόνα 31: Σύνοψη διαστάσεων CCSMM). Οι 6 διαστάσεις είναι οι εξής:

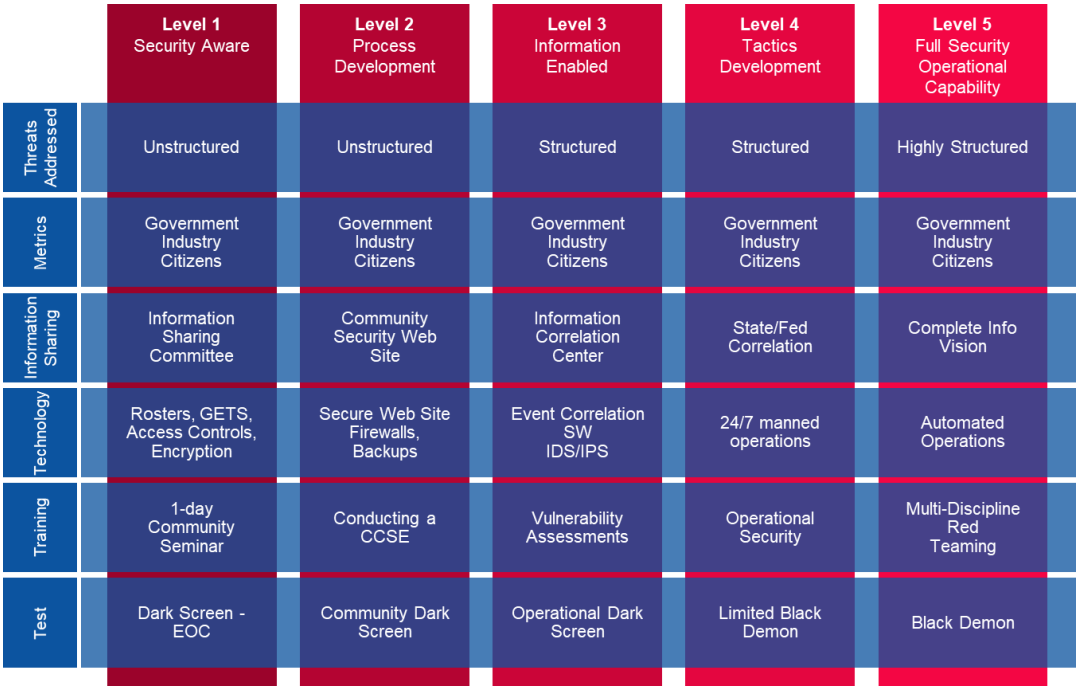
i Απειλές που αντιμετωπίζονται·
ii Ποσοτικοί δείκτες·
iii Ανταλλαγή πληροφοριών·
iv Τεχνολογία·
v Κατάρτιση· και
vi Δοκιμή.

Επίπεδα ωριμότητας

Το CCSMM βασίζεται σε **5 επίπεδα ωριμότητας** ανάλογα με τους βασικούς τύπους απειλών και δραστηριοτήτων κάθε επιπέδου:

- **Επίπεδο 1: Επίγνωση Ασφαλείας**
  Το βασικό θέμα των δραστηριοτήτων σε αυτό το επίπεδο είναι να διασφαλιστεί ότι τα άτομα και οι οργανισμοί έχουν επίγνωση των απειλών, των προβλημάτων, και των ζητημάτων που σχετίζονται με την ασφάλεια στον κυβερνοχώρο.
- **Επίπεδο 2: Ανάπτυξη Διεργασιών**
  Επίπεδο που έχει σχεδιαστεί για να συνδράμει τις κοινότητες στη θέσπιση και τη βελτίωση των διεργασιών ασφαλείας που απαιτούνται για την αποτελεσματική αντιμετώπιση προβλημάτων ασφάλειας στον κυβερνοχώρο·
- **Επίπεδο 3: Αξιοποίηση Πληροφοριών**
  Έχει σχεδιαστεί για τη βελτίωση των μηχανισμών ανταλλαγής πληροφοριών εντός της κοινότητας προκειμένου η κοινότητα να είναι σε θέση να συσχετίσει φαινομενικά ανομοιογενείς πληροφορίες.
- **Επίπεδο 4: Ανάπτυξη Τακτικών**
  Τα στοιχεία αυτού του επιπέδου είναι σχεδιασμένα για την ανάπτυξη καλύτερων και πιο προορατικών μεθόδων για τον εντοπισμό και την αντιμετώπιση επιθέσεων. Σε αυτό το επίπεδο, θα πρέπει να εφαρμόζονται ήδη οι περισσότερες μέθοδοι πρόληψης.
- **Επίπεδο 5: Πλήρης Επιχειρησιακή Ικανότητα Ασφαλείας**
  Αυτό το επίπεδο αντιπροσωπεύει τα στοιχεία που θα πρέπει να υφίστανται σε κάθε οργανισμό προκειμένου να θεωρείται πλήρως λειτουργικός και έτοιμος να αντιμετωπίσει κάθε είδους κυβερνοαπειλή.

Εικόνα 31: Σύνοψη διαστάσεων CCSMM ανά επίπεδο



Level 1 Security Aware	Επίπεδο 1 Επίγνωση ασφαλείας
Level 2 Process Development	Επίπεδο 2 Ανάπτυξη διεργασιών
Level 3 Information Enabled	Επίπεδο 3 Αξιοποίηση πληροφοριών
Level 4 Tactics Development	Επίπεδο 4 Ανάπτυξη τακτικών
Level 5 Full Security Operational Capability	Επίπεδο 5 Πλήρης επιχειρησιακή ικανότητα ασφαλείας
Threats Addressed	Απειλές που αντιμετωπίζονται
Metrics	Ποσοτικοί δείκτες
Information sharing	Ανταλλαγή πληροφοριών
Technology	Τεχνολογία
Training	Κατάρτιση
Test	Δοκιμή
Unstructured	Αδόμητο
Governement Industry Citizens	Κυβέρνηση Κλάδος Πολίτες
Information Sharing Committee	Επιτροπή Ανταλλαγής Πληροφοριών
Rosters, GETS, Assess Controls, Encryption	Μητρώα, GETS, Έλεγχοι Πρόσβασης, Κρυπτογράφηση
1-dat Community Seminar	Μονοήμερο Σεμινάριο Κοινότητας
Dark Screen – EOC	Dark Screen – EOC
Unstructured	Αδόμητο
Governement Industry Citizens	Κυβέρνηση Κλάδος Πολίτες
Community Security Web site	Ιστότοπος για την Ασφάλεια της Κοινότητας
Secure Web Site Firewalls, Backups	Τείχη προστασίας ασφαλών ιστοτόπων, Δημιουργία εφεδρικών αντιγράφων
Conudcting a CCSE	Διεξαγωγή κατάρτισης CCSE
Community Dark Screen	Community Dark Screen
Structured	Δομημένο
Governement Industry Citizens	Κυβέρνηση Κλάδος Πολίτες
Information Correlation Center	Κέντρο Συσχέτισης Πληροφοριών
Event Correlation SW IDS/IPS	Συσχέτιση περιστατικών SW IDS/IPS
Vulnerability Assessment	Αξιολόγηση τρωτών σημείων
Operational Dark Screen	Operational Dark Screen

Structured	Δομημένο
Governement Industry Citizens	Κυβέρνηση Κλάδος Πολίτες
State/Fed Correlation	Συσχέτιση πολιτείας/ομοσπονδίας
24/7 manned operations	Επανδρωμένες επιχειρήσεις κάθε ημέρα όλη ημέρα
Operational Security	Λειτουργική ασφάλεια δικτύου
Limited Black Demon	Limited Black Demon
Highly Structured	Εξαιρετικά δομημένο
Complete Info Vision	Ολοκληρωμένη εικόνα πληροφοριών
Automated Operations	Αυτοματοποιημένες εργασίες
Multi-Discipline Red Teaming	Πολυτομεακή Red Teaming
Black Demon	Black Demon

Μέθοδος αξιολόγησης

Ως μέθοδος αξιολόγησης, το CCSMM προορίζεται για χρήση από κοινότητες με πληροφορίες από πολιτειακές και ομοσπονδιακές υπηρεσίες επιβολής του νόμου. Στόχος του είναι να βοηθά μια κοινότητα να προσδιορίζει τι έχει πιο μεγάλη σημασία, ποιοι είναι οι πιο πιθανοί στόχοι και πού πρέπει να παράσχει προστασία (και σε τι βαθμό). Με βάση αυτούς τους στόχους, μπορούν να καταρτιστούν σχέδια προκειμένου κάθε πτυχή της κοινότητας να φτάσει στο απαραίτητο επίπεδο ωριμότητας ασφάλειας στον κυβερνοχώρο. Οι συγκεκριμένες πληροφορίες ασφαλείας που παράγονται από το CCSMM συμβάλλουν στον προσδιορισμό των στόχων διάφορων δοκιμών και ασκήσεων που μπορούν να χρησιμοποιηθούν για τη μέτρηση της αποτελεσματικότητας των καθορισμένων προγραμμάτων.

A.7 Μοντέλο ωριμότητας για την ασφάλεια των πληροφοριών για το πλαίσιο του NIST για την ασφάλεια στον κυβερνοχώρο (ISMM)

Το Μοντέλο ωριμότητας για την ασφάλεια των πληροφοριών για το πλαίσιο του NIST για την ασφάλεια στον κυβερνοχώρο (ISMM) έχει αναπτυχθεί από τη Σχολή Επιστημών Πληροφορικής και Μηχανικής του Πανεπιστημίου Πετρελαίου και Ορυκτών King Fahd στη Σαουδική Αραβία. Προτείνει ένα καινούριο μοντέλο ωριμότητας ικανοτήτων για τη μέτρηση της εφαρμογής των μέτρων για την ασφάλεια στον κυβερνοχώρο. Στόχος του ISMM είναι να δώσει στους οργανισμούς τη δυνατότητα να μετρούν την πρόοδο υλοποίησης με την πάροδο του χρόνου χρησιμοποιώντας το ίδιο εργαλείο μέτρησης σε τακτική βάση για να διασφαλίσουν τη διατήρηση της επιθυμητής στάσης ασφαλείας. Το ISMM αναπτύχθηκε το 2017.

Χαρακτηριστικά Γνωρίσματα/ Διαστάσεις

Το ISMM βασίζεται στους υφιστάμενους αξιολογούμενους τομείς του πλαισίου NIST και προσδίδει μια διάσταση σχετικά με την αξιολόγηση της συμμόρφωσης. Επομένως, το μοντέλο διαθέτει **23 αξιολογούμενους τομείς** για τη στάση ασφαλείας ενός οργανισμού. Οι 23 αξιολογούμενοι τομείς είναι οι εξής:

i Διαχείριση περιουσιακών στοιχείων·
ii Επιχειρηματικό περιβάλλον·
iii Διακυβέρνηση·
iv Εκτίμηση κινδύνου·
v Στρατηγική διαχείρισης κινδύνων·
vi Αξιολόγηση συμμόρφωσης·
vii Έλεγχος πρόσβασης·
viii Ενημέρωση και κατάρτιση·
ix Ασφάλεια δεδομένων·
x Διεργασίες και διαδικασίες προστασίας πληροφοριών·
xi Συντήρηση·
xii Προστατευτική τεχνολογία·
xiii Ανωμαλίες και συμβάντα·

xiv Συνεχής παρακολούθηση ασφαλείας·
xv Διεργασίες εντοπισμού·
xvi Σχεδιασμός απόκρισης·
xvii Επικοινωνίες απόκρισης·
xviii Ανάλυση απόκρισης·
xix Μετριασμός απόκρισης·
xx Βελτιώσεις απόκρισης·
xxi Σχεδιασμός ανάκαμψης·
xxii Βελτιώσεις ανάκαμψης· και
xxiii Επικοινωνίες ανάκαμψης.

Επίπεδα ωριμότητας

Το ISMM βασίζεται σε **5 επίπεδα ωριμότητας**, τα οποία, δυστυχώς, δεν αναλύονται λεπτομερώς στη διαθέσιμη τεκμηρίωση.

- **Επίπεδο 1:** Υλοποιηθείσα Διεργασία·
- **Επίπεδο 2:** Διαχειριζόμενη Διεργασία·
- **Επίπεδο 3:** Πάγια Διεργασία·
- **Επίπεδο 4:** Προβλέψιμη Διεργασία· και
- **Επίπεδο 5:** Διεργασία Βελτιστοποίησης.

Μέθοδος αξιολόγησης

Το ISMM δεν προτείνει κάποια συγκεκριμένη μεθοδολογία για τη διεξαγωγή της αξιολόγησης οργανισμών.

A.8 Μοντέλο Μονάδας Εσωτερικού Ελέγχου (MMEE) για τον δημόσιο τομέα

Το Μοντέλο Κλιμακίων Εσωτερικού Ελέγχου (IA-CM) αναπτύχθηκε από το Ερευνητικό Ίδρυμα του Ινστιτούτου Εσωτερικών Ελεγκτών με στόχο την ανάπτυξη ικανοτήτων και την υποστήριξη μέσω της αυτοαξιολόγησης στον δημόσιο τομέα. Το IA-CM απευθύνεται σε επαγγελματίες στον τομέα του λογιστικού ελέγχου και παρέχει μια επισκόπηση του ίδιου του μοντέλου παράλληλα με έναν Οδηγό Εφαρμογής που λειτουργεί βοηθητικά στη χρήση του μοντέλου ως εργαλείου αυτοαξιολόγησης.

