Ε.Ε.Παρ.ΙΙΙ(Ι) **Κ.Δ.Π. 245/2024**
Αρ. 5882, 5.7.2024

Αριθμός 245

Ο ΠΕΡΙ ΑΣΦΑΛΕΙΑΣ ΔΙΚΤΥΩΝ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ ΝΟΜΟΣ (ΝΟΜΟΣ 89(Ι) ΤΟΥ 2020)

Απόφαση δυνάμει των άρθρων 17(ιζ), 17(ιη), 17(ιθ), 17(κβ), 17(κγ), 17(κστ), 19, 20(1)(α), 20(1)(β), 20(1)(γ), 20(1)(δ), 20(1)(ε), 21, 35(1), 35(2), 36, 37(1), 37(2), 37(3), 37(4), 38, 39, 40(1), 40(9), 43, 46 και 54

Προοίμιο. Η Αρχή Ψηφιακής Ασφάλειας, ασκώντας τις εξουσίες που της παρέχουν τα άρθρα 17(ιζ), 17(ιη), 17(ιθ), 17(κβ), 17(κγ), 17(κστ), 19, 20(1)(α), 20(1)(β), 20(1)(γ), 20(1)(δ), 20(1)(ε), 21, 35(1), 35(2), 36, 37(1), 37(2), 37(3), 37(4), 38, 39, 40(1), 40(9), 43, 46 και 54 του περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών Νόμου του 2020, ως εκάστοτε τροποποιείται, εκδίδει την παρούσα Απόφαση με την οποία καθορίζεται η διαδικασία διενέργειας ελέγχων ωριμότητας κυβερνοασφάλειας των Φορέων, που διενεργείται με τη χρήση μοντέλου ωριμότητας κυβερνοασφάλειας (cybersecurity maturity model) και το Πλαίσιο εγγραφής ελεγκτών κυβερνοασφάλειας.

ΜΕΡΟΣ Ι
Εισαγωγικές Διατάξεις

Συνοπτικός τίτλος. 1. Η παρούσα Απόφαση θα αναφέρεται ως η περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών (Έλεγχοι Ωριμότητας Κυβερνοασφάλειας) Απόφαση του 2024.

Ορισμοί. 2.- (1) Στην παρούσα Απόφαση,στα Παραρτήματα και Προσαρτήματα αυτής, εκτός αν από το κείμενο προκύπτει διαφορετική έννοια-

«αιτητής» ή «υποψήφιος ελεγκτής» σημαίνει το πρόσωπο το οποίο έχει υποβάλει αίτηση για να ενταχθεί στο Μητρώο Ελεγκτών Κυβερνοασφάλειας·

«αξιολόγηση» σημαίνει τη μέθοδο είτε διαδικασία, προκειμένου να αξιολογηθεί κατά πόσον ένα πρόσωπο πληροί τις απαιτήσεις ικανότητας για να εγγραφεί στο Μητρώο Ελεγκτών Κυβερνοασφάλειας·

Κ.Δ.Π. 389/2020.
Κ.Δ.Π. 40/2022.

«Απόφαση Κ.Δ.Π. 389/2020» σημαίνει την περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών (Μέτρα Ασφάλειας Φορέων Εκμετάλλευσης Βασικών Υπηρεσιών και Φορέων Κρίσιμων Υποδομών Πληροφοριών) Απόφαση του 2020, ως εκάστοτε τροποποιείται ή αντικαθίσταται·

«Ανθρωποημέρα» σημαίνει την μονάδα μέτρησης του χρόνου ελέγχου και η διάρκεια μιας ανθρωποημέρας ελέγχου κυμαίνεται μεταξύ εφτάμιση (7.5) και οχτώ (8) ωρών, αναλόγως του ωραρίου του Φορέα, περιλαμβανομένων διαλειμμάτων (ενός 30 συνεχόμενων λεπτών και ενός 15 συνεχόμενων λεπτών ή με κάποιον άλλον τρόπο που να βολεύει το σύνολο των εμπλεκόμενων μερών)·

«ανωτέρα βία» σημαίνει κάθε γεγονός απρόβλεπτο που δεν μπορεί να αποτραπεί, ακόμη και με την επίδειξη άκρας επιμέλειας και σύνεσης όπως είναι ο θάνατος, ο πόλεμος, το πραξικόπημα, οι απρόβλεπτες κυβερνητικές απαγορεύσεις, η ξαφνική βαριά ασθένεια, οι αιφνίδιες φυσικές καταστροφές (σεισμός, πλημμύρα, τσουνάμι, έκρηξη ηφαιστείου κ.λπ.), τα ακραία καιρικά φαινόμενα, η πανδημία κ.α.·

«Αρχή» σημαίνει την Αρχή Ψηφιακής Ασφάλειας·

«γνωστικό αντικείμενο» σημαίνει τη θεματική ενότητα γνώσεων/δεξιοτήτων ή/και ικανοτήτων στην οποία εκπαιδεύεται ο υποψήφιος ελεγκτής και βάσει των οποίων εκδίδει πιστοποιητικό επιτυχίας ο εξεταστικός φορέας·

«δεοντολογικοί κανόνες επαγγέλματος» σημαίνει τον κώδικα δεοντολογίας που αποτελείται από μία σειρά κανόνων επαγγελματικής συμπεριφοράς/διαγωγής, που διέπουν το φάσμα των επαγγελματικών δραστηριοτήτων των εγγεγραμμένων ελεγκτών στο Μητρώο Ελεγκτών Κυβερνοασφάλειας, ως το ΠΡΟΣΑΡΤΗΜΑ 1 του ΠΑΡΑΡΤΗΜΑΤΟΣ ΣΤ της παρούσας Απόφασης·

«Διαδικασία Διενέργειας Ελέγχων Ωριμότητας Κυβερνοασφάλειας» σημαίνει τη διαδικασία ως ορίζεται στην παρούσα Απόφαση·

«Διαχειριστής Τράπεζας Θεμάτων Εξέτασης» σημαίνει τον οργανισμό που ορίζεται από την Αρχή για να διαχειρίζεται το σύνολο των ερωτήσεων της Τράπεζας Θεμάτων που χρησιμοποιούνται στην εξέταση·

«δόκιμος (junior) ελεγκτής» σημαίνει τον ελεγκτή που είναι εγγεγραμμένος στο Μητρώο Ελεγκτών Κυβερνοασφάλειας, έχει περάσει την κατάσταση εκπαιδευόμενος και που δικαιούται να διενεργήσει ελέγχους σε Φορείς με επίπεδο κρισιμότητας «Μέτριο», «Χαμηλό» ή/και «Πολύ Χαμηλό». Κατά την διενέργεια του ελέγχου θα συνοδεύεται για επιτήρηση από την Αρχή και αν η επιτήρησή του είναι επιτυχής τότε θα αλλάζει κατάσταση στο Μητρώο Ελεγκτών Κυβερνοασφάλειας από δόκιμο (junior) σε ελεγκτή·

«εκπαιδευόμενος ελεγκτής» σημαίνει τον ελεγκτή που είναι εγγεγραμμένος στο Μητρώο Ελεγκτών Κυβερνοασφάλειας, αλλά δεν κατέχει την επαγγελματική εμπειρία ως αυτή ορίζεται στην

παράγραφο 6.1 στο ΠΑΡΑΡΤΗΜΑ ΣΤ της παρούσας Απόφασης. Ο εκπαιδευόμενος ελεγκτής, για να αλλάξει η κατάστασή του στο Μητρώο Ελεγκτών Κυβερνοασφάλειας από εκπαιδευόμενος σε δόκιμο (junior) ελεγκτή, οφείλει να συνοδεύσει ελεγκτή και να παρακολουθήσει δύο (2) ολοκληρωμένους ελέγχους με ελάχιστη συνολική διάρκεια δέκα (10) ημερών·

«εκπρόσωπος του Φορέα» σημαίνει τον εργαζόμενο που εκπροσωπεί τον Φορέα καθ' όλη τη διενέργεια του ελέγχου·

«ελεγκτής» σημαίνει τον εγκεκριμένο ελεγκτή ωριμότητας κυβερνοασφάλειας που είναι εγγεγραμμένος στο Μητρώο Ελεγκτών Κυβερνοασφάλειας και δικαιούται να διενεργεί ελέγχους για σκοπούς εφαρμογής της νομοθεσίας της Αρχής σε Φορείς, ανεξαρτήτως της κρισιμότητάς τους·

«έλεγχος» σημαίνει την επιθεώρηση ασφάλειας και τον έλεγχο ωριμότητας κυβερνοασφάλειας των Φορέων που διενεργείται με τη χρήση μοντέλου ωριμότητας κυβερνοασφάλειας (cybersecurity maturity model) το οποίο αναπτύχθηκε βάσει των απαιτήσεων της Απόφασης Κ.Δ.Π. 389/2020·

«εξειδικευμένες κάθετες απαιτήσεις» σημαίνει τα κάθετα μέτρα ασφάλειας για συγκεκριμένους τομείς και για τα οποία εκδίδει Αποφάσεις η Αρχή·

«εξέταση» σημαίνει την εξέταση των αιτητών που επιθυμούν να εγγραφούν στο Μητρώο Ελεγκτών Κυβερνοασφάλειας, η οποία καθορίζεται στο κεφάλαιο 8 του ΠΑΡΑΡΤΗΜΑΤΟΣ ΣΤ·

«εξεταστικός φορέας (ΕΦ)»: σημαίνει α) το Ίδρυμα Τριτοβάθμιας εκπαίδευσης αναγνωρισμένο από το Δ.Ι.Π.Α.Ε (Φορέας Διασφάλισης και Πιστοποίησης της Ποιότητας της Ανώτερης Εκπαίδευσης) ή β) τον Φορέα Πιστοποίησης προσώπων διαπιστευμένος για ISO/IEC 17024 ο οποίος διεξάγει εξετάσεις σε πιστοποιημένη δομή επαγγελματικής κατάρτισης, από την ΑΝΑΔ (Αρχή Ανάπτυξης Ανθρώπινου Δυναμικού)·

«εξοπλισμός» σημαίνει τον ηλεκτρονικό υπολογιστή που έχει τη δυνατότητα πρόσβασης στην ηλεκτρονική πλατφόρμα διαχείρισης των ελέγχων που παρέχει η Αρχή·

«επικεφαλής ελεγκτής» σημαίνει τον ελεγκτή που είναι ο επικεφαλής του ελέγχου και που θα ορίσει ρητά στη συμφωνία ο Φορέας·

«επιθεώρηση τρίτου μέρους (3rd party audit)» σημαίνει την επιθεώρηση που διενεργείται από ανεξάρτητους φορείς επιθεώρησης, όπως είναι εκείνοι που παρέχουν πιστοποίηση ή καταχώρηση σε μητρώο συμμόρφωσης ή από κρατικές υπηρεσίες·

«επίπεδο διαβάθμισης ωριμότητας» σημαίνει τις τιμές από 0 μέχρι 5 ως αυτές προνοούνται στο μοντέλο ωριμότητας κυβερνοασφάλειας στο ΠΑΡΑΡΤΗΜΑ Ε της παρούσας Απόφασης·

«επιτηρητής» σημαίνει το εξουσιοδοτημένο άτομο από τον εξεταστικό φορέα, είτε μόνιμος εργαζόμενος είτε εξωτερικός συνεργάτης, που είναι αρμόδιο να επιβλέπει την ορθή διεξαγωγή των εξετάσεων και δεν απαιτείται να διαθέτει ικανότητες αξιολόγησης της επάρκειας των υποψηφίων·

«ένσταση» σημαίνει το αίτημα από τον Φορέα, τον υποψήφιο ελεγκτή, τον ελεγκτή για αναθεώρηση απόφασης·

«ημερολογιακός μήνας» σημαίνει τον μήνα όπως καθορίζεται ονομαστικά από το ημερολόγιο»·

156(I)/2002
10(I)/2010
57(I)/2011
69(I)/2012
120(I)/2012.

«Κυπριακός Οργανισμός Τυποποίησης (CYS)» σημαίνει τον επίσημο Εθνικό Φορέα Τυποποίησης που ανέλαβε τη δραστηριότητα της Τυποποίησης με βάση το Νόμο 156(I)/2002, ως εκάστοτε τροποποιείται ή αντικαθίσταται και είναι υπεύθυνος να διατηρεί το Μητρώο Ελεγκτών Κυβερνοασφάλειας στο οποίο είναι εγγεγραμμένοι ελεγκτές ή δύναται να εγγραφούν ελεγκτές·

«Μητρώο Ελεγκτών Κυβερνοασφάλειας» σημαίνει το μητρώο που είναι δημόσια διαθέσιμο, αποτελεί ιδιοκτησία της Αρχής και υπεύθυνος να το διατηρεί και να το διαχειρίζεται είναι ο Κυπριακός Οργανισμός Τυποποίησης (CYS) και στο οποίο είναι εγγεγραμμένοι οι ελεγκτές, συμπεριλαμβανομένων των δόκιμων (junior) και εκπαιδευόμενων ελεγκτών·

«μοντέλο ωριμότητας κυβερνοασφάλειας (cybersecurity maturity model)» σημαίνει το μοντέλο που περιλαμβάνει εξειδίκευση και διασαφήνιση των απαιτήσεων του ΠΑΡΑΡΤΗΜΑΤΟΣ ΙΙΙ της Απόφασης Κ.Δ.Π. 389/2020, με αντιστοίχισή τους προς διακριτά επίπεδα ωριμότητας για το κάθε μέτρο ασφάλειας·

89(I)/2020.

«Νόμος» σημαίνει ο περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών Νόμος του 2020 και περιλαμβάνει κάθε Νόμο που τον τροποποιεί ή τον αντικαθιστά·

«ομάδα ελέγχου» σημαίνει τους ελεγκτές συμπεριλαμβανομένου τον επικεφαλής ελεγκτή, σε περίπτωση που ο έλεγχος θα διενεργηθεί με πέραν του ενός ελεγκτή·

«παράπονο» σημαίνει την εκδήλωση δυσαρέσκειας του Φορέα, του υποψήφιου ελεγκτή, του ελεγκτή και του επικεφαλής ελεγκτή·

«παραπονούμενος» σημαίνει τον Φορέα, τον υποψήφιο ελεγκτή και τον ελεγκτή που δύναται να υποβάλλει στην Αρχή παράπονα, καταγγελίες και ενστάσεις·

«πεδίο εφαρμογής του ελέγχου» σημαίνει το εύρος και τα όρια που θα διενεργηθεί ο έλεγχος. Δύναται το πεδίο εφαρμογής του ελέγχου να είναι περιορισμένο είτε σε συγκεκριμένη φυσική είτε

σε συγκεκριμένες κατηγορίες μέτρων ασφαλείας σύμφωνα με την Απόφαση Κ.Δ.Π. 389/2020·

«πιστοποιητικό επιτυχίας στην εξέταση» σημαίνει το επίσημο έγγραφο βάσει του οποίου πιστοποιείται ότι ο εξεταζόμενος διαθέτει την απαιτούμενη επάρκεια γνώσεων στα γνωστικά αντικείμενα που αυτό καλύπτει και αφορά αποκλειστικά τον εξεταζόμενο στον οποίο χορηγήθηκε·

«Πλαίσιο εγγραφής ελεγκτών κυβερνοασφάλειας» σημαίνει το πλαίσιο σύμφωνα με το οποίο εγκρίθηκε ο ελεγκτής για να διεξάγει ελέγχους για σκοπούς εφαρμογής της νομοθεσίας της Αρχής και το οποίο προνοείται στο ΠΑΡΑΡΤΗΜΑ ΣΤ της παρούσας Απόφασης·

«προγραμματισμός» σημαίνει την προτεραιοποίηση και καθορισμό της συχνότητας των ελέγχων·

«καταγγελία» σημαίνει την καταγγελία από τον Φορέα, τον υποψήφιο ελεγκτή, τον ελεγκτή και τον επικεφαλής ελεγκτή για μία παράνομη πράξη ή για μη συμμόρφωσή τους με τις υποχρεώσεις που απορρέουν από την παρούσα Απόφαση·

«συνολικός αριθμός εργαζομένων» ή «αριθμός εργοδοτουμένων» σημαίνει το σύνολο των ατόμων του Φορέα που εμπλέκονται άμεσα στο πεδίο εφαρμογής του ελέγχου. Για τον υπολογισμό του συνολικού αριθμού των εργαζομένων δεν λαμβάνεται υπόψη ο τρόπος εργοδότησης και μετρώνται εργαζόμενοι που διενεργούν εργασία στο πλαίσιο του πεδίου εφαρμογής ακόμα και αν είναι με σύμβαση ή ορισμένου χρόνου. Σε περίπτωση που υπάρχει προσωπικό το οποίο εργάζεται με σύστημα βάρδιας ή μερική απασχόληση, μετατρέπονται τα σχετικά μεγέθη χρησιμοποιώντας την έννοια του ισοδύναμου προσωπικού·

«Φορέας» σημαίνει τον φορέα εκμετάλλευσης βασικών υπηρεσιών, τον φορέα κρίσιμων υποδομών πληροφοριών, τον παροχέα δικτύων ή/και υπηρεσιών ηλεκτρονικών επικοινωνιών και τον παροχέα ψηφιακών υπηρεσιών, όπως αυτοί ορίζονται από τον περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών Νόμο ή/και οποιαδήποτε άλλη οντότητα οριστεί από καιρού εις καιρό βάσει του περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών Νόμο·

«χρόνος ελέγχου» σημαίνει το χρόνο που χρειάζεται να δαπανήσει ένας ελεγκτής προκειμένου να διενεργήσει το σύνολο των διαδικασιών και δραστηριοτήτων του ελέγχου ως αυτές προνοούνται στην παρούσα Απόφαση·

«χρόνος επιτόπιου ελέγχου» σημαίνει το υποσύνολο του χρόνου ελέγχου και περιέχει όλες τις δραστηριότητες που διενεργούνται στους χώρους/τοποθεσίες του Φορέα όπως είναι η εναρκτήρια και καταληκτική σύσκεψη, η ανασκόπηση εγγράφων και αρχείων·

(2) Όροι που χρησιμοποιούνται στην παρούσα Απόφαση, στα Παραρτήματα και στα Προσαρτήματα αυτής και δεν ορίζονται διαφορετικά, έχουν την έννοια που αποδίδει σε αυτούς ο Νόμος.

Πεδίο Εφαρμογής.

3. Η παρούσα Απόφαση πραγματεύεται το σύνολο των διαδικασιών και απαιτήσεων για την διενέργεια ελέγχων συμμόρφωσης των Φορέων επί του συστήματος διαβάθμισης ωριμότητας.

Σκοπός.

4. Σκοπός της παρούσας Απόφασης είναι η αναγνώριση του επιπέδου ωριμότητας των Φορέων έναντι των απαιτήσεων της Απόφασης Κ.Δ.Π. 389/2020, η ενημέρωση της Αρχής σχετικά με το επίπεδο ωριμότητας των Φορέων και ο καθορισμός πλάνου ενεργειών από τους Φορείς για την συμμόρφωση τους σύμφωνα με τις πρόνοιες της Απόφασης Κ.Δ.Π. 389/2020 για τη βελτίωση του επιπέδου ασφάλειας των δικτύων και συστημάτων πληροφοριών τους.

ΜΕΡΟΣ ΙΙ
Κυρίως Μέρος
Κεφάλαιο Ι – Προγραμματισμός Ελέγχων

Προγραμματισμός Ελέγχων από την Αρχή.

5. Η Αρχή, σε ετήσια βάση (κατά το έτος (χ)), καταρτίζει πρόγραμμα ελέγχων των Φορέων, λαμβάνοντας υπόψη, μεταξύ άλλων, ένα ή περισσότερα από τα ακόλουθα κριτήρια:

(α) Το επίπεδο κρισιμότητας των Φορέων·

(β) τα περιστατικά κυβερνοασφάλειας που εκδηλώνονται στα συστήματα δικτύων και πληροφοριών των Φορέων κατά τη χρονιά χ-1·

(γ) τον βαθμό ανταπόκρισης των Φορέων στις υποχρεώσεις τους όπως αυτές απορρέουν από τη νομοθεσία της Αρχής·

(δ) τις ενημερώσεις που θα λαμβάνει από εθνικές και διεθνείς αξιόπιστες πηγές, όπως είναι ο ENISA, αναφορικά με κυβερνοεπιθέσεις και το τοπίο των κυβερνοαπειλών· και

(ε) οποιοδήποτε άλλο κατάλληλο κριτήριο που δύναται να προκύψει λόγω του εξελισσόμενου τεχνολογικού πεδίου.

Πρόγραμμα ελέγχων.

6. Το πρόγραμμα των ελέγχων, περιλαμβάνει τα ονόματα των Φορέων που θα διενεργηθεί ο έλεγχος για το έτος χ:

Νοείται ότι, ο έλεγχος δύναται να επεκταθεί και σε εξειδικευμένες κάθετες απαιτήσεις, βάσει Αποφάσεων που εκδίδει η Αρχή.

Διενέργεια έκτακτου ή προγραμματισμένου ελέγχου.

7. Ανεξάρτητα από τις διατάξεις των άρθρων 5 και 6 της παρούσας Απόφασης, η Αρχή δύναται να διενεργήσει η ίδια ή να ζητήσει να διενεργηθεί έκτακτος ή προγραμματισμένος έλεγχος σε οποιονδήποτε Φορέα, ανεξάρτητα με το χρονικό διάστημα ολοκλήρωσης του προηγούμενου ελέγχου και, μεταξύ άλλων, όταν αυτό δικαιολογείται, λόγω σημαντικού περιστατικού ή παραβίασης των προνοιών του Νόμου και της δυνάμει αυτού εκδοθείσας δευτερογενούς νομοθεσίας από τον Φορέα.

Ενημέρωση Φορέων που εντάσσονται στο πρόγραμμα ελέγχου.

8.- (1) Η Αρχή, εντός ενός (1) μηνός από την ημερομηνία κατάρτισης του προγράμματος των ελέγχων για το έτος χ, ενημερώνει τους Φορείς που επιλέγηκαν και εντάσσονται στο πρόγραμμα ελέγχου και τους ζητά να συμπληρώσουν σχετικό ερωτηματολόγιο για ανανέωση των βασικών στοιχείων του, που περιλαμβάνουν τουλάχιστον τα εξής:

(α) Τον συνολικό αριθμό των εργαζομένων του Φορέα·

(β) τον αριθμό φυσικών τοποθεσιών·

(γ) το σύνολο των εξυπηρετητών (servers)·

(δ) το σύνολο των δικτύων· και

(ε) οποιαδήποτε άλλη πληροφορία κρίνει η Αρχή ότι είναι αναγκαία για τον σκοπό, τηρουμένων των διατάξεων του άρθρου 19 του Νόμου 89(Ι)/2020.

(2) Οι Φορείς υποχρεούνται να συμπληρώσουν και να υποβάλουν στην Αρχή, με τρόπο που καθορίζει η Αρχή, το ερωτηματολόγιο για ανανέωση των βασικών στοιχείων τους τηρουμένης της παραγράφου (1) του παρόντος άρθρου, εντός προθεσμίας ενός (1) μηνός.

Πληροφόρηση που παρέχεται στα πλαίσια της ενημέρωσης των Φορέων.

9. Η Αρχή στα πλαίσια ενημέρωσης των Φορέων και τηρουμένου του άρθρου 8 της παρούσας Απόφασης, παρέχει στον κάθε Φορέα πληροφόρηση σχετικά με:

(α) τις διατάξεις του Νόμου, της Απόφασης Κ.Δ.Π. 389/2020 και της παρούσας Απόφασης, βάσει των οποίων διενεργούνται οι έλεγχοι,

(β) το πεδίο εφαρμογής του ελέγχου,

(γ) τον εκτιμώμενο χρόνο διάρκειας του ελέγχου, αφού η Αρχή επεξεργαστεί τις απαντήσεις του ερωτηματολογίου και προσδιορίσει ενδεικτικά τον χρόνο ελέγχου, σύμφωνα με το οριζόμενα στο ΠΑΡΑΡΤΗΜΑ Α:

Νοείται ότι, ο Φορέας, σε συνεννόηση με τον επικεφαλής ελεγκτή, επαναϋπολογίζει και συμφωνεί τον χρόνο διάρκειας του ελέγχου σε ανθρωποημέρες και καθορίζει και συμφωνεί τις ημερομηνίες για τη διενέργεια του ελέγχου πριν τη σύναψη συμφωνίας με τον/τους ελεγκτή/ές, σύμφωνα με τα οριζόμενα στο ΠΑΡΑΡΤΗΜΑ Α,

(δ) τη δυνατότητα επιλογής ελεγκτή ή ελεγκτών από το Μητρώο Ελεγκτών Κυβερνοασφάλειας, για τη διενέργεια του ελέγχου και την υποχρέωση σύναψης συμφωνίας σύμφωνα με τα οριζόμενα στο Κεφάλαιο ΙΙ της παρούσας Απόφασης και

(ε) την υποχρέωση όλων των εμπλεκόμενων μερών για τήρηση εμπιστευτικότητας για το σύνολο της σχετιζόμενης πληροφορίας.

Υποχρεώσεις Φορέων.

10.- (1) Οι Φορείς υποχρεούνται να ενημερώσουν γραπτώς την Αρχή για το χρονικό διάστημα, με αναφορά σε συγκεκριμένες ημερομηνίες για τη διενέργεια του ελέγχου, τη συνολική διάρκεια του σε ανθρωποημέρες και τον ελεγκτή ή τους ελεγκτές που θα διενεργήσει/ούν τον έλεγχο:

Νοείται ότι, ενόψει της γραπτής ενημέρωσης της Αρχής από τον Φορέα για τη διενέργεια του Ελέγχου, η Αρχή έχει την δυνατότητα, εάν το κρίνει απαραίτητο, να παρευρίσκεται ως παρατηρητής, είτε ύστερα από ειδοποίηση είτε χωρίς ειδοποίηση προς τον Φορέα και τον επικεφαλής Ελεγκτή.

(2) Οι Φορείς δεν πρέπει να συμβάλλονται με τον ίδιο ελεγκτή πέραν από τρεις (3) συνεχόμενους ελέγχους.

(3) Τηρουμένων των διατάξεων του άρθρου 36 (4) του Νόμου, το κόστος του ελέγχου επιβαρύνει τους Φορείς.

(4) Ο Φορέας υποχρεούται να παρέχει στον ελεγκτή, για επιτόπιο έλεγχο, οποιαδήποτε πληροφορία και έγγραφα του ζητηθούν και είναι σχετικά με το αντικείμενο του ελέγχου:

84(Ι)/2021
79(Ι)/2023.

Νοείται ότι, σε περίπτωση που η πληροφορία ή/και τα έγγραφα που ζητά ο ελεγκτής έχουν χαρακτηριστεί ως διαβαθμισμένα σύμφωνα με τον περί Κανόνων Ασφαλείας Διαβαθμισμένων Πληροφοριών, Εγγράφων και Υλικού και για Συναφή Θέματα Νόμο, θα ισχύουν οι πρόνοιες του εν λόγω Νόμου και των Διαταγμάτων που εκδίδονται δυνάμει αυτού και ο ελεγκτής ή ο Φορέας δύναται να ζητήσουν όπως παρευρίσκεται κατά τον έλεγχό τους και εξουσιοδοτημένο μέλος του προσωπικού της Αρχής για το χειρισμό διαβαθμισμένων πληροφοριών/εγγράφων:

Νοείται περαιτέρω ότι, ο ελεγκτής θα ζητά πληροφορίες και έγγραφα που αφορούν αποκλειστικά τους σκοπούς διεξαγωγής του ελέγχου.

Διαβούλευση μεταξύ Φορέα και ελεγκτή ή ελεγκτών.

11. Πριν τη σύναψη συμφωνίας ο Φορέας και ο/οι ελεγκτής/ές θα πρέπει να διαβουλεύονται, να συζητούν και να αποφασίζουν τουλάχιστον για τα πιο κάτω:

(α) την πρόσβαση του/των ελεγκτή/ών στις εγκαταστάσεις που πρόκειται να διενεργηθεί ο έλεγχος και σε τυχόν εγκαταστάσεις τρίτων μερών που φιλοξενούν στοιχεία ενεργητικού του Φορέα·

(β) την προηγούμενη ενημέρωση για λήψη άδειας πρόσβασης στις εγκαταστάσεις του Φορέα και κανόνες που δύναται να τηρούνται εντός των εγκαταστάσεων·

(γ) τα στοιχεία ταυτοποίησης του/των ελεγκτή/ών·

(δ) τις σχετικές προθεσμίες διενέργειας του ελέγχου μέχρι την ολοκλήρωσή του·

(ε) τα στοιχεία επικοινωνίας των εμπλεκομένων στον έλεγχο· και

(στ) τυχόν άλλες απαιτήσεις, όπως είναι για παράδειγμα ο τρόπος διάθεσης εγγράφων που θα ανασκοπηθούν στον έλεγχο.

Κεφάλαιο ΙΙ – Σύναψη συμφωνίας για τη διενέργεια του ελέγχου

Σύναψη συμφωνίας για τη διενέργεια του ελέγχου.

12.- (1) Η συμφωνία για τη διενέργεια του ελέγχου, ως προνοείται στο σημείο (δ) του άρθρου 9 της παρούσας Απόφασης, δύναται να συναφθεί είτε από φυσικό, είτε από νομικό πρόσωπο εκ μέρους του ελεγκτή ή των ελεγκτών, ο οποίος/οι οποίοι πρέπει να αναφέρεται/αναφέρονται ειδικά στη συμφωνία:

Νοείται ότι, σε περίπτωση κοινοπραξίας φυσικών ή/και νομικών προσώπων θα πρέπει να αναφέρονται τα στοιχεία για την κοινοπραξία και τα στοιχεία κάθε μέλους της κοινοπραξίας.

(2) Σε περίπτωση που ο εκτιμώμενος χρόνος του ελέγχου, όπως υπολογίστηκε από τον Φορέα σε συνεννόηση με τον επικεφαλής ελεγκτή, ξεπερνά τις 15 ανθρωποημέρες, τότε ο Φορέας υποχρεούται να συνάψει συμφωνία με ελεγκτές πέραν του ενός, εάν είναι φυσικό πρόσωπο, και στην περίπτωση που η συμφωνία συναφθεί με νομικό πρόσωπο θα πρέπει να αναφέρονται σε αυτήν όλοι οι ελεγκτές που θα διενεργήσουν τον έλεγχο οι οποίοι πρέπει να είναι πέραν του ενός.

(3) Φορείς με επίπεδο κρισιμότητας «Υψηλό» ή «Πολύ Υψηλό» υποχρεούνται να συνάψουν συμφωνία μόνο με ελεγκτές που είναι εγγεγραμμένοι στο Μητρώο Ελεγκτών Κυβερνοασφάλειας, αλλά δεν είναι δόκιμοι (junior) και εκπαιδευόμενοι ελεγκτές.

(4) Φορείς με επίπεδο κρισιμότητας «Μέτριο», «Χαμηλό» και «Πολύ Χαμηλό» δύναται να συνάψουν συμφωνία με δόκιμους (junior) ελεγκτές:

Νοείται ότι, στην περίπτωση που θα επιλεγούν δόκιμοι (junior) ελεγκτές, οι ελεγκτές αυτοί θα συνοδεύονται και με προσωπικό της Αρχής ή με άτομο που θα ορίσει η Αρχή, κατά τη διενέργεια του ελέγχου, για σκοπούς επιτήρησής τους.

Σύναψη συμφωνίας πέραν του ενός ελεγκτή.

13. Σε περίπτωση που Φορέας συνάψει συμφωνία με περισσότερους ελεγκτές από ένα, τότε θα πρέπει να αποφασίσει ποιος από τους συμβαλλόμενους ελεγκτές θα είναι ο επικεφαλής ελεγκτής και να αναφέρεται ρητά στη συμφωνία:

Νοείται ότι, σε περίπτωση που Φορέας συνάψει συμφωνία με ένα μόνον ελεγκτή τότε ορίζεται αυτομάτως ως επικεφαλής ελεγκτής του ελέγχου.

Καθήκοντα Επικεφαλής Ελεγκτή.

14. Ο επικεφαλής ελεγκτής, πέραν από τα καθήκοντα που ορίζονται στο άρθρο 30 της παρούσας Απόφασης, επιβαρύνεται με τα ακόλουθα επιπρόσθετα καθήκοντα πέραν της διενέργειας του ελέγχου:

(α) να προσδιορίζει τα μέρη του πεδίου εφαρμογής που θα αναλάβουν οι υπόλοιποι ελεγκτές, λαμβάνοντας υπόψη τα μέτρα ασφάλειας και τα βασικά στοιχεία του Φορέα όπως αναφέρονται στο άρθρο 8 της παρούσας και να ετοιμάζει ενιαίο πλάνο ελέγχου με σκοπό την ενημέρωση του Φορέα·

(β) να συγχωνεύει τα αποτελέσματα των ελέγχων που θα λαμβάνει από όλους τους ελεγκτές·

(γ) να επιλύει τυχόν διαφορές σε περίπτωση διαφορετικών αποτελεσμάτων σε ίδιους ελέγχους:

Νοείται ότι, αυτό δύναται να παρουσιαστεί στις περιπτώσεις όπου ο Φορέας έχει εγκαταστάσεις πέραν μίας τοποθεσίας και πραγματοποιείται έλεγχος σε όλες τις τοποθεσίες·

(δ) να συντάσσει/ετοιμάζει την Έκθεση Ελέγχου Ωριμότητας Κυβερνοασφάλειας, σύμφωνα με το ΠΑΡΑΡΤΗΜΑ Β:

Νοείται ότι, η Έκθεση Ελέγχου Ωριμότητας Κυβερνοασφάλειας πρέπει να είναι γραμμένη στην ελληνική γλώσσα και δύναται να χρησιμοποιούνται και αγγλικοί όροι.

(ε) να τηρεί παρουσιολόγιο κατά τη διάρκεια του ελέγχου, της εναρκτήριας και καταληκτικής σύσκεψης:

Νοείται ότι, σε περίπτωση που ο έλεγχος διενεργείται από περισσότερους τους ενός ελεγκτή τότε όλοι οι ελεγκτές οφείλουν να τηρούν παρουσιολόγιο για τους ελέγχους που διενεργούν.

Περιεχόμενο συμφωνίας.

15. Η συμφωνία που θα συνάψει ο Φορέας με τον ελεγκτή ή τους ελεγκτές θα πρέπει να προνοεί τουλάχιστον τα ακόλουθα:

(α) τις διατάξεις του Νόμου, της Απόφασης Κ.Δ.Π. 389/2020 και της παρούσας Απόφασης, βάσει των οποίων διενεργούνται οι έλεγχοι·

(β) τα στοιχεία του Φορέα (επωνυμία Φορέα, αριθμό εγγραφής της εταιρείας σε περίπτωση που είναι εταιρεία, στοιχεία επικοινωνίας, διεύθυνση και οποιαδήποτε άλλα στοιχεία είναι χρήσιμα για την σύναψη της συμφωνίας.)·

(γ) το πεδίο εφαρμογής του ελέγχου, ως ορίζεται στο άρθρο 2 της παρούσας Απόφασης·

(δ) το χρονικό διάστημα διενέργειας του ελέγχου, το οποίο δεν πρέπει να ξεπερνά τον έναν (1) ημερολογιακό μήνα·

(ε) την ελάχιστη διάρκεια του ελέγχου που προκύπτει από τον υπολογιζόμενο χρόνο ελέγχου, ως τον υπολόγισε ο Φορέας σύμφωνα με το ΠΑΡΑΡΤΗΜΑ Α·

(στ) το όνομα και τα στοιχεία επικοινωνίας του υπεύθυνου του Φορέα·

(ζ) τα στοιχεία επικοινωνίας του ελεγκτή (όνομα, επίθετο, αριθμό μητρώου ελεγκτή)·

(η) το ρόλο του ελεγκτή στον έλεγχο, ήτοι επικεφαλής ελεγκτής ή ελεγκτής·

(θ) την υποχρέωση ετοιμασίας Έκθεσης Ελέγχου Ωριμότητας Κυβερνοασφάλειας·

(ι) ρήτρες Καθυστέρησης εξ' υπαιτιότητας του ελεγκτή·

(ια) ρήτρες Καθυστέρησης εξ' υπαιτιότητας του Φορέα·

(ιβ) τη διαδικασία επίλυσης των διαφορών μεταξύ τους·

(ιγ) τις υποχρεώσεις του ελεγκτή·

(ιδ) Δήλωση Εμπιστευτικότητας·

(ιε) Δήλωση Προστασίας Προσωπικών Δεδομένων·

(ιστ) Δήλωση Ανεξαρτησίας και Αμεροληψίας (μη σύγκρουση συμφερόντων)·

(ιζ) την υποχρέωση ετοιμασίας του πλάνου ελέγχου από τον επικεφαλής ελεγκτή, το οποίο περιλαμβάνει το πεδίο εφαρμογής του ελέγχου και των φυσικών τοποθεσιών στις οποίες θα γίνει ο έλεγχος·

(ιη) πρόνοια ότι ο έλεγχος δεν εξασφαλίζει ότι δεν μπορεί ή δεν πρόκειται να συμβεί κάποιο περιστατικό κυβερνοασφάλειας, καθώς και ότι ο Φορέας δεν απαλλάσσεται από οποιαδήποτε ευθύνη σύμφωνα με τις πρόνοιες του Νόμου και της νομοθεσίας που εκδίδεται βάσει αυτού·

(ιθ) τήρηση από τον ελεγκτή ενεργούς ασφάλειας Επαγγελματικής Ευθύνης (Professional Indemnity insurance) ή/και Ασφάλειας Σφαλμάτων και Παραλείψεων (Errors and Omissions insurance), περιλαμβανομένων και των προβλεπόμενων μέτρων και αποζημίωση ύψους όπως προβλέπεται στη σχετική νομοθεσία, με ποσό κάλυψης τουλάχιστον 200 χιλιάδες ευρώ, με ισχύ τουλάχιστον μέχρι έξι (6) μήνες μετά την ολοκλήρωση του ελέγχου·

(κ) πρόνοια ότι αρμόδια για την επίλυση οποιασδήποτε διαφοράς σχετικής με τη συμφωνία που δυνατό να προκύψει μεταξύ του Φορέα και του ελεγκτή ή των ελεγκτών και που δεν μπορεί να διευθετηθεί μεταξύ τους είναι τα Δικαστήρια της Κυπριακής Δημοκρατίας·

(κα) πρόνοια ότι με την ολοκλήρωση του συνόλου των βημάτων του ελέγχου, ο ελεγκτής καταστρέφει με ασφάλεια όλα τα αρχεία σχετικά με τον έλεγχο, πρωτότυπα ή/και αντίγραφα, συμπεριλαμβανομένης και της Έκθεσης Ελέγχου Ωριμότητας Κυβερνοασφάλειας· και

(κβ) όρους πληρωμής.

Κεφάλαιο ΙΙΙ – Διενέργεια Βημάτων του Ελέγχου

Προετοιμασία / Προγραμματισμός του ελέγχου.

16.- (1) Ο ελεγκτής ή οι ελεγκτές υποχρεούται/νται να ετοιμάζει/ουν κατάλληλο πλάνο ελέγχου (audit plan) για τον έλεγχο και να τον κοινοποιεί/ούν στον Φορέα, με τρόπο που θα συμφωνηθεί μεταξύ τους, τουλάχιστον δύο (2) εβδομάδες πριν τη διενέργεια του ελέγχου:

Νοείται ότι, ο ελεγκτής ή οι ελεγκτές υποχρεούται/νται να κοινοποιεί/ούν το πλάνο ελέγχου (audit plan) για τον έλεγχο και στην Αρχή.

(2) Ενόψει της κοινοποίησης στην Αρχή, ως προνοείται στην παράγραφο (1) του παρόντος άρθρου, η Αρχή ενημερώνεται για το πρόγραμμα ελέγχων που θα διενεργείται στους Φορείς και έχει τη δυνατότητα να παρευρίσκεται ως παρατηρητής στη διαδικασία στις περιπτώσεις που κρίνει απαραίτητο, είτε ύστερα από ειδοποίηση είτε χωρίς ειδοποίηση προς τον Φορέα και τον επικεφαλής ελεγκτή.

(3) Ελεγκτές που εγγράφηκαν ως εκπαιδευόμενοι στο Μητρώο Ελεγκτών Κυβερνοασφάλειας δύναται να παρευρίσκονται σε επικείμενο έλεγχο, κατόπιν συνεννόησης με τον ελεγκτή που επιλέγηκε από τον Φορέα για διενέργεια του ελέγχου, με σκοπό να αποκτήσουν τις ελάχιστες απαιτήσεις ως αυτές καταγράφονται στο ΠΑΡΑΡΤΗΜΑ ΣΤ. Το αίτημα για συνοδεία θα διεκπεραιώνεται μέσω της ηλεκτρονικής πλατφόρμας διαχείρισης των ελέγχων:

Νοείται ότι, οι εκπαιδευόμενοι ελεγκτές δεσμεύονται με όλες τις πρόνοιες της συμφωνίας που έχει συνάψει ο Φορέας με τον/τους ελεγκτή/ες.

Δημιουργία πλάνου ελέγχου.

17.- (1) Με σκοπό την εξασφάλιση επαρκούς χρόνου για τη διενέργεια του ελέγχου και την προετοιμασία του πλάνου ελέγχου, ο/οι ελεγκτής/ές υποχρεούται να ετοιμάσει/ουν πλάνο ελέγχου λαμβάνοντας υπόψη τουλάχιστον τα ακόλουθα:

(α) Τον εκτιμώμενο χρόνο που υπολογίστηκε σύμφωνα με το άρθρο 9 της παρούσας Απόφασης,

(β) τον τομέα στον οποίο δραστηριοποιείται ο Φορέας,

(γ) την κρισιμότητα των εργασιών του τομέα στον οποίο δραστηριοποιείται ο Φορέας,

(δ) την εξοικείωση του/τους με τον Φορέα ή συγκεκριμένες από τις διαδικασίες του,

(ε) το συνολικό αριθμό των εργαζομένων του Φορέα,

(στ) την πολυπλοκότητα των συστημάτων του Φορέα,

(ζ) την υποχρέωση συμμόρφωσης του Φορέα με εξειδικευμένες κάθετες απαιτήσεις, βάσει Αποφάσεων που εκδίδει η Αρχή,

(η) πιθανούς κινδύνους (risks),

(θ) το ωράριο εργασίας του Φορέα και την ύπαρξη ή όχι συστήματος βάρδιας, και

(ι) τις τοποθεσίες που πρέπει να ελεγχθούν κατά τη διενέργεια του ελέγχου και τον χρόνο που χρειάζεται για να μετακινηθεί στις άλλες τοποθεσίες, σε περίπτωση που υπάρχουν.

(2) Κατά τη δημιουργία του πλάνου ελέγχου, ο/οι ελεγκτής/ές υποχρεούται/νται να προβλέψει/ουν και τον απαιτούμενο χρόνο για την ανασκόπηση των σχετικών εγγράφων που θα παρέχει ο Φορέας στον ελεγκτή για επιτόπιο έλεγχο, κατά τη διενέργεια των ελέγχων.

(3) Κατά τη δημιουργία του πλάνου ελέγχου, ο/οι ελεγκτής/ές υποχρεούται/νται να προβλέψει/ουν χρόνο μετά το πέρας του ελέγχου και πριν την διενέργεια της καταληκτικής σύσκεψης για την σύνταξη της σχετικής έκθεσης ελέγχου.

(4) Ο/οι ελεγκτής/ές υποχρεούται/νται να συντάξει/ουν το πλάνο ελέγχου σύμφωνα με το ΠΑΡΑΡΤΗΜΑ Γ.

Υλοποίηση του ελέγχου.

18.- (1) Η υλοποίηση του ελέγχου αποτελείται από τα ακόλουθα στάδια:

(α) Ενέργειες πριν από τη διενέργεια του ελέγχου

(β) Εναρκτήρια σύσκεψη (opening meeting)

(γ) Διενέργεια ελέγχου

(δ) Προετοιμασία σύνταξης Έκθεσης Ελέγχου Ωριμότητας Κυβερνοασφάλειας

(ε) Καταληκτική σύσκεψη (closing meeting)

(2) Σε περίπτωση που, πριν ή κατά τη διενέργεια του ελέγχου, η Αρχή κρίνει απαραίτητο, εκπρόσωποί της δύναται να παρουσιαστούν στη διενέργεια του ελέγχου, είτε ύστερα από ειδοποίηση είτε χωρίς ειδοποίηση προς τον Φορέα και τον επικεφαλής ελεγκτή.