Μολονότι το IA-CM εστιάζει στις ικανότητες εσωτερικού ελέγχου, και όχι στη δημιουργία ικανοτήτων ασφάλειας στον κυβερνοχώρο, έχει σχεδιαστεί ως εργαλείο αυτοαξιολόγησης ωριμότητας για οντότητες του δημόσιου τομέα το οποίο μπορεί να εφαρμοστεί σε παγκόσμιο επίπεδο για τη βελτίωση των διεργασιών και της αποτελεσματικότητας. Δεδομένου ότι το πεδίο εφαρμογής του δεν εστιάζει στην ασφάλεια στον κυβερνοχώρο, δεν θα αναλυθούν τα χαρακτηριστικά γνωρίσματα του μοντέλου. Το IA-CM ολοκληρώθηκε το 2009.

Επίπεδα ωριμότητας

Το Μοντέλο Κλιμακίων Εσωτερικού Ελέγχου (IA-CM) περιλαμβάνει **5 επίπεδα ωριμότητας**, το καθένα από τα οποία περιγράφει τα χαρακτηριστικά και τις ικανότητες της δραστηριότητας Εσωτερικού Ελέγχου στο εν λόγω επίπεδο. Τα επίπεδα ικανοτήτων του μοντέλου προσφέρουν έναν χάρτη πορείας για συνεχή βελτίωση.

- **Επίπεδο 1: Αρχικό**
  Δεν υφίστανται βιώσιμες, επαναλαμβανόμενες ικανότητες, εξάρτηση από ατομικές προσπάθειες
  - Ad hoc ή αδόμητο.
  - Μεμονωμένοι ατομικοί έλεγχοι ή επανεξέταση εγγράφων και συναλλαγών για σκοπούς ακρίβειας και συμμόρφωσης.
  - Τα αποτελέσματα εξαρτώνται από τις δεξιότητες του συγκεκριμένου προσώπου που κατέχει τη θέση.
  - Δεν έχουν θεσπιστεί επαγγελματικές πρακτικές πέρα από εκείνες που προβλέπονται από τις επαγγελματικές ενώσεις.

- Έγκριση χρηματοδότησης από τη διοίκηση, όπως απαιτείται.
- Έλλειψη υποδομής.
- Οι ελεγκτές είναι πιθανόν μέλη μιας ευρύτερης οργανωτικής μονάδας.
- Δεν έχει αναπτυχθεί θεσμική ικανότητα.

Επίπεδο 2: Υποδομή

Βιώσιμες και επαναλαμβανόμενες πρακτικές και διεργασίες

- Το βασικό ερώτημα ή πρόκληση για το Επίπεδο 2 είναι πώς μπορεί να εδραιωθεί και να διατηρηθεί η επαναληψιμότητα των διεργασιών και, κατά συνέπεια, μια επαναλαμβανόμενη ικανότητα.
- δημιουργούνται σχέσεις υποβολής αναφορών εσωτερικού ελέγχου, υποδομή διαχείρισης και διοίκησης, και επαγγελματικές πρακτικές και διεργασίες (καθοδήγηση, διεργασίες και διαδικασίες εσωτερικού ελέγχου).
- Ο σχεδιασμός του ελέγχου βασίζεται κυρίως σε προτεραιότητες της διοίκησης.
- Συνεχής εξάρτηση από τις δεξιότητες και τις ικανότητες συγκεκριμένων προσώπων.
- Μερική συμμόρφωση με τα πρότυπα.

Επίπεδο 3: Ολοκληρωμένο

Εφαρμόζονται ομοιόμορφα πρακτικές διαχείρισης και επαγγελματικές πρακτικές

- Οι πολιτικές, διεργασίες και διαδικασίες εσωτερικού ελέγχου είναι προσδιορισμένες, τεκμηριωμένες και ενσωματωμένες τόσο μεταξύ τους όσο και στην υποδομή του οργανισμού.
- Οι πρακτικές διαχείρισης και επαγγελματικές πρακτικές του εσωτερικού ελέγχου είναι παγιωμένες και εφαρμόζονται ομοιόμορφα στο σύνολο της δραστηριότητας εσωτερικού ελέγχου.
- Ο εσωτερικός έλεγχος αρχίζει να ευθυγραμμίζεται με την επιχειρηματική δραστηριότητα του οργανισμού και με τους κινδύνους που αντιμετωπίζει.
- Ο εσωτερικός έλεγχος εξελίσσεται από την απλή διενέργεια του παραδοσιακού εσωτερικού ελέγχου στην ενσωμάτωση στο πλαίσιο της ομάδας και στην παροχή συμβουλών για την απόδοση και τη διαχείριση κινδύνων.
- Δίνεται έμφαση στη δημιουργία ομάδων και στην ικανότητα της δραστηριότητας εσωτερικού ελέγχου και στην ανεξαρτησία και την αντικειμενικότητά του.
- Σε γενικές γραμμές, υφίσταται συμμόρφωση με τα πρότυπα.

Επίπεδο 4: Διαχειριζόμενο

Ενσωματώνει πληροφορίες από το σύνολο του οργανισμού για τη βελτίωση της διακυβέρνησης και της διαχείρισης κινδύνου

- Ο εσωτερικός έλεγχος είναι ευθυγραμμισμένος με τις προσδοκίες των βασικών ενδιαφερόμενων παραγόντων.
- Εφαρμόζονται δείκτες μέτρησης της απόδοσης με σκοπό τη μέτρηση και την παρακολούθηση των διεργασιών και των αποτελεσμάτων εσωτερικού ελέγχου.
- Αναγνωρίζεται η σημαντική συνεισφορά του εσωτερικού ελέγχου για τον οργανισμό.
- Οι λειτουργίες εσωτερικού ελέγχου αποτελούν αναπόσπαστο μέρος της διακυβέρνησης και της διαχείρισης κινδύνου του οργανισμού.
- Ο εσωτερικός έλεγχος είναι μια επιχειρηματική μονάδα υπό ορθή διαχείριση.
- Η μέτρηση και η διαχείριση των κινδύνων είναι ποσοτική.
- Υφίστανται αναγκαίες δεξιότητες και ικανότητες με τη δυνατότητα για ανανέωση και ανταλλαγή γνώσεων (στο πλαίσιο του εσωτερικού ελέγχου και σε όλον τον οργανισμό).

Επίπεδο 5: Βελτιστοποίησης

Μαθήματα από το εσωτερικό και το εξωτερικό του οργανισμού για συνεχή βελτίωση

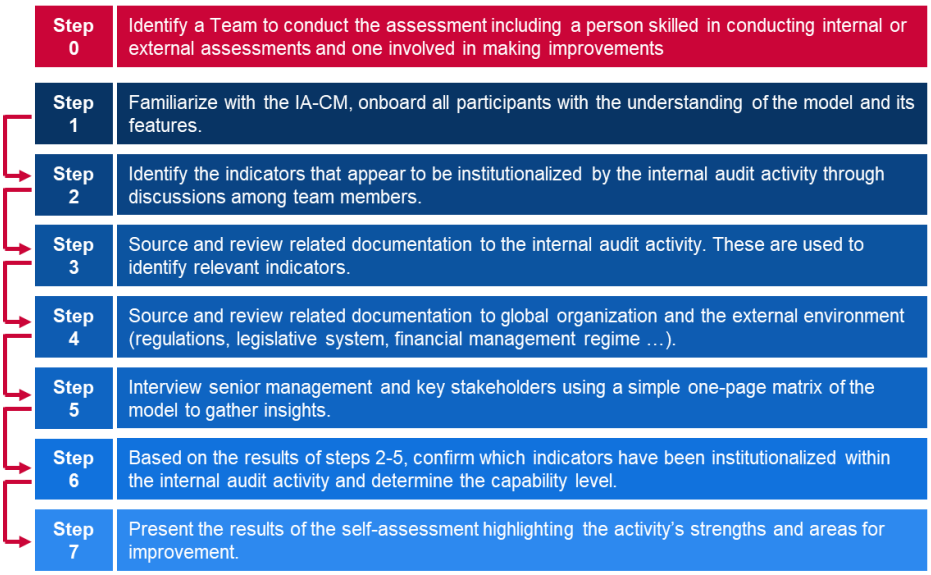
- Ο εσωτερικός έλεγχος είναι εποικοδομητικός οργανισμός με συνεχείς βελτιώσεις διεργασιών και καινοτομία.
- Ο εσωτερικός έλεγχος αξιοποιεί πληροφορίες εντός και εκτός του οργανισμού για να συμβάλει στην επίτευξη στρατηγικών στόχων.
- Εφαρμόζονται οι πρακτικές παγκοσμίου επιπέδου/συνιστώμενες πρακτικές/βέλτιστες πρακτικές.
- Ο εσωτερικός έλεγχος είναι κρίσιμο στοιχείο της δομής διακυβέρνησης του οργανισμού.
- Επαγγελματικές και εξειδικευμένες δεξιότητες ανωτάτου επιπέδου.

- Τα μέτρα αποδοτικότητας σε ατομικό επίπεδο, επίπεδο μονάδας και επίπεδο οργανισμού είναι πλήρως ενσωματωμένα για
- την προώθηση βελτιώσεων απόδοσης.

Μέθοδος αξιολόγησης

Το Μοντέλο Κλιμακίων Εσωτερικού Ελέγχου είναι σαφώς σχεδιασμένο για σκοπούς αυτοαξιολόγησης. Περιλαμβάνει αναλυτικά βήματα χρήσης και δείγμα παρουσιάσεων προς εξατομίκευση. Πριν από την έναρξη της αυτοαξιολόγησης, θα πρέπει να οριστεί μια εξειδικευμένη ομάδα, η οποία θα περιλαμβάνει, τουλάχιστον, ένα άτομο εξειδικευμένο στη διεξαγωγή εσωτερικών ή εξωτερικών αξιολογήσεων εσωτερικών ελέγχων και ένα άτομο που ασχολείται με την υλοποίηση βελτιώσεων στο εν λόγω πεδίο.

Εικόνα 12: Βήματα Αυτοαξιολόγησης IC-AM



Step 0	Βήμα 0
Step 1	Βήμα 1
Step 2	Βήμα 2
Step 3	Βήμα 3
Step 4	Βήμα 4
Step 5	Βήμα 5
Step 6	Βήμα 6
Step 7	Βήμα 7
Identify a Team to conduct the assessment includiong a person skilled in conducting internal of external assessments and one involved in making improvments.	Προσδιορισμός μιας Ομάδας για τη διενέργεια της αξιολόγησης, η οποία θα περιλαμβάνει ένα άτομο εξειδικευμένο στη διεξαγωγή εσωτερικών ή εξωτερικών αξιολογήσεων εσωτερικών ελέγχων και ένα άτομο που ασχολείται με την υλοποίηση βελτιώσεων.
Familiarize with the IA-CM, onboard all participants with the understanding of the model and its features.	Εξοικείωση με το IA-CM, εξοικείωση όλων των συμμετεχόντων με την κατανόηση του μοντέλου και των χαρακτηριστικών του.
Identify the indicators that appear to be institutionalized by the internal audit activity through discussion among team members.	Προσδιορισμός των δεικτών που προκύπτει ότι έχουν θεσμοθετηθεί από τη δραστηριότητα του εσωτερικού ελέγχου, μέσω συζήτησης με τα μέλη της ομάδας.
Source and review related documentation to the internal audit activity. These are used to identify relevant indicators.	Εύρεση και μελέτη εγγράφων τεκμηρίωσης για τη δραστηριότητα εσωτερικού ελέγχου. Τα εν λόγω έγγραφα χρησιμοποιούνται για τον προσδιορισμό σχετικών δεικτών.
Source and review realted documentation to global organisation and the external environment (regulations, legislative system, financial management regime …).	Εύρεση και εξέταση σχετικών εγγράφων τεκμηρίωσης για τον διεθνή οργανισμό και το εξωτερικό περιβάλλον (κανονισμοί, νομοθετικό σύστημα, καθεστώς χρηματοοικονομικής διαχείρισης...).
Interview senior management and key stakeholders using a simple one-page matrix of the model to gather insights.	Συνέντευξη με την ανώτατη διοίκηση και τους βασικούς ενδιαφερόμενους παράγοντες με τη χρήση ενός απλού μονοσέλιδου πίνακα του μοντέλου για τη συλλογή πληροφοριών.
Based on the results of steps 2-5, confirm which indicators have been institutionalized within the internal audit activity and determine the capacity level.	Βάσει των αποτελεσμάτων των βημάτων 2-5, επιβεβαίωση των δεικτών που έχουν θεσμοθετηθεί στο πλαίσιο της δραστηριότητας εσωτερικού ελέγχου και καθορισμός του επιπέδου ικανότητας.
Present the results of the self-assessment highlighting the activity's strenghts and areas for improvement.	Παρουσίαση των αποτελεσμάτων αυτοαξιολόγησης μέσω της επισήμανσης των πλεονεκτημάτων της δραστηριότητας και των τομέων που επιδέχονται βελτίωση.

A.9 Ο παγκόσμιος δείκτης ασφάλειας στον κυβερνοχώρο (GCI)

Ο Παγκόσμιος Δείκτης Ασφάλειας στον Κυβερνοχώρο (GCI) είναι μια πρωτοβουλία της Διεθνούς Ένωσης Τηλεπικοινωνιών (ΔΕΤ) που αποσκοπεί στην εξέταση της δέσμευσης ασφάλειας στον κυβερνοχώρο και της κατάστασης σε όλες τις περιφέρειες της ΔΕΤ: Αφρική, Αμερική, Αραβικά κράτη, Ασία-Ειρηνικός, ΚΑΚ και Ευρώπη, και τοποθετεί τις χώρες με υψηλή δέσμευση και ενδεδειγμένες πρακτικές στο επίκεντρο. Στόχος του GCI είναι να συνδράμει τις χώρες στον προσδιορισμό τομέων που επιδέχονται βελτίωση στο πεδίο της ασφάλειας στον κυβερνοχώρο, καθώς και να τις κινητροδοτήσει να αναλάβουν δράση για τη βελτίωση της κατάταξής τους, και, συνεπώς, να τις βοηθήσει να αυξήσουν το γενικό επίπεδο ασφάλειας στον κυβερνοχώρο σε παγκόσμιο επίπεδο.

Επειδή ο GCI είναι δείκτης και όχι μοντέλο ωριμότητας, δεν χρησιμοποιεί επίπεδα ωριμότητας αλλά βαθμολογία κατάταξης και σύγκρισης της συνολικής δέσμευσης εθνών και περιφερειών στην ασφάλεια στον κυβερνοχώρο.

Χαρακτηριστικά Γνωρίσματα/ Διαστάσεις

Ο Παγκόσμιος Δείκτης Ασφάλειας στον Κυβερνοχώρο (GCI) βασίζεται στους πέντε πυλώνες της Παγκόσμιας Ατζέντας Ασφάλειας στον Κυβερνοχώρο (GCA). Αυτοί οι πυλώνες σχηματίζουν τους πέντε υποδείκτες του GCI και καθένας εξ αυτών περιλαμβάνει ένα σύνολο δεικτών. Οι πέντε πυλώνες και δείκτες είναι οι εξής:

i **Νομικός**: μέτρα που βασίζονται στην ύπαρξη νομικών οργάνων και πλαισίων που αφορούν την ασφάλεια στον κυβερνοχώρο και το κυβερνοέγκλημα.
- Δίκαιο για το κυβερνοέγκλημα·
- Κανονισμός για την κυβερνοασφάλεια·
- Περιορισμός/έλεγχος της νομοθεσίας για τα ανεπιθύμητα ηλεκτρονικά μηνύματα

ii **Τεχνικός**: μέτρα που βασίζονται στην ύπαρξη τεχνικών οργάνων και πλαισίων που αφορούν την ασφάλεια στον κυβερνοχώρο και το κυβερνοέγκλημα.
- CERT/CIRT/CSRIT·
- Πλαίσιο υλοποίησης προτύπων·
- Οργανισμός Τυποποίησης·
- Τεχνικοί μηχανισμοί και ικανότητες που χρησιμοποιούνται για την καταπολέμηση των ανεπιθύμητων ηλεκτρονικών μηνυμάτων·
- Χρήση υπολογιστικού νέφους για σκοπούς ασφάλειας στον κυβερνοχώρο· και
- Μηχανισμοί διαδικτυακής προστασίας για παιδιά·

iii **Οργανωτικός**: Μέτρα που βασίζονται στην ύπαρξη φορέων και στρατηγικών πολιτικού συντονισμού για την ανάπτυξη της ασφάλειας στον κυβερνοχώρο σε εθνικό επίπεδο.
- Εθνική στρατηγική για την ασφάλεια στον κυβερνοχώρο·
- Αρμόδια Υπηρεσία· και
- Ασφάλεια στον κυβερνοχώρο.

iv **Δημιουργία ικανοτήτων**: μέτρα που βασίζονται στην ύπαρξη έρευνας και ανάπτυξης, προγράμματα εκπαίδευσης και κατάρτισης, πιστοποιημένοι επαγγελματίες και υπηρεσίες δημόσιου τομέα που ενθαρρύνουν την οικοδόμηση ικανοτήτων.
- Εκστρατείες ευαισθητοποίησης του κοινού·
- Πλαίσιο πιστοποίησης και διαπίστευσης επαγγελματιών ασφάλειας στον κυβερνοχώρο·
- Μαθήματα επαγγελματικής κατάρτισης στην ασφάλεια στον κυβερνοχώρο·
- Εκπαιδευτικά προγράμματα ή ακαδημαϊκό πρόγραμμα για την ασφάλεια στον κυβερνοχώρο·
- Προγράμματα Ε&Α στην ασφάλεια στον κυβερνοχώρο· και
- Μηχανισμοί κινητροδότησης.

v **Συνεργασία**: Μέτρα βάσει της ύπαρξης εταιρικών σχέσεων, πλαισίων συνεργασίας και δικτύων ανταλλαγής πληροφοριών.
- Διμερείς συμφωνίες·
- Πολυμερείς συμφωνίες·
- Συμμετοχή σε διεθνή fora/οργανώσεις·
- Εταιρικές σχέσεις δημοσίου-ιδιωτικού τομέα·
- Διυπηρεσιακές/ενδουπηρεσιακές εταιρικές σχέσεις και
- Βέλτιστες πρακτικές.

Μέθοδος αξιολόγησης

Ο GCI είναι ένα εργαλείο αυτοαξιολόγησης που έχει σχεδιαστεί μέσω μιας έρευνας[30] δυαδικών, προκωδικοποιημένων, και ανοιχτών ερωτήσεων. Η χρήση δυαδικών απαντήσεων αποκλείει την αξιολόγηση βάσει γνώμης και οποιαδήποτε πιθανή μεροληψία προς ορισμένους τύπους απαντήσεων. Οι ήδη κωδικοποιημένες απαντήσεις εξοικονομούν χρόνο και επιτρέπουν μεγαλύτερη ακρίβεια κατά την ανάλυση δεδομένων. Επιπλέον, μια διττή κλίμακα επιτρέπει την ταχύτερη και πιο πολύπλοκη αξιολόγηση, διότι δεν απαιτεί μεγάλες απαντήσεις, γεγονός που επιταχύνει και απλουστεύει τη διαδικασία των απαντήσεων και της περαιτέρω αξιολόγησης. Οι συμμετέχοντες θα πρέπει απλώς να επιβεβαιώσουν την παρουσία ή την έλλειψη ορισμένων προκαθορισμένων λύσεων ασφάλειας στον κυβερνοχώρο. Ένας μηχανισμός διαδικτυακής έρευνας που χρησιμοποιείται για τη συλλογή απαντήσεων και τη μεταφόρτωση σχετικού υλικού επιτρέπει την κατάρτιση ορθών πρακτικών και μιας σειράς θεματικών ποιοτικών αξιολογήσεων από ένα πάνελ εμπειρογνωμόνων.

Η συνολική διαδικασία του GCI εφαρμόζεται ως εξής:

- Αποστέλλεται επιστολή πρόσκλησης προς όλους τους συμμετέχοντες, μέσω της οποίας ενημερώνονται για την πρωτοβουλία και τους ζητείται να ορίσουν ένα σημείο επαφής αρμόδιο για τη συλλογή όλων των σχετικών δεδομένων και για τη συμπλήρωση του διαδικτυακού ερωτηματολογίου του GCI. Κατά τη διάρκεια της διαδικτυακής έρευνας, η ΔΕΤ απευθύνει επίσημη πρόσκληση στο σημείο επαφής για τη συμπλήρωση του ερωτηματολογίου·
- Συλλογή πρωτογενών δεδομένων (για χώρες που δεν συμπληρώνουν το ερωτηματολόγιο):
  - Η ΔΕΤ καταρτίζει ένα αρχικό σχέδιο απάντησης στο ερωτηματολόγιο χρησιμοποιώντας δημοσίως διαθέσιμα δεδομένα και διαδικτυακή έρευνα·
  - Το σχέδιο ερωτηματολογίου αποστέλλεται στα σημεία επαφής για αναθεώρηση·
  - Τα σημαία επαφής βελτιώνουν το επίπεδο ακρίβειας του σχεδίου ερωτηματολογίου και το επιστρέφουν·
  - Το διορθωμένο σχέδιο ερωτηματολόγιου αποστέλλεται σε κάθε σημείο επαφής για τελική έγκριση· και
  - Το επαληθευμένο ερωτηματολόγιο χρησιμοποιείται για σκοπούς ανάλυσης, βαθμολόγησης και κατάταξης.
- Συλλογή δευτερογενών δεδομένων (για χώρες που συμπληρώνουν το ερωτηματολόγιο):
  - Η ΔΕΤ εντοπίζει τυχόν ελλείψεις σε απαντήσεις, υποστηρικτικά έγγραφα, συνδέσμους, κ.λπ.·
  - Το σημείο επαφής βελτιώνει την ακρίβεια των απαντήσεων όπου απαιτείται·
  - Το διορθωμένο σχέδιο ερωτηματολόγιου αποστέλλεται σε κάθε σημείο επαφής για τελική έγκριση· και
  - Το επαληθευμένο ερωτηματολόγιο χρησιμοποιείται για σκοπούς ανάλυσης, βαθμολόγησης και κατάταξης.

A.10 Ο Δείκτης Ισχύος Κυβερνοχώρου (CPI)

Ο Δείκτης Ισχύος Κυβερνοχώρου (CPI) σχεδιάστηκε το 2011 στο πλαίσιο του ερευνητικού προγράμματος της μονάδας πληροφοριών του Economist που χρηματοδοτείται από την Booz Allen Hamilton. Ο CPI είναι ένα «δυναμικό ποσοτικό και ποιοτικό μοντέλο, [...] που μετρά συγκεκριμένα χαρακτηριστικά γνωρίσματα του περιβάλλοντος του κυβερνοχώρου σε τέσσερις παράγοντες της ισχύος κυβερνοχώρου: νομικό και κανονιστικό πλαίσιο· οικονομικό και κοινωνικό πλαίσιο· τεχνολογική υποδομή· και εφαρμογή στον τομέα, που εξετάζει την ψηφιακή πρόοδο στους βασικούς τομείς»[31]. Στόχος του Δείκτη Ισχύος Κυβερνοχώρου είναι να αποτελέσει κριτήριο αξιολόγησης της ικανότητας των χωρών της G20 να αντέξουν κυβερνοεπιθέσεις και να αξιοποιήσουν τις απαιτούμενες ψηφιακές υποδομές για μια ακμάζουσα και ασφαλή οικονομία. Η συγκριτική αξιολόγηση που παρέχει ο CPI εστιάζει σε 19 από τις

[30] https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv4/GCIv4_English.pdf
[31] www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/EIU%20-%20Cyber%20Power%20Index%20Findings%20and%20Methodology.pdf

χώρες της G20 (εξαιρουμένης της ΕΕ). Στη συνέχεια, οι χώρες κατατάσσονται για κάθε δείκτη με βάση το σημείο αναφοράς.

Χαρακτηριστικά Γνωρίσματα/ Διαστάσεις

Ο Δείκτης Ισχύος Κυβερνοχώρου (CPI) βασίζεται σε τέσσερις παράγοντες ισχύος κυβερνοχώρου. Κάθε κατηγορία μετράται μέσω πολλαπλών δεικτών για να δοθεί μια συγκεκριμένη βαθμολογία σε κάθε χώρα. Οι κατηγορίες και οι πυλώνες έχουν ως εξής:

i **Νομικό και κανονιστικό πλαίσιο**
- Κυβερνητική δέσμευση για την εξέλιξη στον κυβερνοχώρο
- Πολιτικές προστασίας στον κυβερνοχώρο
- Λογοκρισία στον κυβερνοχώρο (ή έλλειψη λογοκρισίας)
- Πολιτική αποτελεσματικότητα
- Προστασία της διανοητικής ιδιοκτησίας

ii **Οικονομικό και κοινωνικό πλαίσιο**
- Μορφωτικά επίπεδα
- Τεχνικές δεξιότητες
- Ανοικτός χαρακτήρας εμπορίου
- Βαθμός καινοτομίας στο επιχειρηματικό περιβάλλον

iii **Τεχνολογικές υποδομές**
- Πρόσβαση στην τεχνολογία των πληροφοριών και των επικοινωνιών
- Ποιότητα τεχνολογίας των πληροφοριών και των επικοινωνιών
- Οικονομική προσιτότητα τεχνολογίας των πληροφοριών και των επικοινωνιών
- Δαπάνες στην τεχνολογία πληροφοριών
- Αριθμός ασφαλών εξυπηρετητών

iv **Εφαρμογή στον τομέα**
- Έξυπνα δίκτυα
- Ηλεκτρονική υγεία
- Ηλεκτρονικό εμπόριο
- Έξυπνες μεταφορές
- Ηλεκτρονική διακυβέρνηση

Μέθοδος αξιολόγησης

Ο CPI είναι ένα ποσοτικό και ποιοτικό μοντέλο βαθμολόγησης. Η αξιολόγηση διεξήχθη από τη μονάδα πληροφοριών του Economist με τη χρήση ποσοτικών δεικτών από διαθέσιμες στατιστικές πηγές και με τη διατύπωση εκτιμήσεων στις περιπτώσεις που δεν υπήρχαν δεδομένα. Οι κύριες πηγές που αξιοποιήθηκαν ήταν η μονάδα πληροφοριών του Economist· η Εκπαιδευτική Επιστημονική και Πολιτιστική Οργάνωση των Ηνωμένων Εθνών (UNESCO)· η Διεθνής Ένωση Τηλεπικοινωνιών (ΔΕΤ)· και η Παγκόσμια Τράπεζα.

A.11 Ο Δείκτης Ισχύος Κυβερνοχώρου (CPI)

Η παρούσα ενότητα συνοψίζει τα κύρια ευρήματα της ανάλυσης των υφιστάμενων μοντέλων ωριμότητας. Ο Πίνακας 5: Επισκόπηση των μοντέλων ωριμότητας **που** αναλύθηκαν παρέχει μια επισκόπηση των βασικών χαρακτηριστικών κάθε μοντέλου σύμφωνα με το τροποποιημένο μοντέλο του Becker. Ο Πίνακας 6 Σύγκριση Επιπέδων Ωριμότητας παρέχει τους ορισμούς για τα υψηλά επίπεδα ωριμότητας των μοντέλων που αναλύθηκαν. Ο Πίνακας 7 παρέχει μια επισκόπηση των διατάξεων ή των χαρακτηριστικών γνωρισμάτων σε κάθε μοντέλο.