(3) Κατά τη διενέργεια του ελέγχου και εάν ο/οι ελεγκτής/ές το κρίνει/νουν απαραίτητό και κατόπιν συνεννόησης με τον Φορέα, ο/οι ελεγκτής/ές δύναται να συνοδεύεται/νται από τεχνικό εμπειρογνώμονα με εξειδικευμένες γνώσεις (π.χ. operational technology/industrial control systems/SCADA) στο αντικείμενο ελέγχου:

Νοείται ότι, σε περίπτωση που ο/οι ελεγκτής/ές συνοδεύεται/νται από τεχνικό εμπειρογνώμονα, ο ελεγκτής/ές υποχρεούται/νται να ενημερώνει γραπτώς και εκ των προτέρων την Αρχή και συμπληρώνει κατάλληλα το σχετικό σημείο στο πλάνο ελέγχου:

Νοείται περαιτέρω ότι, τα καθήκοντα του τεχνικού εμπειρογνώμονα, περιορίζονται μόνο στην παροχή τεχνικών συμβουλών προς τον/τους ελεγκτή/ές και σε καμιά περίπτωση ο τεχνικός εμπειρογνώμονας δεν λειτουργεί ως ελεγκτής και δεν προβάλλει τις επιστημονικές του απόψεις στον Φορέα:

Νοείται έτι περαιτέρω ότι, ο τεχνικός εμπειρογνώμονας που θα συνοδεύει τον ελεγκτή/ές κατά τη διενέργεια του ελέγχου υποχρεούται να συνάψει Δήλωση Εμπιστευτικότητας, Δήλωση Ανεξαρτησίας και Αμεροληψίας (μη σύγκρουση συμφερόντων) και Δήλωση Προστασίας των Προσωπικών Δεδομένων και δεσμεύεται και με όλες τις πρόνοιες της συμφωνίας που έχει συνάψει ο Φορέας με τον/τους ελεγκτή/ές.

(4) Το κόστος του τεχνικού εμπειρογνώμονα επιβαρύνει τον ελεγκτή, εκτός αν συμφωνηθεί διαφορετικά μεταξύ του Φορέα και του/των ελεγκτή/ών.

Ενέργειες πριν από τη διενέργεια του ελέγχου.

19.- (1) Με σκοπό την αποτελεσματική διενέργεια του ελέγχου, ο/οι ελεγκτής/ές μεταβαίνει/ουν στις εγκαταστάσεις του Φορέα την προκαθορισμένη ημέρα και ώρα, έχοντας μαζί του/τους όλα τα απαραίτητα έγγραφα και τον απαιτούμενο εξοπλισμό για τη διενέργεια του ελέγχου:

Νοείται ότι, κατά το στάδιο του προγραμματισμού του ελέγχου, ως προνοείται στο άρθρο 16 της παρούσας Απόφασης, επιλύθηκαν τα ζητήματα που σχετίζονται με την αδειοδότηση και την δυνατότητα πρόσβασης/εισόδου στις ελεγχόμενες εγκαταστάσεις και η πρόσβαση/είσοδος στις εγκαταστάσεις που δραστηριοποιείται ο Φορέας πραγματοποιείται χωρίς περιττές καθυστερήσεις.

(2) Ο/οι ελεγκτής/ές, κατά την άφιξή τους, ζητούν και συναντούν τον εκπρόσωπο του Φορέα που ανέλαβε τη διαχείριση του ελέγχου, σύμφωνα με το πλάνο ελέγχου, και μεταβαίνει/νουν συνοδευόμενος/νοι στο χώρο που ορίστηκε να διεξαχθεί η εναρκτήρια σύσκεψη.

Εναρκτήρια σύσκεψη (opening meeting).

20.- (1) Η εναρκτήρια σύσκεψη πραγματοποιείται πριν την έναρξη διενέργειας του ελέγχου και με τους αρμόδιους εκπροσώπους που ορίζονται από τον Φορέα και συστήνεται να μην ξεπερνά σε διάρκεια τη μία (1) ώρα.

(2) Σκοπός της εναρκτήριας σύσκεψης είναι η παροχή από τον/τους ελεγκτή/ές μίας σύντομης επισκόπησης και επεξήγησης των βασικών αρχών, λειτουργιών και δραστηριοτήτων του ελέγχου που πρόκειται να διενεργηθεί.

(3) Η εναρκτήρια σύσκεψη δύναται να περιλαμβάνει τουλάχιστον τα ακόλουθα:

(α) Παρουσίαση από τον επικεφαλής Ελεγκτή και σύντομη επεξήγηση του ρόλου τους κατά τη διενέργεια του ελέγχου, συμπεριλαμβανομένων και των εκπαιδευόμενων ελεγκτών ή/και τυχόν τεχνικών εμπειρογνωμόνων.

(β) Επιβεβαίωση του πεδίου ελέγχου.

(γ) Επιβεβαίωση του προγράμματος ελέγχου.

(δ) Επιβεβαίωση ότι υπάρχουν οι κατάλληλοι πόροι και ο κατάλληλος εξοπλισμός για τη βέλτιστη διενέργεια του ελέγχου από τους ελεγκτές.

(ε) Αναφορά στην υποχρέωση για εμπιστευτικότητα του συνόλου της πληροφορίας που αφορά τον έλεγχο, όπως προκύπτει από την σχετική συμφωνία που σύνηψε ο Φορέας με τον ελεγκτή ή τους ελεγκτές.

(στ) Επιβεβαίωση ότι υπάρχει το κατάλληλο προσωπικό του Φορέα που θα συνοδεύσει, είτε ως καθοδηγητής είτε ως παρατηρητής, τον ελεγκτή ή τους ελεγκτές.

(ζ) Τη διαδικασία του ελέγχου και τις βασικές αρχές που διέπουν το μοντέλο ωριμότητας κυβερνοασφάλειας, με έμφαση στον τρόπο βαθμολόγησης καθώς και την ειδική έννοια της βαθμίδας 3.

(η) Τη μορφή της Έκθεσης Ελέγχου Ωριμότητας Κυβερνοασφάλειας (βασικό κείμενο, πίνακας που περιέχει τις ενότητες σύμφωνα με την Απόφαση Κ.Δ.Π. 389/2020 συνοδευόμενες από το επίπεδο που διαβάθμισης που έχει επιτευχθεί πλήρως).

(θ) Αναφορά στην υποχρέωση που υπέχει ο ελεγκτής ή οι ελεγκτές προς την Αρχή, να επαληθεύσει/ουν τις απαιτήσεις του ελέγχου μέσω αντικειμενικών αποδείξεων (audit evidence).

(ι) Αναφορά ότι, με το πέρας της διενέργειας του ελέγχου, η Έκθεση Ελέγχου Ωριμότητας Κυβερνοασφάλειας θα κοινοποιηθεί στην Αρχή από τον επικεφαλής ελεγκτή.

(ια) Αναφορά στον Φορέα, από τον επικεφαλής ελεγκτής, σχετικά με την υποχρέωση του να καταρτίσει πλάνο ενεργειών που πρέπει να θέσει ο ίδιος ο Φορέας με σκοπό τη διόρθωση των σημείων όπου ο Φορέας δεν καλύπτει τις απαιτήσεις του επιπέδου διαβάθμισης 3 (μη συμμόρφωσης):

Νοείται ότι, το πλάνο θα τυγχάνει έγκρισης από την Αρχή πριν την υλοποίηση του.

(ιβ) Αναφορά από τον επικεφαλής ελεγκτή, ότι ο έλεγχος στηρίζεται στην εύρεση αντικειμενικών αποδείξεων με δειγματοληπτικό τρόπο, ως ορίζεται στο ΠΑΡΑΡΤΗΜΑ Δ, και επεξήγηση σχετικά με τους περιορισμούς που ενέχει ο συγκεκριμένος τρόπος ελέγχου.

(ιγ) Δήλωση από τον επικεφαλής ελεγκτή, ότι ο έλεγχος δεν εξασφαλίζει ότι δεν μπορεί ή δεν πρόκειται να συμβεί κάποιο περιστατικό κυβερνοασφάλειας, καθώς και ότι ο Φορέας δεν απαλλάσσεται από οποιαδήποτε ευθύνη σύμφωνα με τις πρόνοιες του Νόμου και της νομοθεσίας που εκδίδεται βάσει αυτού.

(ιδ) Την επιβεβαίωση του χρόνου και του τόπου της καταληκτικής σύσκεψης, στην οποία θα ζητηθεί και υπογραφή της σχετικής Έκθεσης Ελέγχου Ωριμότητας Κυβερνοασφάλειας από εκπρόσωπο της ανώτατης διοίκησης του Φορέα.

(ιε) Υποβολή ερωτήσεων από τον Φορέα και παροχή απαντήσεων προς τον Φορέα εκ μέρους του ελεγκτή.

Διενέργεια του ελέγχου.

21.- (1) Κατά τη διενέργεια του ελέγχου, ο/οι ελεγκτής/ές υποχρεούται/νται να ζητήσει/ουν από τον Φορέα για ανασκόπηση, αντικειμενικές αποδείξεις για να μπορεί/ούν να εκτιμηθεί το επίπεδο ωριμότητας του Φορέα σχετικά με κάθε απαίτηση που προνοείται στην Απόφαση Κ.Δ.Π. 389/2020.

(2) Η επιλογή των αντικειμενικών στοιχείων γίνεται με δειγματοληπτικό τρόπο. Σε περιπτώσεις που η διαθέσιμη πληροφορία δεν δύναται να ελεγχθεί πλήρως, όπως είναι οι περιπτώσεις που υπάρχει 100% δείγμα, ο ελεγκτής υποχρεούται να εφαρμόζει κατάλληλη μέθοδο δειγματοληψίας, ως ορίζεται στο ΠΑΡΑΡΤΗΜΑ Δ.

(3) Κατά τη διάρκεια του ελέγχου διενεργούνται τα ακόλουθα:

(α) Κάθε ελεγκτής, μαζί με τον εκπρόσωπο του Φορέα, μεταβαίνει στις εγκαταστάσεις του Φορέα και διενεργεί τον έλεγχο των σημείων που χρειάζεται να ελέγξει, σύμφωνα με το πλάνο ελέγχου.

(β) Κάθε ελεγκτής υποχρεούται να εφαρμόζει τα μέτρα δέουσας επιμέλειας ως προς την αποτελεσματική ολοκλήρωση του κάθε ελέγχου, εντός των καθορισμένων χρονικών περιθωρίων στο πλάνο ελέγχου:

Νοείται ότι, σε περίπτωση που είναι αδύνατη η υλοποίηση του ελέγχου εντός των καθορισμένων χρονικών περιθωρίων λόγω ανωτέρας βίας ή άλλων αντικειμενικών και αιτιολογημένων δυσκολιών, ο ελεγκτής υποχρεούται να συνεννοηθεί με τον εκπρόσωπο του Φορέα για την χρονική επέκταση του ελέγχου και να γίνει καταγραφή των σχετικών στοιχείων όπως είναι τουλάχιστον η αιτία καθυστέρησης, ο επιπλέον χρόνος που χρειάζεται, η ημερομηνία, η τοποθεσία, τα σημεία ελέγχου που θα ελεγχθούν.

(γ) Ο ελεγκτής, για την εφαρμογή κατάλληλης μεθόδου δειγματοληψίας, δύναται να ζητά πληροφορίες που είναι σχετικές με τον σκοπό του ελέγχου, το πεδίο εφαρμογής του ελέγχου και άλλες σχετικές πληροφορίες:

Νοείται ότι, κατά τη διάρκεια του ελέγχου, ο ελεγκτής δεν δύναται να ζητά από τον Φορέα πληροφορίες που αφορούν τη λειτουργία, την οικονομική κατάσταση, την εμπορική θέση, τη στρατηγική, το πελατολόγιο, την πολιτική μισθοδοσίας του προσωπικού του Φορέα:

Νοείται περαιτέρω ότι, ο ελεγκτής δύναται να ζητά πληροφορίες που προνοούνται στην πρώτη επιφύλαξη της παρούσας παραγράφου μόνο στην περίπτωση που υποστηρίζουν την κάλυψη κάποιας απαίτησης.

(δ) Ο ελεγκτής υποχρεούται όπως κάθε πληροφορία που ζητά από τον Φορέα για ανασκόπηση και ελέγχεται από αυτόν να την καταχωρεί ως αναφορά (reference) στο κατάλληλο σημείο της Έκθεσης Ελέγχου Ωριμότητας Κυβερνοασφάλειας, ως αποδεικτικό του ελέγχου (αντικειμενική απόδειξη) (audit evidence).

(ε) Ο ελεγκτής δύναται να χρησιμοποιήσει διαφορετικές μεθόδους συλλογής αντικειμενικών αποδείξεων όπως οι συνεντεύξεις, παρακολούθηση διεργασιών και δραστηριοτήτων, παρατήρηση του περιβάλλοντος χώρου και των σχετικών συνθηκών, ανασκόπηση τεκμηριωμένης πληροφορίας, αρχείων, μελετών, αναλύσεων στοιχείων, ανασκόπηση αναφορών από διάφορες πηγές, επισκόπησης παραμετροποιήσεων βάσεων δεδομένων και επισκόπησης των περιεχομένων τους.

(στ) Ο ελεγκτής υποχρεούται, με την συνδρομή του Φορέα, να εξασφαλίζει στον μέγιστο βαθμό ότι η πληροφορία που ελέγχει είναι:

(i) πλήρης και περιέχει όλη την πληροφορία που χρειάζεται για να εξαχθεί κάποιο συμπέρασμα,

(ii) πραγματική (αντικατοπτρίζει την πραγματική κατάσταση του εξεταζόμενου στοιχείου),

(iii) συνεπής (η πληροφορία είναι συνεπής προς τα διάφορα σχετικά έγγραφα ή υλοποιήσεις) και επίκαιρη (η πληροφορία είναι επικαιροποιημένη και σύγχρονη και όχι απαρχαιωμένη).

(ζ) Ο ελεγκτής υποχρεούται, με την συνδρομή του Φορέα, να επιβεβαιώνει, στον βαθμό που είναι δυνατόν, την ακεραιότητα της ληφθείσας πληροφορίας με κατάλληλο τρόπο και όπου είναι δυνατόν αυτή να επιβεβαιώνεται μέσω δεδομένων ιχνηλάτισης (audit trails) ή/και αυτοματοποιημένων καταστάσεων συστήματος.

(η) Ο ελεγκτής υποχρεούται να αρχίζει τη διαδικασία συλλογής αντικειμενικών στοιχείων από το επίπεδο διαβάθμισης ωριμότητας 1 και για κάθε επίπεδο διαβάθμισης ωριμότητας τα αποδεικτικά στοιχεία του ελέγχου που συγκρίνονται προς τις απαιτήσεις του κάθε επιπέδου, με σκοπό να εξεταστεί κατά πόσο υπάρχει πλήρης συμμόρφωση με τις απαιτήσεις του επιπέδου:

Νοείται ότι, σε περίπτωση που για το εξεταζόμενο επίπεδο διαβάθμισης ωριμότητας δεν προκύπτει πλήρης συμμόρφωση προς τις απαιτήσεις του, ο ελεγκτής σημειώνει στο κατάλληλο σημείο του ερωτηματολογίου το μέρος της απαίτησης που δεν καλύπτεται από το εξεταζόμενο επίπεδο και εξάγεται ως συμπέρασμα ότι ο Φορέας επιτυγχάνει πλήρως το προηγούμενο επίπεδο διαβάθμισης ωριμότητας.

Νοείται περαιτέρω ότι, σε περίπτωση που υπάρχουν αποδεικτικά στοιχεία πλήρους συμμόρφωσης σ' ένα επίπεδο διαβάθμισης ωριμότητας, ο ελεγκτής συνεχίζει τη διαδικασία συλλογής αντικειμενικών στοιχείων για το επόμενο επίπεδο διαβάθμισης ωριμότητας.

(θ) Ο ελεγκτής υποχρεούται να σημειώνει στο ερωτηματολόγιο του ελέγχου, με ευδιάκριτο τρόπο, το επίπεδο διαβάθμισης ωριμότητας ανά απαίτηση, που έχει επιτευχθεί από τον Φορέα.

(ι) Ο ελεγκτής υποχρεούται να διενεργεί τον έλεγχο τουλάχιστον μέχρι το επίπεδο διαβάθμισης ωριμότητας 3.

(ια) Κατά τη διάρκεια του ελέγχου, ο ελεγκτής δεν χειρίζεται οποιονδήποτε πληροφοριακό εξοπλισμό ή άλλου τύπου εξοπλισμό του Φορέα, ακόμη και στις περιπτώσεις που είναι άριστα καταρτισμένος ή πιστοποιημένος ή/και κατάλληλα εκπαιδευμένος:

Νοείται ότι, σε εξαιρετικές περιπτώσεις που ο ελεγκτής ζητήσει παρέμβαση σε πληροφοριακό εξοπλισμό, θα γίνεται μετά από έγκριση του Φορέα και μόνο στη παρουσία εκπροσώπου του Φορέα.

Ολοκλήρωση του ελέγχου και ετοιμασία της Έκθεσης Ελέγχου Ωριμότητας Κυβερνο-ασφάλειας.

22.- (1) Μετά την ολοκλήρωση του ελέγχου, η ομάδα ελέγχου πραγματοποιεί σύσκεψη με τον επικεφαλής ελεγκτή και χωρίς την παρουσία εκπροσώπων του Φορέα, με σκοπό να συζητηθεί η συνολική εικόνα για τη συμμόρφωση του Φορέα με τις απαιτήσεις της Απόφασης Κ.Δ.Π. 389/2020 και το επίπεδο διαβάθμισης ωριμότητας που έχει επιτύχει ο Φορέας σε κάθε μέτρο ασφάλειας.

(2) Σε περίπτωση που πραγματοποιηθεί έλεγχος σε περισσότερες τοποθεσίες όπου έχει εγκαταστάσεις ο Φορέας και υπάρχουν διαφορετικά αποτελέσματα/επίπεδα διαβάθμισης ωριμότητας σε ίδιους ελέγχους, ο επικεφαλής ελεγκτής, αναλόγως της περίπτωσης, αναλαμβάνει την εξάλειψη/επίλυση των διαφορών και τη συγχώνευσή τους.

(3) Ο επικεφαλής ελεγκτής, καταγράφει στην Έκθεση Ελέγχου Ωριμότητας Κυβερνοασφάλειας το επίπεδο ωριμότητας που έχει επιτύχει ο Φορέας σε κάθε ένα μέτρο ασφάλειας που προνοείται στο ΠΑΡΑΡΤΗΜΑ ΙΙΙ της Απόφασης Κ.Δ.Π. 389/2020. Στις περιπτώσεις που ο Φορέας δεν έχει επιτύχει το επιθυμητό επίπεδο ωριμότητας 3, ο επικεφαλής ελεγκτής υποχρεούται να επισημαίνει τις σχετικές αποκλίσεις και την τεκμηρίωση που έλαβε κατά την ανασκόπηση αντικειμενικών αποδείξεων.

(4) Η Έκθεση Ελέγχου Ωριμότητας Κυβερνοασφάλειας αφού συμπληρωθεί υπογράφεται από όλους τους ελεγκτές που διενήργησαν τον έλεγχο.

(5) Η ομάδα ελέγχου οφείλει να προετοιμάζεται για την καταληκτική σύσκεψη, κατά τη διάρκεια της οποίας θα παρουσιαστούν τα αποτελέσματα του ελέγχου και τα οποία έχουν καταγραφεί στο έντυπο της Έκθεσης Ελέγχου Ωριμότητας Κυβερνοασφάλειας.

Καταληκτική σύσκεψη.

23.- (1) Η καταληκτική σύσκεψη πραγματοποιείται με σκοπό την παρουσίαση στον Φορέα των αποτελεσμάτων του ελέγχου και το επίπεδο διαβάθμισης ωριμότητας που έχει επιτύχει για κάθε μέτρο ασφάλειας, ως αυτά ορίζονται στην Απόφαση Κ.Δ.Π. 389/2020.

(2) Στην καταληκτική σύσκεψη υποχρεούται/υποχρεούνται να συμμετέχει/συμμετέχουν εκπρόσωπος/εκπρόσωποι της ανώτατης διοίκησης του Φορέα και, όποτε απαιτείται, ο εκπρόσωπος του Φορέα που ανέλαβε τη διαχείριση του ελέγχου και συμμετείχε στη διενέργεια του ελέγχου.

(3) Η καταληκτική σύσκεψη δύναται να περιλαμβάνει τουλάχιστον τις ακόλουθες αναφορές από τον επικεφαλής ελεγκτή:

(α) Ότι ο έλεγχος που διενεργήθηκε βασίστηκε στην ανασκόπηση αντικειμενικών στοιχείων με δειγματοληπτικό τρόπο.

(β) Στον τρόπο βάσει του οποίου ετοιμάστηκε η Έκθεση Ελέγχου Ωριμότητας Κυβερνοασφάλειας.

(γ) Στο επίπεδο διαβάθμισης ωριμότητας για κάθε μέτρο ασφάλειας που βρίσκεται ο Φορέας, ως αυτό ορίζεται στην Απόφαση Κ.Δ.Π. 389/2020, και αναφορά εάν ο Φορέας επιτυγχάνει ή όχι το επιθυμητό επίπεδο διαβάθμισης ωριμότητας 3, με τρόπο που να είναι κατανοητός από τη διοίκηση του Φορέα.

(δ) Στο χρονοδιάγραμμα το οποίο ο Φορέας υποχρεούται να υποβάλει ένα πλάνο ενεργειών στην Αρχή για την διόρθωση των σημείων των οποίων ο Φορέας δεν καλύπτει τις απαιτήσεις του επιπέδου διαβάθμισης ωριμότητας 3.

(4) Σε περίπτωση που υπάρχουν αποκλίνουσες απόψεις όσον αφορά τα συμπεράσματα του ελέγχου μεταξύ του/των ελεγκτή/τών και του Φορέα, πρέπει να συζητούνται και, αν είναι δυνατόν, να επιλύονται. Οι αποκλίνουσες απόψεις, θα πρέπει να καταγράφονται στην Έκθεση Ελέγχου Ωριμότητας Κυβερνοασφάλειας, έστω και αν επιλυθήκαν.

Ενέργειες μετά το πέρας του ελέγχου.

24.- (1) Η διαδικασία του ελέγχου ολοκληρώνεται όταν ο επικεφαλής ελεγκτής παραδίδει στον εκπρόσωπο της ανώτατης διοίκησης του Φορέα την Έκθεση Ελέγχου Ωριμότητας Κυβερνοασφάλειας και ο εκπρόσωπος της ανώτατης διοίκησης του Φορέα υποχρεούται να την υπογράψει ως αποδοχή των αποτελεσμάτων που έχουν καταγραφεί στη σχετική Έκθεση. Σε περίπτωση που τηρηθεί η πρόνοια της παραγράφου (4) του άρθρου 23 της παρούσας και ο Φορέας αρνείται να υπογράψει την Έκθεση Ελέγχου Ωριμότητας Κυβερνοασφάλειας, τότε η εν λόγω Έκθεση θεωρείται μη ολοκληρωμένη και ότι ο Φορέας δεν συμμορφώνεται με τις υποχρεώσεις του, ως αυτές προνοούνται στο Νόμο και στη δυνάμει αυτού εκδοθείσα νομοθεσία:

Νοείται ότι, σε περίπτωση που ο Φορέας αρνείται να υπογράψει την Έκθεση Ελέγχου Ωριμότητας Κυβερνοασφάλειας ως ορίζεται στην παρούσα παράγραφο, ο ελεγκτής ενημερώνει γραπτώς την Αρχή για τη μη ολοκλήρωση της έκθεσής του και ότι ο Φορέας δεν συμμορφώνεται με τις υποχρεώσεις του ως αυτές προνοούνται στο Νόμο και στη δυνάμει αυτού εκδοθείσα νομοθεσία.

(2) Ο επικεφαλής ελεγκτής υποχρεούται να κοινοποιεί στην Αρχή αντίγραφο της Έκθεσης Ελέγχου Ωριμότητας Κυβερνοασφάλειας του Φορέα, η οποία θα είναι υπογεγραμμένη από τον Φορέα και από όλους τους ελεγκτές που διενήργησαν τον έλεγχο, και να ενημερώνει την Αρχή για την ολοκλήρωση του ελέγχου.

(3) Ο Φορέας υποχρεούται εντός τριάντα (30) ημερολογιακών ημερών να ετοιμάσει και να αποστείλει στην Αρχή το χρονοδιάγραμμα με το πλάνο ενεργειών των σημείων μη συμμόρφωσης με τις απαιτήσεις του επιπέδου διαβάθμισης ωριμότητας 3. Σε περίπτωση που η Αρχή κρίνει ότι το πλάνο ενεργειών ή/και το χρονοδιάγραμμα που έθεσε ο Φορέας δεν είναι ικανοποιητικά, τότε δύναται να ενημερώσει γραπτώς τον Φορέα και να ζητήσει αναθεώρησή τους:

Νοείται ότι, σε εξαιρετικές περιπτώσεις, ο Φορέας έχει το δικαίωμα να αποστείλει γραπτό αιτιολογημένο αίτημα προς την Αρχή και να ζητήσει παράταση ετοιμασίας του πλάνου ενεργειών μόνο για συγκεκριμένα μέτρα. Η Αρχή υποχρεούται, ανά περίπτωση, να εξετάσει το αίτημα και εάν το κρίνει αιτιολογημένο να αποδεχτεί την παράταση, η οποία δεν θα υπερβαίνει τις επιπλέον τριάντα (30) ημερολογιακές ημέρες.

(4) Τηρουμένων των διατάξεων της παραγράφου 3 του παρόντος άρθρου, η Αρχή δύναται, βάσει του χρονοδιαγράμματος που έθεσε ο Φορέας, να προγραμματίσει και να ενημερώσει γραπτώς τον Φορέα ότι προτίθεται να προβεί σε επιτόπιο έλεγχο συμμόρφωσης του πλάνου ενεργειών που έθεσε ο Φορέας με σκοπό την άρση μη συμμόρφωσης των μέτρων που εντοπίστηκαν κατά τη διενέργεια του ελέγχου.

Κεφάλαιο IV – Μοντέλο Ωριμότητας Κυβερνοασφάλειας

Περιεχόμενο μοντέλου ωριμότητας κυβερνο-ασφάλειας.

25.- (1) Το μοντέλο ωριμότητας κυβερνοασφάλειας (cybersecurity maturity model), ως ορίζεται στο ΠΑΡΑΡΤΗΜΑ Ε της παρούσας Απόφασης, καλύπτει το πλήρες εύρος των απαιτήσεων ασφαλείας ως προνοούνται στο ΠΑΡΑΡΤΗΜΑ ΙΙΙ της Απόφασης Κ.Δ.Π. 389/2020 και στους τρείς σχετικούς πυλώνες προετοιμασίας (Prepare), προστασίας και εντοπισμού (Protect and Detect) και ανταπόκρισης (Respond).

(2) Το μοντέλο ωριμότητας κυβερνοασφάλειας (cybersecurity maturity model) βασίζεται σε διεθνείς βέλτιστες πρακτικές και πρότυπα και περιέχει πέντε (5) διακριτά επίπεδα ωριμότητας κυβερνοασφάλειας. Το επίπεδο 3 περιέχει εξειδίκευση και διασαφήνιση των απαιτήσεων της Απόφασης Κ.Δ.Π. 389/2020 και δύναται να αναγνωρίσει το επίπεδο των Φορέων που συμμορφώθηκαν με τις απαιτήσεις της Απόφασης Κ.Δ.Π. 389/2020 αλλά και των Φορέων που ακόμη να συμμορφωθούν.

(3) Το μοντέλο ωριμότητας κυβερνοασφάλειας (cybersecurity maturity model) χρησιμοποιείται ως βάση για τη διενέργεια των ελέγχων και αξιολογεί το επίπεδο συμμόρφωσης του Φορέα με τις απαιτήσεις της Απόφασης Κ.Δ.Π. 389/2020.

Κεφάλαιο V – Ελεγκτής κυβερνοασφάλειας

Αρμοδιότητα και υποχρεώσεις του ελεγκτή.

26.- (1) Ο ελεγκτής είναι αρμόδιός να διενεργεί τους ελέγχους με τη χρήση του μοντέλου ωριμότητας κυβερνοασφάλειας (cybersecurity maturity model) της Αρχής, το οποίο είναι δομημένο και καλύπτει τις απαιτήσεις του Παραρτήματος ΙΙΙ: Πλαίσιο μέτρων ασφαλείας της Απόφασης Κ.Δ.Π. 389/2020.

(2) (α) Ο ελεγκτής δύναται να διενεργεί ελέγχους εφόσον είναι εγγεγραμμένος στο Μητρώο Ελεγκτών Κυβερνοασφάλειας, κατ' εφαρμογή των διατάξεων στο Κεφάλαιο V της παρούσας Απόφασης.

(β) Ο ελεγκτής υποχρεούται να αποδέχεται αιτήματα για συνοδεία από εκπαιδευόμενο ελεγκτή κατά τη διενέργεια των ελέγχων.

(γ) Ο μέγιστος αριθμός συνοδευόμενων εκπαιδευόμενων ελεγκτών κατά τη διενέργεια των ελέγχων είναι δύο (2).

Βασικές Δεξιότητες Ελεγκτή.

27. Ο ελεγκτής υποχρεούται να διαθέτει τις ακόλουθες βασικές δεξιότητες:

(α) Ακολουθεί και εφαρμόζει βέλτιστες πρακτικές για την διενέργεια των ελέγχων και τη Διαδικασία Διενέργειας Ελέγχων Ωριμότητας Κυβερνοασφάλειας·

(β) κατά την κατάρτιση του πλάνου δειγματοληψίας, εφαρμόζει μέθοδο δειγματοληψίας ανά μέτρο ασφαλείας ως αυτό ορίζεται στο ΠΑΡΑΡΤΗΜΑ ΙΙΙ της Απόφασης Κ.Δ.Π. 389/2020·

(γ) επεξηγεί στο σύνολο του προσωπικού τις απαιτήσεις και τον τρόπο λειτουργίας του μοντέλου ωριμότητας κυβερνοασφάλειας (cybersecurity maturity model)·

(δ) οργανώνει και εργάζεται στα πλαίσια του ελέγχου με συστηματικό και ανεξάρτητο τρόπο·

(ε) αναγνωρίζει τις πηγές πληροφοριών που μπορεί να αποτελέσουν αντικειμενικές αποδείξεις για τον έλεγχο και τις ανασκοπεί με κατάλληλο τρόπο·

(στ) συγκρίνει τις αντικειμενικές αποδείξεις προς τις απαιτήσεις του ελέγχου και εξάγει αντικειμενικά συμπεράσματα·

(ζ) διενεργεί τους ελέγχους με ακεραιότητα, αμεροληψία και ανεξαρτησία·

(η) καταγράφει με αποτελεσματικό τρόπο τα συμπεράσματα από τη διενέργεια του ελέγχου·

(θ) καταγράφει με απλό και κατανοητό τρόπο τις αντικειμενικές αποδείξεις και το επίπεδο διαβάθμισης ωριμότητας που έχει επιτευχθεί από τον Φορέα·

(ι) ικανότητα χρήσης ηλεκτρονικών υπολογιστών και ιδιαίτερα προγραμμάτων όπως το Microsoft Office (όπως Word, Excel, PowerPoint κλπ) και άλλα ηλεκτρονικά εργαλεία που δύναται να καθορίσει η Αρχή· και

(ια) ακεραιότητα χαρακτήρα, εχεμύθεια, οργανωτικές και διοικητικές ικανότητες, πρωτοβουλία, υπευθυνότητα, ευθυκρισία και ικανότητα αποτελεσματικής συνεργασίας.

Βασικές γνώσεις ελεγκτή.

28.- (1) Ο ελεγκτής υποχρεούται να διαθέτει τις ακόλουθες βασικές γνώσεις:

(α) Γνωρίζει τις πρόνοιες του Νόμου βάσει των οποίων εκδόθηκε η Απόφαση Κ.Δ.Π. 389/2020 και το σύνολο των προνοιών της Απόφασης Κ.Δ.Π. 389/2020, με έμφαση στα μέτρα του ΠΑΡΑΡΤΗΜΑΤΟΣ ΙΙΙ της Απόφασης Κ.Δ.Π. 389/2020·

(β) διαθέτει την ικανότητα να ανακαλέσει γνώσεις σχετικά με τα μέτρα και τις λύσεις κυβερνοασφάλειας που συνδέονται με τα μέτρα του ΠΑΡΑΡΤΗΜΑΤΟΣ ΙΙΙ της Απόφασης Κ.Δ.Π. 389/2020·

(γ) κατανοεί και διαθέτει την ικανότητα να ερμηνεύσει όταν μία συγκεκριμένη πληροφορία συνδέεται με τις απαιτήσεις των μέτρων του ΠΑΡΑΡΤΗΜΑΤΟΣ ΙΙΙ της Απόφασης Κ.Δ.Π. 389/2020·

(δ) κατανοεί και διαθέτει την ικανότητα να εξηγήσει τη σύνδεση συγκεκριμένων λειτουργιών πληροφορικής και ασφάλειας με τις απαιτήσεις των μέτρων του ΠΑΡΑΡΤΗΜΑΤΟΣ ΙΙΙ της Απόφασης Κ.Δ.Π. 389/2020·

(ε) διαθέτει την ικανότητα να ανακαλέσει γνώσεις σχετικά με την σχετική αποτελεσματικότητα των μέτρων ασφαλείας και ειδικά αυτών του ΠΑΡΑΡΤΗΜΑΤΟΣ ΙΙΙ της Απόφασης Κ.Δ.Π. 389/2020·

(στ) κατανοεί και διαθέτει την ικανότητα να συγκρίνει και να εξηγήσει τεχνικές και μεθόδους για την ανασκόπηση αντικειμενικών αποδείξεων στο πλαίσιο διενέργειας των ελέγχων·

(ζ) κατανοεί και διαθέτει την ικανότητα να συγκρίνει και να επεξηγήσει την αξία, τα μειονεκτήματα, τις επιλογές και τον τρόπο επιλογής μεθόδου δειγματοληψίας στα μέτρα ασφαλείας για την ανασκόπηση αντικειμενικών αποδείξεων στο πλαίσιο διενέργειας των ελέγχων·

(η) κατανοεί τις έννοιες της συστηματικότητας, ανεξαρτησίας, αμεροληψίας, αντικειμενικότητας και τεκμηρίωσης στο πλαίσιο διενέργειας των ελέγχων·

(θ) γνωρίζει και μπορεί να αναγνωρίσει και να ανακαλέσει τις σχετικές νομικές και κανονιστικές απαιτήσεις στο πλαίσιο διενέργειας των ελέγχων·

(ι) κατανοεί την έννοια της προστασίας του προσωπικού και του εμπορικού απόρρητου και τις σχετικές υποχρεώσεις ως αυτές απορρέουν από την ισχύουσα Νομοθεσία και

(ια) γνωρίζει την ισχύουσα νομοθεσία σε θέματα Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

(2) Ο ελεγκτής απαιτείται όπως διαθέτει γνώσεις σε ενότητες μέτρων όπως, ενδεικτικά, είναι:

(α) η αξιολόγηση κινδύνων

(β) η ασφάλεια ανθρώπινων πόρων

(γ) η ασφάλεια δεδομένων

(δ) η ασφάλεια δικτύου

(ε) η ασφάλεια εφαρμογών

(στ) η ασφάλεια συστημάτων

(ζ) η διακυβέρνηση

(η) η διαχείριση αλλαγών

(θ) η διαχείριση ευπαθειών και ενημερώσεων ασφάλειας

(ι) η διαχείριση κινδύνων

(ια) η διαχείριση στοιχείων ενεργητικού

(ιβ) η διαχείριση συμβάντων και περιστατικών

(ιγ) η διαχείριση ταυτότητας και πρόσβασης

(ιδ) η επιχειρησιακή συνέχεια και ανθεκτικότητα

(ιε) η επιχειρησιακή συνέχεια και αντιμετώπιση Εκτάκτων Συνθηκών

(ιστ) η ευαισθητοποίηση και εκπαίδευση

(ιζ) η εφαρμογή Συστήματος/Πλαισίου Διαχείρισης Ασφάλειας - Εφαρμογή Τεχνικών και Οργανωτικών Μέτρων

(ιη) η καταγραφή και παροχή Πληροφοριών

(ιθ) η στρατηγική

(κ) η φυσική ασφάλεια

(κα) η διαχείριση τρίτων μερών και προμηθευτών

Προσόντα και επαγγελματική εμπειρία ελεγκτή.

29. Ο ελεγκτής υποχρεούται να διαθέτει τα προσόντα και την επαγγελματική πείρα ως αυτά περιγράφονται στην παράγραφο 6.1 του ΠΑΡΑΡΤΗΜΑΤΟΣ ΣΤ.

Καθήκοντα ελεγκτή.

30. Ο ελεγκτής έχει τουλάχιστον τα ακόλουθα καθήκοντα:

(α) Επικοινωνεί με τον Φορέα σχετικά με τους ελέγχους ωριμότητας κυβερνοασφάλειας, σύμφωνα με τις απαιτήσεις του ΠΑΡΑΡΤΗΜΑΤΟΣ ΙΙΙ της Απόφασης Κ.Δ.Π. 389/2020, με σκοπό τον προγραμματισμό και την προετοιμασία για την διενέργεια κάθε ελέγχου·

(β) σε περίπτωση που χρειαστεί, επικουρεί την Αρχή για τον καλύτερο προσδιορισμό της διάρκειας του ανατεθειμένου ελέγχου·

(γ) για κάθε ανατιθέμενο έλεγχο επικοινωνεί με τον Φορέα και ακολουθεί πλάνο ελέγχου, σύμφωνα με το χρονοδιάγραμμα που προβλέπει η Διαδικασία Διενέργειας Ελέγχων Ωριμότητας Κυβερνοασφάλειας·

(δ) ακολουθεί τις βέλτιστες πρακτικές ελέγχου, όπως είναι το πρότυπο ISO:19011 (Κατευθυντήριες οδηγίες για την επιθεώρηση συστημάτων διαχείρισης) και ISO/IEC:17021 (Αξιολόγηση της συμμόρφωσης – απαιτήσεις για φορείς επιθεώρησης και πιστοποίησης συστημάτων διαχείρισης), τις προδιαγραφές της Διαδικασία Διενέργειας Ελέγχων Ωριμότητας Κυβερνοασφάλειας, τις σχετικές νομικές, κανονιστικές και συμβατικές απαιτήσεις κατά τη διάρκεια διενέργειας του ελέγχου·

(ε) ανασκοπεί αντικειμενικές αποδείξεις για κάθε επιτεύξιμο επίπεδο ωριμότητας του Φορέα και τις καταγράφει στον κατάλληλο χώρο εντός του ερωτηματολογίου ελέγχου·

(στ) συγκρίνει τις αντικειμενικές αποδείξεις με τις απαιτήσεις του μοντέλου ωριμότητας κυβερνοασφάλειας και εξάγει ανεξάρτητα και αντικειμενικά αποτελέσματα σχετικά με το μέγιστο επίπεδο που έχει επιτύχει ανά περίπτωση ο Φορέας·

(ζ) συντάσσει την Έκθεση Ελέγχου Ωριμότητας Κυβερνοασφάλειας, τηρουμένης της Διαδικασίας Διενέργειας Ελέγχων Ωριμότητας Κυβερνοασφάλειας, την παραδίδει στον Φορέα και λαμβάνει την επιβεβαίωση από αυτόν·

(η) υποβάλλει, με τρόπο που διασφαλίζεται η ασφάλεια των πληροφοριών, αντίγραφο της υπογεγραμμένης Έκθεσης Ελέγχου Ωριμότητας Κυβερνοασφάλειας στην Αρχή·

(θ) προστατεύει την ακεραιότητα, διαθεσιμότητα και εμπιστευτικότητα των σχετικών αρχείων ελέγχου κατά τη διενέργεια του ελέγχου·

(ι) με την ολοκλήρωση του συνόλου των βημάτων του ελέγχου, καταστρέφει με ασφάλεια όλα τα αρχεία σχετικά με τον έλεγχο, πρωτότυπα ή/και αντίγραφα, συμπεριλαμβανομένης και της Έκθεσης Ελέγχου Ωριμότητας Κυβερνοασφάλειας·

(ια) είναι διαθέσιμος για πιθανές διευκρινίσεις που δύναται να ζητήσει η Αρχή ή ο Φορέας σχετικά με τους ελέγχους που διενήργησε·

(ιβ) κατά την διενέργεια των ελέγχων και μετά το πέρας αυτών, οφείλει να τηρεί τις υποχρεώσεις σε σχέση με την ηθική, την εχεμύθεια και την επαγγελματική συμπεριφορά, ως προνοούνται στις σχετικές συμφωνίες·

(ιγ) τηρεί ενεργή ασφάλεια Επαγγελματικής Ευθύνης (Professional Indemnity insurance) ή/και Ασφάλεια Σφαλμάτων και Παραλείψεων (Errors and Omissions insurance), περιλαμβανομένων και των προβλεπόμενων μέτρων και αποζημίωση ύψους όπως προβλέπεται στη σχετική νομοθεσία, με ποσό κάλυψης τουλάχιστον 200 χιλιάδες ευρώ, με ισχύ τουλάχιστον μέχρι έξι (6) μήνες μετά την ολοκλήρωση του ελέγχου· και

(ιδ) παρέχει οποιαδήποτε πληροφόρηση που δύναται να ζητήσει η Αρχή, σχετικά με τους ελέγχους που διενήργησε.

Παραδοτέα επικεφαλής ελεγκτή.

31. Ο επικεφαλής ελεγκτής υποχρεούται να παραδώσει στην Αρχή και τον Φορέα τα ακόλουθα:

(α) Το πλάνο ελέγχου (audit plan) του εκάστοτε ανατεθειμένου ελέγχου, σύμφωνα με το χρονοδιάγραμμα που προβλέπει η Διαδικασία Διενέργειας Ελέγχων Ωριμότητας Κυβερνοασφάλειας.

(β) Συμπληρωμένη την Έκθεση Ελέγχου Ωριμότητας Κυβερνοασφάλειας, που περιλαμβάνει το ερωτηματολόγιο του μοντέλου ωριμότητας κυβερνοασφάλειας για όλα τα μέτρα του ελέγχου που διενεργήθηκε.

Κεφάλαιο VI – Διαδικασία ένταξης στο Μητρώο Ελεγκτών Κυβερνοασφάλειας

Διαδικασία ένταξης στο Μητρώο στο Μητρώο Ελεγκτών Κυβερνο-ασφάλειας

32.- (1) Για να ενταχθεί κάποιος στο Μητρώο Ελεγκτών Κυβερνοασφάλειας προαπαιτείται να κατέχει όσα προνοούνται στο Κεφάλαιο V της παρούσας Απόφασης και να ακολουθήσει τα βήματα που προνοούνται στο ΠΑΡΑΡΤΗΜΑ ΣΤ «Πλαίσιο εγγραφής ελεγκτών κυβερνοασφάλειας».

Κεφάλαιο VII – Υποβολή και διαχείριση παραπόνων/καταγγελιών/ενστάσεων

Υποβολή Παραπόνων, Καταγγελιών και Ενστάσεων.

33.- (1) Ο Φορέας και ο ελεγκτής ή ο επικεφαλής ελεγκτής δύναται να υποβάλλουν παράπονο/ καταγγελία/ ένσταση στην Αρχή ηλεκτρονικά, σε συγκεκριμένη πλατφόρμα που θα θέσει σε λειτουργία προς τον σκοπό αυτόν η Αρχή και σύμφωνα με τη διαδικασία που ορίζεται στο ΠΑΡΑΡΤΗΜΑ Ζ:

Νοείται ότι, εάν για οποιοδήποτε λόγο η ηλεκτρονική υποβολή του εκάστοτε παραπόνου, καταγγελίας και ένστασης δεν είναι εφικτή στη συγκεκριμένη πλατφόρμα, τότε ο παραπονούμενος υποβάλλει παράπονο / καταγγελία / ένσταση κατόπιν συνεννόησης με την Αρχή.

(2) Σε περίπτωση που ο Φορέας δεν συμφωνεί με τα αποτελέσματα του ελέγχου όπως τα καταγράφει/ουν ο/οι ελεγκτής/ές στην Έκθεση Ελέγχου δύναται να υποβάλει παράπονο, καταγγελία και ένσταση στην Αρχή, τηρουμένης της παραγράφου 1 του παρόντος άρθρου:

Νοείται ότι, σε εξαιρετικές περιπτώσεις, ο Φορέας έχει το δικαίωμα να αποστείλει γραπτό αιτιολογημένο αίτημα προς την Αρχή και να ζητήσει αναστολή της ετοιμασίας του πλάνου ενεργειών ή την αναστολή της ετοιμασίας του πλάνου ενεργειών για συγκεκριμένα μέτρα που υπέβαλε παράπονο/ καταγγελία/ ένσταση. Η Αρχή, ανά περίπτωση, δύναται να εξετάσει το αίτημα και εάν το κρίνει αιτιολογημένο να αποδεχτεί την αναστολή, μέχρι την ολοκλήρωση της διαδικασίας χειρισμού παραπόνου/ καταγγελίας/ ένστασης και την έκδοση της σχετικής Απόφασης.

Διαχείριση παραπόνων, καταγγελιών και ενστάσεων.

34.- (1) Η Αρχή είναι αρμόδια να χειρίζεται παράπονα, καταγγελίες και ενστάσεις που λαμβάνει από τον παραπονούμενο.

(2) Η Αρχή υποχρεούται, εντός πέντε (5) εργάσιμων ημερών από τη λήψη ενός παραπόνου, καταγγελίας και ένστασης, να επιβεβαιώσει εάν αφορούν τις διαδικασίες της παρούσας Απόφασης και των Παραρτημάτων αυτής και να ενημερώσει τον παραπονούμενο σχετικά με τη λήψη του/της. Σε περίπτωση που το παράπονο, η καταγγελία και η ένσταση εμπίπτουν στις διαδικασίες της παρούσας Απόφασης, η Αρχή οφείλει να χειριστεί το παράπονο, την καταγγελία και την ένταση και να εκδώσει σχετική Απόφαση.

(3) Η Αρχή, πριν την έκδοση της Απόφασης, υποχρεούται να συγκεντρώσει και να επαληθεύσει τις πληροφορίες που θα αναφέρονται στο παράπονο, την καταγγελία και την ένσταση.

(4) Η Αρχή είναι αρμόδια να εκδίδει τις Αποφάσεις, δεόντως αιτιολογημένες, που σχετίζονται με τον χειρισμό των παραπόνων, καταγγελιών και ενστάσεων:

Νοείται ότι, η υποβολή, ο χειρισμός και η Απόφαση που δύναται να εκδώσει η Αρχή επί του παραπόνου, της καταγγελίας και της ένστασης δεν δύναται να οδηγεί σε διακρίσεις εις βάρος του Φορέα, όσον αφορά την υλοποίηση των απαιτήσεων που προνοούνται στην Απόφαση Κ.Δ.Π. 389/2020.

(5) Η Αρχή οφείλει να κοινοποιεί την Απόφασή της στον παραπονούμενο και με την κοινοποίηση της Απόφασης της Αρχής νοείται το τέλος της διαδικασίας χειρισμού του παραπόνου, της καταγγελίας και της ένστασης.

Κεφάλαιο VIII – Συνοπτική Επίλυση Διαφορών

Συνοπτική Επίλυση Διαφορών.

35.- (1) (α) Η Αρχή αναλαμβάνει την επίλυση διαφοράς ή χειρισμού υπόθεσης είτε με δική της πρωτοβουλία είτε κατόπιν παραπόνου/καταγγελίας/ένστασης. Στην περίπτωση καταχώρησης παραπόνου/καταγγελίας/ένστασης, η Αρχή έχει την εξουσία να απορρίψει το παράπονο/την καταγγελία/την ένσταση, εάν κατά τη γνώμη της είναι προφανώς αβάσιμη. Σε όλες τις άλλες περιπτώσεις, η Αρχή θα διαβιβάζει αντίγραφο του παραπόνου/της καταγγελίας/της ένστασης στο ενδιαφερόμενο πρόσωπο και δύναται να αποτελέσει το αντικείμενο εξέτασης ή/και έρευνας από την Αρχή, εάν αυτή δεν ικανοποιείται με την απάντηση του προσώπου εναντίον του οποίου στρέφεται το παράπονο/ η καταγγελία/ η ένσταση ή εάν ο παραπονούμενος υποβάλει γραπτή ειδοποίηση ότι δεν υπήρξε ικανοποιητικός χειρισμός του παραπόνου/ της καταγγελίας/ της ένστασης:

Νοείται ότι, η Αρχή έχει το δικαίωμα και εάν το κρίνει αναγκαίο, να καλέσει οποιοδήποτε πρόσωπο ενώπιόν της για προφορικές παραστάσεις και επεξηγήσεις ή να προβεί σε γραπτές παραστάσεις.

(β) Δυνάμει της παραγράφου (α) του παρόντος άρθρου, η Αρχή δύναται να προβεί στην έκδοση μιας Απόφασης η οποία είναι δεσμευτική για το πρόσωπο αυτό.

(2) Τηρουμένων των εξουσιών που απονέμονται στην Αρχή δυνάμει του άρθρου 23(1) και (2) του Νόμου, η Αρχή δύναται να διεξάγει έρευνα για τις δραστηριότητες και εργασίες οποιουδήποτε Φορέα και ελεγκτή, σε σχέση με τον οποίο υποβάλλεται παράπονο/ καταγγελία/ ένσταση από οποιονδήποτε παραπονούμενο.

(3) Κατόπιν της υποβολής παραπόνων, καταγγελιών και ενστάσεων κατά την παράγραφο (2) του παρόντος άρθρου στην Αρχή, η Αρχή δύναται να εκδώσει Απόφαση η οποία είναι δεσμευτική για το πρόσωπο εναντίον του οποίου στρέφεται το παράπονο/η καταγγελία/η ένσταση.

Κεφάλαιο IX – Ευθύνη Φορέα και Ελεγκτή

Ευθύνη Φορέα.

36. Σε περίπτωση που ο Φορέας δεν λαμβάνει τα κατάλληλα μέτρα για την αποτροπή και την ελαχιστοποίηση του αντίκτυπου συμβάντων που επηρεάζουν την ασφάλεια δικτύων και συστημάτων πληροφοριών του, όπως αυτά ορίζονται στη Νομοθεσία της Αρχής καθώς και στις κατευθυντήριες γραμμές και δεσμευτικές οδηγίες που εκδίδει η Αρχή για την αποκατάσταση των ελλείψεων που έχουν εντοπιστεί, με αποτέλεσμα να προκληθεί ζημιά σε εθνικό επίπεδο, συμπεριλαμβανομένης και της απώλειας ζωής, ο Φορέας φέρει το βάρος της ευθύνης για τις συνέπειες μιας τέτοιας παράλειψης.

Έκδοση κατευθυντήριων γραμμών, δεσμευτικών οδηγιών και επιβολή διοικητικού προστίμου.

37.- (1) Η Αρχή δύναται, στηριζόμενη σε ευρήματα του/των ελεγκτή/τών που θα έχει ενώπιόν της, μετά από τη διενέργεια του ελέγχου, να εκδίδει προς τον Φορέα κατευθυντήριες γραμμές και δεσμευτικές οδηγίες για την αποκατάσταση των ελλείψεων που έχουν εντοπιστεί:

Νοείται ότι, η Αρχή δύναται, σε περίπτωση που κρίνει απαραίτητη την επιβεβαίωση των ευρημάτων του ελέγχου (στο σύνολό του ή σε συγκεκριμένο μέτρο), να διενεργήσει επαναληπτικό έλεγχο ή επαλήθευση στοιχείων είτε με προσωπικό της Αρχής είτε με άτομο που θα ορίσει η Αρχή, πριν εκδώσει προς τον Φορέα κατευθυντήριες γραμμές και δεσμευτικές οδηγίες για την αποκατάσταση των ελλείψεων που έχουν εντοπιστεί.

Κ.Δ.Π. 251/2021.

(2) Σε περίπτωση μη συμμόρφωσης του Φορέα με τις κατευθυντήριες γραμμές και δεσμευτικές οδηγίες που εξέδωσε η Αρχή δυνάμει της παραγράφου ένα (1) του παρόντος άρθρου, η Αρχή, τηρουμένων των διατάξεων του άρθρου 43 του Νόμου, των άρθρων 19 και 20 της Απόφασης Κ.Δ.Π. 389/2020 και τις διατάξεις της Απόφασης περί Συλλογής Πληροφοριών και Επιβολής Διοικητικού Προστίμου, ως εκάστοτε τροποποιείται ή αντικαθίσταται, δύναται να εκδώσει Απόφαση για επιβολή διοικητικού προστίμου:

Νοείται ότι, σε περίπτωση που αποδειχθεί ότι η Απόφαση επιβολής διοικητικού προστίμου που έχει εκδώσει η Αρχή και η οποία στηρίχθηκε στα ευρήματα της αξιολόγησης των πληροφοριών ή των αποτελεσμάτων του ελέγχου είναι λανθασμένη λόγω λάθους που εντοπίστηκε στα ευρήματα του ελεγκτή, η Αρχή οφείλει να ανακαλέσει την εκδιδόμενη Απόφαση επιβολής διοικητικού προστίμου και να στραφεί εναντίον του/των ελεγκτή/των για τυχόν ζημιά που προκλήθηκε στην Αρχή και θα την επωμιστεί η Αρχή.

ΜΕΡΟΣ ΙΙΙ

Τελικές Διατάξεις

Τροποποιήσεις.

38. Η Αρχή δύναται με Απόφασή της να καταργεί/αντικαθιστά, τροποποιεί ή/και να συμπληρώνει την παρούσα Απόφαση, τα Παραρτήματα και τα Προσαρτήματά της. Για την τροποποίηση ή συμπλήρωση της παρούσας Απόφασης, των Παραρτημάτων και των Προσαρτημάτων της, η Αρχή δύναται να προβαίνει σε δημόσια διαβούλευση. Η εκάστοτε τροποποίηση θα δημοσιεύεται στην Επίσημη Εφημερίδα της Δημοκρατίας και θα αναρτάται στην ιστοσελίδα της Αρχής.

Έναρξη ισχύος.

39. Η παρούσα Απόφαση τίθεται σε ισχύ από την ημερομηνία δημοσίευσής της στην Επίσημη Εφημερίδα της Δημοκρατίας.

ΠΑΡΑΡΤΗΜΑ Α: ΜΕΘΟΔΟΛΟΓΙΑ ΠΡΟΣΔΙΟΡΙΣΜΟΥ ΧΡΟΝΟΥ ΕΛΕΓΧΟΥ

Για τον προσδιορισμό του ελάχιστου χρόνου ελέγχου (ανά έλεγχο), διενεργούνται τα ακόλουθα βήματα:

1. Το επίπεδο ωριμότητας κυβερνοασφάλειας 3 περιέχει εξειδίκευση και διασαφήνιση των απαιτήσεων της Απόφασης Κ.Δ.Π. 389/2020 και δύναται να αναγνωρίσει το επίπεδο τόσο των Φορέων που συμμορφώθηκαν με τις υποχρεώσεις της Απόφασης Κ.Δ.Π. 389/2020 όσο και των Φορέων που δεν έχουν συμμορφωθεί. Κατά τον προσδιορισμό του χρόνου ελέγχου πρέπει να λαμβάνεται υπόψη το γεγονός ότι ο έλεγχος θα καλύπτει τουλάχιστον μέχρι το επίπεδο ωριμότητας κυβερνοασφάλειας 3. Ο υπολογιζόμενος χρόνος ελέγχου θα λαμβάνει ψηλότερο επίπεδο ωριμότητας κυβερνοασφάλειας από το 3, στις περιπτώσεις όπου πριν από διενέργεια οποιουδήποτε ελέγχου ο Φορέας θεωρεί ότι ανήκει σε ψηλότερο επίπεδο ωριμότητας κυβερνοασφάλειας ή αν ο προηγούμενος έλεγχος τον ανέδειξε σε ψηλότερο επίπεδο ωριμότητας κυβερνοασφάλειας.

2. Προσδιορισμός του συνολικού αριθμού εργαζομένων εντός πεδίου εφαρμογής του ελέγχου.

3. Επίπεδο κρισιμότητας του Φορέα.

4. Προσδιορισμός των σημείων στα οποία θα διενεργηθεί ο έλεγχος. Ο έλεγχος δύναται να διενεργηθεί σε μια ή σε περισσότερες φυσικές τοποθεσίες. Ο Φορέας αφού καταγράψει όλες τις φυσικές τοποθεσίες που στεγάζονται οι υποδομές, οι λειτουργίες ή/και υπηρεσίες του, σε συνεννόηση με τον ελεγκτή μπορούν να αποφασίσουν και να επιλέξουν τις τοποθεσίες που διαθέτουν βασικά συστήματα και διαδικασίες ή/και σχετίζονται με την ασφάλεια των πληροφοριών και συστημάτων. Για κατάληξη στον αριθμό φυσικών σημείων ελέγχου δύναται να λαμβάνονται υπόψη μεταξύ άλλων:

   Κεντρικά γραφεία, επαρχιακά γραφεία και υποκαταστήματα, Κέντρα δεδομένων και εξυπηρετητών (Data Centers), Τοποθεσίες παραγωγής με εξοπλισμό δικτυών επιχειρησιακής τεχνολογίας (OT) και συστήματα βιομηχανικού ελέγχου (ICS), Κέντρα έρευνας και ανάπτυξης (R&D), Τηλεφωνικά κέντρα, κέντρα διανομής, Κέντρα κατάρτισης και εκπαίδευσης, τοποθεσίες συνεργατών και άλλων τρίτων μερών εντός της εφοδιαστικής αλυσίδας (supply chain) που εμπίπτουν στο πεδίο εφαρμογής του ελέγχου, και άλλα ανάλογα με το αντικείμενο του κάθε εποπτευομένου φορέα.

   Ο ελεγκτής οφείλει να καταλήξει στο πλήθος των φυσικών σημείων ελέγχου εφαρμόζοντας κανόνες δειγματοληψίας, όπως τετραγωνική ρίζα (√) του πλήθους των φυσικών σημείων ελέγχου με στρογγυλοποίηση προς τον επόμενο ακέραιο αριθμό.

   Για παράδειγμα εάν ένας οργανισμός έχει 7 φυσικά σημεία στο πεδίο εφαρμογής του ελέγχου, εφαρμόζοντας στρογγυλοποίηση προς το επόμενο ακέραιο αριθμό του ρίζα (7), τότε θα πρέπει να ελεγχθούν 3 σημεία στα πλαίσια του συγκεκριμένου ελέγχου. Νοείτε ότι σε αυτά πρέπει να περιλαμβάνονται τα κεντρικά γραφεία όπου γίνεται η διαχείριση και τυχόν χώρος disaster recovery.

5. Προσδιορισμός της τεχνικής πολυπλοκότητας του πεδίου εφαρμογής του ελέγχου.
   Η τεχνική πολυπλοκότητα περιλαμβάνει το πλήθος δικτύων, πλήθος εξυπηρετητών και τύπο συστημάτων του Φορέα (IT συστήματα αφορούν την τεχνολογία πληροφοριών, OT συστήματα αφορούν την λειτουργική τεχνολογία και αφορούν συστήματα βιομηχανικού ελέγχου (ICS)).

   Πλήθος δικτύων αναφέρεται στα ξεχωριστά και λογικά τμηματοποιημένα δίκτυα υπολογιστών της συνολικής δικτυακής υποδομής ενός οργανισμού. Στον αριθμό δικτύων δύναται να λαμβάνονται υπόψη μεταξύ άλλων:

   - Φυσικά δίκτυα: συλλογή υπολογιστικών συσκευών που συνδέονται μεταξύ τους με κάποιο μέσο μετάδοσης π.χ. LAN (Local Area Networks), WAN (Wide Area Networks) και των MAN (Metropolitan Area Networks).
   - Λογικά δίκτυα: εικονικά τμήματα εντός ενός φυσικού δικτύου, τα οποία δημιουργούνται με τη χρήση VLANs (Virtual Local Area Networks).
   - Υποδικτύωση (Subnets): αναφέρεται στην πρακτική της διαίρεσης ενός δικτύου σε δύο ή μικρότερα δίκτυα.
   - Ζώνες δικτύου (network zones), τμήματα εντός ενός δικτύου που ορίζονται από διαφορετικές πολιτικές ασφαλείας, όπως DMZ (Demilitarized Zone).
   - Απομακρυσμένα δίκτυα: Δίκτυα που επεκτείνουν τη συνδεσιμότητα του κυρίως δικτύου π.χ VPN.
   - Ασύρματα δίκτυα: δίκτυα τα οποία παρέχουν συνδεσιμότητα μέσω ασύρματων πρωτοκόλλων (Wi-Fi).
   - Δίκτυα επιχειρησιακής τεχνολογίας (OT): δίκτυα που υποστηρίζουν βιομηχανικά συστήματα ελέγχου (ICS) και άλλες επιχειρησιακές τεχνολογίες.

Πλήθος Εξυπηρετητών αναφέρεται στο σύνολο των εξυπηρετητών της τεχνολογικής υποδομής του φορέα. Στο πλήθος εξυπηρετητών δύναται να λαμβάνονται υπόψη μεταξύ άλλων:

- Φυσικοί εξυπηρετητές (Physical servers, on premise or off-site),
- Εικονικοί εξυπηρετητές (Virtual Servers) όπως VMs και Containers,
- Εξυπηρετητές στο Cloud (IAAS, PAAS),
- Εξειδικευμένοι Εξυπηρετητές (Database Servers, Web Servers, Application Servers, File Servers, Mail Servers, Test/Development Servers).

6. Χρήση των πιο κάτω πινάκων, για την εξαγωγή του εκτιμώμενου χρόνου ελέγχου.

Επίπεδο διαβάθμισης ωριμότητας		
Ποσοστό των μέτρων ασφαλείας εντός πεδίου ελέγχου	Επίπεδο διαβάθμισης ωριμότητας	Τιμή βάσης χρόνου ελέγχου (ΤΒΧ)
>75% των μέτρων ασφαλείας	1	2 ημέρες
>75% των μέτρων ασφαλείας	2	4 ημέρες
>75% των μέτρων ασφαλείας	3	6 ημέρες
>75% των μέτρων ασφαλείας	4	8 ημέρες
>75% των μέτρων ασφαλείας	5	10 ημέρες

Πίνακας Α.2. Επίπεδο διαβάθμισης ωριμότητας και τιμή βάσης χρόνου ελέγχου

Συνολικός αριθμός εργαζομένων εντός πεδίου εφαρμογής του ελέγχου	
Ομάδα πλήθους προσωπικού	Ποσοστό αύξησης επί της τιμής βάσης (ΠΑ)
1 – 15	0.0%
16 – 65	5.0%
65 – 125	10.0%
126 – 425	15.0%
426 – 625	20.0%
> 626	25.0%

Πίνακας Α.2. Ομάδα αριθμού εργαζομένων και ποσοστό αύξησης επί της τιμής βάσης χρόνου ελέγχου

Επίπεδο κρισιμότητας του Φορέα	
Επίπεδο κρισιμότητας	Ποσοστό μεταβολής επί της τιμής βάσης (ΠΜΚ)
Πολύ Χαμηλό	0.0%
Χαμηλό	5.0%
Μεσαίο	10.0%
Υψηλό	15.0%
Πολύ Υψηλό	20.0%

Πίνακας Α.3. 3. Επίπεδο κρισιμότητας του Φορέα και ποσοστό μεταβολής επί της τιμής βάσης χρόνου ελέγχου

Φυσικά Σημεία Ελέγχου	
Πλήθος φυσικών σημείων ελέγχου	Ποσοστό μεταβολής επί της τιμής βάσης (ΠΜΦ)
1	0.0%
2	5.0%
3	10.0%
4	15.0%
>4	25.0%

Πίνακας Α.4. Φυσικά Σημεία Ελέγχου και ποσοστό μεταβολής επί της τιμής βάσης χρόνου ελέγχου

Τεχνική Πολυπλοκότητα	
Πλήθος Δικτύων	Ποσοστό μεταβολής επί της τιμής βάσης (ΠΜΠ)
1	0.00%
2 – 5	10.00%
6 – 10	20.00%
11 – 20	25.00%
> 20	30.00%
Πλήθος Εξυπηρετητών	Ποσοστό μεταβολής επί της τιμής βάσης (ΠΜΠ)
1 – 10	0.0%
11 – 50	15.0%
> 51	20.0%
IT vs OT	Ποσοστό μεταβολής επί της τιμής βάσης (ΠΜΠ)
IT	0.0%
IT & OT	30.0%

Πίνακας Α.5. Τεχνική πολυπλοκότητα και ποσοστό μεταβολής επί της τιμής βάσης χρόνου ελέγχου

Ο τελικός υπολογισμός προκύπτει από την ακόλουθη συνάρτηση:

Χρόνος Ελέγχου = ΤΒΧ + (ΠΑ* ΤΒΧ) + (ΠΜΚ*ΤΒΧ) + (ΠΜΦ*ΤΒΧ) + (max(ΠΜΠ*ΤΒΧ))

Σημειώσεις:

i. Ο χρόνος επιτόπιου ελέγχου δεν μπορεί να είναι λιγότερος από το 70% του χρόνου ελέγχου.
ii. Ο χρόνος επιτόπιου ελέγχου μετριέται σε ανθρωποημέρες.

ΠΑΡΑΡΤΗΜΑ Β: ΥΠΟΔΕΙΓΜΑ ΕΚΘΕΣΗΣ ΕΛΕΓΧΟΥ ΩΡΙΜΟΤΗΤΑΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

<table>
<tr><th colspan="5">ΕΚΘΕΣΗ ΕΛΕΓΧΟΥ ΩΡΙΜΟΤΗΤΑΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ[1]</th></tr>
<tr><td colspan="5">1.0 ΣΤΟΙΧΕΙΑ ΦΟΡΕΑ</td></tr>
<tr><td>ΕΠΩΝΥΜΙΑ:</td><td colspan="4"></td></tr>
<tr><td>ΔΙΕΥΘΥΝΣΗ:
(κεντρικής εγκατάστασης)</td><td colspan="4"></td></tr>
<tr><td>ΣΤΟΙΧΕΙΑ ΕΠΙΚΟΙΝΩΝΙΑΣ</td><td colspan="4">Υπεύθυνος επικοινωνίας: _____
Ρόλος υπεύθυνου επικοινωνίας: _____
Τηλέφωνο επικοινωνίας: _____
Διεύθυνση ηλεκτρονικού ταχυδρομείου (email): _____</td></tr>
<tr><td>ΔΙΕΥΘΥΝΣΕΙΣ ΣΗΜΕΙΩΝ ΠΟΥ ΔΙΕΝΕΡΓΗΘΗΚΕ Ο ΕΛΕΓΧΟΣ</td><td colspan="4"></td></tr>
<tr><td>ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ ΤΟΥ ΕΛΕΓΧΟΥ</td><td colspan="4"></td></tr>
<tr><td>ΑΡΙΘΜΟΣ ΕΡΓΟΔΟΤΟΥΜΕΝΩΝ (εντός πεδίου εφαρμογής του ελέγχου)</td><td></td><td colspan="2">ΠΡΟΔΙΑΓΕΓΡΑΜΜΕΝΗ ΕΛΑΧΙΣΤΗ ΔΙΑΡΚΕΙΑ ΕΛΕΓΧΟΥ</td><td></td></tr>
<tr><td colspan="5">2.0 ΣΤΟΙΧΕΙΑ ΕΛΕΓΧΟΥ</td></tr>
<tr><td rowspan="3">ΚΡΙΤΗΡΙΑ ΕΛΕΓΧΟΥ</td><td>☐</td><td colspan="3">Μέτρα ασφάλειας όπως περιγράφονται στο ΠΑΡΑΡΤΗΜΑ ΙΙΙ της Απόφασης Κ.Δ.Π. 389/2020.</td></tr>
<tr><td>☐</td><td colspan="3">Μέτρα ασφάλειας όπως περιγράφονται στα ΜΕΡΗ ΙΙΙ – VII της Απόφασης Κ.Δ.Π.408/2020.</td></tr>
<tr><td>☐</td><td colspan="3">Άλλο:</td></tr>
<tr><td rowspan="4">ΕΓΓΡΑΦΑ ΕΛΕΓΧΟΥ</td><td>☐</td><td colspan="3">Ερωτηματολόγιο μοντέλου ωριμότητας κυβερνοασφάλειας (cybersecurity maturity model) έκδοση 1.0.</td></tr>
<tr><td>☐</td><td colspan="3">Διαδικασία διενέργειας ελέγχων ωριμότητας κυβερνοασφάλειας, έκδοση 1.0.</td></tr>
<tr><td>☐</td><td colspan="3">Έκθεση Ελέγχου Ωριμότητας Κυβερνοασφάλειας, έκδοση 1.0</td></tr>
<tr><td>☐</td><td colspan="3">Άλλο:</td></tr>
</table>

[1] Συντάσσεται μόνο στην ελληνική γλώσσα (με χρήση και ξενόγλωσσων όρων όπου απαιτείται).

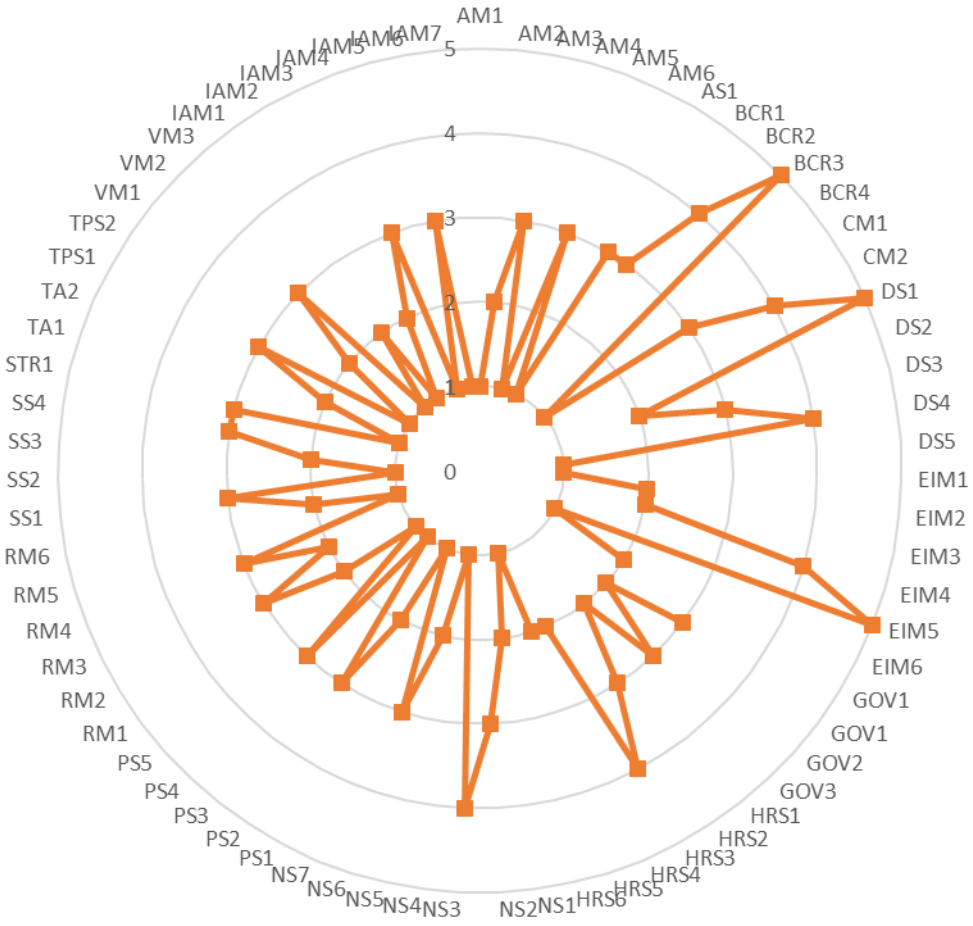
ΕΚΘΕΣΗ ΕΛΕΓΧΟΥ ΩΡΙΜΟΤΗΤΑΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ[1]			
ΣΚΟΠΟΣ ΕΛΕΓΧΟΥ	➢ Για να διενεργηθεί ο έλεγχος που περιγράφεται στο παρόν έγγραφο, ο Φορέας έχει συμφωνήσει (όπως αποτυπώνεται στο πεδίο Επωνυμία παραπάνω). Ο έλεγχος διενεργείται σύμφωνα με τη Διαδικασία διενέργειας ελέγχων ωριμότητας κυβερνοασφάλειας της Αρχής, όπως προβλέπεται στην σχετική νομοθεσία, με σκοπό να επιτευχθεί: 1. Η αναγνώριση του επιπέδου ωριμότητας κυβερνοασφάλειας των Φορέων έναντι των απαιτήσεων του ΠΑΡΑΡΤΗΜΑΤΟΣ ΙΙΙ της Απόφασης Κ.Δ.Π. 389/2020, 2. ο προσδιορισμός των περιπτώσεων (ανά μέτρο ασφαλείας) όπου η συμμόρφωση του Φορέα είναι σε επίπεδο μικρότερο από τις απαιτήσεις της Απόφασης Κ.Δ.Π. 389/2020 (μικρότερο του 3), 3. ο προσδιορισμός των περιπτώσεων (ανά μέτρο ασφαλείας) που η συμμόρφωση του Φορέα είναι σε επίπεδο υψηλότερο από τις απαιτήσεις της Απόφασης Κ.Δ.Π. 389/2020 (τουλάχιστον 3), 4. η ενημέρωση του Φορέα μέσω της παράδοσης της παρούσας έκθεσης ελέγχου, σχετικά με τα αποτελέσματα των παραπάνω και 5. η δυνατότητα συντονισμού, πρόσκλησης και παρακολούθησης της λήψης μέτρων του Φορέα υπό την εποπτεία της Αρχής. ➢ Τα δεδομένα του ελέγχου καλύπτονται από υποχρέωση εχεμύθειας για όλα τα εμπλεκόμενα μέρη (Ελεγκτές, Φορέα και Αρχή). ➢ Ιδιοκτήτης της παρούσας αναφοράς είναι ο Φορέας και η παρούσα αναφορά θα κοινοποιείται από τον ελεγκτή ή τον επικεφαλής ελεγκτή) στην Αρχή.		
3.0 ΟΜΑΔΑ ΕΛΕΓΧΟΥ			
Ελεγκτής 1 (επικεφαλής ελεγκτής)		Αριθμός Μητρώου Ελεγκτή	
Ελεγκτής 2		Αριθμός Μητρώου Ελεγκτή	
Ελεγκτής 3		Αριθμός Μητρώου Ελεγκτή	
Ελεγκτής 4		Αριθμός Μητρώου Ελεγκτή	
Εκπαιδευόμενος Ελεγκτής		Αριθμός Μητρώου Ελεγκτή	
Εκπαιδευόμενος Ελεγκτής		Αριθμός Μητρώου Ελεγκτή	
Εκπρόσωπος της Αρχής 1			
Εκπρόσωπος της Αρχής 2			
4.0 ΗΜΕΡΟΜΗΝΙΕΣ ΥΛΟΠΟΙΗΣΗΣ ΕΛΕΓΧΟΥ			
ΗΜΕΡΟΜΗΝΙΕΣ ΕΛΕΓΧΟΥ	Από: Ως: Ή τις ημερομηνίες		
Σχόλια επί του προγραμματισμού	□	Ο προδιαγεγραμμένος χρόνος (βάσει ανάθεσης από τον ελεγχόμενο Φορέα) ήταν επαρκής και δεν χρειάστηκε κάποια αναπροσαρμογή.	
	□	Ο προδιαγεγραμμένος χρόνος (βάσει ανάθεσης από τον ελεγχόμενο Φορέα) δεν ήταν επαρκής και χρειάστηκε προσθήκη [ ] ημέρας/ών ελέγχου.	
	□	Ο προδιαγεγραμμένος χρόνος (βάσει ανάθεσης από τον ελεγχόμενο Φορέα) ήταν παραπάνω από επαρκής και δεν απαιτήθηκε η χρήση [ ] ημέρας/ών ελέγχου.	

ΕΚΘΕΣΗ ΕΛΕΓΧΟΥ ΩΡΙΜΟΤΗΤΑΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ[1]		
	Σχόλια σχετικά με την απόκλιση από την προγραμματισμένη διάρκεια ελέγχου	[Παραδείγματα] - *Ο Φορέας έχει εντάξει εντός του πεδίου εφαρμογής ένα σύνολο νέων συστημάτων που δεν είχαν ελεγχθεί σε προηγούμενους ελέγχους με αποτέλεσμα να απαιτηθεί 0,5 ημέρες παραπάνω για την ορθή υλοποίησή της.* - *Ο Φορέας έχει εισάγει νέο σύστημα αυτοματοποίησης και ελέγχου που επέτρεψε την ταχύτερη υλοποίηση του ελέγχου στις ενότητες …… κατά 0,5 μέρες.*
5.0 ΑΠΟΤΕΛΕΣΜΑΤΑ ΕΛΕΓΧΟΥ		
Δηλώσεις Ελεγκτή	☐	Ο έλεγχος κάλυψε το σύνολο του πεδίου εφαρμογής της ανάθεσης και το σύνολο των απαιτήσεων που αναφέρονται στην ενότητα Κριτήρια Ελέγχου.
	☐	Τα στοιχεία σχετικά με τις ημερομηνίες και τις τοποθεσίες ελέγχου είναι ακριβή και αποτυπώνουν την πραγματική διάρκεια και εύρος του ελέγχου.
	☐	Για την υλοποίηση του ελέγχου ακολουθήθηκαν οι σχετικές βέλτιστες πρακτικές ελέγχου και συλλέχθηκαν αντικειμενικές αποδείξεις οι οποίες περιλαμβάνονται στο σχετικό ερωτηματολόγιο ελέγχου.
	☐	Για την αναγνώριση και συλλογή των αντικειμενικών αποδείξεων χρησιμοποιήθηκε δειγματοληψία η οποία αποτυπώνεται στο σχετικό ερωτηματολόγιο ελέγχου ανά απαίτηση. Η διαδικασία δειγματοληψίας των διαθέσιμων πληροφοριών και οι μέθοδοι ελέγχου που χρησιμοποιήθηκαν ήταν συνεντεύξεις, παρατηρήσεις, παρακολούθηση δραστηριοτήτων και συστημάτων και ανασκόπηση τεκμηρίωσης και αρχείων.
	☐	Τα συμπεράσματα του ελέγχου στηρίχτηκαν στις αντικειμενικές αποδείξεις και ενδέχεται να μην αναπαριστούν πλήρως την πραγματική εικόνα του Φορέα. (Περιορισμός λόγω δειγματοληψίας).
	☐	Κατά τη διάρκεια του ελέγχου δεν εμφανίστηκαν κάποια εμπόδια ή άλλοι παράμετροι που να επηρέασαν αρνητικά τη διενέργεια του ελέγχου.
	☐	Κατά τη διάρκεια του ελέγχου προέκυψαν τα ακόλουθα, τα οποία είχαν δυσμενή επίδραση στη διενέργεια του ελέγχου - …. - …. Λόγω των παραπάνω, [παράδειγμα : *ο ελεγκτής δηλώνει ότι οι ακόλουθες περιοχές ελέγχου δεν έχουν ελεγχθεί πλήρως*.]
	☐	Για την εξαγωγή των συμπερασμάτων του ελέγχου έχουν αξιολογηθεί οι αντικειμενικές αποδείξεις που έχουν συλλεχθεί ανά σημείο ελέγχου και ανά επίπεδο ωριμότητας κυβερνοασφάλειας, έναντι των απαιτήσεων του σημείου ελέγχου ανά επίπεδο διαβάθμισης ωριμότητας όπως αποτυπώνεται στο σχετικό ερωτηματολόγιο.

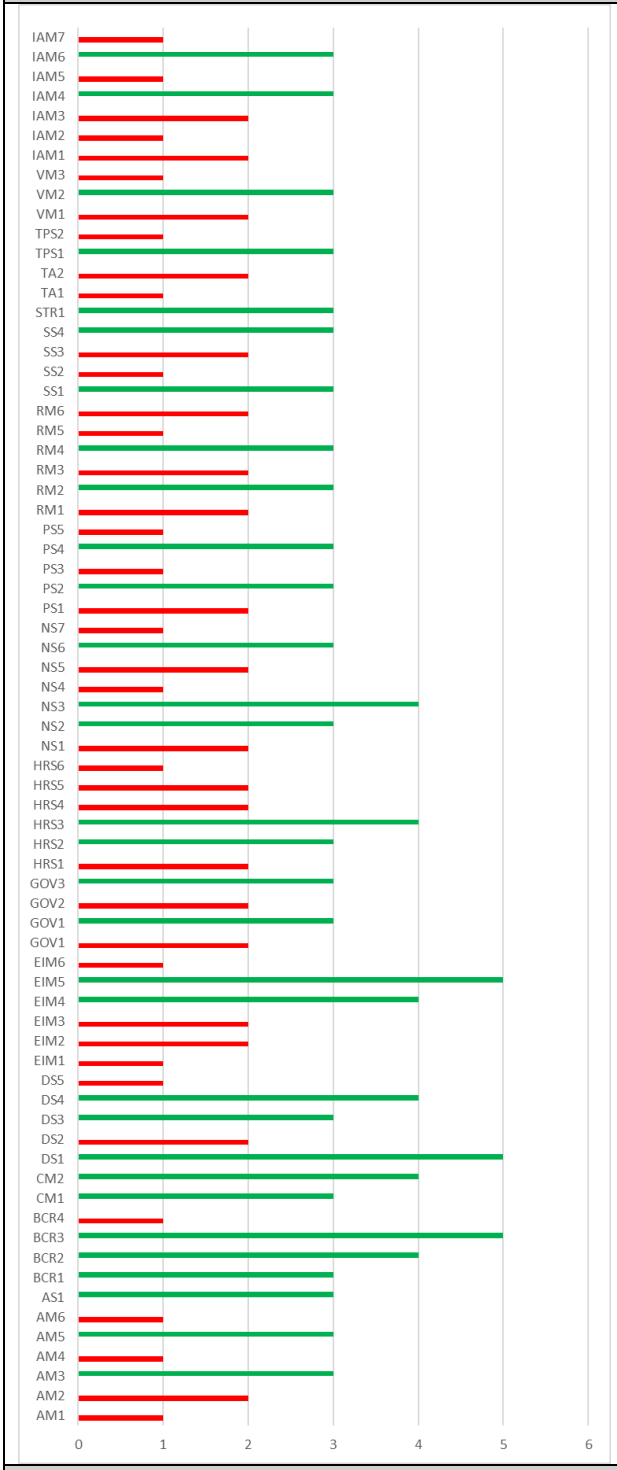
ΕΚΘΕΣΗ ΕΛΕΓΧΟΥ ΩΡΙΜΟΤΗΤΑΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ[1]		
	☐	Τα αποτελέσματα που περιέχονται στην παρούσα έκθεση ελέγχου αντικατοπτρίζουν το επίπεδο ωριμότητας κυβερνοασφάλειας του Φορέα ανά σημείο ελέγχου, όπως έγιναν αντιληπτά από τον ελεγκτή κατά τη διάρκεια του ελέγχου.
	☐	Η ευθύνη της συνεχιζόμενης υλοποίησης και συμμόρφωσης του Φορέα προς τις απαιτήσεις της νομοθεσίας βαρύνει τον ίδιο τον Φορέα.
	☐	Ο ελεγκτής δεν εξέτασε θέματα του Φορέα που σχετίζονται με συμμόρφωση με οποιοδήποτε άλλο νομοθετικό ή κανονιστικό πλαίσιο.

Επιτευχθέν Επίπεδο ωριμότητας κυβερνοασφάλειας ανά απαίτηση			
AM1	EIM1	NS3	SS3
AM2	EIM2	NS4	SS4
AM3	EIM3	NS5	STR1
AM4	EIM4	NS6	TA1
AM5	EIM5	NS7	TA2
AM6	EIM6	PS1	TPS1
AS1	GOV1	PS2	TPS2
BCR1	GOV1	PS3	VM1
BCR2	GOV2	PS4	VM2
BCR3	GOV3	PS5	VM3
BCR4	HRS1	RM1	IAM1
CM1	HRS2	RM2	IAM2
CM2	HRS3	RM3	IAM3
DS1	HRS4	RM4	IAM4
DS2	HRS5	RM5	IAM5
DS3	HRS6	RM6	IAM6
DS4	NS1	SS1	IAM7
DS5	NS2	SS2	

Επιτευχθέν Επίπεδο ωριμότητας κυβερνοασφάλειας ανά απαίτηση (σε γραφική παράσταση Radar)

ΕΚΘΕΣΗ ΕΛΕΓΧΟΥ ΩΡΙΜΟΤΗΤΑΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ[1]

Επιτευχθέν Επίπεδο ωριμότητας κυβερνοασφάλειας ανά απαίτηση (σε γραφική παράσταση Cluster Column)

ΕΚΘΕΣΗ ΕΛΕΓΧΟΥ ΩΡΙΜΟΤΗΤΑΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ[1]



6.0 ΣΥΝΟΨΗ ΑΠΟΚΛΙΣΕΩΝ ΑΠΟ ΤΟ ΕΠΙΠΕΔΟ 3
Στον πίνακα που ακολουθεί περιλαμβάνονται τα μέτρα ασφαλείας τα οποία βρίσκονται σε επίπεδο ωριμότητας μικρότερο του 3. Σημειώνεται ότι, για να θεωρείται ότι ένα μέτρο ασφαλείας έχει επιτύχει το επίπεδο διαβάθμισης ωριμότητας του κάθε επιπέδου, απαιτείται να έχει καλύψει το σύνολο της απαίτησης όπως παρουσιάζεται στο αντίστοιχο σημείο του ερωτηματολογίου. Στον παρακάτω πίνακα, εκτός από τα μέτρα στα οποία το επίπεδο είναι μικρότερο του 3, περιλαμβάνονται και οι απαιτήσεις που ο Φορέας δεν ικανοποιεί για αυτό το επίπεδο ανά μέτρο ασφάλειας.