Πίνακας 5: Επισκόπηση των μοντέλων ωριμότητας που αναλύθηκαν

Όνομα μοντέλου	Θεσμική Πηγή	Σκοπός	Στόχος	Αριθμός Επιπέδων	Αριθμός χαρακτηριστικών γνωρισμάτων	Μέθοδος αξιολόγησης	Αναπαράσταση Αποτελεσμάτων
Εθνικό μοντέλο ωριμότητας ικανοτήτων για την ασφάλεια στον κυβερνοχώρο (CMM)	Παγκόσμιο Κέντρο Ικανοτήτων Ασφάλειας στον κυβερνοχώρο Πανεπιστήμιο της Οξφόρδης	Αύξηση της κλίμακας και της αποτελεσματικότητας της δημιουργίας υποδομής ασφάλειας στον κυβερνοχώρο σε παγκόσμιο επίπεδο	Χώρες	5	5 βασικές διαστάσεις	Συνεργασία με τοπικό οργανισμό για την τελειοποίηση του μοντέλου πριν από την εφαρμογή του σε εθνικό πλαίσιο	Ραντάρ πέντε τμημάτων
Μοντέλο ωριμότητας ικανοτήτων ασφάλειας στον κυβερνοχώρο (C2M2)	Υπουργείο Ενέργειας των ΗΠΑ (DOE)	Βοηθά τους οργανισμούς να αξιολογούν και να βελτιώνουν τα οικεία προγράμματα ασφάλειας στον κυβερνοχώρο και να ενισχύουν την επιχειρησιακή ανθεκτικότητά τους	Οργανισμοί κάθε τομέα, τύπου και μεγέθους	4	10 βασικοί τομείς	Μεθοδολογία αυτοαξιολόγησης και εργαλειοθήκη	Κάρτα βαθμολογίας με κυκλικά διαγράμματα
Πλαίσιο για τη βελτίωση της κρίσιμης υποδομής για την ασφάλεια στον κυβερνοχώρο	Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST)	Στόχος του πλαισίου είναι η καθοδήγηση των δραστηριοτήτων για την ασφάλεια στον κυβερνοχώρο και η διαχείριση των κινδύνων στο εσωτερικό ενός οργανισμού	Οργανισμοί	Δ/Υ (4 Βαθμίδες)	5 βασικές λειτουργίες	Αυτοαξιολόγηση	-
Μοντέλο ωριμότητας ικανοτήτων του Κατάρ για την ασφάλεια στον κυβερνοχώρο (Q-C2M2)	Νομική Σχολή Πανεπιστημίου του Κατάρ	Προσφέρει ένα πρακτικό μοντέλο που μπορεί να χρησιμοποιηθεί ως σημείο αναφοράς, για σκοπούς μέτρησης και ανάπτυξης του πλαισίου του Κατάρ για την ασφάλεια στον κυβερνοχώρο	Οργανισμοί του Κατάρ	5	5 βασικοί τομείς	-	-
Πιστοποίηση του μοντέλου ωριμότητας ασφάλειας στον κυβερνοχώρο (CMMC)	Υπουργείο Άμυνας των ΗΠΑ	Ανάπτυξη βέλτιστων πρακτικών για τη διασφάλιση των πληροφοριών	Οργανισμοί τομέα Βιομηχανικής Βάσης Άμυνας (DIB)	5	17 βασικοί τομείς	Αξιολόγηση από εξωτερικούς ελεγκτές	-
Το κοινοτικό μοντέλο ωριμότητας ασφάλειας στον κυβερνοχώρο (CCSMM)	Κέντρο για τη Διασφάλιση και την Ασφάλεια Υποδομών του Πανεπιστημίου του Τέξας	Προσδιορισμός της τρέχουσας κατάστασης μιας κοινότητας ως προς την κυβερνοετοιμότητά της και παροχή ενός χάρτη πορείας τον οποίο μπορούν να ακολουθούν οι κοινότητες στο πλαίσιο των προσπαθειών προετοιμασίας τους.	Κοινότητες (τοπικές ή πολιτειακές κυβερνήσεις)	5	6 βασικές διαστάσεις	Αξιολόγηση εντός κοινοτήτων με πληροφορίες από κρατικές και ομοσπονδιακές υπηρεσίες επιβολής του νόμου	-
Μοντέλο ωριμότητας ασφάλειας των πληροφοριών για το πλαίσιο ασφάλειας στον κυβερνοχώρο του NIST (ISMM)	Σχολή Επιστημών Πληροφορικής και Μηχανικής Πανεπιστήμιο Πετρελαίου και Ορυκτών King Fahd, Dhahran, Σαουδική Αραβία	Παροχή δυνατότητας στους οργανισμούς να μετρούν την πρόοδο υλοποίησης με την πάροδο του χρόνου για να διασφαλιστεί ότι διατηρούν την επιθυμητή θέση ασφαλείας	Οργανισμοί	5	23 τομείς που αξιολογήθηκαν	-	-
Μοντέλο Μονάδας Εσωτερικού Ελέγχου	Ερευνητικό Ίδρυμα του Ινστιτούτου Εσωτερικών Ελεγκτών	Δημιουργία ικανοτήτων και υποστήριξη για τη μονάδα εσωτερικού ελέγχου μέσω αυτοαξιολόγησης στον δημόσιο τομέα	Οργανισμοί δημόσιου τομέα	5	6 στοιχεία	Αυτοαξιολόγηση	-

(MMEE) για τον δημόσιο τομέα							
Ο παγκόσμιος δείκτης ασφάλειας στον κυβερνοχώρο (GCI)	Διεθνής Ένωση Τηλεπικοινωνιών (ΔΕΤ)	Αναθεώρηση της δέσμευσης στην κυβερνοασφάλεια και της κατάστασης ασφάλειας στον κυβερνοχώρο και συνδρομή των χωρών στον προσδιορισμό τομέων που επιδέχονται βελτίωση στον τομέα αυτόν	Χώρες	Δ/Υ	5 πυλώνες	Αυτοαξιολόγηση	Πίνακας κατάταξης
Ο Δείκτης Ισχύος Κυβερνοχώρου (CPI)	Μονάδα πληροφοριών του Economist & Booz Allen Hamilton	Συγκριτική αξιολόγηση της ικανότητας των χωρών της G20 να αντέξουν κυβερνοεπιθέσεις και να αξιοποιήσουν τις απαιτούμενες ψηφιακές υποδομές για μια ακμάζουσα και ασφαλή οικονομία.	Χώρες G20	Δ/Υ	4 κατηγορίες	Συγκριτική αξιολόγηση από τη μονάδα πληροφοριών του Economist (Economist Intelligence Unit)	Πίνακας κατάταξης

Πίνακας 6 Σύγκριση Επιπέδων Ωριμότητας

Μοντέλο	Επίπεδο 1	Επίπεδο 2	Επίπεδο 3	Επίπεδο 4	Επίπεδο 5
Εθνικό μοντέλο ωριμότητας ικανοτήτων για την ασφάλεια στον κυβερνοχώρο (CMM)	**Εκκίνηση** Είτε δεν υφίσταται ωριμότητα ασφάλειας στον κυβερνοχώρο, είτε βρίσκεται σε πολύ πρώιμο στάδιο. Ενδέχεται να υπάρχουν αρχικές συζητήσεις για τη δημιουργία ικανοτήτων ασφάλειας στον κυβερνοχώρο, όμως δεν έχουν αναληφθεί συγκεκριμένες δράσεις. Δεν υπάρχουν εμφανή αποδεικτικά στοιχεία στο παρόν στάδιο.	**Στάδιο Διαμόρφωσης** Ορισμένα χαρακτηριστικά των πτυχών έχουν αρχίσει να αναπτύσσονται και να διαμορφώνονται, όμως ενδέχεται να είναι ad-hoc, ανοργάνωτα, ασαφώς καθορισμένα ή απλώς «νέα». Ωστόσο, υπάρχουν εμφανή τα αποδεικτικά στοιχεία αυτής της δραστηριότητας.	**Παγιωμένο στάδιο** Εφαρμόζονται αποτελεσματικά τα στοιχεία ως προς αυτήν την πτυχή. Ωστόσο, δεν έχει σχεδιαστεί προσεκτικά η σχετική κατανομή των πόρων. Έχουν ληφθεί ελάχιστες συμβιβαστικές αποφάσεις αναφορικά με τις «σχετικές» επενδύσεις στα διάφορα στοιχεία της πτυχής. Ωστόσο, η πτυχή είναι λειτουργική και καθορισμένη.	**Στρατηγικό Στάδιο** Έχουν πραγματοποιηθεί επιλογές όσον αφορά ποια στοιχεία της πτυχής είναι πιο σημαντικά, και ποια είναι λιγότερο σημαντικά για τον συγκεκριμένο οργανισμό ή κράτος. Το στρατηγικό στάδιο αντανακλά το γεγονός ότι αυτές οι επιλογές έχουν ολοκληρωθεί, και εξαρτώνται από τις συνθήκες στη χώρα ή στον οργανισμό.	**Δυναμικό στάδιο** Υφίστανται σαφείς μηχανισμοί για την μεταβολή της στρατηγικής ανάλογα με τις επικρατούσες συνθήκες όπως η τεχνολογία του περιβάλλοντος απειλών, οι συγκρούσεις σε παγκόσμιο επίπεδο ή μια σημαντική αλλαγή σε έναν τομέα ενδιαφέροντος (π.χ. κυβερνοέγκλημα ή ιδιωτική ζωή). Οι δυναμικοί οργανισμοί έχουν αναπτύξει μεθόδους για τη γρήγορη μεταβολή των στρατηγικών. Στα χαρακτηριστικά αυτού του σταδίου περιλαμβάνονται η ταχεία λήψη αποφάσεων, η ανακατανομή των πόρων, και η συνεχής παρακολούθηση του μεταβαλλόμενου περιβάλλοντος.
Μοντέλο ωριμότητας ικανοτήτων ασφάλειας στον κυβερνοχώρο (C2M2)	**MIL0** Δεν εφαρμόζονται οι πρακτικές.	**MIL1** Εφαρμόζονται αρχικές πρακτικές, αλλά σε ad hoc βάση.	**MIL2** Χαρακτηριστικά διαχείρισης: • Οι πρακτικές είναι τεκμηριωμένες· • Παρέχονται επαρκείς πόροι για την υποστήριξη της διαδικασίας·	**MIL3** Χαρακτηριστικά διαχείρισης: • Οι δραστηριότητες κατευθύνονται από πολιτικές (ή άλλες οργανωτικές οδηγίες)· • Καθορίζονται στόχοι απόδοσης για τις δραστηριότητες του τομέα οι οποίοι υπόκεινται σε	-

			• Το προσωπικό που εφαρμόζει τις πρακτικές έχει επαρκείς δεξιότητες και γνώσεις· και • Έχει ανατεθεί η ευθύνη και η αρμοδιότητα για την εφαρμογή των πρακτικών. Χαρακτηριστικό προσέγγισης: • Οι πρακτικές είναι πιο ολοκληρωμένες ή προχωρημένες σε σχέση με το MIL1.	εποπτεία για την παρακολούθηση της επίτευξής τους· και • Οι τεκμηριωμένες πρακτικές για δραστηριότητες του τομέα τυποποιούνται και βελτιώνονται σε όλη την επιχείρηση. Χαρακτηριστικό προσέγγισης: • Οι πρακτικές είναι πιο ολοκληρωμένες ή προχωρημένες σε σχέση με το MIL2.	
Μοντέλο ωριμότητας για την ασφάλεια των πληροφοριών για το πλαίσιο του NIST για την ασφάλεια στον κυβερνοχώρο (ISMM)	**Εκτελεσθείσα Διεργασία**	**Διαχειριζόμενη Διεργασία**	**Πάγια Διεργασία**	**Προβλεπόμενη Διεργασία**	**Διεργασία Βελτιστοποίησης**
Μοντέλο ωριμότητας ικανοτήτων του Κατάρ για την ασφάλεια στον κυβερνοχώρο (Q-C2M2)	**Εκκίνηση** Εφαρμόζονται ad-hoc πρακτικές και διεργασίες ασφάλειας στον κυβερνοχώρο σε μερικούς τομείς.	**Ανάπτυξη** Έχουν υλοποιηθεί πολιτικές και πρακτικές για την ανάπτυξη και τη βελτίωση των δραστηριοτήτων ασφάλειας στον κυβερνοχώρο στους τομείς με στόχο την πρόταση νέων δραστηριοτήτων προς υλοποίηση.	**Υλοποίηση** Έχουν υιοθετηθεί πολιτικές για την υλοποίηση όλων των δραστηριοτήτων ασφάλειας στον κυβερνοχώρο στους τομείς με στόχο την ολοκλήρωση της υλοποίησης σε έναν ορισμένο χρόνο.	**Προσαρμοστική** Πραγματοποιείται αναθεώρηση και επανεξέταση των δραστηριοτήτων ασφάλειας στον κυβερνοχώρο και υιοθετούνται πρακτικές βάσει των προγνωστικών δεικτών που προκύπτουν από προηγούμενες εμπειρίες και μέτρα.	**Ευελιξία** Συνεχίζεται η εφαρμογή του σταδίου της προσαρμογής με επιπλέον έμφαση στην ευελιξία και την ταχύτητα κατά την υλοποίηση των δραστηριοτήτων στους τομείς.
Πιστοποίηση του μοντέλου ωριμότητας ασφάλειας στον κυβερνοχώρο (CMMC)	**Διεργασίες: Υλοποιηθείσες** Επειδή ο οργανισμός μπορεί να είναι σε θέση να υλοποιεί αυτές τις πρακτικές μόνο σε ad hoc βάση και μπορεί να βασίζεται σε τεκμηρίωση ή όχι, η ωριμότητα των διεργασιών δεν αξιολογείται για το Επίπεδο 1. **Πρακτικές: Βασική Κυβερνοϋγιεινή** Το επίπεδο 1 εστιάζει στην προστασία των FCI (Ομοσπονδιακές Συμβατικές Πληροφορίες) και αποτελείται μόνο από πρακτικές που αντιστοιχούν στις βασικές απαιτήσεις διασφάλισης.	**Διεργασίες: Τεκμηριωμένες** Το επίπεδο 2 προϋποθέτει από τον οργανισμό τη θέσπιση και τεκμηρίωση πρακτικών και πολιτικών που θα κατευθύνουν την υλοποίηση των προσπαθειών του CMMC. Η τεκμηρίωση δίνει τη δυνατότητα επαναλαμβανόμενης εφαρμογής των πρακτικών. Οι οργανισμοί αναπτύσσουν ώριμες ικανότητες τεκμηριώνοντας τις διεργασίες τους και εφαρμόζοντάς τις, στη συνέχεια, όπως είναι τεκμηριωμένες. **Πρακτικές: Μέτρια Κυβερνοϋγιεινή** Το επίπεδο 2 λειτουργεί ως πρόοδος από το Επίπεδο 1 στο	**Διεργασίες: Διαχειριζόμενες** Το επίπεδο 3 προϋποθέτει από έναν οργανισμό τη θέσπιση, συντήρηση και υποστήριξη ενός σχεδίου που παρουσιάζει τη διαχείριση δραστηριοτήτων για την υλοποίηση της πρακτικής. Το σχέδιο μπορεί να περιλαμβάνει πληροφορίες σχετικά με αποστολές, στόχους, σχέδια έργων, πόρους, απαιτούμενη κατάρτιση και συμμετοχή σχετικών ενδιαφερόμενων παραγόντων. **Πρακτικές: Καλή Κυβερνοϋγιεινή** Το επίπεδο 3 επικεντρώνεται στην προστασία των CUI και (Ελεγχόμενες Μη Διαβαθμισμένες Πληροφορίες)	**Διεργασίες: Αναθεωρημένες.** Το επίπεδο 4 προϋποθέτει από τον οργανισμό την αναθεώρηση και τη μέτρηση των πρακτικών ως προς την αποτελεσματικότητα. Πέρα από τη μέτρηση των πρακτικών ως προς την αποτελεσματικότητα, οι οργανισμοί σε αυτό το επίπεδο μπορούν να αναλαμβάνουν διορθωτικές ενέργειες όταν είναι απαραίτητο και να ενημερώνουν τα υψηλότερα επίπεδα διοίκησης για καταστάσεις ή ζητήματα σε επαναλαμβανόμενη βάση. **Πρακτικές: Προορατικές** Το επίπεδο 4 επικεντρώνεται στην προστασία των CUI (Ελεγχόμενες	**Διεργασίες: Βελτιστοποίησης** Το επίπεδο 5 προϋποθέτει από τον οργανισμό την τυποποίηση και τη βελτιστοποίηση της υλοποίησης διεργασιών στο εσωτερικό του. **Πρακτικές: Προηγμένες/Προορατικές** Το επίπεδο 5 εστιάζει στην προστασία των CUI (Ελεγχόμενες Μη Διαβαθμισμένες Πληροφορίες). Οι επιπρόσθετες πρακτικές αυξάνουν το βάθος και την εξειδίκευση των ικανοτήτων ασφάλειας στον κυβερνοχώρο.

		Επίπεδο 3 και αποτελείται από ένα υποσύνολο απαιτήσεων ασφαλείας που καθορίζονται στο NIST SP 800-171, καθώς και πρακτικών από άλλα πρότυπα και σημεία αναφοράς.	περιλαμβάνει όλες τις απαιτήσεις ασφαλείας που προσδιορίζονται στο NIST SP 800-171, καθώς και επιπρόσθετες πρακτικές από άλλα πρότυπα και σημεία αναφοράς για τον μετριασμό των απειλών.	Μη Διαβαθμισμένες Πληροφορίες) και περιλαμβάνει ένα υποσύνολο των ενισχυμένων απαιτήσεων ασφαλείας. Αυτές οι πρακτικές βελτιώνουν τις ικανότητες εντοπισμού και απόκρισης ενός οργανισμού για να ανταποκρίνεται και να προσαρμόζεται στις μεταβαλλόμενες τακτικές, τεχνικές και διεργασίες.	
Το κοινοτικό μοντέλο ωριμότητας ασφάλειας στον κυβερνοχώρο (CCSMM)	**Επίγνωση Ασφαλείας** Το βασικό θέμα των δραστηριοτήτων σε αυτό το επίπεδο είναι να διασφαλιστεί ότι τα άτομα και οι οργανισμοί έχουν επίγνωση των απειλών, των προβλημάτων, και των ζητημάτων που σχετίζονται με την ασφάλεια στον κυβερνοχώρο.	**Ανάπτυξη Διεργασιών** Επίπεδο που έχει σχεδιαστεί για να συνδράμει τις κοινότητες στη θέσπιση και τη βελτίωση των διεργασιών ασφάλειας που απαιτούνται για την αποτελεσματική αντιμετώπιση προβλημάτων κυβερνοασφάλειας.	**Αξιοποίηση Πληροφοριών** Έχει σχεδιαστεί για τη βελτίωση των μηχανισμών ανταλλαγής πληροφοριών εντός της κοινότητας προκειμένου η κοινότητα να είναι σε θέση να συσχετίσει φαινομενικά ανομοιογενείς πληροφορίες.	**Ανάπτυξη Τακτικών** Τα στοιχεία αυτού του επιπέδου είναι σχεδιασμένα για την ανάπτυξη καλύτερων και πιο προορατικών μεθόδων για τον εντοπισμό και την αντιμετώπιση επιθέσεων. Σε αυτό το επίπεδο, θα πρέπει να εφαρμόζονται ήδη οι περισσότερες μέθοδοι πρόληψης.	**Πλήρης Επιχειρησιακή Ικανότητα Ασφαλείας** Αυτό το επίπεδο αντιπροσωπεύει τα στοιχεία που θα πρέπει να εφαρμόζονται σε κάθε οργανισμό ώστε να θεωρηθεί πλήρως λειτουργικός και έτοιμος να αντιμετωπίσει κάθε είδους κυβερνοαπειλή.
Μοντέλο Μονάδας Εσωτερικού Ελέγχου (ΜΜΕΕ) για τον δημόσιο τομέα	**Αρχικό** Δεν υφίστανται βιώσιμες, επαναλήψιμες ικανότητες, οι οποίες εξαρτώνται από ατομικές προσπάθειες	**Υποδομή** Βιώσιμες και επαναλήψιμες πρακτικές και διεργασίες	**Ολοκληρωμένο** Εφαρμόζονται ομοιόμορφα πρακτικές διαχείρισης και επαγγελματικές πρακτικές	**Διαχειριζόμενες** Ενσωματώνονται πληροφορίες από το σύνολο του οργανισμού για τη βελτίωση της διακυβέρνησης και της διαχείρισης κινδύνου	**Βελτιστοποίησης** Εκμάθηση από το εσωτερικό και το εξωτερικό του οργανισμού για συνεχή βελτίωση

Πίνακας 7: Σύγκριση Χαρακτηριστικών Γνωρισμάτων/ Διαστάσεων

	Εθνικό μοντέλο ωριμότητας ικανοτήτων για την ασφάλεια στον κυβερνοχώρο (CMM)	Μοντέλο ωριμότητας ικανοτήτων ασφάλειας στον κυβερνοχώρο (C2M2)	Μοντέλο ωριμότητας ικανοτήτων του Κατάρ για την ασφάλεια στον κυβερνοχώρο (Q-C2M2)	Πιστοποίηση του μοντέλου ωριμότητας ασφάλειας στον κυβερνοχώρο (CMMC)	Πιστοποίηση του μοντέλου ωριμότητας ασφάλειας στον κυβερνοχώρο (CMMC)	Μοντέλο ωριμότητας για την ασφάλεια των πληροφοριών για το πλαίσιο του NIST για την ασφάλεια στον κυβερνοχώρο (ISMM)	Πλαίσιο για τη βελτίωση της κρίσιμης υποδομής για την ασφάλεια στον κυβερνοχώρο	Ο παγκόσμιος δείκτης ασφάλειας στον κυβερνοχώρο (GCI)	Ο Δείκτης Ισχύος Κυβερνοχώρου (CPI)
Επίπεδα	Πέντε διαστάσεις που διαιρούνται σε αρκετούς παράγοντες οι οποίοι με τη σειρά τους περιλαμβάνουν πολλαπλές οπτικές και δείκτες (Εικόνα 4)	Δέκα τομείς, συμπεριλαμβανομένου ενός μοναδικού στόχου διαχείρισης και αρκετών στόχων προσέγγισης (Εικόνα 6)	Πέντε τομείς που διαιρούνται σε υποτομείς	Δεκαεπτά τομείς που αναλύονται σε διαδικασίες και αντιστοιχούν σε πολλές ικανότητες που με τη σειρά τους αναλύονται σε πρακτικές (Εικόνα 9).	Έξι βασικές διαστάσεις	Είκοσι τρεις αξιολογούμενοι τομείς	Πέντε Λειτουργίες με υποκείμενες βασικές Κατηγορίες και Υποκατηγορίες (Εικόνα).	Πέντε πυλώνες συμπεριλαμβανομένων αρκετών δεικτών	Τέσσερις κατηγορίες με αρκετούς δείκτες
Χαρακτηριστικά Γνωρίσματα/ Διαστάσεις	i Χάραξη πολιτικής και στρατηγικής για την ασφάλεια στον κυβερνοχώρο· ii Ενθάρρυνση υπεύθυνης κουλτούρας ασφάλειας στον κυβερνοχώρο εντός της κοινωνίας· iii Ανάπτυξη γνώσεων ασφάλειας στον κυβερνοχώρο· iv Θέσπιση αποτελεσματικών νομικών και κανονιστικών πλαισίων· και v Έλεγχος κινδύνων μέσω προτύπων, οργανισμών και τεχνολογιών.	i Διαχείριση κινδύνων· ii Διαχείριση περιουσιακών στοιχείων, αλλαγής και διαμόρφωσης· iii Διαχείριση ταυτότητας και πρόσβασης· iv Διαχείριση απειλών και τρωτών σημείων· v Επίγνωση της κατάστασης· vi Απόκριση σε συμβάντα και περιστατικά· vii Διαχείριση αλυσίδας εφοδιασμού και εξωτερικών εξαρτήσεων· viii Διαχείριση εργατικού δυναμικού· ix Αρχιτεκτονική ασφάλειας στον κυβερνοχώρο· x Διαχείριση προγράμματος ασφάλειας στον κυβερνοχώρο.	i Κατανόηση (Διακυβέρνηση στον κυβερνοχώρο, Περιουσιακά Στοιχεία, Κίνδυνοι και Κατάρτιση)· ii Ασφάλεια (Ασφάλεια Δεδομένων, Τεχνολογική Ασφάλεια, Ασφάλεια του Ελέγχου Πρόσβασης, Ασφάλεια των Επικοινωνιών και Ασφάλεια Προσωπικού)· iii Έκθεση (Παρακολούθηση, Διαχείριση Περιστατικών, Εντοπισμός, Ανάλυση, και Έκθεση)· iv Απόκριση (Σχεδιασμός της Απόκρισης, Μετριασμός και Επικοινωνία της Απόκρισης)· v Συντήρηση (Σχεδιασμός της Ανάκαμψης, Διαχείριση της Συνέχειας, Βελτίωση και Εξωτερικές Εξαρτήσεις).	i Έλεγχος πρόσβασης· ii Διαχείριση περιουσιακών στοιχείων· iii Λογιστικός έλεγχος και λογοδοσία· iv Ενημέρωση και κατάρτιση· v Διαχείριση διαμόρφωσης· vi Ταυτοποίηση και επαλήθευση ταυτότητας· vii Απόκριση σε περιστατικά· viii Συντήρηση· ix Προστασία μέσων· x Ασφάλεια προσωπικού· xi Φυσική προστασία· xii Ανάκαμψη· xiii Διαχείριση κινδύνων· xiv Αξιολόγηση ασφάλειας· xv Επίγνωση της κατάστασης· xvi Προστασία συστήματος και επικοινωνιών xvii Ακεραιότητα συστήματος και πληροφοριών	i Απειλές που αντιμετωπίζονται· ii Ποσοτικοί δείκτες· iii Ανταλλαγή πληροφοριών· iv Τεχνολογία· v Κατάρτιση· vi Δοκιμή.	i Διαχείριση περιουσιακών στοιχείων· ii Επιχειρηματικό περιβάλλον· iii Διακυβέρνηση· iv Εκτίμηση κινδύνου· v Στρατηγική διαχείρισης κινδύνων· vi Αξιολόγηση συμμόρφωσης· vii Έλεγχος πρόσβασης· viii Ενημέρωση και κατάρτιση· ix Ασφάλεια δεδομένων· x Διεργασίες και διαδικασίες προστασίας πληροφοριών· xi Συντήρηση· xii Προστατευτική τεχνολογία· xiii Ανωμαλίες και συμβάντα· xiv Συνεχής παρακολούθηση ασφαλείας· xv Διεργασίες εντοπισμού· xvi Σχεδιασμός απόκρισης· xvii Επικοινωνίες απόκρισης· xviii Ανάλυση απόκρισης· xix Μετριασμός απόκρισης· xx Βελτιώσεις απόκρισης· xxi Σχεδιασμός ανάκαμψης· xxii Βελτιώσεις ανάκαμψης· xxiii Επικοινωνίες ανάκαμψης.	i Προσδιορισμός· ii Προστασία· iii Εντοπισμός· iv Απόκριση· v Ανάκαμψη.	i Νομικός· ii Τεχνικός· iii Οργανωτικός· iv Δημιουργία ικανοτήτων· v Συνεργασία.	i Νομικό και κανονιστικό πλαίσιο· ii Οικονομικό και κοινωνικό πλαίσιο· iii Τεχνολογικές υποδομές· iv Εφαρμογή στον τομέα.