Μέτρο	Σημεία αποκλίσεων που ΔΕΝ καλύπτει ο Φορέας το επίπεδο 3

ΕΚΘΕΣΗ ΕΛΕΓΧΟΥ ΩΡΙΜΟΤΗΤΑΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ[1]	
STR1	Υπάρχει καταγεγραμμένη στρατηγική για την ασφάλεια πληροφοριών. Η στρατηγική περιγράφει λεπτομερώς συγκεκριμένους στόχους αναφορικά με την ασφάλεια, καθώς και την προσέγγιση για την ασφάλεια και τη διαχείριση του κινδύνου και τα μέσα για την επικύρωση της αποτελεσματικότητας της στρατηγικής με την υποστήριξη από βασικούς δείκτες επιδόσεων. Η στρατηγική ασφάλειας πληροφοριών αντικατοπτρίζεται στην πολιτική ασφάλειας πληροφοριών όπως περιγράφεται στο μέτρο [GOV3]. Τα στελέχη γνωρίζουν τη στρατηγική και την πολιτική ασφάλειας πληροφοριών, όπως περιγράφεται στο μέτρο [TA1]. Οι ενέργειες που έχουν προκύψει για υλοποίηση από την στρατηγική υποστηρίζονται από τη διοίκηση με την παροχή πόρων, γνώσεων και χρόνου.
GOV1	Οι ρόλοι και οι αρμοδιότητες αντικατοπτρίζονται στην πολιτική ασφάλειας των πληροφοριών [GOV3] και όλα τα στελέχη του Φορέα έχουν λάβει την απαραίτητη ενημέρωση και επίγνωση των ρόλων και των ευθυνών τους όσον αφορά την ασφάλεια δικτύων και πληροφοριών όπως ορίζεται στα μέτρα [TA1, TA2]. Γίνεται ανασκόπηση και ενημέρωση των ρόλων και αρμοδιοτήτων χωρίς αυτό να είναι συστηματικό.
GOV2	Ο Φορέας έχει δημιουργήσει και διατηρεί κεντρικό αποθετήριο με όλες τις σχετικές νομοθετικές, κανονιστικές και ρυθμιστικές απαιτήσεις, και συμβατικές απαιτήσεις όσον αφορά την ασφάλεια δικτύων και πληροφοριών. Ο Φορέας έχει δημιουργήσει σχετική διαδικασία και διενεργεί εσωτερικό έλεγχο τουλάχιστον ετήσια για την διαπίστωση της συμμόρφωσης με όλες τις σχετικές νομοθετικές, κανονιστικές και ρυθμιστικές απαιτήσεις, καθώς και συμβατικές απαιτήσεις όσον αφορά την ασφάλεια δικτύων και πληροφοριών. Ο Φορέας συμμορφώνεται με όλες τις υποχρεώσεις που ορίζονται στην Απόφαση Κ.Δ.Π. 389/2020.
GOV3	Ο Φορέας έχει δημιουργήσει πολιτική ασφάλειας πληροφοριών που περιγράφονται αναλυτικά τα μέτρα που έχει λάβει, όπως επίσης και λεπτομερή περιγραφή της εφαρμογής τους. Η πολιτική ασφάλειας πληροφοριών αντικατοπτρίζει τους στόχους που περιγράφονται στη στρατηγική ασφάλειας πληροφοριών [STR1] και περιλαμβάνει τους ρόλους και τις αρμοδιότητες σε επίπεδο οργάνωσης όπως ορίζεται στο [GOV1]. Ο Φορέας έχει δημιουργήσει μία σειρά από πολιτικές, οδηγίες και τυποποιημένες διαδικασίες λειτουργίας οι οποίες και εφαρμόζονται για την ασφάλεια πληροφοριών σε σχέση με συγκεκριμένες επεξεργασίες, συστήματα ή δραστηριότητες, ανάλογα με τις ανάγκες. Όλες οι πολιτικές και οι διαδικασίες έχουν εγκριθεί από τη διοίκηση του Φορέα και το προσωπικό έχει ενημερωθεί και εκπαιδευτεί σχετικά.
RM1	Ο Φορέας έχει θεσπίσει και καταγράψει μεθοδολογία για τη διαχείριση κινδύνων. Η μεθοδολογία περιέχει τη διαδικασία εκτίμησης κινδύνων, προσδιορίζει τα κριτήρια ανάλυσης κινδύνου (τα οποία είναι κατ΄ ελάχιστον κριτήρια επιπτώσεων, κριτήρια πιθανότητας, και συναρτήσεις για την εξαγωγή της βαθμολογίας κινδύνου), των κριτηρίων αποδοχής κινδύνων και της πολιτικής ανάληψης κινδύνων από τον Φορέα. Ο ρόλος του ιδιοκτήτη κινδύνων ορίζεται και περιγράφονται οι ρόλοι και οι αρμοδιότητές τους σε σχέση με τη διαχείριση κινδύνων. Η μεθοδολογία διαχείρισης κινδύνου θα επιτρέψει στον Φορέα να αξιολογήσει τους κινδύνους για την ασφάλεια πληροφοριών που αντιμετωπίζει και να εφαρμόσει τα κατάλληλα μέτρα για την αντιμετώπιση ή τον μετριασμό τους, λαμβάνοντας υπόψη το πλαίσιο λειτουργίας του. Ο Φορέας έχει θέσει σε εφαρμογή διαδικασίες και εργαλεία, ανάλογα με την περίπτωση, προκειμένου να στηρίξει τις διαδικασίες διαχείρισης κινδύνων, έχοντας κατ' ελάχιστον ένα μητρώο κινδύνων, ένα σχέδιο αντιμετώπισης κινδύνων και μια δομή διακυβέρνησης της ασφάλειας πληροφοριών στην οποία θα περιγράφονται λεπτομερώς οι ρόλοι και οι αρμοδιότητες. Η οριζόμενη μεθοδολογία διαχείρισης κινδύνων επικυρώνεται, συμφωνείται και υποστηρίζεται από τη διοίκηση ανώτατου επιπέδου και άλλους σχετικούς φορείς εντός του Φορέα. Η μεθοδολογία ορίζει ότι εφαρμόζεται εντός του Φορέα σε τακτά χρονικά διαστήματα και τουλάχιστον σε ετήσια βάση. Ο Φορέας έχει δημιουργήσει μια διακριτή πολιτική ανάληψης κινδύνων η οποία έχει άμεση σχέση με τους στόχους, το πλαίσιο λειτουργίας και τη στρατηγική του και αποτυπώνεται και στα σχετικά κριτήρια αποδοχής κινδύνου.
7.0 ΑΛΛΑ ΣΤΟΙΧΕΙΑ	
8.0 ΣΥΝΟΨΗ ΕΛΕΓΧΟΥ	
9.0 ΑΠΟΚΛΙΝΟΥΣΕΣ ΑΠΟΨΕΙΣ ΕΛΕΓΚΤΗ/ΕΛΕΓΚΤΩΝ ΚΑΙ ΦΟΡΕΑ	

ΕΚΘΕΣΗ ΕΛΕΓΧΟΥ ΩΡΙΜΟΤΗΤΑΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ[1]

10.0 ΕΓΚΡΙΣΗ ΚΑΙ ΑΠΟΔΟΧΗ

Έχοντας πλήρη επίγνωση των συνεπειών του περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών Νόμου του 2020 και της δυνάμει αυτού εκδοθείσας δευτερογενούς νομοθεσίας, ως εκάστοτε τροποποιούνται ή/και αντικαθίστανται, δηλώνω ότι όλα τα στοιχεία που περιέχονται στην παρούσα έκθεση είναι αληθή και ορθά και ότι αποτελεί πραγματική απεικόνιση του επιπέδου διαβάθμισης ωριμότητας του Φορέα, ανά απαίτηση των κριτηρίων που αναφέρονται στην ενότητα 2 της παρούσας Έκθεσης, λαμβάνοντας υπόψη τους περιορισμούς που αναφέρονται στην ενότητα 5 – Δηλώσεις του ελεγκτή της παρούσας Έκθεσης.

Ελεγκτής 1 (Επικεφαλής Ελεγκτής)	Ελεγκτής 2	Ελεγκτής 3	Ελεγκτής 4
Ονοματεπώνυμο:	Ονοματεπώνυμο:	Ονοματεπώνυμο:	Ονοματεπώνυμο:
Υπογραφή:	Υπογραφή:	Υπογραφή:	Υπογραφή:

Εκπρόσωπος της Ανώτατης Διοίκησης του Φορέα

Ονοματεπώνυμο:

Υπογραφή:

* Με την υπογραφή της παρούσας, συμφωνώ με το περιεχόμενο της έκθεσης. Τυχόν αποκλίνουσες απόψεις ή/και διαφωνίες έχουν σημειωθεί στην ενότητα 9.0 (ΑΠΟΚΛΙΝΟΥΣΕΣ ΑΠΟΨΕΙΣ ΕΛΕΓΚΤΗ/ΕΛΕΓΚΤΩΝ ΚΑΙ ΦΟΡΕΑ)

ΠΑΡΑΡΤΗΜΑ Γ: ΥΠΟΔΕΙΓΜΑ ΠΛΑΝΟΥ ΕΛΕΓΧΟΥ

Πλάνο Ελέγχου Μοντέλου Ωριμότητας Κυβερνοασφάλειας (cybersecurity maturity model)			
1.0 ΣΤΟΙΧΕΙΑ ΦΟΡΕΑ			
ΕΠΩΝΥΜΙΑ:			
ΔΙΕΥΘΥΝΣΗ: (κεντρικής εγκατάστασης)			
ΣΤΟΙΧΕΙΑ ΕΠΙΚΟΙΝΩΝΙΑΣ	Υπεύθυνος επικοινωνίας: Ρόλος: Τηλέφωνο επικοινωνίας: Email επικοινωνίας:		
ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ			
ΑΡΙΘΜΟΣ ΕΡΓΟΔΟΤΟΥΜΕΝΩΝ (εντός πεδίου εφαρμογής του ελέγχου)		ΠΡΟΔΙΑΓΕΓΡΑΜΜΕΝΗ ΕΛΑΧΙΣΤΗ ΔΙΑΡΚΕΙΑ ΕΛΕΓΧΟΥ	
2.0 ΣΤΟΙΧΕΙΑ ΕΛΕΓΚΤΗ & ΣΥΝΟΔΩΝ			
ΣΤΟΙΧΕΙΑ ΕΠΙΚΟΙΝΩΝΙΑΣ	Ονοματεπώνυμο: Αριθμός Μητρώου Ελεγκτή: Τηλέφωνο επικοινωνίας: Email επικοινωνίας:		
ΣΥΝΟΔΟΙ ΣΤΟΝ ΕΛΕΓΧΟ (ΟΝΟΜΑΤΕΠΩΝΥΜΟ/ΡΟΛΟΣ)			

3.0 ΛΕΠΤΟΜΕΡΕΙΕΣ ΠΛΑΝΟΥ ΕΛΕΓΧΟΥ					
Ενδεικτική Ημερ/νία	Ενδεικτική Διάρκεια	Κατηγορίες Μέτρων / Συγκεκριμένο Μέτρο	Τοποθεσία Ελέγχου	Ελεγκτής	Ελεγχόμενος
		Ασφάλεια Εφαρμογών [AS]			
		Επιχειρησιακή συνέχεια και Ανθεκτικότητα [BCR]			
		Κύκλος ζωής της εργοδότησης [HRS1]			
		Παρακολούθηση εργαζομένων [HRS2]			

Πλάνο Ελέγχου Μοντέλου Ωριμότητας Κυβερνοασφάλειας (cybersecurity maturity model)					
		Διαχείριση Συμβάντων και περιστατικών [EIM]			
		Διακυβέρνηση [GOV]			
		Ασφάλεια Περιμέτρου [NS1]			

ΠΑΡΑΡΤΗΜΑ Δ: ΟΔΗΓΙΕΣ ΔΕΙΓΜΑΤΟΛΗΨΙΑΣ

Για τις περιπτώσεις που δεν είναι δυνατό να εξεταστεί το σύνολο των παραγόμενων αντικειμενικών αποδείξεων και πληροφοριών, ο ελεγκτής θα πρέπει να διαλέξει μέθοδο δειγματοληψίας. Ο στόχος της χρήσης δειγματοληψίας είναι, μέσω της επιλογής του κατάλληλου δείγματος, να δώσει στον ελεγκτή την αυτοπεποίθηση ότι έχουν καλυφθεί αποτελεσματικά οι στόχοι του ελέγχου για τη συγκεκριμένη απαίτηση.

Ο κίνδυνος που προκύπτει από τη χρήση της δειγματοληψίας είναι το γεγονός ότι τα δείγματα μπορεί να μην είναι αντιπροσωπευτικά στο συνολικό αριθμό των εργαζομένων από τον οποίο έχουν επιλεγεί. Σε αυτήν την περίπτωση τα συμπεράσματα που θα εξάγει ο ελεγκτής, βάσει του επιλεγμένου δείγματος, μπορεί να είναι διαφορετικά από αυτά στα οποία θα κατέληγε αν μπορούσε να εξετάσει ολόκληρο το σύνολο του αριθμού των εργαζομένων.

Ο κάθε ελεγκτής καλείται, ανά περίπτωση, να εξετάσει τον σχετικό κίνδυνο και το μέγεθος του διαθέσιμου συνολικού αριθμού των εργαζομένων και να επιλέξει την προτιμητέα μέθοδο δειγματοληψίας.

Οι πιθανές μέθοδοι δειγματοληψίας είναι οι ακόλουθες:

1) Στατιστική δειγματοληψία
2) Δειγματοληψία κατά την κρίση του ελεγκτή

Όποια μεθοδολογία επιλέξει ανά περίπτωση και ανά μέτρο ασφαλείας ο κάθε ελεγκτής, θα πρέπει να καταγράφεται στις σημειώσεις του ελεγκτή και στο ερωτηματολόγιο του μοντέλου ωριμότητας κυβερνοασφάλειας (cybersecurity maturity model).

1) Στατιστική δειγματοληψία

Η μέθοδος της στατιστικής δειγματοληψίας μπορεί να εφαρμοστεί σε περιπτώσεις που μπορεί να εκτιμηθεί η ποσότητα του συνολικού αριθμού των εργαζομένων. Για παράδειγμα, ο ελεγκτής επιθυμεί να ελέγξει τα δικαιώματα των χρηστών του Φορέα σε μια συγκεκριμένη εφαρμογή. Στην περίπτωση αυτή ο συνολικός αριθμός των εργαζομένων σχετίζεται με το πλήθος των χρηστών της εφαρμογής.

Η στατιστική δειγματοληψία δίνει τη δυνατότητα εξαγωγής μιας ποσότητας τυχαίου δείγματος.

Η συνάρτηση του προσδιορισμού του δείγματος είναι η ακόλουθη:

$$\text{Unlimited population: } n = \frac{z^2 \times \hat{p}(1-\hat{p})}{\varepsilon^2}$$

$$\text{Finite population: } n' = \frac{n}{1+\frac{z^2 \times \hat{p}(1-\hat{p})}{\varepsilon^2 N}}$$

Όπου:
z είναι το z score
ε είναι το περιθώριο σφάλματος
N είναι ο πληθυσμός
p̂ είναι το population proportion

Ενα πρακτικό παράδειγμα υπολογισμού για το παράδειγμα της εφαρμογής παραπάνω που υπάρχουν 100 χρήστες. Για το παρακάτω παράδειγμα έχουμε διαλέξει 15% περιθώριο σφάλματος, 80% confidence (το οποίο έχει z value = 1,28), και population proportion 80%. Η τιμή του δείγματος που προκύπτει είναι 11.

Αντίστοιχα, θα μπορούσαμε να είχαμε διαλέξει 75% confidence και η τιμή του δείγματος που θα είχε προκύψει θα ήταν 9. Υπάρχουν μια σειρά από συναρτήσεις στο Excel, και online free εργαλεία για τον προσδιορισμό του δείγματος ανά περίπτωση.

https://select-statistics.co.uk/calculators/sample-size-calculator-population-proportion/

Δεδομένου ότι υπάρχει μια σχετική δυσκολία κατά τη διάρκεια του ελέγχου ώστε να γίνει ο σχετικός υπολογισμός, ο ελεγκτής μπορεί να έχει εξάγει από πριν έναν σχετικό πίνακα δειγματοληψίας με σταθερές τιμές περιθωρίου σφάλματος και λοιπών παραμέτρων και αλλαγή μόνο στον πληθυσμό.

π.χ.

Πληθυσμός	Δείγμα

2) Δειγματοληψία κατά την κρίση του ελεγκτή

Η δειγματοληψία κατά την κρίση του ελεγκτή βασίζεται στις γνώσεις, τις δεξιότητες και την εμπειρία του.

Για τη δειγματοληψία με βάση την κρίση, μπορούν να ληφθούν υπόψη τα ακόλουθα:

- η προηγούμενη ελεγκτική εμπειρία εντός του πεδίου εφαρμογής του ελέγχου,
- η πολυπλοκότητα των απαιτήσεων (συμπεριλαμβανομένων των νομικών απαιτήσεων) για την επίτευξη των στόχων του ελέγχου,
- η πολυπλοκότητα και αλληλεπίδραση των διαδικασιών και των στοιχείων της υλοποίησης των μέτρων ασφάλειας του Φορέα,
- ο βαθμός αλλαγής στην τεχνολογία, τον ανθρώπινο παράγοντα ή των υλοποιήσεων σε σχέση με τα μέτρα ασφάλειας,
- προηγούμενοι εντοπισμένοι βασικοί τομείς κινδύνου και τομείς βελτίωσης,
- βασικοί τομείς όπως έχουν αναγνωριστεί από προηγούμενους ελέγχους κίνδυνοι ή σημεία προς βελτίωση, και
- αποτελέσματα από την παρακολούθηση των μέτρων ασφάλειας σύμφωνα με τις διατάξεις της Απόφασης Κ.Δ.Π. 389/2020.

Ένα μειονέκτημα της παρούσας δειγματοληψίας είναι το γεγονός ότι δεν μπορεί να υπάρξει στατιστική εκτίμηση της επίδρασης της αβεβαιότητας στα ευρήματα του ελέγχου και στα συμπεράσματα που προκύπτουν.

ΠΑΡΑΡΤΗΜΑ Ε: ΜΟΝΤΕΛΟ ΩΡΙΜΟΤΗΤΑΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Πίνακας Περιεχομένων

Κατηγορία		ΣΤΡΑΤΗΓΙΚΗ
STR1		Μέτρο: Στρατηγική για την ασφάλεια πληροφοριών Στόχος Μέτρου: Να θεσπιστεί στρατηγική ασφάλειας πληροφοριών στην οποία να αναλύονται οι στόχοι και η προσέγγιση υψηλού επιπέδου με σκοπό τον μετριασμό των κινδύνων για την ασφάλεια πληροφοριών. Περιγραφή Μέτρου: Καθορισμός του οράματος και της δέσμευσης για την ασφάλεια πληροφοριών σε μια στρατηγική που θα περιγράφει λεπτομερώς συγκεκριμένους στόχους αναφορικά με την ασφάλεια, καθώς και την προσέγγιση για την ασφάλεια και τη διαχείριση του κινδύνου, και τα μέσα για την επικύρωση της αποτελεσματικότητας της στρατηγικής με την υποστήριξη από βασικούς δείκτες επιδόσεων. Η στρατηγική ασφάλειας πληροφοριών αντικατοπτρίζεται στην πολιτική ασφάλειας πληροφοριών, όπως περιγράφεται στο μέτρο [GOV3]. Τα στελέχη γνωρίζουν τη στρατηγική και την πολιτική ασφάλειας πληροφοριών, όπως περιγράφεται στο μέτρο [TA1]. Πηγή: C2M2 (Program)
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν έχει δομήσει με οποιοδήποτε τρόπο ή εκφράσει με οποιοδήποτε τρόπο την στρατηγική του για την ασφάλεια πληροφοριών.
1	1	Υπάρχει κατεγραμμένη μια στρατηγική για την ασφάλεια πληροφοριών.
1	2	Η στρατηγική περιέχει μια λίστα από στόχους σε σχέση με την ασφάλεια πληροφοριών, σχετικές ενέργειες για υλοποίηση και τουλάχιστον ένα πλάνο υψηλού επιπέδου (high level) για την υλοποίησή τους.
1	3	Η διαχείριση και η υλοποίηση της συγκεκριμένης στρατηγικής είναι τουλάχιστον ad-hoc.
2	1	Το πλάνο υλοποίησης περιέχει τουλάχιστον στοιχεία σχετικά με το 1) Τι χρειάζεται να υλοποιηθεί, 2) μέχρι πότε χρειάζεται να υλοποιηθεί, 3) σε ποιόν έχει ανατεθεί η υπευθυνότητα παρακολούθησης / ολοκλήρωσης της υλοποίησης, 4) ποιοι πόροι απαιτούνται για την αποτελεσματική υλοποίηση και 5) με ποιον τρόπο και από ποιόν ρόλο θα διενεργηθεί η αξιολόγηση της ορθώς και αποτελεσματικής υλοποίησης.
3	1	Η στρατηγική που υπάρχει κατεγραμμένη, περιγράφει λεπτομερώς συγκεκριμένους στόχους αναφορικά με την ασφάλεια, καθώς και την προσέγγιση για την ασφάλεια και τη διαχείριση του κινδύνου, και τα μέσα για την επικύρωση της αποτελεσματικότητας της στρατηγικής με την υποστήριξη από βασικούς δείκτες επιδόσεων.
3	2	Η στρατηγική ασφάλειας πληροφοριών αντικατοπτρίζεται στην πολιτική ασφάλειας πληροφοριών, όπως περιγράφεται στο μέτρο [GOV3].
3	3	Τα στελέχη γνωρίζουν τη στρατηγική και την πολιτική ασφάλειας πληροφοριών, όπως περιγράφεται στο μέτρο [TA1].
3	4	Οι ενέργειες που έχουν προκύψει για υλοποίηση από την στρατηγική υποστηρίζονται από την διοίκηση με την παροχή πόρων, γνώσεων και χρόνου.
4	1	Έχει δημιουργηθεί και καταγραφεί διαδικασία μέσω της οποίας γίνεται διαχείριση του κύκλου ζωής της στρατηγικής.
4	2	Στα πλαίσια της διαδικασίας προβλέπεται η ανασκόπηση για την καταλληλότητα των σχετικών στοιχείων τουλάχιστον μια φορά το χρόνο και οι αλλαγές που προκύπτουν υλοποιούνται στα πλαίσια της διαδικασίας διαχείρισης αλλαγών.
4	3	Στα πλαίσια της διαδικασίας προβλέπεται ο έλεγχος της συμβατότητας της πολιτικής με τους στόχους του οργανισμού και τις απαιτήσεις του εσωτερικού και εξωτερικού του περιβάλλοντος (context).
4	4	Στα πλαίσια της διαδικασίας προβλέπεται ο τρόπος με το οποίο θα επικυρώνεται η αποτελεσματικότητας των επιμέρους ενεργειών της στρατηγικής.
4	5	Στα πλαίσια της διαδικασίας προβλέπεται η εξαγωγή βασικών δεικτών επιδόσεων άμεσα συνδεδεμένων με τους στόχους του οργανισμού.
5	1	Η στρατηγική για την ασφάλεια πληροφοριών αποτελεί μια υπό-ενότητα της επιχειρησιακής στρατηγικής του οργανισμού.
5	2	Η στρατηγική εντάσσεται στο συνολικό πλαίσιο διακυβέρνησης (governance) του οργανισμού.
5	3	Μέσω της διακυβέρνησης ο οργανισμός δίνει την στρατηγική κατεύθυνση ώστε να καλύπτει τις υποχρεώσεις του (νομικές, κανονιστικές, συμβατικές και άλλες), να διαχειρίζεται με αποτελεσματικό τρόπο τον κίνδυνο, να χρησιμοποιεί αποτελεσματικά τους πόρους του, και να καλύπτει τους σχετικούς του στόχους.
5	4	Οι λειτουργίες της διακυβέρνησης υποστηρίζονται από μια επίσημη δομή επίβλεψης ασφάλειας πληροφοριών (cybersecurity oversight committee).

5	5	Οι λειτουργίες της διακυβέρνησης υποστηρίζονται από ένα σύστημα μέσω του οποίου διενεργούνται σχετικοί έλεγχοι σε τακτική βάση, αποτελεσματικά.
5	6	Οι λειτουργίες της διακυβέρνησης υποστηρίζονται από αναφορές προς την ανώτατη διοίκηση σχετικά με την υλοποίηση της στρατηγικής και την εκπλήρωση των στόχων, για τους υψηλούς κινδύνους και την πορεία των μέτρων αντιμετώπισης.
5	7	Οι λειτουργίες της διακυβέρνησης υποστηρίζονται από αναφορές σχετικά με περιστατικά ασφαλείας ή παραλίγο περιστατικά ασφαλείας.
5	8	Οι λειτουργίες της διακυβέρνησης υποστηρίζονται από αναλύσεις τάσεων (trend analysis) και προτάσεις για βελτίωση
5	9	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	10	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.

Κατηγορία		ΔΙΑΚΥΒΕΡΝΗΣΗ
GOV1		Μέτρο: Ρόλοι και αρμοδιότητες σχετικά με την ασφάλεια πληροφοριών Στόχος Μέτρου: Να καθοριστούν οι ρόλοι και οι αρμοδιότητες σχετικά με την ασφάλεια πληροφοριών εντός του οργανισμού. Περιγραφή Μέτρου: Καθορισμός των ρόλων και των αρμοδιοτήτων όσον αφορά την ασφάλεια δικτύων και πληροφοριών για όλα τα στελέχη που ασχολούνται με την επεξεργασία πληροφοριών ή έχουν πρόσβαση σε συστήματα επεξεργασίας πληροφοριών. Οι καθορισμένοι ρόλοι και αρμοδιότητες αντικατοπτρίζονται στην πολιτική ασφάλειας των πληροφοριών [GOV3]. Τα στελέχη πρέπει να είναι επαρκώς ενημερωμένα και να έχουν επίγνωση των ρόλων και των ευθυνών τους όσον αφορά την ασφάλεια δικτύων και πληροφοριών, όπως ορίζεται στα μέτρα [TA1, TA2]. Οι ρόλοι και οι αρμοδιότητες που σχετίζονται με την ασφάλεια των πληροφοριών θα πρέπει να καθορίζονται από τη διοίκηση, ώστε να εξασφαλίζεται η υπευθυνότητα για τις αποφάσεις της διοίκησης που σχετίζονται με την ασφάλεια δικτύων και συστημάτων πληροφοριών. Πηγή: C2M2, ISO 27002
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν κάποιο συστηματικό τρόπο με τον οποίο να αναγνωρίζει τις εφαρμοστέες νομικές και κανονιστικές υποχρεώσεις όσον αφορά την ασφάλεια δικτύων και πληροφοριών.
1	1	Έχει πραγματοποιηθεί ο καθορισμός των ρόλων και των αρμοδιοτήτων όσον αφορά την ασφάλεια δικτύων και πληροφοριών για όλα τα στελέχη που ασχολούνται με την επεξεργασία πληροφοριών ή έχουν πρόσβαση σε συστήματα επεξεργασίας πληροφοριών.
2	1	Έχει γίνει καταγραφή των ρόλων και αρμοδιοτήτων και έχουν ανατεθεί στο αντίστοιχο προσωπικό. Η καταγραφή γίνεται με τρόπο συστηματικό και τεκμηριωμένο.
2	2	Υπάρχει έγκριση από τη διοίκηση του οργανισμού για τους ρόλους και αρμοδιότητες και για την ανάθεσή τους.
2	3	Τα αντικρουόμενα καθήκοντα και οι τομείς ευθύνης διαχωρίζονται για να μειωθούν οι ευκαιρίες για μη εξουσιοδοτημένη ή/και ακούσια τροποποίηση ή/και κατάχρηση των περιουσιακών στοιχείων του οργανισμού.
2	4	Έχει οριστεί από τον οργανισμό Υπεύθυνος για την ασφάλεια δικτύων και συστημάτων πληροφοριών.
2	5	Οι ελάχιστες αρμοδιότητες και τα χαρακτηριστικά της θέσης του Υπεύθυνου ασφάλειας δικτύων και πληροφοριών που αναφέρονται στη νομοθεσία (ΚΔΠ 389/2020, Άρθρο 12(3) και (4)) πληρούνται όλες.
2	6	Ο Υπεύθυνος ασφάλειας δικτύων και πληροφοριών έχει διοριστεί βάσει επαγγελματικών προσόντων και κυρίως βάσει ειδικών γνώσεων στον τομέα της ασφάλειας δικτύων και πληροφοριών και της ικανότητας εκπλήρωσης των καθηκόντων που αναφέρονται στο εδάφιο (3) της σχετικής νομοθεσίας.
2	7	Ο υπεύθυνος ασφάλειας δικτύων και πληροφοριών εκτελεί αποκλειστικά αυτά τα καθήκοντα. (Για μικρούς οργανισμούς, δύναται να εκτελεί και άλλα καθήκοντα μόνο όταν δεν οδηγούν σε σύγκρουση συμφερόντων και λαμβάνοντας υπόψη το επίπεδο κρισιμότητας του φορέα, με την έγκριση της Αρχής.)
2	8	Ο φορέας έχει κοινοποιήσει στην Αρχή τα στοιχεία επικοινωνίας του υπεύθυνου ασφάλειας δικτύων και πληροφοριών.
2	9	Ο φορέας διασφαλίζει ότι οι υποψήφιοι για τη θέση του υπεύθυνου ασφάλειας δικτύων και πληροφοριών ελέγχονται επαρκώς (screening), και εξασφαλίζει ότι το εν λόγω πρόσωπο θα διεκπεραιώνει τα καθήκοντά του δεόντως.
3	1	Οι ρόλοι και οι αρμοδιότητες αντικατοπτρίζονται στην πολιτική ασφάλειας των πληροφοριών [GOV3] και όλα τα στελέχη του οργανισμού έχουν λάβει την απαραίτητη ενημέρωση και επίγνωση των ρόλων και των ευθυνών τους όσον αφορά την ασφάλεια δικτύων και πληροφοριών, όπως ορίζεται στα μέτρα [TA1, TA2].
3	2	Γίνεται ανασκόπηση και ενημέρωση των ρόλων και αρμοδιοτήτων χωρίς αυτό να πραγματοποιείται κατ' ανάγκη με συστηματικό τρόπο.
4	1	Πραγματοποιείται ανασκόπηση και ενημέρωση (όπου αυτό χρειάζεται) των ρόλων και των αρμοδιοτήτων τουλάχιστον σε ετήσια βάση ή όταν έχουν υπάρξει κρίσιμες αλλαγές στον οργανισμό που επηρέασαν ρόλους ή αρμοδιότητες. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
4	2	Οι κίνδυνοι που σχετίζονται με αντικρουόμενα καθήκοντα έχουν εντοπισθεί, αξιολογηθεί και αντιμετωπιστεί όπως απαιτείται.
5	1	Οι ανατεθειμένοι ρόλοι και αρμοδιότητες διαχειρίζονται έτσι ώστε να διασφαλίζεται η επάρκεια και ο πλεονασμός της κάλυψης, συμπεριλαμβανομένου του σχεδιασμού διαδοχής.

5	2	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	3	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
GOV2		Μέτρο: Συμμόρφωση με νομικές και κανονιστικές υποχρεώσεις Στόχος Μέτρου: Να εξασφαλιστεί η συμμόρφωση με όλες τις εφαρμοστέες νομικές και κανονιστικές υποχρεώσεις όσον αφορά την ασφάλεια δικτύων και πληροφοριών. Περιγραφή Μέτρου: Δημιουργία και διατήρηση κεντρικού αποθετηρίου, και συμμόρφωση με όλες τις σχετικές νομοθετικές, κανονιστικές και ρυθμιστικές απαιτήσεις, και συμβατικές απαιτήσεις όσον αφορά την ασφάλεια δικτύων και πληροφοριών. Πηγή: ISMM (Compliance), ISO 27002 (18.1), NIST 800-53(AU-6, AU-11), C2M2 (Program)
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν έχει κάποιο συστηματικό τρόπο με τον οποίο να αναγνωρίζει τις εφαρμοστέες νομικές και κανονιστικές υποχρεώσεις όσον αφορά την ασφάλεια δικτύων και πληροφοριών.
1	1	Έχουν αναγνωρισθεί και καταγραφεί κάποιες νομοθετικές, κανονιστικές και ρυθμιστικές απαιτήσεις, και συμβατικές απαιτήσεις όσον αφορά την ασφάλεια δικτύων και πληροφοριών.
1	2	Οι διαδικασίες αναγνώρισης και ελέγχου συμμόρφωσης είναι τουλάχιστον ad-hoc.
2	1	Έχουν αναγνωρισθεί και καταγραφεί στο σύνολό τους νομοθετικές, κανονιστικές και ρυθμιστικές απαιτήσεις, και συμβατικές απαιτήσεις όσον αφορά την ασφάλεια δικτύων και πληροφοριών.
2	2	Έχει ανατεθεί σε ρόλο εσωτερικά ο έλεγχος προς την συμμόρφωση προς τις συγκεκριμένες απαιτήσεις.
3	1	Έχει δημιουργηθεί και διατηρείται κεντρικό αποθετήριο με όλες τις σχετικές νομοθετικές, κανονιστικές και ρυθμιστικές απαιτήσεις, και συμβατικές απαιτήσεις όσον αφορά την ασφάλεια δικτύων και πληροφοριών.
4	1	Έχει δημιουργηθεί σχετική διαδικασία και διενεργείται εσωτερικός έλεγχος (Τμήμα Εσωτερικού Ελέγχου του οργανισμού ή/και παροχή υπηρεσιών) τουλάχιστον ετήσια για την διαπίστωση της συμμόρφωσης με όλες τις σχετικές νομοθετικές, κανονιστικές και ρυθμιστικές απαιτήσεις, και συμβατικές απαιτήσεις όσον αφορά την ασφάλεια δικτύων και πληροφοριών.
4	2	Στη διαδικασία τηρούνται οι κατάλληλες προβλέψεις για έγκαιρη αναγνώριση των σχετικών νομοθετικών, κανονιστικών και ρυθμιστικών απαιτήσεων, και συμβατικών απαιτήσεων, αναφορικά με την ασφάλεια δικτύων και πληροφοριών.
4	3	Το κεντρικό αποθετήριο επικαιροποιείται σε περίπτωση νέων απαιτήσεων ή τροποποίησης υπαρχόντων.
4	4	Τα περιεχόμενα του αποθετηρίου επικοινωνούνται στο αρμόδιο προσωπικό όπως και όταν απαιτείται.
4	5	Σε περίπτωση αναγνώρισης απόκλισης από μία ή περισσότερες απαιτήσεις δημιουργείται καταγεγραμμένο πλάνο ενεργειών συμμόρφωσης. Το πλάνο ενεργειών συμμόρφωσης περιέχει στοιχεία σχετικά με το 1) Τι χρειάζεται να υλοποιηθεί, 2) μέχρι πότε χρειάζεται να υλοποιηθεί, 3) σε ποιόν έχει ανατεθεί η υπευθυνότητα παρακολούθησης / ολοκλήρωσης της υλοποίησης, 4) ποιοι πόροι απαιτούνται για την αποτελεσματική υλοποίηση και 5) με ποιον τρόπο και από ποιόν ρόλο θα διενεργηθεί η αξιολόγηση της ορθώς και αποτελεσματικής υλοποίησης.
4	6	Οι σχετικές πολιτικές και διαδικασίες ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Ο οργανισμός εξουσιοδοτεί τη διενέργεια εξωτερικών επιθεωρήσεων / ελέγχων για τον έλεγχο της συμμόρφωσης με όλες τις σχετικές νομοθετικές, κανονιστικές και ρυθμιστικές απαιτήσεις, και συμβατικές απαιτήσεις όσον αφορά την ασφάλεια δικτύων και πληροφοριών.
5	2	Τα δεδομένα των επιθεωρήσεων, (εσωτερικά και εξωτερικά) προστατεύονται από μη εξουσιοδοτημένη πρόσβαση και διατηρούνται για τουλάχιστον 5 χρόνια, εκτός αν προβλέπεται διαφορετικά από την σχετική νομοθεσία.
5	3	Όπου αυτό είναι εφικτό ο οργανισμός συμμετέχει σε δραστηριότητες και λειτουργίες ώστε να ενημερώνεται για επικείμενες αλλαγές ή νέες προσθήκες απαιτήσεων όσο πιο γρήγορα γίνεται.
5	4	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	5	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.

GOV3		Μέτρο: Πολιτικές, πρότυπα, κατευθυντήριες γραμμές και διαδικασίες ασφάλειας πληροφοριών. Στόχος Μέτρου: Να θεσπιστούν πολιτικές, πρότυπα, κατευθυντήριες γραμμές και διαδικασίες για την ασφάλεια πληροφοριών που να αντικατοπτρίζουν τη στρατηγική ασφάλειας πληροφοριών. Περιγραφή Μέτρου: Καθορισμός των μέτρων ασφάλειας πληροφοριών και λεπτομερής περιγραφή της εφαρμογής τους στα πλαίσια μιας πολιτικής ασφάλειας πληροφοριών που θα αντικατοπτρίζει τους στόχους που περιγράφονται στη στρατηγική ασφάλειας πληροφοριών [STR1]. Η πολιτική ασφάλειας των πληροφοριών θα πρέπει να περιλαμβάνει τους ρόλους και τις αρμοδιότητες σε επίπεδο οργάνωσης, όπως ορίζεται στο [GOV1]. Εφαρμογή συγκεκριμένων πολιτικών και διαδικασιών για την ασφάλεια πληροφοριών σε σχέση με συγκεκριμένες επεξεργασίες, συστήματα ή δραστηριότητες, ανάλογα με τις ανάγκες. Καθορισμός επιχειρησιακών κατευθυντήριων γραμμών για την ασφάλεια πληροφοριών και τυποποιημένες διαδικασίες λειτουργίας για συγκεκριμένες δραστηριότητες που σχετίζονται με πληροφορίες ή συστήματα επεξεργασίας πληροφοριών σε επιχειρησιακό επίπεδο. Πηγή: ISO 27002
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Δεν έχουν καθοριστεί από τον οργανισμό πολιτικές, οδηγίες και διαδικασίες σε σχέση με την ασφάλεια πληροφοριών.
1	1	Ακολουθείται μία σειρά από διαδικασίες και οδηγίες σε σχέση με την ασφάλεια πληροφοριών.
1	2	Οι πολιτικές και οι διαδικασίες εφαρμόζονται τουλάχιστον μερικώς και το προσωπικό ίσως να μην είναι ενημερωμένο ή να μην είναι πλήρως ενημερωμένο.
2	1	Έχει δημιουργηθεί μια πολιτική ασφάλειας πληροφοριών στην οποία γίνεται συνοπτική αναφορά και περιγραφή των μέτρων που έχουν ληφθεί.
3	1	Έχει δημιουργηθεί πολιτική ασφάλειας πληροφοριών όπου περιγράφονται αναλυτικά τα μέτρα που έχουν ληφθεί, όπως επίσης και λεπτομερή περιγραφή της εφαρμογής τους.
3	2	Η πολιτική ασφάλειας πληροφοριών αντικατοπτρίζει τους στόχους που περιγράφονται στη στρατηγική ασφάλειας πληροφοριών [STR1]
3	3	Η πολιτική ασφάλειας πληροφοριών περιλαμβάνει τους ρόλους και τις αρμοδιότητες σε επίπεδο οργάνωσης, όπως ορίζεται στο [GOV1].
3	4	Έχουν δημιουργηθεί μία σειρά από πολιτικές, οδηγίες και τυποποιημένες διαδικασίες λειτουργίας οι οποίες και εφαρμόζονται για την ασφάλεια πληροφοριών σε σχέση με συγκεκριμένες επεξεργασίες, συστήματα ή δραστηριότητες, ανάλογα με τις ανάγκες. και το προσωπικό έχει ενημερωθεί και εκπαιδευτεί σχετικά.
3	5	Όλες οι πολιτικές και οι διαδικασίες έχουν εγκριθεί από τη διοίκηση του οργανισμού.
3	6	Το προσωπικό έχει ενημερωθεί και εκπαιδευτεί σχετικά με τις πολιτικές και οι διαδικασίες.
4	1	Όλες οι πολιτικές και διαδικασίες ανασκοπούνται για την καταλληλότητά τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
4	2	Η ανασκόπηση περιλαμβάνει αξιολόγηση ευκαιριών για βελτίωση των πολιτικών, οδηγιών και διαδικασιών και της προσέγγισης του οργανισμού για τη διαχείριση της ασφάλειας των πληροφοριών ως απάντηση σε αλλαγές στο οργανωτικό περιβάλλον, τις επιχειρηματικές συνθήκες, τις νομικές συνθήκες ή το τεχνικό περιβάλλον.
5	1	Ο οργανισμός υλοποιεί αυτοματοποιημένα συστήματα για την διαχείριση της σχετικής τεκμηρίωσης.
5	2	Οι πολιτικές και οι διαδικασίες υλοποιούνται σε ένα μεγάλο βαθμό μέσα από αυτόματες ροές και παρέχεται η δυνατότητα απευθείας ενσωμάτωσης των διαφόρων δεδομένων, των εγκρίσεων και της υλοποίησης.
5	3	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους
5	4	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.

Κατηγορία		ΔΙΑΧΕΙΡΙΣΗ ΚΙΝΔΥΝΩΝ
RM1		Μέτρο: Μεθοδολογία Στόχος Μέτρου: Να θεσπιστεί μεθοδολογία διαχείρισης κινδύνων, η οποία αντικατοπτρίζει τη διαδικασία εκτίμησης κινδύνου του οργανισμού, τα κριτήρια ανάλυσης κινδύνου, τα κριτήρια αποδοχής κινδύνων και την πολιτική ανάληψης κινδύνων. Περιγραφή Μέτρου: Θέσπιση μεθοδολογίας για τη διαχείριση κινδύνων μέσω του καθορισμού της διαδικασίας εκτίμησης κινδύνων, των κριτηρίων ανάλυσης κινδύνου (δηλαδή των κριτηρίων επιπτώσεων, των κριτηρίων πιθανότητας, της βαθμολογίας κινδύνου), των κριτηρίων αποδοχής κινδύνων και της πολιτικής ανάληψης κινδύνων από τον οργανισμό. Η μεθοδολογία διαχείρισης κινδύνου θα επιτρέψει στον οργανισμό να αξιολογήσει τους κινδύνους για την ασφάλεια πληροφοριών που αντιμετωπίζει, και να εφαρμόσει τα κατάλληλα μέτρα για την αντιμετώπιση ή τον μετριασμό τους. Ο οργανισμός θα πρέπει να θέσει σε εφαρμογή διαδικασίες και εργαλεία, ανάλογα με την περίπτωση, προκειμένου να στηρίξει τις διαδικασίες διαχείρισης κινδύνων, έχοντας κατ’ ελάχιστον ένα μητρώο κινδύνων, ένα σχέδιο αντιμετώπισης κινδύνων και μια δομή διακυβέρνησης της ασφάλειας πληροφοριών στην οποία θα περιγράφονται λεπτομερώς οι ρόλοι και οι αρμοδιότητες. Η οριζόμενη μεθοδολογία διαχείρισης κινδύνων θα πρέπει να επικυρώνεται, να συμφωνείται και να υποστηρίζεται από τη διοίκηση ανώτατου επιπέδου και άλλους σχετικούς φορείς εντός του οργανισμού. Πηγή: C2M2 (Risk), NIST 800-53 (PM-9), ISO 27001 6.1
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν υλοποιεί ενέργειες για την διαχείριση κινδύνων σχετικά με την ασφάλεια των πληροφοριών και των δικτύων.
1	1	Διενεργούνται σε ad hoc βάση, ή έχουν τουλάχιστον διενεργηθεί μια φορά κατά τα τελευταία 2 χρόνια ανάλυση και αποτίμηση κινδύνων σχετικά με την ασφάλεια των πληροφοριών και των δικτύων.
1	2	Η διαδικασία είναι τουλάχιστον μερικώς καταγεγραμμένη και αποτυπώνεται μέσα από τα αρχεία που διατηρήθηκαν κατά την υλοποίηση.
2	1	Έχει δημιουργηθεί και καταγραφεί διαδικασία για την διαχείριση κινδύνων ασφάλειας πληροφοριών και δικτύων.
2	2	Η διαδικασία περιέχει κατ' ελάχιστο ρόλους και αρμοδιότητες, κριτήρια για την διενέργεια της αξιολόγηση κινδύνων και τα σχετικά αρχεία που πρέπει να τηρούνται.
2	4	Μέσα από την εφαρμογή της διαδικασίας προκύπτει κατ' ελάχιστο μια προτεραιοποίηση των αναγνωρισμένων κινδύνων.
2	3	Όλες οι σχετικές πληροφορίες σε σχέση με τη διαχείριση των κινδύνων ασφάλειας πληροφοριών έχουν καταγραφεί και η εν λόγω πληροφόρηση παρέχεται στην Αρχή ετήσια ή και κατόπιν αιτήματος.
3	1	Έχει θεσπίστει και καταγράφει μεθοδολογία για τη διαχείριση κινδύνων.
3	2	Η μεθοδολογία περιέχει την διαδικασία εκτίμησης κινδύνων, προσδιορίζει τα κριτήρια ανάλυσης κινδύνου (τα οποία είναι κατ΄ ελάχιστον κριτήρια επιπτώσεων, κριτήρια πιθανότητας, και συναρτήσεις για την εξαγωγή της βαθμολογίας κινδύνου), των κριτηρίων αποδοχής κινδύνων και της πολιτικής ανάληψης κινδύνων από τον οργανισμό.
3	3	Ο ρόλος του ιδιοκτήτη κινδύνων ορίζεται στη μεθοδολογία και περιγράφονται οι ρόλοι και οι αρμοδιότητές τους σε σχέση με την διαχείρισης κινδύνων.
3	4	Η μεθοδολογία διαχείρισης κινδύνου επιτρέπει στον οργανισμό να αξιολογεί τους κινδύνους για την ασφάλεια πληροφοριών που αντιμετωπίζει, και να εφαρμόζει τα κατάλληλα μέτρα για την αντιμετώπιση ή τον μετριασμό τους λαμβάνοντας υπόψη το πλαίσιο λειτουργίας του.
3	5	Έχουν τεθεί σε εφαρμογή διαδικασίες και εργαλεία, ανάλογα με την περίπτωση για υποστήριξη των διαδικασιών διαχείρισης κινδύνων, έχοντας κατ’ ελάχιστον ένα μητρώο κινδύνων, ένα σχέδιο αντιμετώπισης κινδύνων και μια δομή διακυβέρνησης της ασφάλειας πληροφοριών στην οποία περιγράφονται λεπτομερώς οι ρόλοι και οι αρμοδιότητες.
3	6	Η οριζόμενη μεθοδολογία διαχείρισης κινδύνων επικυρώνεται, συμφωνείται και υποστηρίζεται από τη διοίκηση ανώτατου επιπέδου και άλλους σχετικούς φορείς εντός του οργανισμού.
3	7	Η μεθοδολογία ορίζει ότι εφαρμόζεται (ως μεθοδολογία) εντός του οργανισμού σε τακτά χρονικά διαστήματα και τουλάχιστον ετησίως.
4	1	Η μεθοδολογία για τη διαχείριση κινδύνων ακολουθεί διεθνείς σχετικές βέλτιστες πρακτικές.