ΠΑΡΑΡΤΗΜΑ Β – ΒΙΒΛΙΟΓΡΑΦΙΑ ΤΗΣ ΔΕΥΤΕΡΟΓΕΝΟΥΣ ΕΡΕΥΝΑΣ ΤΕΚΜΗΡΙΩΣΗΣ

Almuhammadi, S. and Alsaleh, M. (2017) «Information Security Maturity Model for Nist Cyber Security Framework», στο επιστημονικό περιοδικό Computer Science & Information Technology (CS & IT). Έκτη Διεθνής Διάσκεψη για την Σύγκλιση της Τεχνολογίας πληροφοριών και τις Υπηρεσίες, Κέντρο Συνεργασίας Ακαδημαϊκής και Βιομηχανικής Έρευνας (AIRCC).

Almuhammadi, S. and Alsaleh, M. (2017) «Information Security Maturity Model for Nist Cyber Security Framework», στο επιστημονικό περιοδικό Computer Science & Information Technology (CS & IT). Διατίθεται στη διεύθυνση: https://airccj.org/CSCP/vol7/csit76505.pdf

Anna, S. et al. (2016) Stocktaking, analysis and recommendations on the protection of CIIs. Διατίθεται στη διεύθυνση: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0415821:EN:HTML

Becker, J., Knackstedt, R. et al. (2009) Developing Maturity Models for IT Management – A Procedure Model and its Application. Διατίθεται στη διεύθυνση: https://link.springer.com/content/pdf/10.1007/s12599-009-0044-5.pdf.

Η στρατηγική ασφάλειας στον κυβερνοχώρο της κυβέρνησης του Βελγίου (2012) Διατίθεται στη διεύθυνση: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/belgian-cyber-security-strategy/@@download_version/a9d8b992ee7441769e647ea7120d7e67/file_en

Bellasio, J. et al. (2018) Developing Cybersecurity Capacity: A proof-of-concept implementation guide. RAND Corporation. Διατίθεται στη διεύθυνση: https://www.rand.org/content/dam/rand/pubs/research_reports/RR2000/RR2072/RAND_RR2072.pdf

Bourgue, R. (2012) «Introduction to Return on Security Investment».

Πανεπιστήμιο Carnegie Mellon Ινστιτούτο Μηχανικής Λογισμικού Pittsburg Ηνωμένες Πολιτείες (2019) «Cybersecurity Capability Maturity Model (C2M2) Version 2.0.» Διατίθεται στην διεύθυνση https://apps.dtic.mil/sti/pdfs/AD1078768.pdf

Center for Security Studies (CSS), ETH Zürich (2019) National Cybersecurity Strategies in Comparison – Challenges for Switzerland. Διατίθεται στη διεύθυνση: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2019-08-National%20Cybersecurity%20Strategies%20in%20Comparison.pdf

Πορτογαλικό Υπουργικό Συμβούλιο (2019) Επίσημη Εφημερίδα Πορτογαλίας Τόμος 1 — Αριθ. 108 - Ψήφισμα Υπουργικού Συμβουλίου αριθ. 92/2019. Διατίθεται στη διεύθυνση: https://cncs.gov.pt/content/files/portugal_-_ncss_2019_2023_en.pdf

Creese, S. (2016) Cybersecurity Capacity Maturity Model for Nations (CMM). Πανεπιστήμιο της Οξφόρδης.

CSIRT Maturity - Self-assessment Tool (χωρίς ημερομηνία). Διατίθεται στη διεύθυνση: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-maturity-self-assessment-survey

Έργο CyberCrime@IPA του Συμβουλίου της Ευρώπης και της Ευρωπαϊκής Ένωσης, Global Project on Cybercrime of the Council of Europe and European Union Cybercrime Task Force (2011) Specialised cybercrime units - Good practice study. Διατίθεται στη διεύθυνση: https://rm.coe.int/2467-htcu-study-v30-9nov11/16802f6a33

Σύστημα υποβολής αναφορών και ανάλυσης περιστατικών στον κυβερνοχώρο – Visual Analysis Tool (χωρίς ημερομηνία). Διατίθεται στη διεύθυνση: https://www.enisa.europa.eu/topics/incident-reporting/cybersecurity-incident-report-and-analysis-system-visual-analysis/visual-tool

Darra, E. (2017) Public Private Partnerships (PPP).

Darra, E. (χωρίς ημερομηνία) «Welcome to the NCSS Training Tool».

Dekker, M. A. C. (2014) Technical Guideline on Incident Reporting. Διατίθεται στη διεύθυνση: https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting/Article_13a_ENISA_Technical_Guideline_On_Incident_Reporting_v2_1.pdf

Dekker, M. A. C. (2014) Technical Guideline on Security Measures. Διατίθεται στη διεύθυνση: https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures/Article_13a_ENISA_Technical_Guideline_On_Security_Measures_v2_0.pdf

Dekker, M. A. C. (2015) Guideline on Threats and Assets. Διατίθεται στη διεύθυνση: https://resilience.enisa.europa.eu/article-13/guideline_on_threats_and_assets/Guideline_on_Threats_and_Assets_v_1_1.pdf

Ψηφιακή Σλοβενία (2016) Στρατηγική κυβερνοασφάλειας. Διατίθεται στη διεύθυνση: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-in-slovenia

Domingo-Ferrer, J. *et al.* (2014) *Privacy and data protection by design - from policy to engineering.* Διατίθεται στη διεύθυνση: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0514111:EN:HTML

Ευρωπαϊκή Επιτροπή (2012) Κανονισμός του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά. Διατίθεται στη διεύθυνση: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52012PC0238&from=EL

Οργανισμός της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών (2012) NCSS: Practical Guide on Development and Execution. Ηράκλειο: ENISA.

Οργανισμός της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών (2012) NCSS: Setting the course for national efforts to strengthen security in cyberspac. Ηράκλειο: ENISA.

Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (2016) Guidelines for SMEs on the security of personal data processing.

Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (2016) NCSS good practice guide: designing and implementing national cyber security strategies. Ηράκλειο: ENISA.

Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (2017) Handbook on security of personal data processing. Διατίθεται στη διεύθυνση: http://dx.publications.europa.eu/10.2824/569768

Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (2014) *ENISA CERT inventory inventory of CERT teams and activities in Europe*. Διατίθεται στη διεύθυνση: http://www.enisa.europa.eu/activities/cert/background/inv/files/inventory-of-cert-activities-in-europe

Εκτελεστικό Γραφείο του Προέδρου (2015) Memorandum for Heads of Executive Departments and Agencies. Διατίθεται στη διεύθυνση: https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-04.pdf

Ομοσπονδιακή Καγκελαρία της Δημοκρατίας της Αυστρίας (2013) Αυστριακή στρατηγική για την ασφάλεια στον κυβερνοχώρο. Διατίθεται στη διεύθυνση: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/austrian-cyber-security-strategy/@@download_version/1573800e2e4448b9bdaead56a590305a/file_en

Ομοσπονδιακό Υπουργείο Εσωτερικών Υποθέσεων (2011) Στρατηγική για την ασφάλεια στον κυβερνοχώρο για τη Γερμανία. Διατίθεται στη διεύθυνση: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-for-germany/@@download_version/8adc42e23e194488b2981ce41d9de93e/file_en

Ferette, L. (2016) NIS Directive and national (2015) Information security and privacy standards for SMEs: recommendations to improve the adoption of information security and privacy standards in small and medium enterprises. Διατίθεται στη διεύθυνση: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0215977:EN:HTML

Ferette, L., European Union and European Network and Information Security Agency (2015) The 2015 report on national and international cyber security exercises: survey, analysis and recommendations. Διατίθεται στη διεύθυνση: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0115948:EN:HTML

Γραφείο πρωθυπουργού της Γαλλίας (2014) Εθνική ψηφιακή στρατηγική ασφαλείας. Διατίθεται στη διεύθυνση: https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf

Galan Manso, C. et al. (2015) Information security and privacy standards for SMEs: recommendations to improve the adoption of information security and privacy standards in small and medium enterprises. Διατίθεται στη διεύθυνση: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0215977:EN:HTML

Πανεπιστήμιο της Γάνδης et al. (2017) «Evaluating Business Process Maturity Model», Journal of the Association for Information Systems. Διατίθεται στη διεύθυνση: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1775&context=jais

Κυβέρνηση της Βουλγαρίας (2015) Εθνική στρατηγική για την ασφάλεια στον κυβερνοχώρο - Ανθεκτικότητα της Βουλγαρίας στον κυβερνοχώρο για το 2020.

Κυβέρνηση της Κροατίας (2015) Η εθνική στρατηγική για την ασφάλεια στον κυβερνοχώρο της Δημοκρατίας της Κροατίας. Διατίθεται στη διεύθυνση: https://www.uvns.hr/UserDocsImages/en/dokumenti/Croatian%20National%20Cyber%20Security%20Strategy%20(2015).pdf

Κυβέρνηση της Ελλάδας (2017) Εθνική στρατηγική κυβερνοασφάλειας Διατίθεται στη διεύθυνση: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-greece/view

Κυβέρνηση της Ουγγαρίας (2018) Στρατηγική για την ασφάλεια συστημάτων δικτύων και πληροφοριών Διατίθεται στη διεύθυνση: https://www.kormany.hu/download/2/f9/81000/Strat%C3%A9gia%20honlapon%20k%C3%B6zz%C3%A9t%C3%A9telre-20180103_4829494_2_20190103130721.pdf#!DocumentBrowse

Κυβέρνηση της Ιρλανδίας (2019) Εθνική στρατηγική για την ασφάλεια στον κυβερνοχώρο. Διατίθεται στη διεύθυνση: https://www.dccae.gov.ie/documents/National_Cyber_Security_Strategy.pdf

Κυβέρνηση της Ισπανίας (2019) Εθνική στρατηγική για την ασφάλεια στον κυβερνοχώρο. Διατίθεται στη διεύθυνση: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/the-national-security-strategy/@@download_version/5288044fda714a58b5ca6472a4fd1b28/file_en

Ινστιτούτο Εσωτερικών Ελεγκτών (εκδ.) (2009) Internal audit capability model (IA-CM) for the public sector: overview and application guide. Altamonte Springs, Fla: Ερευνητικό Ίδρυμα του Ινστιτούτου Εσωτερικών Ελεγκτών

Διεθνής Ένωση Τηλεπικοινωνιών (ITU) (2018) The Global Cybersecurity Index. Διατίθεται στη διεύθυνση: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Διεθνής Ένωση Τηλεπικοινωνιών (ITU) (2018) Guide to developing a national cybersecurity strategy. Διατίθεται στη διεύθυνση: https://ccdcoe.org/uploads/2018/10/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

J.D., R. D. B. (2019) «Towards a Qatar Cybersecurity Capability Maturity Model with a Legislative Framework», International Review of Law.

Κυβέρνηση της Λετονίας (2014) Στρατηγική της Λετονίας για την ασφάλεια στον κυβερνοχώρο. Διατίθεται στη διεύθυνση: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss

Liveri, D. et al. (2014) An evaluation framework for national cyber security strategies. Ηράκλειο: ENISA. Διατίθεται στη διεύθυνση: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0714017:EN:HTML.

Mattioli, R. *et al.* (2014) *Methodologies for the identification of critical information infrastructure assets and services: guidelines for charting electronic data communication networks.* Διατίθεται στη διεύθυνση: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0614120:EN:HTML

Υπουργείο Ανταγωνιστικότητας και Ψηφιακής και Ναυτικής Οικονομίας και Οικονομίας Υπηρεσιών (2016) Στρατηγική κυβερνοασφάλειας της Μάλτας Διατίθεται στη διεύθυνση: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-of-malta

Υπουργείο Οικονομικών Υποθέσεων και Επικοινωνιών (2019) Στρατηγική ασφάλειας στον κυβερνοχώρο – Δημοκρατία της Εσθονίας Διατίθεται στη διεύθυνση: https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf

Υπουργείο Εθνικής Άμυνας Δημοκρατίας της Λιθουανίας (2018) Εθνική στρατηγική για την ασφάλεια στον κυβερνοχώρο

Εθνικό Κέντρο Ασφάλειας στον Κυβερνοχώρο (2015) Εθνική στρατηγική για την ασφάλεια στον κυβερνοχώρο της Τσεχικής Δημοκρατίας. Διατίθεται στη διεύθυνση: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf

Εθνικές Στρατηγικές για την Ασφάλεια στον Κυβερνοχώρο - Διαδραστικός Χάρτης (χωρίς ημερομηνία). Διατίθεται στη διεύθυνση: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map.

Εργαλείο Αξιολόγησης Εθνικών Στρατηγικών Ασφάλειας στον Κυβερνοχώρο (2018). Διατίθεται στη διεύθυνση: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool.

Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (2018) Framework for Improving Critical Infrastructure Cybersecurity, έκδοση 1.1 Gaithersburg, MD: Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας Διατίθεται στη διεύθυνση: http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

Object Management Group (2008) Business Process Maturity Model. Διατίθεται στη διεύθυνση: https://www.omg.org/spec/BPMM/1.0/PDF

ΟΟΣΑ, Ευρωπαϊκή Ένωση και Κοινό Κέντρο Ερευνών - Ευρωπαϊκή Επιτροπή (2008) Handbook on Constructing Composite Indicators: Methodology and User Guide. OECD. Διατίθεται στη διεύθυνση: https://www.oecd.org/sdd/42495745.pdf.

Γραφείο Επιτρόπου Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομείων (2012) Στρατηγική Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας.

Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης (2008) ΟΔΗΓΙΑ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ 2008/114/ΕΚ, της 8ης Δεκεμβρίου 2008, σχετικά με τον προσδιορισμό και τον χαρακτηρισμό των ευρωπαϊκών υποδομών ζωτικής σημασίας, και σχετικά με την αξιολόγηση της ανάγκης βελτίωσης της προστασίας τους. Διατίθεται στη διεύθυνση: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32008L0114&from=EL

Οργανισμός για την Οικονομική Συνεργασία και Ανάπτυξη (ΟΟΣΑ) (2012) Cybersecurity policy making at a turning point. Διατίθεται στη διεύθυνση: http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

Ουζούνης, Ε. (2012) «National Cyber Security Strategies - Practical Guide on Development and Execution».

Ουζούνης, Ε. (2012) Good Practice Guide on National Exercises.

Portesi, S. (2017) Improving Cooperation between CSIRTs and Law Enforcement: Legal and Organisational Aspects

Προεδρία του Υπουργικού Συμβουλίου (2017) Το ιταλικό σχέδιο δράσης για την ασφάλεια στον κυβερνοχώρο. Διατίθεται στη διεύθυνση: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-strategic-framework-for-cyberspace-security

Rady Ministrów (2019) Dziennik Urzędowy Rzeczypospolitej Polskiej. Διατίθεται στη διεύθυνση: http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf

Κυβέρνηση της Ρουμανίας (2013) Στρατηγική της Ρουμανίας για την ασφάλεια στον κυβερνοχώρο. Διατίθεται στη διεύθυνση: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-in-romania

Σαρρή, Α., Κυρανούδη, Π. και Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (2019) Good practices in innovation on cybersecurity under the NCSS: good practices in innovation on cybersecurity under the national cyber security strategies. Διατίθεται στη διεύθυνση: https://op.europa.eu/publication/manifestation_identifier/PUB_TP0119830ENN.

Γενική Γραμματεία της Επιτροπής Ασφαλείας (2019) Στρατηγική της Φινλανδίας για την ασφάλεια στον κυβερνοχώρο 2019. Διατίθεται στη διεύθυνση: https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf

Κυβέρνηση της Σλοβακίας (2015) Έννοια της ασφάλειας στον κυβερνοχώρο στη Δημοκρατία της Σλοβακίας. Διατίθεται στη διεύθυνση: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-concept-of-the-slovak-republic

Smith, R. (2015) Directive 2016/1148 /EU of the European Parliament and of the Council of 7 July 2010

Smith, R. (2016) «Directive 2016/1148 /EU of the European Parliament and of the Council of 7 July 2010», στο έργο Smith, R., Core EU Legislation. London: Macmillan Education. Διατίθεται στη διεύθυνση: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016L1148&from=EL.

Σταυρόπουλος, Β. (2017) European Cyber Security Month 2017.

Κυβέρνηση της Σουηδίας (2017) Nationell strategi för samhällets informations- och cybersäkerhet. Διατίθεται στη διεύθυνση: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/swedish-ncss/view

Κυβέρνηση της Δανίας - Υπουργείο Οικονομικών (2018) Δανική στρατηγική για την ασφάλεια στον κυβερνοχώρο και την ασφάλεια των πληροφοριών. Διατίθεται στη διεύθυνση: https://en.digst.dk/media/17189/danish_cyber_and_information_security_strategy_pdf.pdf

Ομοσπονδιακό Συμβούλιο (2018) Εθνική στρατηγική για την προστασία της Ελβετίας έναντι κινδύνων στον κυβερνοχώρο.

Κυβερνητικό Συμβούλιο του Λουξεμβούργου (2018) Εθνική στρατηγική για την ασφάλεια στον κυβερνοχώρο Διατίθεται στη διεύθυνση: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/strategie-nationale-en-matiere-de-cyber-securite/@@download_version/d4af182d7c6e4545ae751c17fcca9cfe/file_en

Κυβέρνηση των Κάτω Χωρών (2018) Εθνική ατζέντα για την ασφάλεια στον κυβερνοχώρο Διατίθεται στη διεύθυνση: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-1/@@download_version/82b3c1a34de449f48cef8534b513caea/file_en

Ο Λευκός Οίκος (2018) National Cyber Strategy of the United States of America. Διατίθεται στη διεύθυνση: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

Τριμίντζιος, Π., et al. (2011) Cyber Europe Report. Διατίθεται στη διεύθυνση: https://www.enisa.europa.eu/publications/ce2010report

Τριμίντζιος, Π., Γαβρίλα, Ρ. και Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (2013) *National-level risk assessments: an analysis report.* Διατίθεται στη διεύθυνση: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0413112:EN:HTML

Τριμίντζιος, Π., Γαβρίλα, Ρ., et al. (2015) Report on cyber-crisis cooperation and management. Διατίθεται στη διεύθυνση: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0514030:EN:HTML

Τριμίντζιος, Π., Ogee, A., et al. (2015) Report on cyber crisis cooperation and management: common practices of EU-level crisis management and applicability to cyber crises. Διατίθεται στη διεύθυνση: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0115966:EN:HTML

Εθνική Στρατηγική για την Ασφάλεια στον Κυβερνοχώρο·του Ηνωμένου Βασιλείου για την περίοδο 2016-2021 (2016). Διατίθεται στη διεύθυνση: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

Πανεπιστήμιο του Ίνσμπρουκ et al. (2009) Understanding Maturity Models.

Wamala, D. F. (2011) «ITU National Cybersecurity Strategy Guide. Διατίθεται στη διεύθυνση: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

White, G. (2007) 'The Community Cyber Security Maturity Model', in 2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)

ΠΑΡΑΡΤΗΜΑ Γ – ΆΛΛΟΙ ΣΤΟΧΟΙ ΠΟΥ ΕΞΕΤΑΣΤΗΚΑΝ

Οι στόχοι που αναλύονται παρακάτω μελετήθηκαν στο πλαίσιο του σταδίου της δευτερογενούς έρευνας τεκμηρίωσης και των συνεντεύξεων που πραγματοποιήθηκαν από τον ENISA. Οι παρακάτω στόχοι δεν εντάσσονται στο Εθνικό Πλαίσιο Αξιολόγησης Ικανοτήτων, όμως επισημαίνουν θέματα που αξίζει να συζητηθούν. Καθένα από τα παρακάτω υποκεφάλαια εξηγεί τους λόγους απόρριψης του στόχου.

- Ανάπτυξη ειδικών ανά τομέα στρατηγικών ασφάλειας στον κυβερνοχώρο·
- Καταπολέμηση των εκστρατειών παραπληροφόρησης·
- Διασφάλιση τεχνολογιών αιχμής (5G, TN, κβαντική υπολογιστική...)·
- Διασφάλιση της κυριαρχίας των δεδομένων· και
- Παροχή κινήτρων για την ανάπτυξη του τομέα της ασφάλισης στον κυβερνοχώρο.

Ανάπτυξη ειδικών ανά τομέα στρατηγικών ασφάλειας στον κυβερνοχώρο

Η έγκριση ειδικών ανά τομέα στρατηγικών που αφορούν τομεακές παρεμβάσεις και κίνητρα εισάγει σαφώς μια ισχυρότερη αποκεντρωμένη ικανότητα. Ενδείκνυται ιδιαίτερα για κράτη μέλη όπου οι φορείς εκμετάλλευσης βασικών υπηρεσιών είναι αντιμέτωποι με διαφορετικά πλαίσια και κανονισμούς και υφίστανται πολλές εξαρτήσεις λόγω της οριζόντιας φύσης της κυβερνοασφάλειας. Πράγματι, σε αρκετά κράτη μέλη, είναι σύνηθες να υφίστανται δεκάδες εθνικές αρχές και ρυθμιστικοί φορείς που γνωρίζουν τις ιδιαιτερότητες κάθε τομέα και έχουν ως αποστολή την επιβολή συγκεκριμένης ρύθμισης για κάθε τομέα.

Η Δανία, για παράδειγμα, κατάρτισε έξι στοχευμένες στρατηγικές που αφορούν προσπάθειες για τη διασφάλιση της κυβερνοασφάλειας και της ασφάλειας των πληροφοριών στους πιο κρίσιμους τομείς για την ανάπτυξη μιας πιο ισχυρής αποκεντρωμένης ικανότητας στην κυβερνοασφάλεια και την ασφάλεια των πληροφοριών. Κάθε «τομεακή ενότητα» θα συμβάλλει, μεταξύ άλλων, σε αξιολογήσεις απειλών σε τομεακό επίπεδο, στην παρακολούθηση, σε ασκήσεις ετοιμότητας, στη δημιουργία συστημάτων ασφαλείας, στην ανταλλαγή γνώσεων και σε οδηγίες. Οι ειδικές ανά τομέα στρατηγικές καλύπτουν τους εξής τομείς:

- Ενέργεια·
- Ιατροφαρμακευτική περίθαλψη·
- Μεταφορές·
- Τηλεπικοινωνίες·
- Χρηματοπιστωτικό Σύστημα· και
- Ναυτιλία.

Άλλα κράτη μέλη έχουν εκφράσει το ενδιαφέρουν τους για τη χάραξη ειδικών ανά τομέα στρατηγικών ασφάλειας στον κυβερνοχώρο που αντανακλούν όλες τις κανονιστικές απαιτήσεις. Ωστόσο, πρέπει να σημειωθεί ότι ένας τέτοιος στόχος μπορεί να μην ενδείκνυται για όλα τα κράτη μέλη ανάλογα με το μέγεθος, τις εθνικές πολιτικές και την ωριμότητά τους. Επειδή είναι ιδιαίτερα δύσκολο να διασφαλιστεί ότι το πλαίσιο μπορεί να περιλαμβάνει όλες τις ιδιαιτερότητες, ο ENISA δεν συμπεριέλαβε αυτόν τον στόχο στο πλαίσιο.

Καταπολέμηση των εκστρατειών παραπληροφόρησης

Τα κράτη μέλη ενσωματώνουν την προστασία θεμελιωδών αρχών όπως τα ανθρώπινα δικαιώματα, η διαφάνεια και η εμπιστοσύνη του κοινού στις οικείες εθνικές στρατηγικές ασφάλειας στον κυβερνοχώρο. Αυτό είναι πολύ σημαντικό ιδίως όσον αφορά την παραπληροφόρηση που διαδίδεται από τα παραδοσιακά μέσα ενημέρωσης ή από πλατφόρμες κοινωνικής δικτύωσης. Επιπλέον, η ασφάλεια στον κυβερνοχώρο είναι μία από τις μεγαλύτερες προκλήσεις των εκλογών. Πράγματι, έχουν παρατηρηθεί δραστηριότητες όπως η διάδοση ψευδών πληροφοριών ή αρνητικής προπαγάνδας σε διάφορες χώρες ενόψει σημαντικών εκλογών. Αυτή η απειλή θα μπορούσε να υπονομεύσει τη δημοκρατική διαδικασία στην ΕΕ. Σε ευρωπαϊκό επίπεδο, η Επιτροπή έχει καταρτίσει ένα Σχέδιο Δράσης[32] για την ενίσχυση των προσπαθειών για την αντιμετώπιση της παραπληροφόρησης στην Ευρώπη: το εν λόγω σχέδιο εστιάζεται σε 4 βασικούς τομείς (εντοπισμός, συνεργασία, συνεργασία με διαδικτυακές πλατφόρμες και ευαισθητοποίηση) και συμβάλλει στη δημιουργία των ικανοτήτων της ΕΕ και την ενίσχυση της συνεργασίας μεταξύ των κρατών μελών.

4 από τις 19 χώρες που συμμετείχαν στις συνεντεύξεις έχουν εκφράσει την πρόθεσή τους να αντιμετωπίσουν το ζήτημα της παραπληροφόρησης και της προπαγάνδας στην ΕΣΑΚ τους.

Για παράδειγμα, η γαλλική ΕΣΑΚ[33] σημειώνει ότι: «το κράτος είναι αρμόδιο για την ενημέρωση των πολιτών σχετικά με τους κινδύνους χειραγώγησης και τις τεχνικές προπαγάνδας που χρησιμοποιούν οι κακόβουλοι παράγοντες του Διαδικτύου. Για παράδειγμα, μετά τις τρομοκρατικές επιθέσεις κατά της Γαλλίας τον Ιανουάριο του 2015, η κυβέρνηση δημιούργησε μια πλατφόρμα πληροφόρησης σχετικά με τους κινδύνους που αφορούν την ισλαμική ριζοσπαστικοποίηση μέσω ηλεκτρονικών δικτύων επικοινωνίας: « Stop-djihadisme.gouv.fr ». Αυτή η προσέγγιση θα μπορούσε να επεκταθεί για να ανταποκρίνεται σε άλλα φαινόμενα προπαγάνδας ή αποσταθεροποίησης.

Ένα άλλο παράδειγμα είναι η πολωνική ΕΣΑΚ για την περίοδο 2019-2024[34] η οποία αναφέρει ότι: «για την αντιμετώπιση δραστηριοτήτων χειραγώγησης όπως οι εκστρατείες παραπληροφόρησης, απαιτούνται συστημικές δράσης για την ευαισθητοποίηση των πολιτών στο πλαίσιο της επαλήθευσης της αυθεντικότητας των πληροφοριών και της απόκρισης σε προσπάθειες διαστρέβλωσής της».

Ωστόσο, κατά τη διάρκεια των συνεντεύξεων του ENISA, αρκετά κράτη μέλη δήλωσαν ότι δεν αντιμετωπίζουν το ζήτημα στο πλαίσιο της ΕΣΑΚ τους ως κυβερνοαπειλή, αλλά σε ένα ευρύτερο κοινωνικό επίπεδο, λόγου χάρη, μέσω πρωτοβουλιών πολιτικής.

Διασφάλιση τεχνολογιών αιχμής (5G, TN, κβαντική υπολογιστική...)

Καθώς το σύγχρονο τοπίο κυβερνοαπειλών εξακολουθεί να επεκτείνεται, η ανάπτυξη νέων τεχνολογιών θα οδηγήσει κατά πάσα πιθανότητα σε αύξηση της έντασης και του αριθμού των κυβερνοεπιθέσεων και στη διαφοροποίηση των μεθόδων, των μέσων και των στόχων των παραγόντων απειλής. Παράλληλα, αυτές οι νέες τεχνολογικές λύσεις υπό τη μορφή τεχνολογιών αιχμής θα μπορούσαν να λειτουργήσουν ως δομικά στοιχεία της ευρωπαϊκής ψηφιακής αγοράς. Για τη διαφύλαξη της αυξανόμενης ψηφιακής ανεξαρτησίας των κρατών μελών και της ανάδυσης νέων τεχνολογιών, είναι απαραίτητη η δημιουργία κινήτρων και η χάραξη πλήρως ανεπτυγμένων πολιτικών για την υποστήριξη της ασφαλούς και αξιόπιστης ανάπτυξης και αξιοποίησης αυτών των τεχνολογιών στην ΕΕ.