4	2	Η μεθοδολογία αποτυπώνει τα ακόλουθα επιμέρους βήματα για την διαχείριση κινδύνων: Πλαίσιο λειτουργίας, αξιολόγηση κινδύνων (που αποτελείται από αναγνώριση κινδύνων, ανάλυση κινδύνων και αποτίμηση κινδύνων), αντιμετώπιση κινδύνων, καταγραφή και αναφορά των κινδύνων, επικοινωνία, παρακολούθηση και ανασκόπηση κινδύνων.
4	3	Τα κριτήρια επιπτώσεων έχουν προσαρμοστεί και ανταποκρίνονται στις επιχειρησιακές ανάγκες και στόχους του οργανισμού όπως αναφέρονται στην σχετική στρατηγική [STR1], με στόχο να μπορούν να εξυπηρετήσουν την καλύτερη κατανόηση της συμπλήρωσης και των αποτελεσμάτων από το σύνολο του εμπλεκόμενου προσωπικού.
4	4	Ο οργανισμός εξάγει, παρακολουθεί και καταγράφει την επίδοση της διαχείρισης κινδύνων μέσω κατάλληλων μετρητών.
4	5	Η μεθοδολογία είναι συμβατή και τροφοδοτεί στοιχεία στην επιχειρησιακού επιπέδου διεργασία διαχείρισης κινδύνων (Enterprise Risk Management process).
4	6	Έχει οριστεί ένας υπεύθυνος που έχει επαρκή εξουσιοδότηση για την συνολική διαχείριση και παρακολούθηση της μεθοδολογίας.
4	7	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
4	8	Η μεθοδολογία αναγράφει σαφώς την συχνότητα εφαρμογής της μεθοδολογίας και την ανάγκη για επικαιροποίηση σε περίπτωση σημαντικών αλλαγών.
4	9	Έχει δημιουργηθεί μια διακριτή πολιτική ανάληψης κινδύνων η οποία έχει άμεση σχέση με τους στόχους, το πλαίσιο λειτουργίας και την στρατηγική του οργανισμού και αποτυπώνεται και στα σχετικά κριτήρια αποδοχής κινδύνου.
5	1	Η μεθοδολογία για τη διαχείριση κινδύνων περιλαμβάνεται στο πλαίσιο διακυβέρνησης του οργανισμού και είναι συμβατό με την σχετική στρατηγική όπως αναφέρεται στο [STR1].
5	2	Γίνονται εξωτερικές επιθεωρήσεις με αντικείμενο τον σχεδιασμό, την λειτουργία και την βελτίωση της μεθοδολογίας διαχείρισης κινδύνων.
5	3	Σε περίπτωση αναγνώρισης απόκλισης από μια ή περισσότερες απαιτήσεις δημιουργείται καταγεγραμμένο πλάνο ενεργειών συμμόρφωσης.
5	4	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους
5	5	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
5	6	Τα στοιχεία σχετικά με τον τρόπο που οργανισμός διαχειρίζεται τους κινδύνους ασφάλειας πληροφοριών και δικτύων επικοινωνούνται στα διάφορα εμπλεκόμενα μέρη όπως απαιτείται. Σε περίπτωση αλλαγής της κατάστασης των σχετικών κινδύνων, ενημερώνονται αντίστοιχα. (τα εμπλεκόμενα μέρη μπορεί να είναι τόσο εσωτερικά όσο και εξωτερικά του οργανισμού)
RM2		Μέτρο: Πλαίσιο Στόχος Μέτρου: Να καταρτιστεί κατάλογος στοιχείων ενεργητικού, συστημάτων και διαδικασιών εντός του οργανισμού. Περιγραφή Μέτρου: Κατάρτιση καταλόγου στοιχείων ενεργητικού, συστημάτων και διαδικασιών εντός του οργανισμού και καταγραφή των εξαρτήσεων και αλληλεξαρτήσεων μεταξύ αυτών των στοιχείων ενεργητικού, των συστημάτων και των διαδικασιών με σκοπό τη σαφή αποτύπωση του πλαισίου / περιβάλλοντος στο οποίο θα πραγματοποιηθεί η εκτίμηση κινδύνου. Μια σαφής εικόνα του πλαισίου του οργανισμού θα επιτρέψει τον εντοπισμό των κινδύνων εντός του οργανισμού Πηγή: C2M2 (Configuration), NIST 800-53 (PM-9), ISO 27001 A.8
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν έχει κάποιο συγκεκριμένο / οργανωμένο τρόπο για την αναγνώριση στοιχείων ενεργητικού, συστημάτων και διαδικασιών εντός του οργανισμού.
1	1	Τα στοιχεία ενεργητικού καταγράφονται τουλάχιστον με μη συστηματικό τρόπο. Τηρείται κάποιο αρχείο, με ή χωρίς κεντρική διαχείριση, το οποίο ενημερώνεται τουλάχιστον ad-hoc.
2	1	Τηρείται κατάλογος στοιχείων ενεργητικού, συστημάτων και διαδικασιών εντός του οργανισμού, ο οποίος μπορεί και να μην περιλαμβάνει τις αλληλεξαρτήσεις μεταξύ τους.
2	2	Υπάρχει ένας αναγνωρισμένος ιδιοκτήτης του καταλόγου, ο οποίος είναι υπεύθυνος για την τήρηση και επικαιροποίηση των σχετικών δεδομένων.
3	1	Στον κατάλογο στοιχείων ενεργητικού έχουν καταγραφεί οι εξαρτήσεις και αλληλεξαρτήσεις μεταξύ αυτών των στοιχείων ενεργητικού, των συστημάτων και των διαδικασιών με σκοπό τη σαφή αποτύπωση του πλαισίου / περιβάλλοντος στο οποίο πραγματοποιείται η εκτίμηση κινδύνου.

3	2	Ο κατάλογος είναι συμβατός και μπορεί να συμπίπτει (να αποτελεί μέρος ή παράγωγο) με αυτόν που αναφέρεται στο [AM2], με την προϋπόθεση της κάλυψης και των 2 ομάδων απαιτήσεων για τα αντίστοιχα επίπεδα, ούτως ώστε η αξιολόγηση κινδύνων να μπορεί να διενεργηθεί σε στοιχεία ή σε ομάδες στοιχείων ενεργητικού με ομοειδή χαρακτηριστικά τα οποία κρίνονται ότι χρειάζονται προστασία.
3	3	Τηρείται διαδικασία για την διαχείριση των πόρων όπως αναφέρεται στο [AM1], μέσω της οποίας εξασφαλίζεται η έγκαιρη ενημέρωση του καταλόγου σε περίπτωση αλλαγών.
4	1	Χρησιμοποιείται αυτόματο σύστημα για την αναγνώριση και καταγραφή στοιχείων ενεργητικού και συστημάτων εντός του οργανισμού αλλά και εκτός του οργανισμού (hosted in third parties).
4	2	Τα στοιχεία που εξάγονται από το αυτόματο σύστημα συμπληρώνονται με στοιχεία διαδικασιών και δημιουργείται αποτύπωση των σχετικών εξαρτήσεων και αλληλεξαρτήσεων με όσο περισσότερο αυτοματοποιημένο τρόπο γίνεται.
4	3	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Διατίθεται αυτόματο σύστημα και διαδικασίες για τον ελέγχου της ακεραιότητας και εγκυρότητας των στοιχείων του καταλόγου στοιχείων ενεργητικού, συστημάτων και διαδικασιών.
5	2	Σε περίπτωση ανίχνευσης στοιχείου που δεν βρίσκεται καταχωρημένο στον κατάλογο διενεργούνται αυτόματες ενέργειες ενημέρωσης του αρμόδιου προσωπικού για τον έλεγχο και επικαιροποίηση των σχετικών στοιχείων.
5	3	Ειδικά σε περίπτωση στοιχείων ενεργητικού, λαμβάνονται άμεσες ενέργειες περιορισμού μέχρι την υλοποίηση της σχετικής διερεύνησης.
5	4	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	5	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
RM3		Μέτρο: Εντοπισμός κινδύνων Στόχος Μέτρου: Να εντοπιστούν οι απειλές, ευπάθειες και κίνδυνοι στους οποίους εκτίθενται τα στοιχεία ενεργητικού, τα συστήματα και οι διαδικασίες του οργανισμού. Περιγραφή Μέτρου: Προσδιορισμός και κατάρτιση καταλόγου απειλών, ευπαθειών και κινδύνων στους οποίους είναι εκτεθειμένος ο οργανισμός όσον αφορά τα στοιχεία ενεργητικού, τα συστήματα και τις διαδικασίες που προσδιορίζονται στο μέτρο [RM2]. Οι κίνδυνοι που θα εντοπιστούν στα πλαίσια αυτής της διαδικασίας πρέπει να αποτυπώνονται σε μητρώο κινδύνων ώστε να μπορεί ο οργανισμός να παρακολουθεί τις απειλές, τις ευπάθειες και τους κινδύνους στους οποίους είναι εκτεθειμένος. Πηγή: C2M2 (RISK), NIST 800-53 (RA-1, RA-5), ISO 27001 6.1., ISO 27005
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν υλοποιεί ενέργειες για την αναγνώριση κινδύνων σχετικά με την ασφάλεια των πληροφοριών και των δικτύων.
1	1	Διενεργούνται τουλάχιστον σε ad hoc βάση, ή έχουν τουλάχιστον διενεργηθεί μια φορά κατά τα τελευταία 2 χρόνια ανάλυση και αποτίμηση κινδύνων (αναγνώριση κινδύνων) σχετικά με την ασφάλεια των πληροφοριών και των δικτύων.
1	2	Η διαδικασία αναγνώρισης κινδύνων δύναται να μην είναι πλήρως καταγεγραμμένη αλλά έχει δημιουργηθεί και διατηρείται τουλάχιστον μια λίστα κινδύνων σχετικά με την ασφάλειας των πληροφοριών και των δικτύων.
2	1	Έχει δημιουργηθεί και καταγραφεί μια πλήρης διαδικασία για την διαχείριση κινδύνων ασφάλειας πληροφοριών και δικτύων στην οποία αναφέρεται και η αναγνώριση κινδύνων.
2	2	Η διαδικασία περιέχει κατ' ελάχιστο ρόλους και αρμοδιότητες, κριτήρια για την διενέργεια της αναγνώρισης κινδύνων και τα σχετικά αρχεία που πρέπει να τηρούνται.
2	3	Οι κίνδυνοι αναγνωρίζονται ανά στοιχείο που περιέχεται στον κατάλογο στοιχείων ενεργητικού, συστημάτων και διαδικασιών εντός του οργανισμού.
3	1	Ο οργανισμός έχει προσδιορίσει και καταρτίσει κατάλογο απειλών, ευπαθειών και κινδύνων στους οποίους είναι εκτεθειμένος ο οργανισμός όσον αφορά τα στοιχεία ενεργητικού, τα συστήματα και τις διαδικασίες που προσδιορίζονται στο μέτρο [RM2].
3	2	Οι κίνδυνοι που εντοπίζονται στα πλαίσια αυτής της διαδικασίας αποτυπώνονται σε μητρώο κινδύνων ώστε να μπορεί ο οργανισμός να παρακολουθεί τις απειλές, τις ευπάθειες και τους κινδύνους στους οποίους είναι εκτεθειμένος.
3	3	Τα στοιχεία του καταλόγου είναι σύμφωνα με διεθνείς βέλτιστες πρακτικές.
3	4	Για κάθε κίνδυνο αναγνωρίζεται ένας τουλάχιστον ιδιοκτήτης κινδύνου όπως ορίζει η σχετική διαδικασία του [RM1].

3	5	Σε κάθε περίπτωση περιλαμβάνονται κίνδυνοι που προκύπτουν από τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, άνευ αδείας κοινοποίηση ή πρόσβαση σε πληροφορίες που διαβιβάζονται, αποθηκεύονται ή υποβάλλονται κατ' άλλο τρόπο σε επεξεργασία καθώς και άλλοι κίνδυνοι που παρουσιάζονται οι οποίοι θα μπορούσαν να επιδράσουν δυνητικά σε ουσιώδεις οικονομικές και κοινωνικές λειτουργίες και υπηρεσίες που παρέχονται από τον ΦΕΒΥ ή ΦΚΥΠ.
4	1	Οι κίνδυνοι έχουν αναγνωριστεί στην βάση του ενημερωμένου καταλόγου στοιχείων ενεργητικού, συστημάτων και διαδικασιών του οργανισμού όπως περιγράφεται στο [RM2].
4	2	Οι κίνδυνοι καλύπτουν όλες τις πιθανές κατηγορίες πηγών κινδύνων (risk sources) ανεξάρτητα από το αν είναι υπό τον έλεγχο του οργανισμού. Ειδικά για τα πολύπλοκα και κρίσιμα σενάρια κινδύνων, η μεθοδολογία επαναλαμβάνεται (iterations - στην αρχή σε high level και στην συνέχεια drilling down σε περισσότερες λεπτομέρειες μέχρι να αναγνωριστεί το ορθό root cause).
4	3	Όπου έχουν γίνει παραδοχές και ομαδοποιήσεις, υπάρχει σχετική καταγραφή που εξηγεί το σκεπτικό και προκύπτει ότι οι κίνδυνοι είναι σχετικοί σε όλα τα επίπεδα σύμφωνα με το πλαίσιο λειτουργίας του οργανισμού.
4	4	Η αναγνώριση κινδύνων είναι βασικό κομμάτι της διαχείρισης κινδύνου και διενεργείται σύμφωνα με την περιοδικότητα που έχει αναγνωριστεί στην σχετική διαδικασία όπως αναφέρεται στο [RM1].
4	5	Όταν τα εμπλεκόμενα μέρη αναγνωρίσουν ότι αδυναμίες, απειλές ή κίνδυνοι δεν είναι πλέον εφαρμόσιμοι, ο σχετικός κατάλογος επικαιροποιείται υποδεικνύοντας ότι η αντίστοιχη εγγραφή δεν είναι πλέον ενεργή. (Η ιστορικότητα αναγνώρισης διατηρείται και τεκμηριώνεται).
4	6	Τα στοιχεία του καταλόγου ενημερώνονται / επικαιροποιούνται / εμπλουτίζονται σε σύνδεση με την διαδικασία καταγραφής και αναφοράς ευπαθειών όπως αναφέρεται στο [VM2].
4	7	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
4	9	Για την αναγνώριση των απειλών, ευπαθειών και κινδύνων στους οποίους είναι εκτεθειμένος ο οργανισμός γίνεται με την συμμετοχή όσο μεγαλύτερου πλήθους εσωτερικών μερών γίνεται.
4	10	Υπάρχει δυνατότητα και διαδικασία γνωστή στο προσωπικό για την παροχή στοιχείων αναγνώρισης απειλών, ευπαθειών και κινδύνων στους οποίους είναι εκτεθειμένος ο οργανισμός από το προσωπικό ad-hoc.
4	11	Γίνεται τακτικός έλεγχος πληρότητας των στοιχείων των καταλόγων έναντι διεθνών έγκυρων πηγών.
5	1	Έγκυρες πληροφορίες Cyber threat intelligence λαμβάνονται έγκαιρα και μεταξύ άλλων χρησιμοποιούνται για την επικαιροποίηση του καταλόγου απειλών, ευπαθειών και κινδύνων στους οποίους είναι εκτεθειμένος ο οργανισμός.
5	2	Τα στοιχεία από τα διδάγματα που έχουν αντληθεί από τα συμβάντα και περιστατικά ασφάλειας πληροφοριών, χρησιμοποιούνται για την ενημέρωση των στοιχείων του καταλόγου (απειλών, ευπαθειών και κινδύνων) σε συμφωνία με τα αναγραφόμενα στο [EIM4].
5	3	Γίνονται τακτικές και εξειδικευμένες συναντήσεις με εσωτερικά και εξωτερικά εμπλεκόμενα μέρη για την υποβοήθηση / εμπλουτισμό και επικαιροποίηση του καταλόγου απειλών, ευπαθειών και κινδύνων στους οποίους είναι εκτεθειμένος ο οργανισμός.
5	4	Τα αποτελέσματα από εσωτερικούς και εξωτερικούς ελέγχους που υποδεικνύουν κενά στην συμμόρφωση του οργανισμού, καταγράφονται ως κίνδυνοι και αναλύονται στον σχετικό κατάλογο.
5	5	Κίνδυνοι που σχετίζονται με την εξάρτηση από άλλες κρίσιμες υποδομές ή τρίτους οργανισμούς περιέχονται στον σχετικό κατάλογο.
5	6	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	7	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.

RM4		Μέτρο: Ανάλυση κινδύνου Στόχος Μέτρου: Να αναλυθούν οι κίνδυνοι για την ασφάλεια πληροφοριών στο πλαίσιο των στοιχείων ενεργητικού ανάλογα με τις διάφορες πιθανότητες και επιπτώσεις. Περιγραφή Μέτρου: Ανάλυση των κινδύνων για την ασφάλεια πληροφοριών όσον αφορά τα στοιχεία ενεργητικού, όπως προσδιορίζονται στο [RM2], λαμβάνοντας υπόψη τις διαφορετικές πιθανότητες και τις βαθμολογίες των επιπτώσεων, όπως ορίζονται στο [RM1]. Ο οργανισμός προσδιορίζει τη βαθμολογία κινδύνου προκειμένου να αξιολογήσει την κατάλληλη στρατηγική μετριασμού της [RM5]. Κατά την αξιολόγηση του κατάλληλου επιπέδου ασφάλειας, λαμβάνονται ιδίως υπόψη οι κίνδυνοι που προκύπτουν από τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, άνευ αδείας κοινοποίηση ή πρόσβαση σε πληροφορίες που διαβιβάζονται, αποθηκεύονται ή υποβάλλονται κατ' άλλο τρόπο σε επεξεργασία. Επίσης, λαμβάνονται υπόψη οι κίνδυνοι που παρουσιάζονται οι οποίοι θα μπορούσαν να επιδράσουν δυνητικά σε ουσιώδεις οικονομικές και κοινωνικές λειτουργίες και υπηρεσίες που παρέχονται από τον ΦΕΒΥ ή ΦΚΥΠ. Τα αποτελέσματα της ανάλυσης κινδύνου θα πρέπει να καταγράφονται στο μητρώο κινδύνων του οργανισμού. Πηγή: C2M2 (RISK), NIST 800-53 (RA-1, RA-6), ISO 27001 6.1., ISO 27005
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν υλοποιεί ενέργειες για την ανάλυση κινδύνων σχετικά με την ασφάλεια των πληροφοριών και των δικτύων.
1	1	Διενεργείται τουλάχιστον σε ad hoc βάση, ή έχει τουλάχιστον διενεργηθεί μια φορά κατά τα τελευταία 2 χρόνια, ανάλυση κινδύνων σχετικά με την ασφάλεια των πληροφοριών και των δικτύων.
1	2	Η διαδικασία ανάλυσης κινδύνων δύναται να μην είναι πλήρως καταγεγραμμένη αλλά τηρείται τουλάχιστον ένα αρχείο που περιέχει τα σχετικά κριτήρια και τα αποτελέσματα της ανάλυσης των κινδύνων.
2	1	Έχει δημιουργηθεί και καταγραφεί μια πλήρης διαδικασία για την διαχείριση κινδύνων ασφάλειας πληροφοριών και δικτύων στην οποία αναφέρεται και το κομμάτι της ανάλυσης κινδύνων.
2	2	Η διαδικασία περιέχει κατ' ελάχιστο ρόλους και αρμοδιότητες, κριτήρια για την διενέργεια της ανάλυσης κινδύνων και τα σχετικά αρχεία που πρέπει να τηρούνται.
2	3	Οι κίνδυνοι αναλύονται ανά στοιχείο που περιέχεται στον κατάλογο στοιχείων ενεργητικού, συστημάτων και διαδικασιών εντός του οργανισμού.
3	1	Υλοποιείται ανάλυση των κινδύνων για την ασφάλεια πληροφοριών όσον αφορά τα στοιχεία ενεργητικού, όπως προσδιορίζονται στο [RM2], λαμβάνοντας υπόψη τις διαφορετικές πιθανότητες και τις βαθμολογίες των επιπτώσεων, όπως ορίζονται στο [RM1].
3	2	Ο κίνδυνος προσδιορίζεται και βαθμολογείται για αξιολόγηση της κατάλληλης στρατηγικής μετριασμού του [RM5].
3	3	Κατά την αξιολόγηση του κατάλληλου επιπέδου ασφάλειας, λαμβάνονται ιδίως υπόψη οι κίνδυνοι που προκύπτουν από τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, άνευ αδείας κοινοποίηση ή πρόσβαση σε πληροφορίες που διαβιβάζονται, αποθηκεύονται ή υποβάλλονται κατ' άλλο τρόπο σε επεξεργασία. Επίσης, λαμβάνονται υπόψη οι κίνδυνοι που παρουσιάζονται οι οποίοι θα μπορούσαν να επιδράσουν δυνητικά σε ουσιώδεις οικονομικές και κοινωνικές λειτουργίες και υπηρεσίες που παρέχονται από τον ΦΕΒΥ ή ΦΚΥΠ.
3	4	Τα αποτελέσματα της ανάλυσης κινδύνου καταγράφονται στο μητρώο κινδύνων του οργανισμού.
4	1	Κατά την εκτίμηση της πιθανότητας αλλά και της σχετικής επίπτωσης, λαμβάνεται υπόψη η υλοποίηση ανεξάρτητων και εξαρτημένων γεγονότων (π.χ. ένα δεύτερο γεγονός που μπορεί να υλοποιηθεί επειδή ένα πρώτο έχει συμβεί).
4	2	Αντίστοιχα υλοποιούνται μέθοδοι και προβλέψεις για τον προσδιορισμό cascading κίνδυνοι και οι επιπτώσεις τους.
4	3	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
4	4	Η ανάλυση των κινδύνων στους οποίους είναι εκτεθειμένος ο οργανισμός γίνεται με την συμμετοχή όσο μεγαλύτερου πλήθους εσωτερικών μερών γίνεται.
4	5	Υπάρχει δυνατότητα και διαδικασία γνωστή στο προσωπικό για την ενημέρωση του αρμόδιου προσωπικού σε περίπτωση αναγνώρισης λάθους ή παράλειψης της ανάλυσης κινδύνων.
4	6	Για τον προσδιορισμό της πιθανότητας αλλά και της επίπτωσης των αναγνωρισμένων κινδύνων, λαμβάνεται υπόψη η υλοποίηση σχετικών (αν υπάρχουν) μέτρων αντιμετώπισης (controls).
5	1	Έγκυρες πληροφορίες Cyber threat intelligence λαμβάνονται έγκαιρα και μεταξύ άλλων χρησιμοποιούνται για την επικαιροποίηση των αποτελεσμάτων της ανάλυσης κινδύνων στους οποίους είναι εκτεθειμένος ο οργανισμός.

5	2	Τα στοιχεία από τα διδάγματα που έχουν αντληθεί από τα συμβάντα και περιστατικά ασφάλειας πληροφοριών, χρησιμοποιούνται για την ενημέρωση των αποτελεσμάτων της ανάλυσης κινδύνων σε συμφωνία με τα αναγραφόμενα στο [EIM4].
5	3	Γίνονται τακτικές και εξειδικευμένες συναντήσεις με εσωτερικά και εξωτερικά εμπλεκόμενα μέρη για την αξιολόγηση της ορθότητας και εγκυρότητας των αποτελεσμάτων της ανάλυσης κινδύνων.
5	4	Τα αποτελέσματα από εσωτερικούς και εξωτερικούς ελέγχους (στο βαθμό που σχετίζονται) χρησιμοποιούνται για την επικαιροποίηση των στοιχείων των αποτελεσμάτων της ανάλυσης κινδύνων.
5	5	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	6	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
5	7	Όπου είναι δυνατό, χρησιμοποιούνται αυτοματοποιημένα εργαλεία και βάσεις δεδομένων τα οποία προσδιορίζουν τις ευπάθειες των διαφόρων στοιχείων, αξιολογούν την ευκολία εκμετάλλευσής τους, καθορίζουν σχετικά σενάρια και διαδρομές επίθεσης και προσδιορίζουν την πιθανότητα υλοποίησης συγκεκριμένων κινδύνων.
5	8	Έχει δημιουργήσει ένα συστηματικό πλαίσιο για τον έλεγχο της αποτελεσματικότητας των μέτρων αντιμετώπισης που έχει υλοποιήσει ο οργανισμός και τα στοιχεία της αποτελεσματικότητας των μέτρων τροφοδοτούν συστηματικά κατάλληλα την ανάλυση κινδύνων.
RM5		Μέτρο: Αξιολόγηση κινδύνων Στόχος Μέτρου: Να αξιολογηθούν οι κίνδυνοι για την ασφάλεια πληροφοριών με βάση την πολιτική ανάληψης κινδύνων του οργανισμού και να καθοριστούν οι κατάλληλες στρατηγικές αντιμετώπισης. Περιγραφή Μέτρου: Καθορισμός κατάλληλων και επαρκών στρατηγικών για την αντιμετώπιση των κινδύνων που αναλύονται σύμφωνα με το [RM4]. Ο οργανισμός λαμβάνει υπόψη τη μείωση του κινδύνου, τη μεταφορά κινδύνου, την αποφυγή του κινδύνου και την αποδοχή (ή τη διατήρηση) κινδύνου ως κατάλληλες στρατηγικές αντιμετώπισης κινδύνων. Κατά την αξιολόγηση των στρατηγικών αντιμετώπισης κινδύνων, ο οργανισμός λαμβάνει υπόψη την πολιτική ανάληψης κινδύνων όπως ορίζεται στο [RM1]. Το αποτέλεσμα της αξιολόγησης κινδύνων θα πρέπει να καταγράφεται στο μητρώο κινδύνων του οργανισμού. Πηγή: C2M2 (RISK), NIST 800-53 (RA-1, RA-6), ISO 27001 6.1., ISO 27005
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν υλοποιεί ενέργειες για την αξιολόγηση κινδύνων σχετικά με την ασφάλεια των πληροφοριών και των δικτύων.
1	1	Διενεργείται τουλάχιστον σε ad hoc βάση, ή έχει τουλάχιστον διενεργηθεί μια φορά κατά τα τελευταία 2 χρόνια, αξιολόγηση κινδύνων σχετικά με την ασφάλεια των πληροφοριών και των δικτύων.
1	2	Η διαδικασία αξιολόγησης κινδύνων δύναται να μην είναι πλήρως καταγεγραμμένη αλλά τηρείται τουλάχιστον ένα αρχείο που περιέχει τα σχετικά κριτήρια και τα αποτελέσματα της αξιολόγησης των κινδύνων.
2	1	Έχει δημιουργηθεί και καταγραφεί μια πλήρης διαδικασία για την διαχείριση κινδύνων ασφάλειας πληροφοριών και δικτύων στην οποία αναφέρεται και το κομμάτι της αξιολόγησης κινδύνων.
2	2	Η διαδικασία περιέχει κατ' ελάχιστο ρόλους και αρμοδιότητες, κριτήρια για την διενέργεια της αξιολόγησης κινδύνων και τα σχετικά αρχεία που πρέπει να τηρούνται.
2	3	Οι κίνδυνοι αξιολογούνται ανά στοιχείο που περιέχεται στον κατάλογο στοιχείων ενεργητικού, συστημάτων και διαδικασιών εντός του οργανισμού.
3	1	Έχουν καθοριστεί κατάλληλες και επαρκείς στρατηγικές για την αντιμετώπιση των κινδύνων που αναλύονται σύμφωνα με το [RM4].
3	2	Λαμβάνεται υπόψη η μείωση του κινδύνου, η μεταφορά κινδύνου, η αποφυγή του κινδύνου και η αποδοχή (ή διατήρηση) κινδύνου ως κατάλληλες στρατηγικές αντιμετώπισης κινδύνων.
3	3	Κατά την αξιολόγηση των στρατηγικών αντιμετώπισης κινδύνων, λαμβάνεται υπόψη η πολιτική ανάληψης κινδύνων όπως ορίζεται στο [RM1].
3	4	Το αποτέλεσμα της αξιολόγησης κινδύνων καταγράφονται στο μητρώο κινδύνων του οργανισμού.
3	5	Οι αποφάσεις σχετικά με τις στρατηγικές που έχουν επιλεγεί ανά περίπτωση τεκμηριώνονται και διατηρούνται.
4	1	Οι πιθανές και επιλεγμένες στρατηγικές ανασκοπούνται περιοδικά από τα κατάλληλα εξουσιοδοτημένα ενδιαφερόμενα μέρη, προκειμένου να εξεταστεί κατά πόσο εξακολουθούν να είναι κατάλληλες και αποτελεσματικές για την διαχείριση των σχετικών κινδύνων για τον οργανισμό.

4	2	Αλλαγές σε σχέση με την τεχνολογία, τις υπηρεσίες ή νέες στρατηγικές συνεργασίες οδηγούν στην ανασκόπηση των σχετικών στρατηγικών και αποφάσεων.
4	3	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
4	4	Ο ιδιοκτήτης του κινδύνου, δίνει την έγγραφη αποδοχή του σχετικά με την αποδοχή του εναπομείναντα κινδύνου και της επιλεγμένης στρατηγικής αντιμετώπισης κινδύνου.
5	1	Κατά το στάδιο του προσδιορισμού των κατάλληλων στρατηγικών, δημιουργείται και διατηρείται σχετική τεκμηρίωση η οποία περιέχει τα υπέρ, τα κατά, καθώς και μια αποτίμηση σε σχέση με το εκτιμώμενο κόστος χρησιμοποιώντας διεθνώς αναγνωρισμένες σχετικές πρακτικές (π.χ. προσδιορισμός ROSI).
5	2	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	3	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
RM6		Μέτρο: Αντιμετώπιση κινδύνων Στόχος Μέτρου: Να καθοριστούν οι δράσεις για την αντιμετώπιση των κινδύνων για την ασφάλεια πληροφοριών. Περιγραφή Μέτρου: Καθορισμός κατάλληλων και επαρκών μέτρων αντιμετώπισης του κινδύνου στα πλαίσια της εφαρμογής της στρατηγικής αντιμετώπισης κινδύνων που καθορίζεται στη διαδικασία αξιολόγησης των κινδύνων, όπως αυτή περιγράφεται στην [RM5]. Κατά τον καθορισμό των μέτρων, ο οργανισμός λαμβάνει υπόψη προληπτικά μέτρα, μέτρα εντοπισμού και μέτρα αντίδρασης από διοικητική, τεχνολογική και φυσική άποψη, προκειμένου να διασφαλίσει, κατά περίπτωση, μια πολυεπίπεδη άμυνα. Κατά τον καθορισμό των δράσεων αντιμετώπισης κινδύνων, ο φορέας εξετάζει τα μέτρα ασφάλειας που περιγράφονται στο Πλαίσιο μέτρων ασφάλειας (το παρόν έγγραφο). Το αποτέλεσμα της αντιμετώπισης κινδύνων θα πρέπει να καταγράφεται στο σχέδιο αντιμετώπισης κινδύνων του οργανισμού. Πηγή: C2M2 (RISK), NIST 800-53 (RA-1, RA-6), ISO 27001 6.1., ISO 27005
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν υλοποιεί δράσεις και ενέργειες για την αντιμετώπιση κινδύνων σχετικά με την ασφάλεια των πληροφοριών και των δικτύων.
1	1	Διενεργούνται τουλάχιστον σε ad hoc βάση, ή έχουν τουλάχιστον διενεργηθεί μια φορά κατά τα τελευταία 2 χρόνια, ενέργειες / δράσεις για την αντιμετώπιση κινδύνων σχετικά με την ασφάλεια των πληροφοριών και των δικτύων.
1	2	Η διαδικασία αντιμετώπισης κινδύνων δύναται να μην είναι πλήρως καταγεγραμμένη αλλά έχει δημιουργηθεί και διατηρείται τουλάχιστον ένα αρχείο που περιέχει τις σχετικές ενέργειες.
2	1	Έχει δημιουργηθεί και καταγραφεί μια πλήρης διαδικασία για την διαχείριση κινδύνων ασφάλειας πληροφοριών και δικτύων στην οποία αναφέρεται και το κομμάτι της αντιμετώπισης κινδύνων.
2	2	Η διαδικασία περιέχει κατ' ελάχιστο ρόλους και αρμοδιότητες, κριτήρια για την διενέργεια της αντιμετώπισης κινδύνων και τα σχετικά αρχεία που πρέπει να τηρούνται.
2	3	Υπάρχει αρχείο που περιέχει τις ενέργειες αντιμετώπισης, το οποίο περιέχει τι θα γίνει, μέχρι πότε, ποιος είναι υπεύθυνος και σε ποιο επίπεδο αναμένεται να βρεθεί το επίπεδο στο οποίο θα βρεθεί ο κίνδυνος μετά την αντιμετώπιση.
3	1	Καθορίζονται κατάλληλα και επαρκή μέτρα αντιμετώπισης του κινδύνου στα πλαίσια της εφαρμογής της στρατηγικής αντιμετώπισης κινδύνων που καθορίζεται στη διαδικασία αξιολόγησης των κινδύνων, όπως αυτή περιγράφεται στην [RM5].
3	2	Κατά τον καθορισμό των μέτρων, λαμβάνονται υπόψη προληπτικά μέτρα, μέτρα εντοπισμού και μέτρα αντίδρασης από διοικητική, τεχνολογική και φυσική άποψη, προκειμένου να διασφαλίζεται, κατά περίπτωση, μια πολυεπίπεδη άμυνα.
3	3	Κατά τον καθορισμό των δράσεων αντιμετώπισης κινδύνων, ο φορέας εξετάζει τα μέτρα ασφάλειας που περιγράφονται στην σχετική νομοθεσία της Αρχής (Κ.Δ.Π. 389/2020).
3	4	Το αποτέλεσμα της αντιμετώπισης κινδύνων καταγράφεται στο σχέδιο αντιμετώπισης κινδύνων του οργανισμού.
3	5	Το σχέδιο κινδύνων περιέχει τουλάχιστον τα ακόλουθα για κάθε κίνδυνο: τι θα γίνει, μέχρι πότε, ποιος είναι υπεύθυνος και σε ποιο επίπεδο αναμένεται να βρεθεί το επίπεδο στο οποίο θα βρεθεί ο κίνδυνος μετά την αντιμετώπιση, ποιοι είναι οι πόροι που απαιτούνται, με ποιόν τρόπο θα ελεγχθεί η αποτελεσματικότητα των ενεργειών, ποιος είναι ο ιδιοκτήτης του κινδύνου.

4	1	Διενεργείται περιοδικά έλεγχος της πορείας υλοποίησης των ενεργειών αντιμετώπισης κινδύνου. Το χρονικό διάστημα στο οποίο ο οργανισμός πρέπει να υλοποιήσει τις σχετικές ενέργειες καθορίζεται σύμφωνα με την κρισιμότητα του κινδύνου όπως αποτυπώνεται και στην σχετική διαδικασία.
4	2	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
4	3	Προκειμένου να αξιολογηθεί η πληρότητα των επιλεγμένων μέτρων, γίνεται σε τακτική βάση, σύγκριση με οργανωμένες λίστες ενεργειών (π.χ. ISO 27002 / ISO 27001 Annex A, ISO 27017, ISO 27011 κ.α.).
4	4	Σε περίπτωση που αναγνωριστεί κάποια ενέργεια η οποία μπορεί να υλοποιηθεί, ο οργανισμός προβαίνει σε κατάλληλη αξιολόγηση διενεργώντας τα βήματα της διαχείρισης κινδύνου με πεδίο τους κινδύνους που μπορεί να καλύψει η συγκεκριμένη ενέργεια.
5	1	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	2	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
5	3	Έχει δημιουργηθεί ένα συστηματικό πλαίσιο για τον έλεγχο της αποτελεσματικότητας των μέτρων αντιμετώπισης που έχει υλοποιήσει ο οργανισμός.
5	4	Ο οργανισμός εξουσιοδοτεί την διενέργεια εξωτερικών επιθεωρήσεων / ελέγχων για τον έλεγχο της αποτελεσματικότητας των υλοποιημένων μέτρων.
5	5	Τα στοιχεία της αποτελεσματικότητας των μέτρων τροφοδοτούν συστηματικά κατάλληλα τα βήματα αξιολόγησης και αντιμετώπισης κινδύνων ώστε να γίνουν τροποποιήσεις όπου απαιτείται.

Κατηγορία		ΕΥΑΙΣΘΗΤΟΠΟΙΗΣΗ ΚΑΙ ΕΚΠΑΙΔΕΥΣΗ
ΤΑ1		Μέτρο: Ευαισθητοποίηση σχετικά με την ασφάλεια πληροφοριών Στόχος Μέτρου: Να θεσπιστεί πρόγραμμα ενημέρωσης σχετικά με την ασφάλεια πληροφοριών για όλα τα στελέχη εντός του οργανισμού, λαμβάνοντας υπόψη τα στοιχεία που περιγράφονται στις πολιτικές, τα πρότυπα, τις κατευθυντήριες γραμμές και τις διαδικασίες ασφάλειας πληροφοριών. Περιγραφή Μέτρου: Καθορισμός προγράμματος ευαισθητοποίησης όσον αφορά την ασφάλεια των πληροφοριών, ώστε να υπάρχει επαρκής ευαισθητοποίηση των στελεχών σχετικά με τους ρόλους και τις ευθύνες όσον αφορά την ασφάλεια δικτύων και πληροφοριών, όπως ορίζεται στο [GOV1]. Πηγή: CIS, ISO 27002
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν έχει θεσπίσει πρόγραμμα ενημέρωσης σχετικά με την ασφάλεια πληροφοριών για τα στελέχη εντός του οργανισμού.
1	1	Έχει δημιουργηθεί ένα πρόγραμμα ενημέρωσης σχετικά με την ασφάλεια πληροφοριών το οποίο δύναται να μην πραγματοποιείται συστηματικά.
1	2	Η εκπαίδευση αφορά κατ'ελάχιστο τις βασικές αρχές για την ασφάλεια πληροφοριών.
2	1	Έχει δημιουργηθεί πρόγραμμα ενημέρωσης σχετικά με την ασφάλεια πληροφοριών το οποίο το παρακολουθούν όλα τα στελέχη του οργανισμού σε συγκεκριμένες περιόδους, ώστε να διασφαλίζεται ότι κατανοούν και επιδεικνύουν τις απαραίτητες συμπεριφορές και δεξιότητες για να διασφαλιστεί η ασφάλεια του οργανισμού.
3	1	Έχει γίνει καθορισμός προγράμματος ευαισθητοποίησης όσον αφορά την ασφάλεια των πληροφοριών, ώστε να υπάρχει επαρκής ευαισθητοποίηση των στελεχών σχετικά με τους ρόλους και τις ευθύνες όσον αφορά την ασφάλεια δικτύων και πληροφοριών, όπως ορίζεται στο [GOV1].
3	2	Το πρόγραμμα ευαισθητοποίησης για την ασφάλεια των πληροφοριών έχει δημιουργηθεί σύμφωνα με τις πολιτικές και τις σχετικές διαδικασίες του οργανισμού, λαμβάνοντας υπόψη τις πληροφορίες του οργανισμού που θα πρέπει να προστατεύονται και τα μέτρα που έχουν εφαρμοστεί για την προστασία των πληροφοριών.
3	3	Το πρόγραμμα ευαισθητοποίησης έχει σχεδιαστεί λαμβάνοντας υπόψη τους ρόλους των εργαζομένων στον οργανισμό.
3	4	Οι δραστηριότητες στο πρόγραμμα ευαισθητοποίησης προγραμματίζονται σε τακτικά χρονικά διαστήματα και τουλάχιστον μια φορά το χρόνο, ώστε οι δραστηριότητες να επαναλαμβάνονται και να καλύπτουν νέους εργαζόμενους.
3	5	Στην περίπτωση νέου εργαζόμενου η εκπαίδευση πραγματοποιείται το συντομότερο μετά την πρόσληψη.
4	1	Το πρόγραμμα ευαισθητοποίησης ενημερώνεται τακτικά, ώστε να είναι σύμφωνο με τις οργανωτικές πολιτικές και διαδικασίες και βασίζεται σε διδάγματα που αντλούνται από συμβάντα ασφάλειας πληροφοριών.
4	2	Περιλαμβάνει μια σειρά από δραστηριότητες ευαισθητοποίησης, όπως εκστρατείες (π.χ. μια «ημέρα ασφάλειας πληροφοριών») και έκδοση φυλλαδίων ή ενημερωτικών δελτίων.
4	3	Η αποτελεσματικότητα του προγράμματος αξιολογείται περιοδικά (τουλάχιστον μία φορά το χρόνο) και γίνονται βελτιώσεις ανάλογα με την περίπτωση. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
4	4	Το πρόγραμμα ευαισθητοποίησης έχει σχεδιαστεί λαμβάνοντας υπόψη τις προσδοκίες του οργανισμού για την ευαισθητοποίηση των εργολάβων, το οποίο τους κοινοποιείται.
5	1	Το πρόγραμμα ευαισθητοποίησης εξετάζει διαφορετικές μορφές εκπαίδευσης και κατάρτισης, π.χ. διαλέξεις ή αυτοδιδασκαλία. Το πρόγραμμα ευαισθητοποίησης περιλαμβάνει συνεχή εκπαίδευση και ευκαιρίες επαγγελματικής ανάπτυξης για το προσωπικό με σημαντικές ευθύνες στην ασφάλεια πληροφοριών.
5	2	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	3	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.

TA2		Μέτρο: Ευαισθητοποίηση και εκπαίδευση σε θέματα ασφάλειας πληροφοριών Στόχος Μέτρου: Να παρέχει εκπαίδευση προς όλα τα στελέχη του οργανισμού, όπως ορίζεται στο πρόγραμμα ασφάλειας πληροφοριών. Περιγραφή Μέτρου: Επαρκής ενημέρωση των στελεχών σχετικά με τους ρόλους και τις αρμοδιότητες τους όσον αφορά την ασφάλεια δικτύων και πληροφοριών, όπως ορίζεται στο [GOV1] μέσω κατάλληλης εκπαίδευσης και κατάρτισης που προσφέρεται με την υποστήριξη της διοίκησης ανώτατου επιπέδου. Οι εκπαιδεύσεις σχετικά με την ασφάλεια πληροφοριών περιλαμβάνουν συγκεκριμένες πληροφορίες σχετικά με τις επιχειρησιακές δραστηριότητες των στελεχών για λογαριασμό του οργανισμού στο πλαίσιο της επεξεργασίας πληροφοριών ή της πρόσβασης σε συστήματα επεξεργασίας πληροφοριών. Πηγή: C2M2, ISO 27002, ISO 27003, ENISA
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν πραγματοποιεί εκπαιδεύσεις στο προσωπικό σε σχέση με την Ασφάλεια Πληροφοριών.
1	1	Πραγματοποιούνται κάποιες εκπαιδεύσεις σε σχέση με την ασφάλεια πληροφοριών στο εμπλεκόμενο προσωπικό.
2	1	Πραγματοποιούνται εκπαιδεύσεις συστηματικά σε όλο προσωπικό σε σχέση με την ασφάλεια πληροφοριών, χωρίς κατ'ανάγκη να υπάρχει πρόγραμμα ενημέρωσης όπως αυτό αναφέρεται στον [TA1].
2	2	Οι στόχοι σχετικά με την εκπαίδευση του προσωπικού για την ασφάλεια πληροφοριών είναι καθορισμένοι και διατηρούνται.
3	1	Παρέχεται επαρκή ενημέρωση των στελεχών σχετικά με τους ρόλους και τις αρμοδιότητες τους όσον αφορά την ασφάλεια δικτύων και πληροφοριών, όπως ορίζεται στο [GOV1] μέσω κατάλληλης εκπαίδευσης και κατάρτισης που προσφέρεται με την υποστήριξη της διοίκησης ανώτατου επιπέδου.
3	2	Οι εκπαιδεύσεις σχετικά με την ασφάλεια πληροφοριών περιλαμβάνουν συγκεκριμένες πληροφορίες σχετικά με τις επιχειρησιακές δραστηριότητες των στελεχών για λογαριασμό του οργανισμού στο πλαίσιο της επεξεργασίας πληροφοριών ή της πρόσβασης σε συστήματα επεξεργασίας πληροφοριών.
3	3	Ακολουθείται το πρόγραμμα ενημέρωσης σχετικά με την ασφάλεια πληροφοριών όπως αναφέρεται στο [TA1].
3	4	Διατηρούνται τεκμηριωμένες πληροφορίες σχετικά με τις εκπαιδεύσεις και τα αποτελέσματα αυτών.
4	1	Πραγματοποιούνται έλεγχοι σε σχέση με την γνώση του προσωπικού όσον αφορά την ασφάλεια πληροφοριών.
4	2	Η αποτελεσματικότητα των εκπαιδεύσεων σε σχέση με ασφάλεια πληροφοριών αξιολογείται περιοδικά, και τουλάχιστον μία φορά το χρόνο, και σύμφωνα με καθορισμένους παράγοντες ενεργοποίησης, όπως αλλαγές συστήματος και εξωτερικά συμβάντα, και γίνονται βελτιώσεις ανάλογα με την περίπτωση.
4	3	Πραγματοποιούνται αρχικές εκπαίδευσεις όχι μόνο σε νέους υπαλλήλους αλλά και σε όσους μεταφέρονται σε νέες θέσεις ή αναλαμβάνουν νέους ρόλους με διαφορετικές απαιτήσεις ασφάλειας πληροφοριών.
5	1	Παρέχονται στο προσωπικό συνεδρίες εκπαίδευσης για την απόκτηση αναγνωρισμένων πιστοποιητικών σε σχέση με την ασφάλεια πληροφοριών ή cybersecurity.
5	2	Έχουν δημιουργηθεί επαφές και κανάλια επικοινωνίας με ομάδες και ενώσεις σχετικές με την ασφάλεια πληροφοριών ώστε να παραμένει το προσωπικό ενημερωμένο με τις πιο πρόσφατες συνιστώμενες πρακτικές, τεχνικές και τεχνολογίες ασφάλειας.
5	3	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	4	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.

Κατηγορία		ΔΙΑΧΕΙΡΙΣΗ ΤΡΙΤΩΝ ΜΕΡΩΝ ΚΑΙ ΠΡΟΜΗΘΕΥΤΩΝ
TPS1		Μέτρο: Δέουσα επιμέλεια για τρίτα μέρη και προμηθευτές Στόχος Μέτρου: Να επιδεικνύει τη δέουσα επιμέλεια σχετικά με τρίτα μέρη και προμηθευτές Περιγραφή Μέτρου: Επίδειξη δέουσας επιμέλειας κατά τον εντοπισμό και τη σύναψη συμβατικών σχέσεων με τρίτα μέρη και προμηθευτές, λαμβανομένων υπόψη των κινδύνων τρίτων μερών, μεταξύ άλλων, της εξάρτησης από τον εκάστοτε προμηθευτή, της διαχείρισης περιστατικών και της ευθύνης σε σχέση με την ασφάλεια δικτύων και πληροφοριών. Ο οργανισμός επιδεικνύει τη δέουσα επιμέλεια ως προς την ασφάλεια πληροφοριών όταν αναλαμβάνει τη συνεργασία με τρίτα μέρη ιδίως στο πλαίσιο της απόκτησης ή της παράδοσης λογισμικού. Πηγή: C2M2, ISO 27002
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν λαμβάνει υπόψη του κατά τον εντοπισμό και τη σύναψη συμβατικών σχέσεων με τρίτα μέρη και προμηθευτές θέματα που επηρεάζουν την ασφάλεια πληροφοριών όπως κινδύνους που μπορεί να παρουσιαστούν από τα τρίτα μέρη, κατά πόσο εξαρτάται ο οργανισμός από τον εκάστοτε προμηθευτή και τον τρόπο διαχείρισης των περιστατικών ασφαλείας και της ευθύνης που έχουν οι προμηθευτές και τα τρίτα μέρη.
1	1	Για την επιλογή των προμηθευτών και των τρίτων μερών ο οργανισμός λαμβάνει υπόψη του την ικανότητα και την επάρκεια τους σε σχέση με την ασφάλεια πληροφοριών, τουλάχιστον με ad hoc τρόπο.
2	1	Εντοπίζονται βασικές εξαρτήσεις και βασικοί κίνδυνοι που προκύπτουν από προμηθευτές και τρίτα μέρη, τουλάχιστον με ad hoc τρόπο και όχι κατ'ανάγκη συστηματικά.
2	2	Αναγνωρίζονται, τουλάχιστον ad hoc και όχι κατ'ανάγκη συστηματικά, τρίτα μέρη ή/και προμηθευτές που έχουν πρόσβαση, έλεγχο ή φύλαξη σε συστήματα ή πληροφορίες που είναι σημαντικά για τον οργανισμό και για την εκτέλεση των εργασιών τους. Η αναγνώριση δύναται να μην αποτυπώνονται σε συμβάσεις.
3	1	Ακολουθείται μια καθορισμένη μέθοδος (διαδικασία) για εντοπισμό κινδύνων που προκύπτουν από προμηθευτές και τρίτα μέρη.
3	2	Ακολουθείται μια καθορισμένη μέθοδος (διαδικασία) για τον εντοπισμό απαιτήσεων σε σχέση με την ασφάλεια πληροφοριών και την εφαρμογή σχετικών μέτρων που προστατεύουν από τους κινδύνους που προκύπτουν από προμηθευτές και τρίτα μέρη.
3	3	Καθορίζεται ο τρόπος πρόσβασης στις πληροφορίες, που επιτρέπεται σε διαφορετικούς τύπους προμηθευτών και τρίτα μέρη, η παρακολούθηση και ο έλεγχος της πρόσβασής τους.
4	1	Οι προμηθευτές και τα τρίτα μέρη βεβαιώνουν περιοδικά την ικανότητά τους να πληρούν τις απαιτήσεις ασφάλειας πληροφοριών που έχουν συμφωνηθεί με τον οργανισμό.
4	2	Όλες οι πολιτικές και διαδικασίες ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Οι απαιτήσεις ασφάλειας για προμηθευτές και τρίτα μέρη περιλαμβάνουν ασφαλές λογισμικό και ασφαλείς απαιτήσεις ανάπτυξης προϊόντων, όπου αυτό είναι εφικτό.
5	2	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	3	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
TPS2		Μέτρο: Σχέσεις με τρίτα μέρη και προμηθευτές Στόχος Μέτρου: Να διασφαλιστεί η ενσωμάτωση συμβατικών ρητρών ασφάλειας πληροφοριών στις σχέσεις με τρίτα μέρη και προμηθευτές. Περιγραφή Μέτρου: Διατήρηση κεντρικού αποθετηρίου προμηθευτών, πωλητών και άλλων τρίτων μερών. Ο οργανισμός θα πρέπει να διασφαλίζει ότι όλες οι σχέσεις με τρίτα μέρη υποστηρίζονται από κατάλληλες συμβατικές ρήτρες, προκειμένου να διασφαλίζεται ότι, μεταξύ άλλων, οι ρόλοι, οι αρμοδιότητες και η ευθύνη σε περίπτωση συμβάντων όσον αφορά την ασφάλεια δικτύων και πληροφοριών είναι δεόντως καταγραμμένα. Πηγή: C2M2, ISO 27002
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν έχει συνάψει συμβάσεις με προμηθευτές ή τρίτα μέρη (προμηθευτές ή τρίτα μέρη που μπορεί να επηρεάσουν την ασφάλεια πληροφοριών).
1	1	Έχουν συναφθεί συμβάσεις με προμηθευτές και τρίτα μέρη.

2	1	Έχουν συναφθεί συμβάσεις με προμηθευτές και τρίτα μέρη στις οποίες περιλαμβάνονται κάποιες απαιτήσεις ασφαλείας, οι οποίες είναι κατ'ελάχιστο ad hoc και όχι κατ'ανάγκη συστηματικά για το σύνολο των προμηθευτών που εμπλέκονται σε θέματα σχετικά με την ασφάλεια πληροφοριών.
3	1	Έχει δημιουργηθεί σχετική λίστα που περιλαμβάνει τους προμηθευτές και τα τρίτα μέρη.
3	2	Έχουν προτεραιοποιηθεί οι προμηθευτές και τα τρίτα μέρη σύμφωνα με προκαθορισμένα κριτήρια που έχουν αποφασιστεί και εγκριθεί.
3	3	Ακολουθείται μια καθορισμένη μέθοδος (διαδικασία) για την αξιολόγηση των προμηθευτών και άλλων τρίτων μερών.
3	4	Εφαρμόζονται πιο αυστηροί έλεγχοι σε σχέση με την ασφάλεια πληροφοριών για προμηθευτές και τρίτα μέρη υψηλότερης προτεραιότητας.
3	5	Περιλαμβάνονται στις συμβάσεις με τους προμηθευτές και τα τρίτα μέρη νομικές και κανονιστικές απαιτήσεις, συμπεριλαμβανομένης της προστασίας δεδομένων, των δικαιωμάτων πνευματικής ιδιοκτησίας και των πνευματικών δικαιωμάτων, και περιγραφή του τρόπου με τον οποίο θα διασφαλίζουν ότι πληρούνται.
3	6	Περιλαμβάνονται στις συμβάσεις με προμηθευτές και τρίτα μέρη απαιτήσεις και διαδικασίες διαχείρισης συμβάντων (ειδικά ειδοποίηση και συνεργασία κατά την αποκατάσταση περιστατικών)
3	7	Έχει δημιουργηθεί πολιτική ασφάλειας η οποία και κοινοποιείται στους προμηθευτές και τα τρίτα μέρη.
4	1	Η προτεραιοποίηση των προμηθευτών και άλλων τρίτων μερών ανασκοπείται περιοδικά και σύμφωνα με καθορισμένους παράγοντες ενεργοποίησης, όπως αλλαγές συστήματος και εξωτερικά συμβάντα. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
4	2	Πραγματοποιούνται σε ετήσια βάση επιτόπιες επιθεωρήσεις σε σχέση με την ασφάλεια πληροφοριών για προμηθευτές ή τρίτα μέρη υψηλότερης προτεραιότητας.
4	3	Όλες οι πολιτικές και διαδικασίες ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
4	4	Περιλαμβάνεται στις συμβάσεις με προμηθευτές και τρίτα μέρη ταξινόμηση των πληροφοριών σύμφωνα με το σχήμα ταξινόμησης του οργανισμού όπως επίσης και χαρτογράφηση (mapping) μεταξύ του συστήματος ταξινόμησης του ίδιου του οργανισμού και του σχήματος ταξινόμησης του προμηθευτή.
5	1	Γίνεται ανάθεση σε ανεξάρτητο τρίτο μέρος η διεξαγωγή επιθεώρησης σε σχέση με την ασφάλεια πληροφοριών για προμηθευτές ή τρίτα μέρη υψηλότερης προτεραιότητας.
5	2	Οι προμηθευτές και τα τρίτα μέρη συμμορφώνονται πλήρως με τι απαιτήσεις ασφάλειας του οργανισμού.
5	3	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	4	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.

Κατηγορία		ΑΣΦΑΛΕΙΑ ΔΕΔΟΜΕΝΩΝ
DS1		Μέτρο: Διαχείριση του κύκλου ζωής των πληροφοριών Στόχος Μέτρου: Να εξασφαλιστεί η προστασία δεδομένων καθ' όλο τον κύκλο ζωής των πληροφοριών, συμπεριλαμβανομένης της συλλογής, καταχώρησης, οργάνωσης, δομής, αποθήκευσης, προσαρμογής ή μεταβολής, ανάκτησης, αναζήτησης, χρήσης, κοινοποίησης με διαβίβαση, διάδοσης ή κάθε άλλη μορφή διάθεσης, συσχέτισης ή συνδυασμού, περιορισμού, διαγραφής ή καταστροφής. Περιγραφή Μέτρου: Θέσπιση, εφαρμογή και διατήρηση μέτρων ασφάλειας πληροφοριών για την προστασία πληροφοριών καθ' όλη τη διάρκεια του κύκλου ζωής των πληροφοριών. Κύκλος ζωής των πληροφοριών θεωρούνται ως όλα τα στάδια που σχετίζονται με την επεξεργασία των πληροφοριών, ενώ η επεξεργασία αφορά κάθε πράξη, ή σειρά πράξεων, που πραγματοποιείται σε δεδομένα προσωπικού χαρακτήρα, ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, είτε με αυτοματοποιημένα μέσα είτε όχι, όπως η συλλογή, καταχώριση, οργάνωση, δομή, αποθήκευση, προσαρμογή ή μεταβολή, ανάκτηση, αναζήτηση, χρήση, κοινοποίηση με διαβίβαση, διάδοση ή κάθε άλλη μορφή διάθεσης, συσχέτιση ή συνδυασμός, περιορισμός, διαγραφή ή καταστροφή. Πηγή: ENISA (PII MEASURES), CNIL
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν έχει κάποια διαδικασία ή άλλο μέσο για την αναγνώριση και εφαρμογή μέτρων για την προστασίας δεδομένων καθ' όλο τον κύκλο ζωής των πληροφοριών τους.
1	1	Εφαρμόζονται κάποια μέτρα για την προστασία των πληροφοριών.
2	1	Έχει δημιουργηθεί διαδικασία για την διαχείριση του συνολικού κύκλου ζωής των πληροφοριών του οργανισμού (προσωπικά και μη προσωπικά δεδομένα).
2	2	Η διαδικασία περιλαμβάνει μια μεθοδολογία / προσέγγιση ή τρόπο για την αναγνώριση των πληροφοριών που επεξεργάζονται από τον οργανισμό στα πλαίσια των λειτουργιών του.
2	3	Οι πληροφορίες (τουλάχιστον σε επίπεδο κατηγοριών π.χ. λειτουργικές διαδικασίες, χρηματοοικονομικά δεδομένα, απλά προσωπικά δεδομένα προσωπικού κ.α.) καταγράφονται σε έναν κατάλογο (ο κατάλογος μπορεί να είναι ο ίδιος ή να συσχετίζεται ή να παράγεται από τον κατάλογο στοιχείων ενεργητικού, συστημάτων και διαδικασιών εντός του οργανισμού όπως αναφέρεται στο [RM2].
2	4	Υπάρχει ένας αναγνωρισμένος ιδιοκτήτης του καταλόγου, ο οποίος είναι υπεύθυνος για την τήρηση και επικαιροποίηση των σχετικών δεδομένων.
3	1	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται μέτρα ασφάλειας πληροφοριών για την προστασία πληροφοριών καθ' όλη τη διάρκεια του κύκλου ζωής των πληροφοριών. (Κύκλος ζωής των πληροφοριών θεωρείται ως όλα τα στάδια που σχετίζονται με την επεξεργασία των πληροφοριών, ενώ η επεξεργασία αφορά κάθε πράξη, ή σειρά πράξεων, που πραγματοποιείται σε δεδομένα προσωπικού χαρακτήρα, ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, είτε με αυτοματοποιημένα μέσα είτε όχι, όπως η συλλογή, καταχώριση, οργάνωση, δομή, αποθήκευση, προσαρμογή ή μεταβολή, ανάκτηση, αναζήτηση, χρήση, κοινοποίηση με διαβίβαση, διάδοση ή κάθε άλλη μορφή διάθεσης, συσχέτιση ή συνδυασμός, περιορισμός, διαγραφή ή καταστροφή.)
3	2	Ο χειρισμός των πληροφοριών γίνεται σύμφωνα σχετικές γραπτές οδηγίες οι οποίες αναφέρουν οδηγίες και περιορισμούς σε σχέση με τον τρόπο χειρισμού των πληροφοριών καθ' όλο τον κύκλο ζωής (από την δημιουργία / συλλογή μέχρι και την καταστροφή).
3	3	Κατ' ελάχιστο τα μέτρα για την καταστροφή πληροφοριών περιλαμβάνουν 1) multiple passes of software-based overwriting για τα επαναχρησιμοποιούμενα μέσα αποθήκευσης ή φυσική καταστροφή για τα υπόλοιπα, 2) cross cut shredding χαρτιών και 3) προβλέψεις σε συμβάσεις με τρίτα μέρη αντίστοιχων μέτρων όπου απαιτούνται.
3	4	Για τα δεδομένα που βρίσκονται σε μεταφορά ή ανταλλάσσονται τα μέτρα πρέπει να συμφωνούν αντίστοιχα με το [DS4].
3	5	Για τα κρίσιμα ή ευαίσθητα δεδομένα που βρίσκονται σε ηρεμία (data at rest), εφαρμόζεται κρυπτογραφία σε συμφωνία με την σχετική πολιτική του [AM5].
3	6	Ο οργανισμός έχει ορίσει μια περίοδο διατήρησης των δεδομένων για όλες τις κατηγορίες δεδομένων και εφαρμόζει τις σχετικές προβλέψεις.
4	1	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
4	2	Για τα δεδομένα προσωπικού χαρακτήρα εφαρμόζονται κατάλληλα μέτρα κατά την μετάδοση (in transit) αλλά και όσο είναι σε ηρεμία.

4	3	Σε περίπτωση που δεν είναι δυνατή η εφαρμογή κρυπτογράφησης, αναγνωρίζεται ως κίνδυνος και γίνεται σχεδιασμός και υλοποίηση άλλων μέτρων για την εξασφάλιση του επιθυμητού επίπεδου ασφαλείας.
4	4	Έχουν σχεδιαστεί κατάλληλες διαδικασίες, πολιτικές για την συμμόρφωση προς τις νομικές και κανονιστικές απαιτήσεις σε σχέση με την προστασία δεδομένων προσωπικού χαρακτήρα.
4	5	Η διαχείριση κινδύνου έχει προσαρμοστεί ώστε να περιλαμβάνει την αναγνώριση, αποτίμηση και αξιολόγηση κινδύνων διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων από την επεξεργασία των δεδομένων τους από τον οργανισμό.
4	6	Υλοποιούνται κατάλληλα τεχνικά και οργανωτικά μέτρα σύμφωνα με τα αποτελέσματα της αξιολόγησης κινδύνων. Ειδικά για την διαγραφή των δεδομένων έχει καταγραφεί μια διαδικασία για την ασφαλή διαγραφή δεδομένων η οποία περιέχει ρόλους, αρμοδιότητες, μεθοδολογίες, κριτήρια και εργαλεία χρησιμοποιούνται για την διαγραφή των δεδομένων κάθε επιπέδου διαβάθμισης σύμφωνα με το [DS2].
4	7	Η διαδικασία προβλέπει επίσης τα μέτρα που εφαρμόζονται όταν μεταφέρονται στοιχεία (πόροι) σε εξωτερικά μέση (π.χ. λόγω λήξης συμβολαίου ενοικίασης, για λόγους επισκευής κλπ.).
4	8	Σε περίπτωση χρησιμοποιείται τρίτο μέρος για την διαγραφή ή καταστροφή, υπάρχουν σχετικές προβλέψεις και όροι που εξασφαλίζουν την ορθή και αποτελεσματική εφαρμογή των σχετικών κανόνων στο σχετικό συμβόλαιο.
4	9	Σε περίπτωση που τα δεδομένα αποθηκεύονται σε τρίτα μέρη (π.χ. Cloud services) δίνονται συγκεκριμένες δεσμεύσεις και αποδείξεις από την μεριά του τρίτου μέρους για την υλοποίηση των συγκεκριμένων ρυθμίσεων. Σε διαφορετική περίπτωση λαμβάνονται άλλα αντισταθμιστικά μέτρα.
4	10	Εφαρμόζονται αυτόματα ή ημιαυτόματα μέσα για την εφαρμογή της περιόδου διατήρησης των δεδομένων.
5	1	Έχει εφαρμοστεί αυτόματο σύστημα για την προστασία των πληροφοριών από διαρροές (DLP).
5	2	Έχουν γίνει οι κατάλληλες ρυθμίσεις σε συμφωνία με το σχήμα διαβάθμισης πληροφοριών και τις οδηγίες για τον χειρισμό των πληροφοριών [DS2].
5	3	Κάθε νέο μέσο ή στοιχείο, κρυπτογραφείται με αυτοματοποιημένο τρόπο όπου αυτό είναι δυνατό, πριν ή κατά την εισαγωγή του στον οργανισμό.
5	4	Για την διαγραφή δεδομένων, σε περίπτωση που αυτή υλοποιείται μέσω λογισμικού, χρησιμοποιούνται επιπλέον μέτρα σε φυσικό επίπεδο (π.χ. degaussing).
5	5	Σε περίπτωση που χρησιμοποιείται τρίτο μέρος για την διαγραφή ή καταστροφή, η ενέργεια αυτή γίνεται στο χώρο του οργανισμού για να αποφευχθούν κίνδυνοι που σχετίζονται με την μεταφορά των δεδομένων. Αν αυτό δεν είναι εφικτό, εφαρμόζονται συγκεκριμένα μέτρα για την αποφυγή του σχετικού κινδύνου (π.χ. κλειδωμένα containers, live feed, παρουσία προσωπικού κλπ.).
5	6	Εφαρμόζονται αυτόματα μέτρα για την εφαρμογή της περιόδου διατήρησης των δεδομένων.
5	7	Στα πλαίσια των ελέγχων που αναφέρονται στο [GOV2] περιλαμβάνονται και έλεγχοι για την τήρηση του διαστήματος διατήρησης των πληροφοριών.
5	8	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	9	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
DS2		Μέτρο: Ταξινόμηση και επισήμανση πληροφοριών Στόχος Μέτρου: Να εξασφαλιστεί ότι τα δεδομένα ταξινομούνται και επισημαίνονται κατά τρόπο ώστε να αντικατοπτρίζεται η ευαισθησία τους ώστε να εξασφαλίζεται η κατάλληλη επεξεργασία τους Περιγραφή Μέτρου: Θέσπιση, εφαρμογή και διατήρηση μιας πολιτικής ταξινόμησης και επισήμανσης που διασφαλίζει την ταξινόμηση και επισήμανση των πληροφοριών, σύμφωνα με την εμπιστευτικότητα και την ευαισθησία τους. Εξέταση ενδεχομένου εφαρμογής συστημάτων ταξινόμησης και επισήμανσης με βάση τις διεθνείς και βιομηχανικές βέλτιστες πρακτικές, όπως το πρωτόκολλο «Traffic Light Protocol». Τουλάχιστον, ο οργανισμός θα πρέπει να γίνεται διάκριση μεταξύ των δημόσιων, ιδιωτικών και διαβαθμισμένων πληροφοριών. Πηγή: CIS (1.3 Data protection), ENISA (SO 23 – Security of data at rest), NIST 800-53 (MP-3)
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου

0	1	Ο οργανισμός δεν έχει κάποια διαδικασία ή άλλο μέσο για την ταξινόμηση και επισήμανση των πληροφοριών τους.
1	1	Αναγνωρίζονται κάποια δεδομένα ως πιο κρίσιμα ή ευαίσθητα τα οποία καταγράφονται τουλάχιστον με ad-hoc τρόπο.
2	1	Έχουν αναγνωριστεί τουλάχιστον 2 κατηγορίες πληροφοριών (εσωτερικές και δημόσιες) και υπάρχει σήμανση τουλάχιστον σε μια από τις δυο κατηγορίες.
2	2	Ο χειρισμός των πληροφοριών γίνεται σύμφωνα με σχετικές γραπτές οδηγίες οι οποίες αναφέρουν οδηγίες και περιορισμούς σε σχέση με τον τρόπο χειρισμού των πληροφοριών καθ' όλο τον κύκλο ζωής (από την δημιουργία / συλλογή μέχρι και την καταστροφή).
3	1	Έχει θεσπιστεί, εφαρμόζεται και διατηρείται πολιτική ταξινόμησης και επισήμανσης που διασφαλίζει την ταξινόμηση και επισήμανση των πληροφοριών, σύμφωνα με την εμπιστευτικότητα και την ευαισθησία τους.
3	2	Η πολιτική επιβάλει κατ΄ ελάχιστο την διάκριση όσον αφορά τις πληροφορίες: Δημόσια, Ιδιωτική και Διαβαθμισμένη.
3	3	Ο χειρισμός των πληροφοριών γίνεται σύμφωνα με σχετικές γραπτές οδηγίες οι οποίες αναφέρουν οδηγίες και περιορισμούς σε σχέση με τον τρόπο χειρισμού των πληροφοριών καθ' όλο τον κύκλο ζωής όπως αναφέρεται στο [DS1].
4	1	Έχει δημιουργηθεί διαδικασία σχετικά με την ταξινόμηση και την επισήμανση των πληροφοριών στην οποία αποτυπώνεται ο τρόπος με τον οποίο γίνεται η διαβάθμιση και η επισήμανση της πληροφορίας.
4	2	Χρησιμοποιείται αυτοματοποιημένος τρόπος (π.χ. λογισμικό) για την επισήμανση και διαχείριση των πληροφοριών σύμφωνα με το σχήμα που έχει εφαρμοστεί.
4	3	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Η διαδικασία ταξινόμησης και επισήμανσης, προβλέπει ότι με την είσοδο ενός εγγράφου / πληροφορίας στον οργανισμό, αναγνωρίζεται ο ιδιοκτήτης και κατατάσσεται και επισημαίνεται σύμφωνα με τα αναγνωρισμένα κριτήρια με την χρήση κατάλληλων εργαλείων. Το ίδιο ισχύει και για πληροφορίες οι οποίες δημιουργούνται από τον οργανισμό, οι οποίες και αυτές κατατάσσονται και επισημαίνονται την στιγμή της δημιουργίας.
5	2	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	3	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
5	4	Διενεργούνται έλεγχοι για την συμμόρφωση προς τις απαιτήσεις ταξινόμησης και επισήμανσης.
DS3		Μέτρο: Εφεδρικά αντίγραφα και ανάκτηση δεδομένων Στόχος Μέτρου: Να καταστεί δυνατή η αποκατάσταση των πληροφοριών στο πλαίσιο συμβάντων και περιστατικών ασφάλειας. Περιγραφή Μέτρου: Θέσπιση, εφαρμογή και διατήρηση διαδικασίας εφεδρικών αντιγράφων και ανάκτησης δεδομένων, προκειμένου να διασφαλίζεται η έγκαιρη και αποτελεσματική αποκατάσταση δεδομένων μετά την ύπαρξη ενός συμβάντος ή περιστατικού, ή κατόπιν αιτήματος. Οι διαδικασίες εφεδρικών αντιγράφων και ανάκτησης δεδομένων θα πρέπει να δοκιμάζονται επαρκώς και συχνά, προκειμένου να διασφαλίζεται η ορθή και αξιόπιστη λειτουργία όλων των υποστηρικτικών διαδικασιών και συστημάτων. Τα συστήματα και οι υποδομές υποστήριξης, που επιτρέπουν την εφεδρεία και την αποκατάσταση δεδομένων, θα πρέπει να είναι γεωγραφικά διεσπαρμένες (αποθήκευση σε άλλη τοποθεσία) προκειμένου να προστατεύονται από φυσικούς κινδύνους ασφάλειας. Πηγή:
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν λαμβάνει αντίγραφα ασφαλείας με οποιαδήποτε μορφή.
1	1	Λαμβάνονται για κάποιες πληροφορίες αντίγραφα ασφαλείας κατ'ελάχιστο ad-hoc και όχι κατ'ανάγκη με συγκεκριμένο / καταγεγραμμένο τρόπο.
2	1	Τηρούνται αντίγραφα ασφαλείας που καλύπτουν το σύνολο του κατάλογου στοιχείων ενεργητικού, συστημάτων και διαδικασιών εντός του οργανισμού.
2	2	Υπάρχει ένας αναγνωρισμένος υπεύθυνος για την λειτουργία και τήρηση των αντιγράφων ασφαλείας.
3	1	Έχει θεσπιστεί, εφαρμόζεται και διατηρείται διαδικασία εφεδρικών αντιγράφων και ανάκτησης δεδομένων, προκειμένου να διασφαλίζεται η έγκαιρη και αποτελεσματική αποκατάσταση δεδομένων μετά την ύπαρξη ενός συμβάντος ή περιστατικού, ή κατόπιν αιτήματος.

3	2	Οι διαδικασίες εφεδρικών αντιγράφων και ανάκτησης δεδομένων δοκιμάζονται επαρκώς και συχνά, προκειμένου να διασφαλίζεται η ορθή και αξιόπιστη λειτουργία όλων των υποστηρικτικών διαδικασιών και συστημάτων.
3	3	Τα συστήματα και οι υποδομές υποστήριξης, που επιτρέπουν την εφεδρεία και την αποκατάσταση δεδομένων, είναι γεωγραφικά διεσπαρμένες (αποθήκευση σε άλλη τοποθεσία) προκειμένου να προστατεύονται από φυσικούς κινδύνους ασφάλειας.
3	4	Τα αντίγραφα ασφαλείας λαμβάνουν το σύνολο της πληροφορίας ή τις αλλαγές της σε ημερήσια βάση τουλάχιστον.
4	1	Η υλοποίηση της διαδικασίας εφεδρικών αντιγράφων και ανάκτησης δεδομένων υποστηρίζεται από κατάλληλο αδειοδοτημένο (όπου απαιτείται) λογισμικό.
4	2	Τα αρχεία εφεδρικών αντιγράφων κρυπτογραφούνται με την χρήση αλγορίθμων όπως προβλέπεται από το [AM1].
4	3	Έχει προβλεφθεί ώστε να υπάρχει δυνατότητα πρόσβασης και ανάκτησης των δεδομένων όπως απαιτείται από τα εφεδρικά αντίγραφα (π.χ. υπάρχει δυνατότητα λήψης, εγκατάστασης ή χρήσης του λογισμικού αντιγράφων ασφαλείας και υπάρχει διαθεσιμότητα των σχετικών κλειδιών).
4	4	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
4	5	Η συχνότητα λήψης αντιγράφων ασφαλείας τουλάχιστον για τα κρίσιμα συστήματα είναι ανά 8 ώρες.
4	6	Έχει δημιουργηθεί ένα σχήμα διατήρησης εφεδρικών αντιγράφων σε επίπεδο ημέρας / εβδομάδας / μήνα και έτους.
5	1	Έχουν εφαρμοστεί λύσεις συγχρονισμού (replication) σε εναλλακτικό χώρο για τα κρίσιμα συστήματα όπως αυτά έχουν αναγνωριστεί σύμφωνα με την ανάλυση επιχειρησιακών επιπτώσεων και τα σχετικά σχέδια επιχειρησιακής συνέχειας και ανάκαμψης από καταστροφή.
5	2	Μια φορά το χρόνο τουλάχιστον γίνεται πλήρης λειτουργική δοκιμή της κατάστασης συγχρονισμού και της δυνατότητας λειτουργίας του οργανισμού από την εναλλακτική τοποθεσία.
5	3	Τηρούνται χωριστά εφεδρικά αντίγραφα και σε τρίτη ασφαλή τοποθεσία, για να μπορεί να προστατευτεί ο οργανισμός και από επιθέσεις κυβερνοεκβιασμού.
5	4	Η συχνότητα λήψης των συγκεκριμένων αντιγράφων είναι κατάλληλη σύμφωνα με το πλαίσιο λειτουργίας, τους στόχους και την στρατηγική του οργανισμού.
5	5	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	6	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
DS4		Μέτρο: Μεταφορές και ανταλλαγή πληροφοριών Στόχος Μέτρου: Να εφαρμοστούν επαρκή μέτρα στο πλαίσιο της διαβίβασης και ανταλλαγής πληροφοριών εσωτερικά ή με τρίτα μέρη, προκειμένου να διασφαλιστεί η ασφαλής μεταφορά δεδομένων. Περιγραφή Μέτρου: Θέσπιση, εφαρμογή και διατήρηση διαδικασιών μεταφοράς και ανταλλαγής πληροφοριών προκειμένου να διασφαλίζεται η προστασία των πληροφοριών κατά τη μεταφορά ή την ανταλλαγή τους εσωτερικά ή με τρίτα μέρη. Η μεταφορά και ανταλλαγή πληροφοριών θα πρέπει να λαμβάνει υπόψη τις κανονιστικές και νομοθετικές απαιτήσεις, όπως ορίζονται στο [GOV2], για παράδειγμα κατά την επεξεργασία πληροφοριών στο πλαίσιο διεθνών διαβιβάσεων δεδομένων. Πηγή: C2M2 (Architecture), ISO 27001, OWASP API, OWASP ASVS
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν έχει κάποια διαδικασία ή άλλο μέσο για την αναγνώριση και εφαρμογή μέτρων για την προστασία δεδομένων κατά την μεταφορά ή ανταλλαγή τους.
1	1	Έχουν τεθεί σε συγκεκριμένα σημεία κάποια μέτρα για την προστασία των δεδομένων κατά την ανταλλαγή ή μεταφορά τους.
2	1	Έχουν αναγνωριστεί τουλάχιστον 2 κατηγορίες πληροφοριών (εσωτερικές και δημόσιες) και υπάρχει σήμανση τουλάχιστον σε μια από τις δυο κατηγορίες.
2	2	Έχουν αναγνωρισθεί όλοι οι τρόποι με τους οποίους μπορεί να γίνει ανταλλαγή των εσωτερικών πληροφοριών και έχουν καταγραφεί σε σχετικές γραπτές οδηγίες.
2	3	Σε περίπτωση που δίνεται πρόσβαση στις πληροφορίες αυτές σε τρίτα μέρη, χρησιμοποιούνται ενότητες μόνο που μπορούν να παρέχουν κατάλληλες διαβεβαιώσεις και εγγυήσεις για την προστασία των δεδομένων σε όλο τον κύκλο ζωής τους.

2	4	Οι γραπτές οδηγίες χειρισμού επικοινωνούνται στο τρίτο μέρος ώστε να συμμορφωθεί.
2	5	Σε περίπτωση αδυναμίας συμμόρφωσης, ο οργανισμός αναγνωρίζει τον σχετικό κίνδυνο και εισάγει κατάλληλα αντισταθμιστικά μέτρα.
3	1	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται διαδικασίες μεταφοράς και ανταλλαγής πληροφοριών προκειμένου να διασφαλίζεται η προστασία των πληροφοριών κατά τη μεταφορά ή την ανταλλαγή τους εσωτερικά ή με τρίτα μέρη.
3	2	Η μεταφορά και ανταλλαγή πληροφοριών λαμβάνει υπόψη τις κανονιστικές και νομοθετικές απαιτήσεις, όπως ορίζονται στο [GOV2], για παράδειγμα κατά την επεξεργασία πληροφοριών στο πλαίσιο διεθνών διαβιβάσεων δεδομένων.
3	3	Ειδικά για τα κρίσιμα ή ευαίσθητα δεδομένα, υλοποιείται κρυπτογράφηση κατά την ανταλλαγή ή μεταφορά. Παραδείγματα τέτοιας υλοποίησης περιλαμβάνει (Transport Layer Security (TLS) and Open Secure Shell (OpenSSH) κα.).
3	4	Τα δεδομένα που μεταφέρονται με φυσικά μέσα, πρώτα κρυπτογραφούνται κατάλληλα και μετά αποστέλλονται.
3	5	Τα κλειδιά κρυπτογράφησης μεταφέρονται χωριστά, με άλλο μέσο (ή τρόπο) χωρίς επισήμανση της χρήσης τους.
3	6	Για σύγχρονη μεταφορά χρησιμοποιούνται πρωτόκολλα όπως είναι οι πιο πρόσφατες σταθερές εκδόσεις πρωτοκόλλων όπως είναι το SFTP ή HTTPS.
4	1	Εφαρμόζονται μηχανισμοίγια την εξασφάλιση της ακεραιότητας και αυθεντικότητας της πληροφορίας που ανταλλάσσεται.
4	2	Οι σχετικές πληροφορίες ανταλλάσσονται χρησιμοποιώντας ψηφιακές υπογραφές.
4	3	Τηρείται μητρώο με τις πληροφορίες που ανταλλάσσονται (κρίσιμες ή ευαίσθητες), καταγράφονται τα μέτρα που εφαρμόστηκαν και οι σχετικές εγγυήσεις από τα σχετικά μέρη.
4	4	Όταν χρησιμοποιούνται προσωρινές τοποθεσίες αποθήκευσης, αυτές ελέγχονται στον προδιαγεγραμμένο χρόνο και οι πληροφορίες διαγράφονται με ασφάλεια.
4	5	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
4	6	Ειδικά για τα ευαίσθητα προσωπικά δεδομένα, εφαρμόζονται μηχανισμοί data masking για την επιπλέον προστασία τους (όπου μπορεί να εφαρμοστεί).
4	7	Για την ανταλλαγή πληροφοριών μέσω APIs, γίνεται κατάλληλος σχεδιασμός, παραμετροποίηση, υλοποίηση και λειτουργίας ώστε να συμμορφώνεται με το επίπεδο ασφάλειας του οργανισμού.
4	8	Βέλτιστες διεθνείς πρακτικές (π.χ. API OWASP Top Ten) εφαρμόζονται.
4	9	Η εμπιστευτικότητα των δεδομένων εξασφαλίζεται είτε με κρυπτογράφηση σε επίπεδο καναλιού είτε με κρυπτογράφηση σε επίπεδο δεδομένων όταν γίνεται μεταφορά σε διαφορετικά δίκτυα ακόμα και εντός του ίδιου του οργανισμού.
5	1	Έχει εφαρμοστεί αυτόματο σύστημα για την προστασία των πληροφοριών από διαρροές (π.χ. Host Based Data Loss Prevention).
5	2	Έχουν γίνει οι κατάλληλες ρυθμίσεις σε συμφωνία με το σχήμα διαβάθμισης πληροφοριών και τις οδηγίες για τον χειρισμό των πληροφοριών [DS2].
5	3	Το σύστημα καλύπτει όλες τις πληροφορίες που επεξεργάζονται ή ανταλλάσσονται εντός του οργανισμού περιλαμβανομένων αυτών που βρίσκονται σε τρίτα μέρη.
5	4	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	5	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
5	6	Γίνονται τακτικοί έλεγχοι για την παρακολούθηση της εφαρμογής και συμμόρφωσης των διαδικασιών από το σχετικό προσωπικό.
5	7	Αντίστοιχοι έλεγχοι υλοποιούνται και σε τεχνικό επίπεδο (π.χ. Penetration tests) ή σε περίπτωση λογισμικού / APIs, security assessments στηριζόμενες σε διεθνείς βέλτιστες πρακτικές (π.χ. Application Security Verification Standard OWASP).
5	8	Σε περίπτωση αναγνώρισης κάποιας απόκλισης ενεργοποιείται άμεσα η διαδικασία ανταπόκρισης περιστατικών ασφαλείας. [EIM1]
DS5		Μέτρο: Πρόληψη απώλειας δεδομένων και διαρροής δεδομένων Στόχος Μέτρου: Να εξασφαλιστεί η προστασία των δεδομένων από εκούσια ή ακούσια απώλεια και διαρροή δεδομένων. Περιγραφή Μέτρου: Θέσπιση, εφαρμογή και διατήρηση εύλογων μέτρων για τη μείωση του κινδύνου απώλειας δεδομένων και διαρροής δεδομένων, λαμβάνοντας τα κατάλληλα τεχνικά και οργανωτικά μέτρα για πρόληψη. Τα μέτρα πρόληψης, απώλειας ή διαρροής

		δεδομένων θα πρέπει να λαμβάνουν υπόψη εξωτερικούς και εσωτερικούς φορείς απειλής που θα μπορούσαν δυνητικά να αποκαλύψουν διαβαθμισμένες ή ευαίσθητες πληροφορίες. Θα πρέπει να εφαρμόζονται επαρκή μέτρα ελέγχου πρόσβασης για διεπαφή με τα μέτρα πρόληψης για την απώλεια δεδομένων και διαρροή δεδομένων. Οι πολιτικές για την ανταλλαγή και κοινοποίηση δεδομένων θα πρέπει να είναι βάσει του ρόλου του χρήστη, όπως ορίζεται στο [IAM1]. Κατά τον καθορισμό των μέτρων πρόληψης για την απώλεια και τη διαρροή δεδομένων, ο οργανισμός θα πρέπει να εξετάζει την ταξινόμηση, την προστασία και την παρακολούθηση των πληροφοριών. Πηγή:
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν έχει κάποια διαδικασία ή μέτρα για την προστασία των δεδομένων από εκούσια ή ακούσια απώλεια και διαρροή δεδομένων.
1	1	Έχουν τεθεί σε συγκεκριμένα σημεία κάποια μέτρα για την προστασία των δεδομένων από εκούσια ή ακούσια απώλεια και διαρροή δεδομένων.
2	1	Έχει θεσπιστεί, εφαρμόζεται και διατηρείται μια πολιτική ελέγχου πρόσβασης για όλα τα δεδομένα στα πλαίσια του καταλόγου στοιχείων σύμφωνα με το [IAM1].
2	2	Για κάθε επίπεδο πληροφορίας σύμφωνα με το [DS2], έχουν επιλεγεί και μέτρα που αποσκοπούν στην προστασία έναντι διαρροών μέσω της χρήσης μεταφερόμενων αποθηκευτικών μέσων [DS1], μέσω της αποστολής πληροφοριών [DS4].
2	3	Μέτρα για την προστασία των δικτύων ακολουθούν τα αναγραφόμενα του [NS1].
3	1	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται εύλογα μέτρα για τη μείωση του κινδύνου απώλειας δεδομένων και διαρροής δεδομένων, λαμβάνοντας τα κατάλληλα τεχνικά και οργανωτικά μέτρα για πρόληψη.
3	2	Τα μέτρα πρόληψης, απώλειας ή διαρροής δεδομένων λαμβάνουν υπόψη εξωτερικούς και εσωτερικούς φορείς απειλής που μπορούν δυνητικά να αποκαλύψουν διαβαθμισμένες ή ευαίσθητες πληροφορίες.
3	3	Εφαρμόζονται επαρκή μέτρα ελέγχου πρόσβασης για διεπαφή με τα μέτρα πρόληψης για την απώλεια δεδομένων και διαρροή δεδομένων.
3	4	Οι πολιτικές για την ανταλλαγή και κοινοποίηση δεδομένων είναι βάσει του ρόλου του χρήστη, όπως ορίζεται στο [IAM1].
3	5	Κατά τον καθορισμό των μέτρων πρόληψης για την απώλεια και τη διαρροή δεδομένων, ο οργανισμός εξετάζει την ταξινόμηση, την προστασία και την παρακολούθηση των πληροφοριών.
3	6	Διενεργείται εκπαίδευση στο προσωπικό σχετικά με τους τρόπους επίθεσης (π.χ. phishing) οι οποίοι μπορεί να οδηγήσουν σε απώλεια δεδομένων.
4	1	Η πρόσβαση σε γνωστά μέσα για την μεταφορά δεδομένων και σε μη εταιρικά συστήματα ανταλλαγής μηνυμάτων απαγορεύεται.
4	2	Η μεταφορά δεδομένων σε USB απαγορεύεται. Σε περίπτωση που δεν μπορεί να απαγορευτεί καθολικά, οι εξαιρέσεις διαχειρίζονται με κατάλληλα οργανωτικά και τεχνικά μέτρα ώστε να εξασφαλίζεται ότι υπάρχει έλεγχος του είδους της πληροφορίας που μεταφέρεται, της αιτιολόγησης της μεταφοράς, της εξουσιοδότησης της μεταφοράς και της εφαρμογής κατάλληλων κρυπτογραφικών μέτρων προστασίας.
4	3	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Εφαρμόζεται αυτόματο σύστημα για την προστασίας των πληροφοριών από διαρροές (π.χ. Host Based Data Loss Prevention).
5	2	Έχουν γίνει οι κατάλληλες ρυθμίσεις σε συμφωνία με το σχήμα διαβάθμισης πληροφοριών και τις οδηγίες για τον χειρισμό των πληροφοριών [DS2].
5	3	Το σύστημα καλύπτει όλες τις πληροφορίες που επεξεργάζονται ή ανταλλάσσονται εντός του οργανισμού περιλαμβανομένων αυτών που βρίσκονται σε τρίτα μέρη.
5	4	Οποιεσδήποτε ανωμαλίες αναγνωρίζονται επί των κανονικών traffic patterns καταγράφεται και αντιμετωπίζεται σύμφωνα με την διαδικασία διαχείρισης περιστατικών ασφαλείας [EIM1].
5	5	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	6	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.