Στη διάρκεια του σταδίου της δευτερογενούς έρευνας τεκμηρίωσης που πραγματοποιήθηκε στις ΕΣΑΚ των κρατών μελών, προέκυψε ότι οι τεχνολογίες αιχμής που ενδιαφέρουν τα κράτη μέλη είναι οι εξής: 5G, TN, κβαντική υπολογιστική, κρυπτογραφία, υπολογιστική παρυφής,

[32] https://ec.europa.eu/digital-single-market/el/news/action-plan-against-disinformation
[33] https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf
[34] http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf

συνδεδεμένα και αυτόνομα οχήματα, μεγάλα και έξυπνα δεδομένα, αλυσίδα συστοιχιών, ρομποτική και διαδίκτυο των πραγμάτων.

Πιο συγκεκριμένα, στις αρχές του 2020, η Ευρωπαϊκή Επιτροπή εξέδωσε ανακοίνωση καλώντας τα κράτη μέλη να αναλάβουν ενέργειες για την εφαρμογή του συνόλου των μέτρων που συνιστώνται στα συμπεράσματα σχετικά με την εργαλειοθήκη για την κυβερνοασφάλεια των δικτύων 5G[35]. Αυτή η εργαλειοθήκη για την κυβερνοασφάλεια των δικτύων 5G δημοσιεύεται στον απόηχο της σύστασης (ΕΕ) 2019/534 σχετικά με την κυβερνοασφάλεια δικτύων 5G που εξέδωσε η Επιτροπή το 2019, μέσω της οποίας απηύθυνε έκκληση για μια ενοποιημένη ευρωπαϊκή προσέγγιση όσον αφορά την ασφάλεια των δικτύων 5G[36].

Κατά τη διάρκεια των συνεντεύξεων που πραγματοποίησε ο ENISA, επισημάνθηκε ότι αυτό το ζήτημα είναι κυρίως ένα οριζόντιο ζήτημα το οποίο πραγματεύεται η ΕΣΑΚ στο σύνολό της και δεν αποτελεί συγκεκριμένο στόχο.

Διασφάλιση της κυριαρχίας των δεδομένων

Από τη μία πλευρά, ο κυβερνοχώρος μπορεί να θεωρηθεί ένας παγκόσμιος, κοινός, εύκολα προσβάσιμος χώρος, ο οποίος παρέχει έναν υψηλό βαθμό συνδεσιμότητας και μπορεί να προσφέρει μεγάλες ευκαιρίες κοινωνικοοικονομικής ανάπτυξης. Από την άλλη πλευρά, ο κυβερνοχώρος χαρακτηρίζεται και από αδύναμη δικαιοδοσία, δυσκολία καταλογισμού ευθυνών για οποιεσδήποτε ενέργειες, απουσία συνόρων, και διασυνδεδεμένα συστήματα που μπορεί να είναι διαπερατά με αποτέλεσμα οι αλλοδαπές κυβερνήσεις να μπορούν να υποκλέψουν ή να αποκτήσουν πρόσβαση στα δεδομένα τους. Πέρα από αυτές τις δύο οπτικές, το ψηφιακό οικοσύστημα χαρακτηρίζεται από τη συγκέντρωση πλατφορμών και υποδομής διαδικτυακών υπηρεσιών στα χέρια ελάχιστων ενδιαφερόμενων παραγόντων. Όλες οι ανωτέρω πτυχές έχουν ως αποτέλεσμα τα κράτη μέλη να προωθούν την τεχνολογική αυτοδυναμία. Η επίτευξη της τεχνολογικής αυτοδυναμίας συνεπάγεται ότι οι πολίτες και οι επιχειρήσεις μπορούν να ακμάζουν πλήρως χρησιμοποιώντας αξιόπιστες ψηφιακές υπηρεσίες και προϊόντα ΤΠΕ χωρίς κανέναν φόβο για τα δεδομένα προσωπικού χαρακτήρα, ή τα ψηφιακά περιουσιακά στοιχεία, την οικονομική αυτονομία ή την πολιτική επιρροή τους.

Η κυριαρχία δεδομένων ή τεχνολογική αυτοδυναμία υποστηρίζεται ένθερμα από τα κράτη μέλη σε εθνικό και ευρωπαϊκό επίπεδο. Τα κράτη μέλη, αν και δεν φαίνεται να αντιμετωπίζουν το ζήτημα άμεσα ως συγκεκριμένο στόχο στις ΕΣΑΚ τους, είτε το αντιμετωπίζουν ως οριζόντια αρχή είτε εκφράζουν την πρόθεσή τους να διασφαλίσουν την τεχνολογική αυτοδυναμία σε εθνικό επίπεδο σε *ad hoc* δημοσιεύσεις εστιάζοντας σε βασικές τεχνολογίες. Για παράδειγμα, στη στρατηγική αναθεώρηση της κυβερνοάμυνας της Γαλλίας για το 2018 αναφερόταν ότι «ο έλεγχος των παρακάτω τεχνολογιών είναι κρίσιμης σημασίας για τη διασφάλιση της τεχνολογικής αυτοδυναμίας: κρυπτογράφηση επικοινωνιών, εντοπισμός κυβερνοεπιθέσεων, επαγγελματικό κινητό ραδιοσύστημα, υπολογιστικό νέφος και τεχνητή νοημοσύνη»[37].

Σε ευρωπαϊκό επίπεδο, τα κράτη μέλη συμμετέχουν ενεργά στη χάραξη της ευρωπαϊκής στρατηγικής για τα δεδομένα (COM/2020/66 final) και στην οικοδόμηση του πλαισίου πιστοποίησης της ΕΕ για τα ψηφιακά προϊόντα, τις υπηρεσίες και τις διεργασίες ΤΠΕ που καθορίστηκαν από την πράξη για την κυβερνοασφάλεια της ΕΕ (2019/881) για τη διασφάλιση της ψηφιακής αυτονομίας σε ευρωπαϊκό επίπεδο.

Όπως φάνηκε στο στάδιο των συνεντεύξεων με τα κράτη μέλη, το ζήτημα της τεχνολογικής αυτοδυναμίας συχνά θεωρείται ευρύτερης φύσης και δεν περιορίζεται στην ασφάλεια στον

[35] https://ec.europa.eu/digital-single-market/en/news/secure-5g-deployment-eu-implementing-eu-toolbox-communication-commission
[36] https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A32019H0534
[37] http://www.sgdsn.gouv.fr/uploads/2018/03/revue-cyber-resume-in-english.pdf

κυβερνοχώρο. Συνεπώς, τα κράτη μέλη δεν καλύπτουν το ζήτημα στις ΕΣΑΚ τους, ενώ τα λίγα που το πράττουν, δεν το αντιμετωπίζουν ως συγκεκριμένο στόχο.

Παροχή κινήτρων για την ανάπτυξη του κλάδου της ασφάλισης στον κυβερνοχώρο

Η τρέχουσα κατάσταση του κλάδου της ασφάλισης στον κυβερνοχώρο είναι ενδεικτική της αδιαμφισβήτητης ανάπτυξης της παγκόσμιας αγοράς. Ωστόσο, η αγορά βρίσκεται ακόμα σε πρώιμο στάδιο, καθώς πρέπει να συλλεγούν στοιχεία και να δημιουργηθούν προηγούμενα (*π.χ.* σιωπηρή κάλυψη, συστημικοί κίνδυνοι στον κυβερνοχώρο...). Περαιτέρω, οι εκτιμώμενες σωρευτικές απώλειες από τις κυβερνοεπιθέσεις ανά τον κόσμο είναι κατά πολύ υψηλότερες από την τρέχουσα ικανότητα κάλυψης του κλάδου ασφάλισης στον κυβερνοχώρο [Έγγραφο εργασίας ΔΝΤ - Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment («Κίνδυνος στον κυβερνοχώρο για τον χρηματοπιστωτικό τομέα: ένα πλαίσιο για ποσοτική αξιολόγηση») WP/18/143]. Ωστόσο, η ανάπτυξη του κλάδου ασφάλισης στον κυβερνοχώρο μπορεί σίγουρα να έχει οφέλη και μπορεί να θέσει τις βάσεις για τη δημιουργία επωφελών μηχανισμών. Πράγματι, οι μηχανισμοί ασφάλισης στον κυβερνοχώρο μπορούν να συμβάλλουν στα εξής:

- Ευαισθητοποίηση σχετικά με τους κινδύνους ασφάλειας στον κυβερνοχώρο σε εταιρείες·
- Ποσοτική αξιολόγηση της έκθεσης σε κινδύνους στον κυβερνοχώρο
- Βελτίωση της διαχείρισης του κινδύνου για την ασφάλεια στον κυβερνοχώρο·
- Παροχή υποστήριξης σε οργανισμούς που πλήττονται από κυβερνοεπιθέσεις· και
- Κάλυψη των ζημιών (υλικών ή μη) που προκαλούνται από μια κυβερνοεπίθεση.

Ορισμένα κράτη μέλη έχουν αρχίσει ήδη να ασχολούνται με αυτό το θέμα. Για παράδειγμα:

- Στην ΕΣΑΚ της, η Εσθονία τηρεί στάση «αναμονής»: «Για τον μετριασμό των κινδύνων στον κυβερνοχώρο στον ιδιωτικό τομέα εν γένει, θα αναλυθεί η ζήτηση και η προσφορά της υπηρεσίας ασφάλισης στον κυβερνοχώρο στην Εσθονία και σε αυτή τη βάση θα συμφωνηθούν αρχές συνεργασίες για τα ενδιαφερόμενα μέρη, συμπεριλαμβανομένης της ανταλλαγής πληροφοριών, της προετοιμασίας της αξιολόγησης κινδύνου, κ.λπ. Στις μέρες μας, οι πάροχοι υπηρεσιών ασφάλισης στον κυβερνοχώρο είναι ελάχιστοι στην αγορά της Εσθονίας και πρέπει αρχικά να εντοπίσουμε τι προσφέρεται από ποιον. Η πολυπλοκότητα της ασφαλιστικής προστασίας θεωρείται συχνά εμπόδιο για την ανάπτυξη της αγοράς ασφάλισης στον κυβερνοχώρο».
- Στο πλαίσιο της ΕΣΑΚ του, το Λουξεμβούργο υποστηρίζει ειδικά την ανάπτυξη του τομέα της ασφάλισης στον κυβερνοχώρο: «Στόχος 1: Δημιουργία νέων προϊόντων και υπηρεσιών. Για την ομαδοποίηση των κινδύνων και την ενθάρρυνση των θυμάτων ψηφιακών κυβερνοπεριστατικών να αναζητήσουν βοήθεια από εμπειρογνώμονες για τη διαχείριση του περιστατικού και την αποκατάσταση ενός συστήματος που επηρεάζεται από μια κακόβουλη πράξη, οι εταιρείες ασφάλισης θα ενθαρρυνθούν να δημιουργήσουν συγκεκριμένα προϊόντα για τον κλάδο της ασφάλισης στον κυβερνοχώρο».

Τα σχόλια των ερωτηθέντων για αυτό το ζήτημα ποικίλλουν: μερικά κράτη μέλη δήλωσαν ότι το ζήτημα της ασφάλισης στον κυβερνοχώρο τέθηκε πρόσφατα προς συζήτηση, ενώ άλλα ανέφεραν ότι, μολονότι αυτό το θέμα είναι πολλά υποσχόμενο, ο κλάδος δεν είναι ακόμη αρκετά ώριμος. Ωστόσο, ένας μεγάλος αριθμός συμμετεχόντων δήλωσαν ότι το ζήτημα δεν αντιμετωπίζεται ως μέρος της ΕΣΑΚ, είτε διότι θεωρείται υπερβολικά συγκεκριμένο είτε διότι θεωρείται ότι δεν υπάγεται στο πεδίο εφαρμογής της ΕΣΑΚ.

TP-02-21-253-EL-N

Πληροφορίες για τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια

Ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια, ο ENISA, είναι ο οργανισμός της Ένωσης που αποσκοπεί να διασφαλίσει υψηλό, κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ευρώπη. Ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια, που ιδρύθηκε το 2004 και ενισχύθηκε από την Πράξη της ΕΕ για την ασφάλεια στον κυβερνοχώρο, συμβάλλει στη χάραξη της πολιτικής της ΕΕ στον τομέα του κυβερνοχώρου, ενισχύει την αξιοπιστία των προϊόντων, υπηρεσιών και διαδικασιών ΤΠΕ με συστήματα πιστοποίησης της κυβερνοασφάλειας, συνεργάζεται με κράτη μέλη και φορείς της ΕΕ και βοηθά την Ευρώπη να προετοιμαστεί για τις μελλοντικές προκλήσεις στον κυβερνοχώρο. Μέσω της ανταλλαγής γνώσεων, της δημιουργίας ικανοτήτων και της ευαισθητοποίησης, ο Οργανισμός συνεργάζεται με τους βασικούς ενδιαφερόμενους φορείς για την ενίσχυση της εμπιστοσύνης στη συνδεδεμένη οικονομία, την υποστήριξη της ανθεκτικότητας των υποδομών της Ένωσης και, τελικά, τη διατήρηση της ψηφιακής ασφάλειας για την κοινωνία και τους πολίτες της Ευρώπης. Για περισσότερες πληροφορίες επισκεφθείτε τη διεύθυνση www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN: 978-92-9204-474-9
DOI: 10.2824/562580