Κατηγορία		ΔΙΑΧΕΙΡΙΣΗ ΑΛΛΑΓΩΝ
CM1		Μέτρο: Διαχείριση αλλαγών Στόχος Μέτρου: Να διασφαλιστεί ότι οι αλλαγές στις διαδικασίες και τα συστήματα πληροφοριών εφαρμόζονται με ασφάλεια, χωρίς να θίγεται το απόρρητο, η ακεραιότητα, η διαθεσιμότητα ή η αυθεντικότητα των πληροφοριών. Περιγραφή Μέτρου: Θέσπιση, εφαρμογή και διατήρηση διαδικασιών διαχείρισης αλλαγών για τον έλεγχο και τη διαχείριση αλλαγών σε συστήματα, εφαρμογές και άλλα υποστηρικτικά στοιχεία ενεργητικού στο πλαίσιο της επεξεργασίας πληροφοριών. Κατά τον καθορισμό της διαδικασίας διαχείρισης αλλαγών, ο οργανισμός πρέπει να προνοεί αιτήσεις αλλαγής, προκειμένου να λαμβάνονται υπόψη οι αλλαγές που ζητούνται από τους συμμετέχοντες. Η διαδικασία διαχείρισης αλλαγών θα πρέπει να επιτρέπει στον οργανισμό να αξιολογεί τους κινδύνους στο πλαίσιο αιτημάτων αλλαγών και να σχεδιάζει αλλαγές λαμβάνοντας υπόψη κατάλληλα μέτρα ασφάλειας. Η διαδικασία διαχείρισης αλλαγών θα πρέπει να περιλαμβάνει την προετοιμασία και την επαλήθευση των αλλαγών. Πηγή:
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν εφαρμόζει κάποια διαχείριση ή έλεγχο επί των αλλαγών.
1	1	Ο οργανισμός υλοποιεί κάποιο έλεγχο πάνω σε αριθμό αλλαγών που διενεργούνται σε κρίσιμα συστήματα.
1	2	Οι καταγραφές είναι τουλάχιστον περιστασιακές και η διαχείριση τους δύναται να γίνεται τουλάχιστον ad-hoc.
2	1	Υπάρχει μια διαδικασία για την διαχείριση των αλλαγών στα κρίσιμα συστήματα.
2	2	Η διαδικασία διαχείρισης αλλαγών είναι καταγεγραμμένη και έχει αναγνωρίσει συγκεκριμένους ρόλους που είναι υπεύθυνοι για την έγκριση των αλλαγών.
3	1	Έχει θεσπιστεί, εφαρμόζεται και διατηρείται διαδικασία διαχείρισης αλλαγών για τον έλεγχο και τη διαχείριση αλλαγών σε συστήματα, εφαρμογές και άλλα υποστηρικτικά στοιχεία ενεργητικού στο πλαίσιο της επεξεργασίας πληροφοριών.
3	2	Κατά τον καθορισμό της διαδικασίας διαχείρισης αλλαγών,προνοούνται αιτήσεις αλλαγής, προκειμένου να λαμβάνονται υπόψη οι αλλαγές που ζητούνται από τους συμμετέχοντες.
3	3	Η διαδικασία διαχείρισης αλλαγών επιτρέπει στον οργανισμό να αξιολογεί τους κινδύνους στο πλαίσιο αιτημάτων αλλαγών και να σχεδιάζει αλλαγές λαμβάνοντας υπόψη κατάλληλα μέτρα ασφάλειας.
3	4	Ειδικά για κρίσιμα συστήματα, σε κάθε περίπτωση διενέργειας αλλαγής, αυτή γίνεται αφού έχει υλοποιηθεί η εγκατάσταση σε δοκιμαστικό / παρόμοιο σύστημα χαμηλού κινδύνου.
3	5	Η διαδικασία διαχείρισης αλλαγών περιλαμβάνει την προετοιμασία και την επαλήθευση των αλλαγών.
3	6	Η διαδικασία διαχείρισης των αλλαγών υλοποιείται με τρόπο που να επιτρέπει την ιχνηλάτηση των αλλαγών.
3	7	Έχουν δημιουργηθεί κατηγορίες αλλαγών (λαμβάνοντας υπόψη τον σχετικό κίνδυνο) και έχει προδιαγραφεί ο τρόπος (βήματα και εγκρίσεις) που γίνεται η διαχείριση της κάθε κατηγορίας. (Συγκεκριμένα, οδηγία για την κατάταξη των αλλαγών σε κατηγορίες κρισιμότητας και προτεραιότητας, καθορίζονται οι ενέργειες αιτιολόγησης, ανάλυσης, δοκιμής, υπαναχώρησης και επιβεβαίωσης που γίνονται πριν να υλοποιηθεί η αλλαγή σε παραγωγικό σύστημα, καθορίζονται οι ρόλοι οι οποίοι εμπλέκονται στον σχεδιασμό, έλεγχο, υλοποίηση και έγκριση της αλλαγής και τα σχετικά αρχεία που τηρούνται).
3	8	Η διαδικασία διαχείρισης αλλαγών περιέχει επίσης προβλέψεις και τρόπο χειρισμού για επείγουσες αλλαγές.
3	9	Όλοι οι εμπλεκόμενοι ενημερώνονται σχετικά με τις λεπτομέρειες τις εκάστοτε αλλαγής.
3	10	Η διαδικασία διαχείρισης αλλαγών περιλαμβάνει σχέδιο roll-back για τις περιπτώσεις που οι αλλαγές είναι ανεπιτυχείς ή όταν έχει προκύψει κάποιο γεγονός που δεν επιτρέπει την επιτυχή ολοκλήρωση της αλλαγής.
3	11	Τα τρίτα μέρη ενημερώνονται για σημαντικές αλλαγές σε κρίσιμα συστήματα που επηρεάζουν τις προσφερόμενες υπηρεσίες.
4	1	Έχει δημιουργηθεί σχετική επιτροπή για τον έλεγχο και την έγκριση των αλλαγών, εξασφαλίζοντας ότι δεν υπάρχει σύγκρουση συμφερόντων ανάμεσα στα άτομα που αιτούνται την αλλαγή, υλοποιούν την αλλαγή και εγκρίνουν την αλλαγή.
4	2	Πραγματοποιούνται δοκιμές στην εφαρμογή της διαδικασίας διαχείρισης αλλαγών ώστε να βεβαιώνεται ότι οι αλλαγές κρίσιμων συστημάτων γίνονται πάντα με προκαθορισμένο τρόπο.
4	3	Δίνεται ιδιαίτερη βαρύτητα σε αλλαγές που προκύπτουν σε παραγωγικό περιβάλλον, και ειδικά κατά τη μεταφορά ενός συστήματος από την ανάπτυξη στο λειτουργικό περιβάλλον.

4	4	Γίνεται ανασκόπηση σε τακτική βάση οι αλλαγές που διενεργούνται στα συστήματα (με αφετηρία την αλλαγή στο σύστημα αλλά και με αφετηρία την τεκμηρίωση της αλλαγής) για τον έλεγχο της τήρησης της διαδικασίες διαχείρισης αλλαγών.
4	5	Η διαδικασία διαχείρισης αλλαγών λαμβάνει εισερχόμενα από το σύνολο των λειτουργιών του οργανισμού όπως αναφέρεται σε διάφορα controls του παρόντος πλαισίου.
4	6	Η διαδικασία διαχείρισης αλλαγών συνδέεται άμεσα με την διαδικασία διαχείρισης διαμόρφωσης όπως αναφέρεται στο [CM2].
5	1	Τηρείται αυτοματοποιημένο σύστημα για την διαχείριση των αλλαγών, το οποίο έχει την δυνατότητα να συνδέσει σε ποιο στοιχείο γίνεται η αλλαγή, να δημιουργήσει αιτήσεις αλλαγών, να δρομολογήσει τις αλλαγές ακολουθώντας προκαθορισμένο πρόγραμμα, να λαμβάνει σαν εισερχόμενο την ανάλυση κινδύνων για την αλλαγή (περιλαμβανομένων κινδύνων για την ασφάλεια), να την κατατάσσει σε κατηγορίες, να επιλέγει εγκριτική ροή με βάση την κατηγορία κινδύνου και την προτεραιότητα, να καταγράφει τις σχετικές εγκρίσεις, να περιέχει τις ενέργειες που έγιναν για την υλοποίηση, ενημέρωση, έλεγχο, δοκιμή της αλλαγής, να περιέχει το σχέδιο roll back και άλλες συναφείς πληροφορίες.
5	2	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	3	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
CM2		Μέτρο: Διαχείριση διαμόρφωσης (configuration) Στόχος Μέτρου: Να εντοπίζονται, να διατηρούνται και να επαληθεύονται οι πληροφορίες για τα στοιχεία ενεργητικού και τις διαμορφώσεις του οργανισμού. Περιγραφή Μέτρου: Θέσπιση, εφαρμογή και διατήρηση διαδικασιών διαχείρισης διαμόρφωσης για τον έλεγχο και τη διαχείριση των διαμορφώσεων των στοιχείων ενεργητικού που υποστηρίζουν δίκτυα και συστήματα πληροφοριών. Ο οργανισμός τηρεί μητρώο των διαμορφώσεων που ισχύουν για τα εν λόγω στοιχεία ενεργητικού. Οι οργανισμοί καθορίζουν και καταγράφουν τις σχέσεις ανάμεσα στις διαμορφώσεις των στοιχείων ενεργητικού με σκοπό τον προσδιορισμό των αλληλεξαρτήσεων και τη διασφάλιση της κατάλληλης διαχείρισης της αλλαγής όσον αφορά την τροποποίηση των διαμορφώσεων. Πηγή: PNNL, NIST 800-53, ENISA
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν διαχειρίζεται με κάποιο τρόπο την διαμόρφωση των στοιχείων του.
1	1	Γίνεται παραμετροποίηση κρίσιμων συστημάτων αλλά συνήθως πριν την υλοποίηση κύριων αλλαγών λαμβάνεται ένα αντίγραφο της διαμόρφωσης.
2	1	Έχει καταγραφεί μια διαδικασία για την διαχείριση των αλλαγών στα κρίσιμα συστήματα και έχουν αναγνωρισθεί συγκεκριμένοι ρόλοι που είναι υπεύθυνοι για την έγκριση των αλλαγών.
2	2	Στα πλαίσια της διαχείρισης αλλαγών καταγράφονται και αλλαγές που έχουν να κάνουν με την παραμετροποίηση κρίσιμων συστημάτων (π.χ. αλλαγή βασικών κανόνων του firewall κ.α.).
3	1	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται διαδικασίες διαχείρισης διαμόρφωσης για τον έλεγχο και τη διαχείριση των διαμορφώσεων των στοιχείων ενεργητικού που υποστηρίζουν δίκτυα και συστήματα πληροφοριών.
3	2	Οι σχέσεις ανάμεσα στις διαμορφώσεις των στοιχείων ενεργητικού με σκοπό τον προσδιορισμό των αλληλεξαρτήσεων και τη διασφάλιση της κατάλληλης διαχείρισης της αλλαγής όσον αφορά την τροποποίηση των διαμορφώσεων καθορίζονται και καταγράφονται.
3	3	Τηρείται μητρώο διαμορφώσεων που ισχύουν για τα εν λόγω στοιχεία ενεργητικού. Με τον όρο διαμόρφωση ορίζεται το σύνολο των παραμέτρων τα οποία μπορούν να αλλαχθούν σε υλισμικό, λογισμικό ή firmware και τα οποία μπορεί να επηρεάσουν την ασφάλεια ή / και την λειτουργικότητα ενός συστήματος.
3	4	Τα ελάχιστα στοιχεία που περιέχονται εντός του μητρώου είναι τα ακόλουθα: registry settings, permission settings σε επίπεδο αρχείων, φακέλων αλλά και άλλων πόρων, ρυθμίσεις που σχετίζονται με ανοικτές θύρες, ενεργοποιημένες ή αποκλεισμένες υπηρεσίες ή πρωτόκολλα, επιτρεπτές ή αποκλεισμένες συνδέσεις.
3	5	Για κάθε αλλαγή που υλοποιείται και μπορεί να επηρεάσει την διαμόρφωση (baseline configuration) να φαίνεται σε κάθε περίπτωση το στοιχείο το οποίο υφίσταται την αλλαγή.
3	6	Ως βασικό βήμα, προβλέπεται η διενέργεια αντιγράφου ασφαλείας της παραμετροποίησης του στοιχείου και αποθήκευση σε προστατευμένο σημείο, με υπόδειξη της αντιστοιχία με την συγκεκριμένη αλλαγή.
3	7	Οι ασφαλείς διαμορφώσεις ακολουθούν τις προδιαγραφές του [SS3].
4	1	Διενεργούνται σωτερικές ή και εξωτερικές επιθεωρήσεις με αντικείμενο την πληρότητα και την ακεραιότητα των διαμορφώσεων των στοιχείων.

4	2	Στα πλαίσια των ελέγχων ιχνηλατούνται αλλαγές με εκκίνηση το documentation μιας αλλαγής (προκειμένου να εξακριβωθεί ότι υπάρχει αρχείο διαμόρφωσης που συσχετίζεται με αυτήν την αλλαγή καθώς και έλεγχοι σύγκρισης της υπάρχουσας διαμόρφωσης προς το διατηρούμενο αρχείο διαμόρφωσης ανά περίπτωση.
4	3	Έχουν προσδιοριστεί στα πλαίσια των σχετικών διαδικασιών το χρονικό διάστημα διατήρησης του ιστορικού διαμόρφωσης.
4	4	Οι διαμορφώσεις προστατεύονται σύμφωνα με το υψηλότερο επίπεδο διαβάθμισης πληροφοριών όπως αναφέρεται στο [DS2] και άρα εφαρμόζεται και αυστηρός έλεγχος πρόσβασης.
4	5	Στοιχεία από περιστατικά ασφαλείας ή από ενημερώσεις σχετικά με αδυναμίες και σημεία βελτίωσης, λαμβάνονται ως εισερχόμενα στην διαδικασία διαχείρισης διαμόρφωσης και ενεργοποιούν σχετικές αλλαγές.
4	6	Έχει προβλέφθεί μια διαδικασία εξαίρεσης από την εφαρμογή συγκεκριμένων secure baselines όπως προβλέπεται.
4	7	Εφαρμόζονται εργαλεία system configuration management, τα οποία επιβάλλουν και ανανεώνουν αυτόματα τις ρυθμίσεις παραμέτρων στα συστήματα, σε προκαθορισμένο χρόνο ή σε περίπτωση περιστατικού ή συμβάντος. Τέτοια εργαλεία μπορεί να είναι το Active Directory Group Policy Objects για συστήματα Microsoft Windows και το Puppet για UNIX συστήματα.
4	8	Οι αλλαγές στα αρχεία αυτά διαχειρίζονται μέσω της διαδικασίας διαχείρισης αλλαγών [CM1]. (Αλλαγές πρέπει να γίνονται για την επικαιροποίηση των updates / patches, στην αλλαγή ρυθμίσεων βάσει στοιχείων περιστατικών ή ενημέρωσης από άλλα αξιόπιστα ενδιαφερόμενα μέρη κ.α.).
4	9	Σε περίπτωση που υπάρχει κάποιο πρόβλημα με κάποιο στοιχείο, αντικαθίσταται με καθαρή υλοποίηση από το αρχείο (baseline).
4	10	Κάθε στοιχείο εντός του δικτύου του οργανισμού είναι μοναδικά αναγνωρίσιμο και περιέχεται μέσα στον κατάλογο στοιχείων ενεργητικού όπως αναφέρεται στο [DS1/RM2].
4	11	Αντίστοιχες διαδικασίες και οδηγίες υπάρχουν και για διαφορετικού είδους λογισμικά όπως είναι εφαρμογές, βάσεις δεδομένων κ.α.
4	12	Εφεδρικά αντίγραφα ασφαλείας λαμβάνονται για τα αρχεία των διαμορφώσεων σύμφωνα με την σχετική πολιτική.
4	13	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Χρησιμοποιούνται αυτοματοποιημένα εργαλεία για την επαλήθευση των βασικών διαμορφώσεων των στοιχείων ενεργητικού ώστε να εντοπίζονται αλλαγές.
5	2	Οι αλλαγές αυτές καταγράφονται και ενημερώνεται ο υπεύθυνος ασφάλειας δικτύων και πληροφοριών και ενεργοποιείται η διαδικασία διαχείρισης περιστατικών ασφαλείας.
5	3	Διατηρούνται τα προηγούμενα αρχεία (baselines) για λόγους ιστορικότητας και δυνατότητας roll back σε περίπτωση ανάγκης.
5	4	Τηρούνται αρχεία (baseline) και για τα συστήματα που χρησιμοποιούνται για την ανάπτυξη και δοκιμή, διακριτά από αυτά που χρησιμοποιούνται για την παραγωγή.
5	5	Διενεργούνται έλεγχοι και δοκιμές για την αξιολόγηση της ανθετικότητας των baseline αρχείων. Σε περίπτωση που διαπιστωθούν αδυναμίες, λαμβάνονται άμεσα μέτρα και ακολουθείται η διαδικασία διαχείρισης αλλαγών.
5	6	Οι συσκευές οι οποίες συνδέονται απομακρυσμένα στα συστήματα ελέγχονται απομακρυσμένα σχετικά τη διαμόρφωση τους, το λογισμικό που έχουν εγκατεστημένο και το επίπεδο ενημέρωσης.
5	7	Οι συσκευές οι οποίες συνδέονται στα συστήματα και αφορούν τρίτα μέρη, ο οργανισμός τους έχει κοινοποιήσει το ελάχιστα αποδεκτό επίπεδο ασφάλειας που έχουν υλοποιήσει και πραγματοποιεί ελέγχους ασφαλείας προτού δοθεί πρόσβαση στα συστήματα του οργανισμού.
5	8	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	9	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.

Κατηγορία		ΔΙΑΧΕΙΡΙΣΗ ΣΤΟΙΧΕΙΩΝ ΕΝΕΡΓΗΤΙΚΟΥ
ΑΜ1		Μέτρο: Διαχείριση του κύκλου ζωής στοιχείων ενεργητικού Στόχος Μέτρου: Να διασφαλιστεί ότι τα στοιχεία ενεργητικού είναι ασφαλή καθ' όλη τη διάρκεια του κύκλου ζωής τους, συμπεριλαμβανομένης της προμήθειας, της ανάπτυξης, της συντήρησης και της διάθεσης τους. Περιγραφή Μέτρου: Θέσπιση, εφαρμογή και διατήρηση μέτρων ασφάλειας πληροφοριών στο πλαίσιο του σχεδίου διαχείρισης του κύκλου ζωής των στοιχείων ενεργητικού, προκειμένου να διασφαλίζεται ότι η ασφάλεια των πληροφοριών είναι αναπόσπαστο κομμάτι αυτού του κύκλου ζωής, δηλαδή την προμήθεια, την εγκατάσταση, τη συντήρηση και τη διάθεση. Η διαχείριση του κύκλου ζωής των πληροφοριών, όπως περιγράφεται στο μέτρο [DS1], θα πρέπει να αποτελεί μέρος του σχεδίου διαχείρισης του κύκλου ζωής των στοιχείων ενεργητικού. Το σχέδιο διαχείρισης του κύκλου ζωής των στοιχείων ενεργητικού πρέπει να περιγράφει όλες τις διαδικασίες για τον χειρισμό των πληροφοριών σύμφωνα με την πολιτική ταξινόμησης και επισήμανσης των δεδομένων, όπως περιγράφεται στο μέτρο [DS2]. Πηγή:
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν έχει κάποιο δομημένο τρόπο με τον οποίο να διαχειρίζεται τους πόρους (στοιχεία ενεργητικού) καθ΄ όλη τη διάρκεια του κύκλου ζωής τους.
1	1	Οι διαδικασίες σχετικά με την απόκτηση και απομάκρυνση στοιχείων ενεργητικού διενεργούνται τουλάχιστον με τρόπο ad-hoc και σύμφωνα με τις γνώσεις του εμπλεκόμενου προσωπικού.
2	1	Υπάρχει μια καταγεγραμμένη διαδικασία η οποία περιγράφει τον τρόπο με τον οποίο διαχειρίζονται τα στοιχεία ενεργητικού κατά τη διάρκεια του κύκλου ζωής τους.
2	2	Η συγκεκριμένη διαδικασία περιλαμβάνει ενέργειες που διενεργούνται από σχετικά εξουσιοδοτημένους ρόλους για την: προμήθεια, την εγκατάσταση, τη συντήρηση και τη διάθεση.
2	3	Σχετικοί ρόλοι και αρμοδιότητες έχουν ανατεθεί στο προσωπικό. Οι αλλαγές στα στοιχεία ενεργητικού γίνονται τουλάχιστον με ad-hoc τρόποκαι διατηρείται η κατ'ελάχιστο βασική τεκμηριωμένη πληροφορία.
3	1	Στα πλαίσια της διαδικασίας περιλαμβάνονται και στοιχεία ασφάλειας πληροφοριών ώστε να διασφαλίζεται ότι η ασφάλεια των πληροφοριών είναι αναπόσπαστο κομμάτι αυτού του κύκλου ζωής, δηλαδή την προμήθεια, την εγκατάσταση, τη συντήρηση και τη διάθεση.
3	2	Η διαχείριση του κύκλου ζωής των πληροφοριών, όπως περιγράφεται στο μέτρο [DS1], αποτελεί μέρος του σχεδίου διαχείρισης του κύκλου ζωής των στοιχείων ενεργητικού.
3	3	Η διαδικασία διαχείρισης του κύκλου ζωής των στοιχείων ενεργητικού περιγράφει όλες τις επιμέρους διαδικασίες για τον χειρισμό των πληροφοριών σύμφωνα με την πολιτική ταξινόμησης και επισήμανσης των δεδομένων, όπως περιγράφεται στο μέτρο [DS2].
3	4	Αλλαγές στα στοιχεία ενεργητικού γίνονται σύμφωνα με την διαδικασία διαχείρισης αλλαγών [CM1].
3	5	Στα πλαίσια του σχεδίου περιγράφονται και τα κριτήρια που χρησιμοποιεί ο οργανισμός προκειμένου να κατανέμει τους πόρους σε κατηγορίες κρισιμότητας.
3	6	Προδιαγραφές ασφαλείας, κατάλληλες για την επικείμενη χρήση του στοιχείου ενεργητικού προδιαγράφονται πριν την προμήθεια.
4	1	Καθορίζονται ανά κατηγορία στοιχείου ενεργητικού και ανά κατηγορία κρισιμότητας, οι ελάχιστες διαδικασίες συντήρησης για τα στοιχεία ενεργητικού.
4	2	Τουλάχιστον μια φορά το χρόνο διενεργείται έλεγχος για την αναγνώριση κατά πόσο το σχέδιο διαχείρισης του κύκλου ζωής των στοιχείων ενεργητικού εφαρμόζεται ορθά και αποτελεσματικά. Από τον έλεγχο προκύπτει επίσης κατά πόσο υπάρχουν επαρκείς πόροι (άνθρωποι, εξοπλισμός, εργαλεία, χρήματα κ.α.) για την αποτελεσματική λειτουργία του σχεδίου.
4	3	Σε περίπτωση που προκύψει απόκλιση ως αποτέλεσμα του ελέγχου, καταγράφεται άμεσα και δρομολογούνται σχετικές διορθωτικές ενέργειες.
4	4	Οι κατηγορίες κρισιμότητας των πόρων χρησιμοποιούνται και είναι συμβατές προς αυτές που χρησιμοποιούνται κατά τη διάρκεια της διαχείρισης διακινδύνευσης.
4	5	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
4	6	Τα δεδομένα καταστρέφονται με ασφάλεια πριν ο εξοπλισμός επαναχρησιμοποιηθεί ή όταν ολοκληρώσει τον κύκλο ζωής του.

5	1	Τα κομμάτια του εξοπλισμού που έχουν την δυνατότητα να διατηρούν δεδομένα, καταστρέφονται φυσικά στο τέλος του κύκλου ζωής τους σύμφωνα με τα προβλεπόμενα του [DS1].
5	2	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	3	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
AM2		Μέτρο: Καταγραφή των στοιχείων ενεργειακού και ιδιοκτησίαΣτόχος Μέτρου: Να διασφαλιστεί ότι τα στοιχεία ενεργητικού καταγράφονται σε κατάλογο και ότι η ιδιοκτησία καθορίζεται με σκοπό την επίτευξη της ιχνηλασιμότητας και της ευθύνης για τα στοιχεία.Περιγραφή Μέτρου: Θέσπιση, εφαρμογή και διατήρηση καταλόγου καταγραφής των στοιχείων ενεργητικού, προκειμένου να διασφαλίσει ότι ο οργανισμός έχει σαφή, ακριβή και ενημερωμένη κατάσταση των στοιχείων (π.χ. υλισμικό, λογισμικό, πληροφορίες) που διατηρεί. Ο κατάλογος θα πρέπει να προσδιορίζει τον ιδιοκτήτη των στοιχείων αυτών. Ο κατάλογος θα πρέπει επίσης να επιτρέπει στον οργανισμό να παρακολουθεί όλα τα στοιχεία ενεργητικού για τα οποία θα πρέπει να εφαρμόζει και να διατηρεί μέτρα ασφάλειας πληροφοριών. Πηγή:
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν έχει κάποιο συγκεκριμένο / οργανωμένο τρόπο για την αναγνώριση στοιχείων ενεργητικού εντός του οργανισμού.
1	1	Καταγράφονται τα στοιχεία ενεργητικού τουλάχιστον ad-hoc.
1	2	Τηρείται κάποιο αρχείο, με ή χωρίς κεντρική διαχείριση, το οποίο ενημερώνεται τουλάχιστον ad-hoc.
2	1	Τηρείται κατάλογος στοιχείων ενεργητικού.
2	2	Υπάρχει ένας αναγνωρισμένος ιδιοκτήτης του καταλόγου, ο οποίος είναι υπεύθυνος για την τήρηση και επικαιροποίηση των σχετικών δεδομένων.
3	1	Έχει θεσπιστεί, εφαρμόζεται και διατηρείται ένας κατάλογος καταγραφής των στοιχείων ενεργητικού, προκειμένου να διασφαλίσει ότι ο οργανισμός έχει σαφή, ακριβή και ενημερωμένη κατάσταση των στοιχείων (π.χ. υλισμικό, λογισμικό, πληροφορίες) που διατηρεί.
3	2	Ο κατάλογος προσδιορίζει τον ιδιοκτήτη των στοιχείων αυτών.
3	3	Ο κατάλογος επίσης να επιτρέπει στον οργανισμό να παρακολουθεί όλα τα στοιχεία ενεργητικού για τα οποία εφαρμόζει και διατηρεί μέτρα ασφάλειας πληροφοριών, τουλάχιστον με χειροκίνητο τρόπο.
3	4	Στον κατάλογο συμπεριλαμβάνονται η περιγραφή της λειτουργίας/χρήσης και της τοποθεσίας των στοιχείων, προκειμένου να υπάρχει πλήρης απογραφή των στοιχείων αυτών.
4	1	Χρησιμοποιείται αυτόματο σύστημα για την αναγνώριση και καταγραφή στοιχείων ενεργητικού και συστημάτων εντός του οργανισμού αλλά και εκτός του οργανισμού (hosted in third parties).
4	2	Τα στοιχεία που εξάγονται από το αυτόματο σύστημα συμπληρώνονται με στοιχεία διαδικασιών και δημιουργείται αποτύπωση των σχετικών εξαρτήσεων και αλληλεξαρτήσεων με όσο περισσότερο αυτοματοποιημένο τρόπο γίνεται.
4	3	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
4	4	Έχει δημιουργηθεί κατάλογος με μη εξουσιοδοτημένες εφαρμογές και κατηγορίες εκτελέσιμων αρχείων και διασφαλίζεται ότι απαγορεύεται η εκτέλεσή τους στα στοιχεία του οργανισμού (application blacklisting).
5	1	Διατίθεται αυτόματο σύστημα και διαδικασίες για τον έλεγχο της ακεραιότητας και εγκυρότητας των στοιχείων του καταλόγου στοιχείων ενεργητικού, συστημάτων και διαδικασιών.
5	2	Σε περίπτωση ανίχνευσης στοιχείου που δεν βρίσκεται καταχωρημένο στον κατάλογο διενεργούνται αυτόματες ενέργειες ενημέρωσης του αρμόδιου προσωπικού για τον έλεγχο και επικαιροποίηση των σχετικών στοιχείων.
5	3	Ειδικά σε περίπτωση στοιχείων ενεργητικού, λαμβάνονται άμεσες ενέργειες περιορισμού μέχρι την υλοποίηση της σχετικής διερεύνησης.
5	4	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	5	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.

AM3		Μέτρο: Παρακολούθηση στοιχείων ενεργητικού Στόχος Μέτρου: Να διασφαλιστεί ότι τα στοιχεία ενεργητικού είναι υπό παρακολούθηση για επιθέσεις, ανωμαλίες και απειλές κατά της ασφάλειας, προκειμένου να ενεργοποιηθούν οι διαδικασίες για την αντιμετώπιση συμβάντων και περιστατικών. Περιγραφή Μέτρου: Θέσπιση, εφαρμογή και διατήρηση δυνατοτήτων παρακολούθησης των στοιχείων ενεργητικού, ώστε ο οργανισμός να είναι σε θέση να εντοπίζει ανωμαλίες σε σχέση με κανονικές συνθήκες (π.χ. τοποθεσία, χρήση) και/ή τη λειτουργία των στοιχείων αυτών. Ο οργανισμός θα πρέπει να αναφέρει στην πολιτική αποδεκτής χρήσης, όπως περιγράφεται στο [HRS6], τι συνιστά αποδεκτή χρήση και/ή λειτουργία των στοιχείων ενεργητικού. Ο οργανισμός θα μπορούσε επίσης να εξετάσει την συμπερίληψη της περιγραφής της αποδεκτής χρήσης, της λειτουργίας και της τοποθεσίας των στοιχείων στον κατάλογο των στοιχείων ενεργητικού, όπως περιγράφεται στο [AM2], προκειμένου να υπάρχει πλήρης απογραφή των στοιχείων αυτών. Όταν εντοπίζονται ανωμαλίες, θα πρέπει να ενεργοποιούνται διαδικασίες διαχείρισης συμβάντων και περιστατικών προκειμένου ο οργανισμός να είναι ανθεκτικός στην παρουσία ανωμαλιών. Πηγή: C2M2 (Situation), PNNL, NIST 800-53, ISO 27001
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν παρακολουθεί τα στοιχεία ενεργητικού του.
1	1	Διενεργείται παρακολούθηση τουλάχιστον σε ένα μέρος των στοιχείων ενεργητικού του, η οποία δύναται να μην είναι πλήρης ή συστηματική.
2	1	Για τα κρίσιμα στοιχεία ενεργητικού, όπως αυτά αποτυπώνονται στον σχετικό κατάλογο [AM2 / RM2], έχει ενεργοποιηθεί παρακολούθηση.
2	2	Η παρακολούθηση περιλαμβάνει κατ' ελάχιστο τις ενέργειες των ατόμων, αντικειμένων και οντοτήτων όταν αποκτούν πρόσβαση ή χρησιμοποιούν τα στοιχεία ενεργητικού, τα γεγονότα που μπορεί να διαταράξουν την ομαλή λειτουργία μιας δραστηριότητας, τις αλλαγές των στοιχείων ενεργητικού που οδηγούν σε διαφοροποίηση από το security baseline, στοιχεία ενεργητικού που συνδέονται (μη-αναμενόμενα) στα δίκτυα του οργανισμού και οποιαδήποτε άλλη ύποπτη δραστηριότητα.
3	1	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται δυνατότητες παρακολούθησης των στοιχείων ενεργητικού, ώστε ο οργανισμός να είναι σε θέση να εντοπίζει ανωμαλίες σε σχέση με κανονικές συνθήκες (π.χ. τοποθεσία, χρήση) και/ή τη λειτουργία των στοιχείων αυτών.
3	2	Αναφέρεται στην πολιτική αποδεκτής χρήσης, όπως περιγράφεται στο [HRS6], τι συνιστά αποδεκτή χρήση και/ή λειτουργία των στοιχείων ενεργητικού.
3	3	Συμπεριλαμβάνεται στην περιγραφή της αποδεκτής χρήσης, η λειτουργία και η τοποθεσία των στοιχείων στον κατάλογο των στοιχείων ενεργητικού όπως αναφέρεται στο [AM2], προκειμένου να υπάρχει πλήρης απογραφή των στοιχείων αυτών.
3	4	Όταν εντοπίζονται ανωμαλίες, ενεργοποιούνται διαδικασίες διαχείρισης συμβάντων και περιστατικών προκειμένου ο οργανισμός να είναι ανθεκτικός στην παρουσία ανωμαλιών.
3	5	Τα αποτελέσματα της παρακολούθησης (logs) περιέχουν κατ' ελάχιστο τις ακόλουθες πληροφορίες: ημερομηνία, ώρα, source address & destination address (όπου αυτό εφαρμόζεται), τύπος καταγραφής, και όποια άλλη πληροφορία μπορεί να δοθεί επιπλέον ως επεξήγηση.
3	6	Εχει προσδιορίστει το είδος της παρακολούθησης που είναι ενεργοποιημένο ανά στοιχείο ενεργητικού (π.χ. System, Security, Application κ.α.), η έκταση της παρακολούθησης σε επίπεδο γεγονότος (π.χ. types of events: audit success, audit failure, login success, object access success, warning, ….), το χρονικό διάστημα διατήρησης των σχετικών εγγραφών (π.χ. 3 μήνες) και η τοποθεσία αποθήκευσης (π.χ. στην συσκευή, σε syslog server, σε άλλο αποθηκευτικό μέσο κ.α.). Τα παραπάνω έχουν εξαχθεί λαμβάνοντας υπόψη το πλαίσιο λειτουργίας του οργανισμού, την στρατηγική και τους στόχους ασφάλειας πληροφοριών όπως αναφέρεται στο [STR1] και το κείμενο νομοθετικό και κανονιστικό πλαίσιο.
4	1	Έχει διενεργηθεί ανάλυση ώστε να προσδιορίσούν οι ανάγκες σε χώρο και υπολογιστική ισχύ για να μπορεί να γίνει η αποθήκευση και διαχείριση των σχετικών δεδομένων παρακολούθησης χωρίς προβλήματα ανά σύστημα.
4	2	Τα δεδομένα της παρακολούθησης ανασκοπούνται ημερησίως με χειροκίνητο ή ημιαυτόματο τρόπο με σκοπό την αναγνώριση πιθανών ανωμαλιών, τάσεων, επερχόμενων επιθέσεων ή πραγματικών επιθέσεων.
4	3	Τουλάχιστον δυο πηγές συγχρονισμού ρολογιού έχουν οριστεί ώστε να εξασφαλίζεται ότι τα στοιχεία της παρακολούθησης έχουν την σωστή χρονοσήμανση.
4	4	Ο συγχρονισμός αφορά όλα τα κρίσιμα στοιχεία ενεργητικού (κατ' ελάχιστον όλοι οι servers και ο εξοπλισμός δικτύου).
4	5	Διενεργείται έλεγχος στα στοιχεία της παρακολούθησης σχετικά με την περίληψη στοιχείων που αναφέρονται στο ML3 (παραπάνω επίπεδο, 3).

4	6	Μέσω κατάλληλων τεχνικών μέτρων, γίνεται παρακολούθηση της κατάστασης των στοιχείων ενεργητικού όπως προβλέπεται από το [AM6].
4	7	Σε περίπτωση που οι δυνατότητες παρακολούθησης αποτυγχάνουν, τότε λαμβάνονται κατάλληλες ενέργειες ώστε να τίθεται εκτός λειτουργίας το συγκεκριμένο στοιχείο μέχρις ότου διερευνηθεί πλήρως ο λόγος της αποτυχίας (Δεν εφαρμόζεται για στοιχεία τα οποία έχουν άμεση σχέση με την διαχείριση της ασφάλειας).
4	8	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Έχει τεθεί σε λειτουργία σύστημα SIEM το οποίο συγκεντρώνει τα στοιχεία παρακολούθησης από το σύνολο των στοιχείων ενεργητικού του οργανισμού.
5	2	Έχουν παραμετροποιηθεί κανόνες και έχουν δημιουργηθεί ενημερώσεις (notifications & alerts) στο κατάλληλο προσωπικό σε περίπτωση ενεργοποίησης κάποιου κανόνα.
5	3	Για την δημιουργία των κανόνων έχουν ληφθεί υπόψη βασικές μέθοδοι επίθεσης. Κατ' ελάχιστον οι κανόνες έχουν παραμετροποιηθεί για να ενημερώνουν 1)σε περίπτωση που ένας λογαριασμός έχει προστεθεί σε ομάδα προνομιακών λογαριασμών ή αν έχουν αναβαθμιστεί τα δικαιώματα υπάρχοντος λογαριασμού ή αν έχει δημιουργηθεί νέος λογαριασμός με δικαιώματα προνομιακής πρόσβασης 2) σε περίπτωση που για κάποιο λογαριασμό με προνομιακό δικαίωμα πρόσβασης έχει αλλάξει ο κωδικός πρόσβασης ή άλλο μυστικό στοιχείο αυθεντικοποίησης 3) αν η σύνδεση έχει γίνει από τοποθεσία η οποία δεν έχει προβλεφθεί από τους σχετικούς κανόνες του οργανισμού, 4) σε περίπτωση (π.χ. >3) αποτυχημένων προσπαθειών πρόσβασης από την ίδια πηγή σε σχετικά μικρό χρονικό διάστημα, 5) σε περίπτωση αποτυχημένων προσπαθειών πρόσβασης από τον ίδιο λογαριασμό σε διαφορετικά μηχανήματα, 6) όταν διενεργείται κάποια σάρωση δικτύου, 7) όταν δημιουργείται κάποιος DHCP εντός του δικτύου 8) όταν ανιχνεύεται κάποια επίθεση που αντιστοιχεί σε κάποιο από τα OWASP Top 10, 9) σε περίπτωση που έχουν δημιουργηθεί alerts για τα IPS / IDS που έχει υλοποιήσει ο οργανισμός, 10) σε περίπτωση που έχουν δημιουργηθεί alerts από το DLP, 11) περιπτώσεις που έχουν διενεργηθεί αλλαγές σε οποιαδήποτε εγγραφή παρακολούθησης περιλαμβανομένης και της διαγραφής του ή της απενεργοποίησης της σχετικής ικανότητας.
5	4	Ο χώρος στον οποίο αποθηκεύονται τα στοιχεία παρακολούθησης είναι προστατευμένος και write only. Σε περίπτωση που αυτό δεν είναι εφικτό, χρησιμοποιούνται χωριστά μηχανήματα στα οποία η πρόσβαση είναι αυστηρά καθορισμένη όπως προβλέπεται και από το [IAM2].
5	5	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	6	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
AM4		Μέτρο: Διαχείριση διαθεσιμότητας Στόχος Μέτρου: Να διασφαλιστεί η διαθεσιμότητα δικτύων και συστημάτων πληροφοριών με την επίτευξη επαρκούς διαθεσιμότητας πόρων, εφεδρείας και συστημάτων / διαδικασιών υψηλής διαθεσιμότητας. Περιγραφή Μέτρου: Θέσπιση, εφαρμογή και διατήρηση διαδικασιών διαχείρισης της διαθεσιμότητας προκειμένου να διασφαλίζεται ότι παρέχεται το επιθυμητό επίπεδο των επιχειρησιακών υπηρεσιών από τον οργανισμό. Ο οργανισμός θα πρέπει να διασφαλίζει ανά πάσα στιγμή τη διαθεσιμότητα των πόρων (π.χ. χώροι, προσωπικό, συστήματα πληροφορικής, κ.λπ.). Όπως περιγράφεται στο μέτρο [NS6], ο οργανισμός θα πρέπει να εγγυάται την εφεδρεία και την υψηλή διαθεσιμότητα όλων των συστημάτων πληροφορικής, προκειμένου να διασφαλίζεται η έγκαιρη και αποτελεσματική ανάκτηση των δεδομένων μετά την ύπαρξη ενός συμβάντος ή περιστατικού, ή κατόπιν αιτήματος. Ο οργανισμός θα πρέπει να δημιουργήσει εφεδρικά αντίγραφα των πληροφοριών που περιγράφονται στο [DS3]. Πηγή:
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν έχει λάβει μέτρα για την εξασφάλιση της διαθεσιμότητας των δικτύων και συστημάτων πληροφορικής.
1	1	Υπάρχει κάποιος εξοπλισμός σε εφεδρεία που μπορεί να χρησιμοποιηθεί σε περίπτωση αστοχίας ενός στοιχείου ενεργητικού.
2	1	Έχουν αναγνωρίσθει τα κρίσιμα στοιχεία ενεργητικού.
2	2	Για τα συγκεκριμένα στοιχεία υπάρχει τουλάχιστον ένα ακόμα στοιχείο σε εφεδρεία (μπορεί να είναι το ίδιο ή αντίστοιχης ικανότητας).
2	3	Τα στοιχεία αυτά περιέχονται μέσα στο κατάλογο στοιχείων ενεργητικού.
3	1	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται διαδικασίες διαχείρισης της διαθεσιμότητας προκειμένου να διασφαλίζεται ότι παρέχεται το επιθυμητό επίπεδο των επιχειρησιακών υπηρεσιών από τον οργανισμό.

3	2	Διασφαλίζεται ανά πάσα στιγμή η διαθεσιμότητα των πόρων (π.χ. χώροι, προσωπικό, συστήματα πληροφορικής, κ.λπ.).
3	3	Όπως περιγράφεται στο μέτρο [NS6], ο οργανισμός εγγυάται την εφεδρεία και την υψηλή διαθεσιμότητα όλων των συστημάτων πληροφορικής, προκειμένου να διασφαλίζεται η έγκαιρη και αποτελεσματική ανάκτηση των δεδομένων μετά την ύπαρξη ενός συμβάντος ή περιστατικού, ή κατόπιν αιτήματος.
3	4	Δημιουργούνται εφεδρικά αντίγραφα των πληροφοριών που περιγράφονται στο [DS3].
3	5	Κατ΄ ελάχιστο ο εξοπλισμός διαθέτει εφεδρείες σε σχέση με την ενέργεια, την χωρητικότητα, το δίκτυο και τον τρόπο διασύνδεσης.
3	6	Δεν υπάρχει κρίσιμος εξοπλισμός που δεν έχει εφεδρικό εντός του ίδιου χώρου σε ενεργή ή και ανενεργή λειτουργία.
3	7	Υπάρχει εξοπλισμός σε δευτερεύον σημείο, ο οποίος έχει σχετικά μελετηθεί ώστε να μπορεί να χρησιμοποιηθεί για να ανακάμψουν οι βασικές δραστηριότητες του οργανισμού ενός συγκεκριμένου χρονικού διαστήματος και σε συγκεκριμένο επίπεδο.
4	1	Μέσω κατάλληλων τεχνικών μέτρων, γίνεται παρακολούθηση της κατάστασης των στοιχείων ενεργητικού συνεχώς. (Συγκεκριμένα γίνεται παρακολούθηση αν τα στοιχεία ενεργητικού του οργανισμού τόσο στον βασικό όσο και στον εφεδρικό χώρο ανταποκρίνονται και βρίσκονται σε καλή κατάσταση λειτουργίας).
4	2	Σε περίπτωση που κάποιο σύστημα ενεργητικού έχει αναγνωριστεί ότι δεν είναι διαθέσιμο (alert), το κατάλληλο προσωπικό ειδοποιείται για την διερεύνηση και την χειροκίνητη μετάβαση στο εφεδρικό σύστημα (αν απαιτείται).
4	3	Έχει προβλεφθεί ώστε να υπάρχει δυνατότητα πρόσβασης και ανάκτησης των δεδομένων όπως απαιτείται από τα εφεδρικά αντίγραφα (π.χ. υπάρχει δυνατότητα λήψης, εγκατάστασης ή χρήσης του λογισμικού αντιγράφων ασφαλείας και υπάρχει διαθεσιμότητα των σχετικών κλειδιών) όπως προβλέπεται από το [DS3].
4	4	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Εφαρμόζονται λύσεις συγχρονισμού (replication) σε εναλλακτικό χώρο για τα κρίσιμα συστήματα όπως αυτά έχουν αναγνωριστεί σύμφωνα με την ανάλυση επιχειρησιακών επιπτώσεων και τα σχετικά σχέδια επιχειρησιακής συνέχειας και ανάκαμψης από καταστροφή.
5	2	Σε περίπτωση αστοχίας ή μη διαθεσιμότητας του πρωτεύοντος εξοπλισμού γίνονται αυτόματες ενέργειες για την ενεργοποίηση του δευτερεύοντος.
5	3	Μια φορά το χρόνο τουλάχιστον γίνεται πλήρης λειτουργική δοκιμή της κατάστασης συγχρονισμού και της δυνατότητας λειτουργίας του οργανισμού από την εναλλακτική τοποθεσία.
5	4	Τηρούνται χωριστά εφεδρικά αντίγραφα και σε τρίτη ασφαλή τοποθεσία, για να μπορεί να προστατευτεί ο οργανισμός και από επιθέσεις κυβερνοεκβιασμού σύμφωνα με τα προβλεπόμενα του [DS3].
5	5	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	6	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
AM5		Μέτρο: Κρυπτογραφία Στόχος Μέτρου: Να διασφαλιστεί η εμπιστευτικότητα, ακεραιότητα και αυθεντικότητα των πληροφοριών με την υιοθέτηση κατάλληλων κρυπτογραφικών λύσεων. Περιγραφή Μέτρου: Θέσπιση, εφαρμογή και διατήρηση πολιτικής σχετικά με τη χρήση κρυπτογραφικών μέτρων, προκειμένου να διασφαλίζονται η εμπιστευτικότητα, η ακεραιότητα και η αυθεντικότητα των δεδομένων κατά την αποθήκευση, τη χρήση και τη μεταφορά. Η πολιτική κρυπτογράφησης θα πρέπει να λαμβάνει υπόψη την εφαρμογή κρυπτογραφικών μέτρων σε όλα τα στάδια του κύκλου ζωής των πληροφοριών και να εξετάζει εφαρμογές, συστήματα, εξοπλισμό δικτύου και διαύλους επικοινωνίας. Πηγή: CSA CCM v4., ANSII guidelines, NIST 800-53, NIST 800-57, CIS
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν υλοποιεί κρυπτογραφία σε καμια της μορφή και εφαρμογή.
1	1	Χρησιμοποιούνται λύσεις κρυπτογραφίας για κάποιους πόρους τουλάχιστον ad-hoc .
2	1	Εφαρμόζεται κρυπτογράφηση στα δεδομένα ή σε ολόκληρες συσκευές που έχουν αναγνωριστεί ως κρίσιμες στον σχετικό κατάλογο πόρων.
2	2	Επίσης εφαρμόζεται κρυπτογράφηση σε αφαιρούμενα μεταφορικά μέσα όπου αυτά χρησιμοποιούνται και σε end point devices.

3	1	Έχει θεσπιστεί, εφαρμόζεται και διατηρείται πολιτική σχετικά με τη χρήση κρυπτογραφικών μέτρων, προκειμένου να διασφαλίζονται η εμπιστευτικότητα, η ακεραιότητα και η αυθεντικότητα των δεδομένων κατά την αποθήκευση, τη χρήση και τη μεταφορά.
3	2	Η πολιτική κρυπτογράφησης λαμβάνει υπόψη την εφαρμογή κρυπτογραφικών μέτρων σε όλα τα στάδια του κύκλου ζωής των πληροφοριών και εξετάζει εφαρμογές, συστήματα, εξοπλισμό δικτύου και διαύλους επικοινωνίας.
3	3	Κατ΄ ελάχιστον εφαρμόζονται τα ακόλουθα: SHA-256, SHA-512 or SHA-341 ως hash function, HMAC με SHA-256, bcrypt, scrypt ή PBKDF2 για την αποθήκευση κωδικών πρόσβασης, AES ή AES-CBC για συμμετρική κρυπτογράφηση; RSA-OAEP όπως ορίζεται στο PKCS#1 v2.1 για ασύμμετρη κρυπτογράφηση και για υπογραφές, RSA-SSA-PSS όπως ορίζεται στο PKCS#1 v2.1.
3	4	Σε κάθε περίπτωση χρησιμοποιούνται κατάλληλα κλειδιά. Ειδικά για AES τα κλειδιά να είναι τουλάχιστον 128 bits και για τους αλγόριθμους που στηρίζονται στο RSA, τα modules και τα secret exponents πρέπει να είναι τουλάχιστον 2048 bits ή 3072 bits, με public exponents, για την κρυπτογράφηση τουλάχιστον μεγαλύτερο από 65536.
3	5	Για την μεταφορά δεδομένων και την προστασία των δεδομένων σε ηρεμία (at rest) εφαρμόζονται τα αντίστοιχα των [DS2] και [DS4].
4	1	Χρησιμοποιείται λογισμικό ή κρυπτογραφικές βιβλιοθήκες οι οποίες έχουν ελεγχθεί από έγκυρα τρίτα μέρη.
4	2	Επιπλέον χρησιμοποιούνται λύσεις που είναι σχετικά πιστοποιημένες (όπου αυτό υπάρχει), λογισμικό όπως VeraCrypt software, για την δημιουργία encrypted containers, το GNU Privacy Guard software, που επιτρέπει την εφαρμογή ασύμμετρης κρυπτογραφίας.
4	3	Κανενός τύπου Wi-Fi enabled εξοπλισμός δεν παραμετροποιείται ώστε να λαμβάνει ή να μοιράζεται κλειδιά κρυπτογράφησης.
4	4	Τα κλειδιά κρυπτογράφησης προστατεύονται ως πληροφορία του υψηλότερου επίπεδου διαβάθμισης όπως αναφέρεται στο [DS2] και υπόκειται σε αυστηρό έλεγχο πρόσβασης.
4	5	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Τηρείται αυτόματο σύστημα για την παρακολούθηση και διαχείριση των πιστοποιητικών και άλλων μέσων κρυπτογράφησης.
5	2	Στις περιπτώσεις που ο οργανισμός διαχειρίζεται (περιλαμβανομένης και της έκδοσης) κρυπτογραφικά κλειδιά, χρησιμοποιείται σύστημα διαχείρισης που του επιτρέπει την δημιουργία, μοναδική χρήση, περιτροπή, ανάκληση, καταστροφή, ενεργοποίηση, απενεργοποίηση, αρχειοθέτηση κλειδιών.
5	3	Υπάρχουν διαδικασίες άμεσης ανταπόκρισης σε περίπτωση που υποκλαπεί ή διαρρεύσει ένα κλειδί κρυπτογράφησης για άμεσα περιορισμό του σχετικού κινδύνου.
5	4	Οι βέλτιστες διεθνείς πρακτικές τόσο για on-premise όσο και για cloud συστήματα που αναφέρονται στο CSA CCM v4.0 στο αντικείμενο του CEK εφαρμόζονται.
5	5	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	6	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
AM6		Μέτρο: Διαχείριση χωρητικότηταςΣτόχος Μέτρου: Να εξασφαλιστεί η κατάλληλη χωρητικότητα και επίδοση των υπηρεσιών των συστημάτων και διαδικασιών πληροφοριών.Περιγραφή Μέτρου: Θέσπιση, εφαρμογή και διατήρηση διαδικασίας διαχείρισης της χωρητικότητας προκειμένου να διασφαλιστεί ότι η χωρητικότητα και οι επιδόσεις των συστημάτων πληροφορικής του οργανισμού δεν επηρεάζονται αρνητικά από αυξημένα επίπεδα ζήτησης υπηρεσιών. Η διαδικασία διαχείρισης χωρητικότητας θα πρέπει να περιλαμβάνει τη διαχείριση της επιχειρησιακής ικανότητας, προκειμένου να διασφαλίζεται ότι οι επιχειρησιακές ανάγκες μετατρέπονται σε απαιτήσεις χωρητικότητας, διαχείριση της χωρητικότητας υπηρεσιών ώστε να γίνεται σωστή διαχείριση της χωρητικότητας των υποσυστημάτων πληροφορικής και ένα μηχανισμό υποβολής εκθέσεων διαχείρισης χωρητικότητας. Πηγή:
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν διαχειρίζεται με κάποιο τρόπο την χωρητικότητα των συστημάτων πληροφορικής.
1	1	Γίνεται παρακολούθηση μερικών στοιχείων για κάποιους πόρους τουλάχιστον σε ad-hoc βάση.
2	1	Έχει αναγνωρισθεί μια σειρά από κρίσιμους πόρους (όπως αυτοί περιέχονται στο κατάλογο στοιχείων ενεργητικού) για τους οποίους γίνεται παρακολούθηση των στοιχείων χωρητικότητας.

2	2	Για τα συγκεκριμένα στοιχεία ενεργητικού έχουν προσδιοριστεί τουλάχιστον τα βασικά στοιχεία παρακολούθησης (κατ' ελάχιστο: δίσκος, μνήμη, επεξεργαστής, bandwidth) και έχουν παραμετροποιηθεί σχετικοί κανόνες.
3	1	Έχει θεσπιστεί, εφαρμόζεται και διατηρείται διαδικασία διαχείρισης της χωρητικότητας προκειμένου να διασφαλιστεί ότι η χωρητικότητα και οι επιδόσεις των συστημάτων πληροφορικής του οργανισμού δεν επηρεάζονται αρνητικά από αυξημένα επίπεδα ζήτησης υπηρεσιών.
3	2	Η διαδικασία διαχείρισης χωρητικότητας περιλαμβάνει τη διαχείριση της επιχειρησιακής ικανότητας, (προκειμένου να διασφαλίζεται ότι οι επιχειρησιακές ανάγκες μετατρέπονται σε απαιτήσεις χωρητικότητας), διαχείριση της χωρητικότητας υπηρεσιών (ώστε να γίνεται σωστή διαχείριση της χωρητικότητας των υποσυστημάτων πληροφορικής) και ένα μηχανισμό υποβολής εκθέσεων διαχείρισης χωρητικότητας.
3	3	Για τα κρίσιμα στοιχεία ενεργητικού του οργανισμού αλλά και τις βασικές λειτουργίες γίνεται αυτόματη παρακολούθηση της διαθεσιμότητας τους.
4	1	Για τα κρίσιμα στοιχεία ενεργητικού του οργανισμού αλλά και τις βασικές λειτουργίες έχουν διεξαχθεί μελέτες για τον σχεδιασμό των κατάλληλων πόρων σε βάθος 5ετίας.
4	2	Οι μελέτες στηρίζονται πάνω σε ιστορικά και πρόσφατα στοιχεία ενώ λαμβάνουν υπόψη τις τάσεις, τα μελλοντικά σχέδια και τους στόχους του οργανισμού όπως αναφέρονται στο [STR1].
4	3	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
4	4	Τα στοιχεία που παρακολουθούνται είναι εγκαταστάσεις, εξοπλισμός, άτομα, γραφεία και άλλα.
4	5	Στα κρίσιμα στοιχεία ενεργητικού του οργανισμού διενεργείται system tuning & monitoring για την εξασφάλιση της βέλτιστης δυνατής επίδοσης σε επίπεδο χωρητικότητας.
5	1	Συνεχής παρακολούθηση της κατάστασης σε σχέση με την χωρητικότητα των συστημάτων.
5	2	Εξάγονται στοιχεία και αναφορές σχετικά με την επίδοση και αναθεωρείται ο σχετικός σχεδιασμός όπως απαιτείται σύμφωνα με τα στοιχεία πραγματικής χρήσης και τάσεων.
5	3	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	4	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
5	5	Διενεργούνται stress tests για την επιβεβαίωση της αποτελεσματικότητας των σχετικών προβλέψεων.

Κατηγορία		ΔΙΑΧΕΙΡΙΣΗ ΤΑΥΤΟΤΗΤΑΣ ΚΑΙ ΠΡΟΣΒΑΣΗΣ
IAM1		Μέτρο: Έλεγχος πρόσβασης βάσει ρόλου Στόχος Μέτρου: Να επαληθευτεί της η αυθεντικότητα και εξουσιοδότηση χρηστών, με βάση το ελάχιστο προνόμιο και τους οργανωτικούς ρόλους και αρμοδιότητες. Περιγραφή Μέτρου: Θέσπιση, εφαρμογή και διατήρηση μέτρων διαχείρισης ταυτότητας και πρόσβασης τα οποία εξετάζουν μέτρα πρόσβασης με βάση το ρόλο, με σκοπό να παρέχουν τεχνικά και οργανωτικά μέσα για την επιβολή της αρχής του ελάχιστου προνομίου και να διαχειρίζονται αντίστοιχα τους προνομιούχους χρήστες. Ο έλεγχος πρόσβασης βάσει ρόλου θα πρέπει να διασφαλίζει ότι χορηγούνται επαρκείς άδειες σε χρήστες με βάση τις αρμοδιότητες τους που συνδέονται με αντίστοιχους ρόλους. Ο έλεγχος πρόσβασης βάσει ρόλου θα πρέπει να γίνεται σύμφωνα με τις διαδικασίες ασφάλειας των ανθρώπινων πόρων, όπως ορίζεται στο [HRS1], προκειμένου να διασφαλιστεί ότι οι ρόλοι πρόσβασης είναι ευθυγραμμισμένοι με τους ρόλους και αρμοδιότητες των στελεχών στο πλαίσιο του οργανισμού. Πηγή:
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν διαχειρίζεται καθόλου την πρόσβαση στα συστήματά του.
1	1	Ο οργανισμός έχει συστήματα για την διαχείριση πρόσβασης στα συστήματα του.
2	1	Υπάρχει μια πολιτική ελέγχου πρόσβασης η οποία καλύπτει όλα τα στοιχεία ενεργητικού και τα κτήρια του οργανισμού όπως εμφανίζονται στον κατάλογο στοιχείων ενεργητικού σύμφωνα με το [AM2].
2	2	Η πολιτική ελέγχου πρόσβασης καλύπτει την πρόσβαση σε εφαρμογές, δίκτυα, πόρους και κτήρια.
3	1	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται μέτρα διαχείρισης ταυτότητας και πρόσβασης τα οποία εξετάζουν μέτρα πρόσβασης με βάση το ρόλο, με σκοπό να παρέχουν τεχνικά και οργανωτικά μέσα για την επιβολή της αρχής του ελάχιστου προνομίου και να διαχειρίζονται αντίστοιχα τους προνομιούχους χρήστες.
3	2	Ο έλεγχος πρόσβασης βάσει ρόλου διασφαλίζει ότι χορηγούνται επαρκείς άδειες σε χρήστες με βάση τις αρμοδιότητες τους που συνδέονται με αντίστοιχους ρόλους.
3	3	Ο έλεγχος πρόσβασης βάσει ρόλουγίνεται σύμφωνα με τις διαδικασίες ασφάλειας των ανθρώπινων πόρων, όπως ορίζεται στο [HRS1], προκειμένου να διασφαλιστεί ότι οι ρόλοι πρόσβασης είναι ευθυγραμμισμένοι με τους ρόλους και αρμοδιότητες των στελεχών στο πλαίσιο του οργανισμού.
3	4	Οι ιδιοκτήτες των πόρων προσδιορίζουν τα κατάλληλα δικαιώματα πρόσβασης και τους κανόνες πρόσβασης για τους ρόλους που πρέπει να έχουν πρόσβαση στους πόρους υπό την ευθύνη τους.
3	5	Ο προσδιορισμός στηρίζεται στην κρισιμότητα του πόρου, την ανάγκη πρόσβασης, την αρχή της ελάχιστης πρόσβασης και τα αποτελέσματα της ανάλυσης κινδύνου.
3	6	Ισχύουν οι ακόλουθες βασικές αρχές : 1) Οι λειτουργίες ασφαλείας είναι περιορισμένες στον ελάχιστο αριθμό χρηστών που είναι απαραίτητες για να εξασφαλίσουν την ασφάλεια των συστημάτων, 2) Αν ένας ρόλος δεν χρειάζεται να έχει πρόσβαση σε μια πληροφορία, τότε δεν πρέπει να έχει πρόσβαση, 3) Τηρείται διαχωρισμός καθηκόντων όπου είναι αυτό δυνατό.
3	7	Η πολιτική ελέγχου πρόσβασης περιγράφει ποιος (groups / entities / users / systems / services κλπ) μπορεί να έχει πρόσβαση σε ποια πληροφορία/ οντότητα / αντικείμενο / σύστημα /υπηρεσία / δίκτυο κ.α. και σε ποιο επίπεδο.
3	8	Διατηρείται μητρώο σχετικών λογαριασμών και οντοτήτων.
4	1	Γίνεται ανάθεση δικαιωμάτων βάσει ρόλου.
4	2	Υπάρχει μια ευθυγράμμιση μεταξύ των επιχειρηματικών ρόλων και των προφίλ ελέγχου πρόσβασης.
4	3	Η πολιτική περιλαμβάνει τη σχετική νομοθεσία και τυχόν συμβατικές υποχρεώσεις σχετικά με τον περιορισμό της πρόσβασης σε δεδομένα ή υπηρεσίες.
4	4	Διενεργείται τακτικός έλεγχος δικαιωμάτων πρόσβασης.
4	5	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Υπάρχει αυτοματοποιημένο σύστημα το οποίο ελέγχει την ύπαρξη λογαριασμών ή οντοτήτων εντός του οργανισμού που δεν είναι explicitly εξουσιοδοτημένος για συγκεκριμένες ενέργειες.

5	2	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	3	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
IAM2		Μέτρο: Έλεγχος εξωτερικής πρόσβασης Στόχος Μέτρου: Να εξασφαλιστούν επαρκή μέτρα στο πλαίσιο της εξωτερικής πρόσβασης σε οργανωτικούς πόρους.Περιγραφή Μέτρου: Θέσπιση, εφαρμογή και διατήρηση μέτρων ελέγχου πρόσβασης για εξωτερική και εξ αποστάσεως πρόσβαση σε οργανωτικούς πόρους. Ο οργανισμός θα πρέπει να διασφαλίζει τη δυνατότητα απομακρυσμένης πρόσβασης στο δίκτυο με τη χρήση εικονικών ιδιωτικών δικτύων (VPN) και την πρόσβαση σε εξ αποστάσεως εφαρμογές μέσω της χρήσης εξωτερικών εφαρμογών διεπαφών. Ο οργανισμός εφαρμόζει επαρκή μέτρα διαχείρισης ταυτότητας και πρόσβασης, ώστε να αντικατοπτρίζει την πολιτική ασφάλειας πληροφοριών, όπως ορίζεται στο [GOV3], και τον ειδικό έλεγχο πρόσβασης βάσει ρόλου, όπως ορίζεται στο μέτρο [IAM1]. Πηγή:
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν διαχειρίζεται με συγκεκριμένο οργανωμένο τρόπο την εξωτερική πρόσβαση σε όλους τους πόρους. Υπάρχει εξωτερική πρόσβαση σε κάποια συστήματα του οργανισμού αλλά ο τρόπος πρόσβασης δεν είναι καθορισμένος και δεν ακολουθεί μια συγκεκριμένη πολιτική.
1	1	Η εξωτερική πρόσβαση σε πόρους του οργανισμού δίνεται μετά από σχετική έγκριση από εξουσιοδοτημένο υπεύθυνο.
1	2	Ο υπεύθυνος τηρεί λίστα με τις εξωτερικές προσβάσεις που έχουν δοθεί ανά σύστημα.
1	3	Μπορεί για κάθε εξωτερική πρόσβαση να υπάρχει διαφορετικός τρόπος πρόσβασης και να εφαρμόζονται διαφορετικά μέτρα.
2	1	Υπάρχει πολιτική για την διαχείριση της εξωτερικής πρόσβασης σε πόρους του οργανισμού.
2	2	Υπάρχει σαφής ιδιοκτήτης της πολιτικής και έχουν καθοριστεί τα βήματα που ακολουθούνται για την ενεργοποίηση εξωτερικής πρόσβασης σε πόρους του οργανισμού.
2	3	Προκειμένου να αποδοθεί εξωτερική πρόσβαση στους πόρους, ακολουθείται διαδικασία έγκρισης από τον αναγνωρισμένο ιδιοκτήτη του πόρου.
3	1	Οι εξωτερικές προσβάσεις σε πόρους του οργανισμού είναι περιορισμένες και υπόκεινται σε αυστηρές διαδικασίες διαχείρισης και ελέγχου πρόσβασης.
3	2	Οι ρόλοι στους οποίους δίνεται το δικαίωμα εξωτερικής πρόσβασης είναι συγκεκριμένοι, διακριτοί και εξουσιοδοτημένοι κατάλληλα από τους ιδιοκτήτες των πόρων ή άλλους κατάλληλους ρόλους (που έχει ορίσει ο οργανισμός με βάσει την δομή και λειτουργία του).
3	3	Για την εξωτερική πρόσβαση χρησιμοποιείται πάντα κρυπτογράφηση.
3	4	Οι εξωτερικές συνδέσεις παρακολουθούνται (logged) αυτόματα από κατάλληλο σύστημα.
4	1	Η πρόσβαση υλοποιείται με MFA.
4	2	Η εξωτερική πρόσβαση γίνεται μέσα από συγκεκριμένες καθορισμένες πύλες πρόσβασης με υλοποιημένα αυστηρά πρωτόκολλα ασφαλείας.
4	3	Σε περίπτωση εξωτερικής πρόσβασης, πριν την διενέργεια της σύνδεσης, η συσκευή ελέγχεται για την συμμόρφωσή της με συγκεκριμένες πολιτικές ασφαλείας του οργανισμού (π.χ. antimalware, USB, firewall, password, applications κ.α.).
4	4	Οι ενέργειες πρόσβασης καταγράφονται (logged) ανεξάρτητα του επιπέδου χρήστη.
4	5	Ελέγχονται σε τακτά χρονικά διαστήματα οι καταγραφές (logs) για την επιβεβαίωση της συμμόρφωσης με την πολιτική ελέγχου πρόσβασης και την ανίχνευση πιθανών αποκλίσεων.
4	6	Αν είναι δυνατό, η διαδικασία αυτά υλοποιείται αυτόματα.
4	7	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Web application firewalls χρησιμοποιούνται για ολες τις εφαρμογές στις οποίες γίνεται πρόσβαση από το Web ή είναι κρίσιμες για τον οργανισμό.
5	2	Απευθείας απόμακρυσμένη πρόσβαση σε κρίσιμους πόρους δεν επιτρέπεται.
5	3	Έχει δημιουργηθεί κατάλληλη αρχιτεκτονική, με κατάλληλους διαχωρισμούς, ώστε να μπορεί να υπάρχει δυνατότητα πρόσβασης σε κρίσιμους πόρους σε περίπτωση ανάγκης χωρίς να επηρεάζεται η ασφάλεια του πόρου.
5	4	Ελέγχονται σε τακτά χρονικά διαστήματα οι καταγραφές (logs) για την επιβεβαίωση της συμμόρφωσης με την πολιτική ελέγχου πρόσβασης και την ανίχνευση πιθανών αποκλίσεων.

5	5	Κατάλληλοι συσχετισμοί / κανόνες και alerts έχουν υλοποιηθεί μέσα στα συστήματα, για την έγκαιρη ενημέρωση του οργανισμού.
5	6	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	7	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
IAM3		Μέτρο: Διαχείριση προνομιούχων χρηστώνΣτόχος Μέτρου: Να εξασφαλιστούν επαρκή μέτρα για τους χρήστες που έχουν προνομιακή πρόσβαση σε οργανωτικούς πόρους, συστήματα και δίκτυα.Περιγραφή Μέτρου: Θέσπιση, εφαρμογή και διατήρηση μέτρων για τη διασφάλιση της ορθής διαχείρισης των προνομιούχων χρηστών, και ενεργοποίηση τους μόνο όταν χρειάζεται. Ο οργανισμός διασφαλίζει ότι στους χρήστες δεν χορηγούνται προνομιακά δικαιώματα εξ ορισμού και ότι εφαρμόζονται κατάλληλα τεχνικά και οργανωτικά μέτρα για τη διασφάλιση της προστασίας των προνομιακών δικαιωμάτων των χρηστών από κακόβουλες πράξεις ή από άλλες αρνητικές συμπεριφορές ή προθέσεις. Ο οργανισμός διασφαλίζει ότι τα συστήματα και οι εφαρμογές δεν λειτουργούν εξ ορισμού με προνομιακά δικαιώματα χρήστη, προκειμένου να μετριάζεται ο κίνδυνος της κλιμάκωσης προνομίων. Πηγή:
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν έχει έλεγχο επί της διαδικασίας παραχώρησης προνομιακών δικαιωμάτων πρόσβασης σε πόρους, συστήματα και δίκτυα.
1	1	Για τους κρίσιμους πόρους, ο οργανισμός έχει περιορίσει το πλήθος των χρηστών που έχουν προνομιακή πρόσβαση σε πόρους, συστήματα και δίκτυα.
2	1	Έχει υλοποιηθεί συγκεκριμένη πολιτική ή και διαδικασία με την οποία γίνεται απόδοση προνομιακών δικαιωμάτων πρόσβασης στους χρήστες.
2	2	Τηρείται λίστα με όλους τους λογαριασμούς (χρηστών / service acccounts κλπ) που έχουν προνομιακή πρόσβαση σε πόρους, συστήματα και δίκτυα.
3	1	Έχει καταγραφεί πολιτική ή διαδικασία για την διαχείριση της προνομιακής πρόσβασης σε πόρους, συστήματα και δίκτυα.
3	2	Η πολιτική ή διαδικασία είναι συμβατή με τις επιχειρησιακές ανάγκες του οργανισμού και την πολιτική ελέγχου πρόσβασης του οργανισμού.
3	3	Τα δικαιώματα προνομιακής πρόσβασης αποδίδονται μόνο σε χρήστες σύμφωνα με την σχετική ανάγκη (need to use basis & event by event basis).
3	4	Οι λογαριασμοί των χρηστών που έχουν δικαιώματα προνομιακής πρόσβασης να είναι διαφορετικοί από αυτούς που χρησιμοποιούν για τις καθημερινές επιχειρησιακές δραστηριότητες τους.
4	1	Για τους λογαριασμούς που έχουν προνομιακή πρόσβαση σε πόρους, συστήματα και δίκτυα, υλοποιείται παρακολούθηση (logging) και εξασφαλίζεται ότι οι σχετικές καταγραφές δεν μπορούν να τροποιηθούν, απενεργοποιηθούν, διαγραφούν ή αλλοιωθούν από τους λογαριασμούς αυτούς.
4	2	Για τους λογαριασμούς με προνομιακή πρόσβαση υλοποιείται MFA, είτε οι πόροι βρίσκονται on-site είτε φιλοξενούνται από τρίτα μέρη.
4	3	Τηρείται λίστα με όλους τους λογαριασμούς (χρηστών / service acccounts κλπ) που έχουν προνομιακή πρόσβαση σε πόρους, συστήματα και δίκτυα.
4	4	Η λίστα περιέχει κατ΄ ελάχιστο τα ακόλουθα: πόρος, λογαριασμός, τύπος προνομιακής πρόσβασης, ημερομηνία εκχώρησης, ιδιοκτήτη πόρου, ημερομηνία ανασκόπησης, σκοπός.
4	5	Διενεργείται, τουλάχιστον κάθε τρίμηνο, ανασκόπηση των προνομιακών δικαιωμάτων για επικύρωση ότι όλοι οι ενεργοί λογαριασμοί είναι εξουσιοδοτημένοι.
4	6	Οι κωδικοί πρόσβασης των λογαριασμών προνομιακής πρόσβασης είναι γνωστοί μόνο στον ανατεθειμένο ιδιοκτήτη τους.
4	7	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Οι λογαριασμοί με προνομιακή πρόσβαση έχουν καθορισμένη πολιτική για την αλλαγή των κωδικών πρόσβασης.
5	2	Γενικοί λογαριασμοί προνομιακής πρόσβασης δεν χρησιμοποιούνται (εκτός από συγκεκριμένες περιπτώσεις στις οποίες δεν υπάρχει άλλη επιλογή).
5	3	Οι κωδικοί πρόσβασης για γενικούς λογαριασμούς προνομιακής πρόσβασης προστατεύονται και είναι προσβάσιμοι μόνο σε περίπτωση που απαιτείται σε συγκεκριμένα εξουσιοδοτημένα άτομα.

5	4	Η χρήση γενικών λογαριασμών προνομιακής πρόσβασης παρακολουθείται (logged) ενώ υπάρχει αυτόματο σύστημα το οποίο ενημερώνει το εξουσιοδοτημένο προσωπικό σχετικά με την χρήση του.
5	5	Τέτοιες περιπτώσεις διαχειρίζονται ως πιθανά περιστατικά ασφαλείας και ενεργοποιείται η αντίστοιχη διαδικασία διαχείρισης περιστατικών ασφαλείας.
5	6	Σε περίπτωση ανάγκης χρήσης γενικών λογαριασμών προνομιακής πρόσβασης, ακολουθείται η διαδικασία διαχείρισης αλλαγών (έκτακτων ή προγραμματισμένων) και δεν χρησιμοποιούνται μέχρι να ολοκληρωθεί η σχετική εξουσιοδότηση.
5	7	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	8	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
IAM4		Μέτρο: Ισχυρά μέτρα για επαλήθευση ταυτότητας Στόχος Μέτρου: Να εξασφαλιστεί ότι γίνεται επαλήθευση της ταυτότητας των εξουσιοδοτημένων ατόμων με ασφάλεια και με τη χρήση μέτρων ισχυρής επαλήθευσης ταυτότητας.Περιγραφή Μέτρου: Θέσπιση, εφαρμογή και διατήρηση ισχυρών μέτρων ελέγχου πρόσβασης και επαλήθευσης της ταυτότητας, προκειμένου να διασφαλίζεται ότι τα εξουσιοδοτημένα άτομα αναγνωρίζονται δεόντως και γίνεται επαλήθευση της ταυτότητας τους κατά την επεξεργασία οργανωτικών πόρων. Ο οργανισμός πρέπει να εξετάσει την επαλήθευση μέσω πολλών παραγόντων προκειμένου να αποδείξει την ταυτότητά ενός ατόμου. Η διαδικασία αυτή πρέπει να περιλαμβάνει τουλάχιστον δύο από τις ακόλουθες αρχές: παροχή ταυτότητας με την κατοχή συγκεκριμένου στοιχείου (π.χ. κλειδί ή άλλο μέσο εξακρίβωσης της ταυτότητας), με τη γνώση ενός στοιχείου (π.χ. κωδικός ή φράση πρόσβασης, ή άλλο μυστικό), με βιομετρικά ή μορφολογικά χαρακτηριστικά (π.χ. σάρωση ίριδας, αποτύπωμα δακτύλου ή οπτική επαλήθευση ταυτότητας από ένα αξιόπιστο μέρος, όπως έναν φρουρό ασφαλείας). Πηγή:
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν έχει υλοποιήσει κάποια συγκεκριμένη / οργανωμένη πολιτική για τον τρόπο με τον οποίο γίνεται η επαλήθευση της ταυτότητας των λογαριασμών πρόσβασης.
1	1	Γίνεται αυθεντικοποίηση της πρόσβασης στα περισσότερα συστήματα του οργανισμού αλλά δύναται να υπάρχουν και κάποιες λειτουργίες (κυρίως εντός δικτύου του οργανισμού) που δεν απαιτείται αυθεντικοποίηση.
2	1	Η επιλογή των μηχανισμών αυθεντικοποίησης (επαλήθευσης της ταυτότητας των εξουσιοδοτημένων ατόμων) γίνεται ως αποτέλεσμα σχετικής διαδικασίας ανάλυσης διακινδύνευσης. (Διαφορετικής κρισιμότητας συστήματα μπορεί να απαιτούν διαφορετικού επιπέδου μέτρα επαλήθευσης ταυτότητας.)
2	2	Η ταυτότητα όλων των χρηστών, διεργασιών, πόρων επαληθεύεται ως προαπαιτούμενο για την παραχώρηση πρόσβασης.
3	1	Έχει καταγραφεί πολιτική ή διαδικασία για την διαχείριση του επαλήθευσης ταυτότητας.
3	2	Η πολιτική ή διαδικασία είναι συμβατή με τις επιχειρησιακές ανάγκες του οργανισμού και την πολιτική ελέγχου πρόσβασης του οργανισμού. (μπορεί να αποτελεί και μέρος της τελευταίας).
3	3	Η πολιτική περιέχει τις κατηγορίες μηχανισμών αυθεντικοποίησης που μπορούν να χρησιμοποιούνται ανά κρισιμότητα συστήματος (π.χ. Single-Sign-On, two-factor authentication, multi-factor authentication κ.α.) τόσο για τους πόρους όσο και για τα δίκτυα (περιλαμβανομένων των remote & wifi) και τις άλλες λειτουργίες (εφαρμογές κ.α.).
3	4	Οι χρήστες και τα συστήματα έχουν μοναδικά αναγνωριστικά και αυθεντικοποιούνται πριν την πρόσβασή στους στις υπηρεσίες και τα συστήματα.
3	5	Το σύστημα αυθεντικοποίησης είναι προστατευμένο έναντι brute force log-on attempts και καταγράφει τις επιτυχημένες και αποτυχημένες προσπάθειες.
3	6	Εφαρμόζεται επαλήθευση μέσω πολλών παραγόντων προκειμένου να αποδειχθεί η ταυτότητά ενός ατόμου.
3	7	Η διαδικασία αυτή περιλαμβάνει τουλάχιστον δύο από τις ακόλουθες αρχές: παροχή ταυτότητας με την κατοχή συγκεκριμένου στοιχείου (π.χ. κλειδί ή άλλο μέσο εξακρίβωσης της ταυτότητας), με τη γνώση ενός στοιχείου (π.χ. κωδικός ή φράση πρόσβασης, ή άλλο μυστικό), με βιομετρικά ή μορφολογικά χαρακτηριστικά (π.χ. σάρωση ίριδας, αποτύπωμα δακτύλου ή οπτική επαλήθευση ταυτότητας από ένα αξιόπιστο μέρος, όπως έναν φρουρό ασφαλείας).
4	1	Οι προκαθορισμένοι λογαριασμοί (λειτουργιών ή κατασκευαστών) απενεργοποιούνται ή μετονομάζονται όπου αυτό είναι δυνατό.
4	2	Για κάθε έναν από τους μηχανισμούς αυθεντικοποίησης έχει προδιαγραφεί και καταγραφεί ο τρόπος λειτουργίας.

4	3	Ειδικά για την περίπτωση χρήσης κωδικών πρόσβασης, υπάρχει καταγεγραμμένη πολιτική κωδικών πρόσβασης με συγκεκριμένες προβλέψεις για πολυπλοκότητα κωδικών, μοναδικότητα / επαναχρησιμοποίηση κωδικών, προσωρινών κωδικών, invalid logon attempts κ.α.
4	4	Οι κωδικοί πρόσβασης προστατεύονται όπου και αν βρίσκονται μέσω κρυπτογράφησης.
4	5	Σε περίπτωση χρήσης άλλων ή επιπλέον μηχανισμών (π.χ. authenticators, one time passwords κλπ), προσδιορίζεται ακριβώς το επίπεδο ασφαλείας των συγκεκριμένων μηχανισμών ανά περίπτωση και συμφωνεί με τα αποτελέσματα της ανάλυσης διακινδύνευσης.
4	6	Ο έλεγχος ταυτότητας είναι replay resistant (Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.)
4	7	Οι πληροφορίες ανταπόκρισης από τα συστήματα ελέγχου ταυτότητας είναι τέτοιες που δεν παρέχουν πληροφορίες που μπορεί να εκμεταλλευτούν από κακόβουλους χρήστες.
4	8	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Ο οργανισμός χρησιμοποιεί port level access control, ακολουθόντας τα πρότυπα 802.1x, και ελέγχει ποιες συσκευές μπορούν να αυθεντικοποιούνται στο δίκτυο.
5	2	Το σύστημα για την αυθεντικοποίηση συνδέεται με τα δεδομένα της φυσικής λίστας πόρων (hardware asset inventory) ώστε να εξασφαλίζεται ότι μόνο εξουσιοδοτημένες συσκευές μπορούν να συνδεθούν στο δίκτυο.
5	3	Ανασκοπήσεις των καταγραφών (logs) που προκύπτουν από την λειτουργία των συστημάτων ελέγχου ταυτότητας γίνονται αυτόματα και ενημερώνεται το εξουσιοδοτημένο προσωπικό σε περίπτωση ανίχνευσης κάποιου κινδύνου ή τάσης.
5	4	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	5	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
IAM5		Μέτρο: Διαχείριση διαπιστευτηρίων Στόχος Μέτρου: Να διασφαλιστεί ασφαλής διαχείριση διαπιστευτηρίων για πρόσβαση σε εταιρικούς πόρους, και ότι επαληθεύεται η ταυτότητα των χρηστών με ασφάλεια για χρήση υπηρεσιών του οργανισμού. Περιγραφή Μέτρου: Θέσπιση, εφαρμογή και διατήρηση διαδικασιών διαχείρισης διαπιστευτηρίων για να εξασφαλίζεται η κατάλληλη διαχείριση των μέσων ταυτοποίησης και επαλήθευσης με τα οποία οι χρήστες μπορούν να έχουν πρόσβαση σε οργανωτικούς πόρους. Ο οργανισμός θα πρέπει να εξετάσει τη χρήση ομαδοποιημένων διαπιστευτηρίων (π.χ. single sign-on) προκειμένου να βελτιώσει την εμπειρία του χρήστη σε θέματα ταυτοποίησης και πρόσβασης. Ο οργανισμός πρέπει να εξετάσει τη διαχείριση διαπιστευτηρίων για τους χρήστες, τα συστήματα και τα δίκτυα προκειμένου να διασφαλίσει τον έλεγχο της πρόσβασης καθ' όλη τη διάρκεια του κύκλου ζωής πληροφοριών, όπως ορίζεται στο μέτρο [DS1]. Πηγή:
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Δεν υπάρχει δομημένος / οργανωμένος τρόπος για την διαχείριση διαπιστευτηρίων για πρόσβαση σε πόρους, συστήματα και δίκτυα. Μπορεί ανά περίπτωση κάποια συστήματα να έχουν κωδικούς πρόσβασης αλλά δεν υπόκειται σε κάποια πολιτική.
1	1	Η πρόσβαση σε κρίσιμους πόρους προστατεύεται με χρήση διαπιστευτηρίων.
1	2	Τα διαπιστευτήρια είναι τουλάχιστον 8 χαρακτήρων για τους απλούς χρήστες και τουλάχιστον 14 για τους χρήστες προνομιακής πρόσβασης.
2	1	Η επιλογή των μηχανισμών αυθεντικοποίησης (επαλήθευσης της ταυτότητας των εξουσιοδοτημένων ατόμων) γίνεται ως αποτέλεσμα σχετικής διαδικασίας ανάλυσης διακινδύνευσης. (Διαφορετικής κρισιμότητας συστήματα μπορεί να απαιτούν διαφορετικού επιπέδου μέτρα επαλήθευσης ταυτότητας.)
2	2	Η ταυτότητα όλων των χρηστών, διεργασιών, πόρων επαληθεύεται ως προαπαιτούμενο για την παραχώρηση πρόσβασης.
3	1	Έχει δημιουργηθεί μια καταγεγραμμένη διαδικασία διαχείρισης διαπιστευτηρίων και εξασφαλίζεται η κατάλληλη διαχείριση των μέσων ταυτοποίησης και επαλήθευσης με τα οποία οι χρήστες έχουν πρόσβαση σε οργανωτικούς πόρους.
3	2	Οι απαιτήσεις προστασίας των διαπιστευτηρίων από τους χρήστες έχουν επικοινωνηθεί από τον οργανισμό σε όλο το εμπλεκόμενο προσωπικό.
3	3	Ειδικές ενέργειες διενεργούνται για τον έλεγχο της αποτελεσματικότητας της συγκεκριμένης επικοινωνίας.

3	4	Σε περίπτωση χρήσης κωδικών πρόσβασης, οι κωδικοί είναι πολύπλοκοι, αλλάζουν με κάποια περιοδικότητα, δεν χρησιμοποιούνται σε πολλαπλά συστήματα και αποθηκεύονται κρυπτογραφημένοι.
3	5	Το σύστημα προστατεύεται έναντι πολλαπλών προσπαθειών αποτυχημένης πρόσβασης.
4	1	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
4	2	Υλοποιήθηκε χρήση ομαδοποιημένων διαπιστευτηρίων (π.χ. single sign-on) προκειμένου να βελτιωθεί η εμπειρία του χρήστη σε θέματα ταυτοποίησης και πρόσβασης.
4	3	Υλοποιήθηκε ένα διαδραστικό σύστημα για την εξασφάλιση της αυτόματης συμμόρφωσης των διαπιστευτηρίων με την σχετική πολιτική.
4	4	Σε περίπτωση χρήσης MFA, προσδιορίζεται ο τύπος της μεθόδου αυθεντικοποίησης και η σχετική του ασφάλεια.
5	1	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	2	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
IAM6		Μέτρο: Ιχνηλασιμότητα και έλεγχος Στόχος Μέτρου: Να διασφαλιστεί η μη-άρνηση ανιχνευσιμότητας των ενεργειών των χρηστών που εκτελούνται στο πλαίσιο των οργανωτικών πόρων, ώστε να είναι δυνατή η ανίχνευση και η διερεύνηση εκούσιων ή ακούσιων δραστηριοτήτων που έχουν αρνητικό αντίκτυπο Περιγραφή Μέτρου: Θέσπιση, εφαρμογή και διατήρηση μέτρων διαχείρισης ταυτότητας και πρόσβασης για τη διασφάλιση της χρονολογικής ιχνηλασιμότητας και της ικανότητας ελέγχου, ώστε να ανατίθεται ευθύνη στους χρήστες που εκτελούν εντολές σε συστήματα επεξεργασίας πληροφοριών. Ο φορέας εξετάζει μέτρα που διασφαλίζουν τη μη- άρνηση από χρήστες. Ο οργανισμός πρέπει να εξετάζει τη δυνατότητα ιχνηλασιμότητας και ελέγχου στο πλαίσιο της διαχείρισης ταυτότητας και πρόσβασης που ισχύει για τα συστήματα, τις εφαρμογές και τα δίκτυα. Πηγή:
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Δεν υπάρχει οργάνωση στην παρακολούθηση των ενεργειών των χρηστών. Τα συστήματα μπορεί ανά περίπτωση να δημιουργούν κάποιες εγγραφές παρακολούθησης ενεργειών αλλά δεν ορίζονται τα χαρακτηριστικά τους και δεν ελέγχονται χειροκίνητα ή αυτόματα.
1	1	Τα συστήματα δημιουργούν, ανά περίπτωση, κάποιες εγγραφές παρακολούθησης ενεργειών, μετά από σχετική παρέμβαση του εξουσιοδοτημένου ιδιοκτήτη πόρου (ή του authorized custodian - π.χ. IT) σε ad-hoc βάση.
2	1	Έχει δημιουργηθεί μια καταγεγραμμένη πολιτική, η οποία ορίζει σε ποια συστήματα γίνεται παρακολούθηση και καταγραφή ενεργειών (logs).
2	2	Η έκταση της παρακολούθησης και καταγραφής ενεργειών προκύπτει από τα αποτελέσματα σχετικής ανάλυσης διακινδύνευσης που διενεργείται με ευθύνη των ιδιοκτητών πόρων.
2	3	Τα βασικά χαρακτηριστικά που καθορίζονται είναι: είδος καγραφής, χρονικό διάστημα διατήρησης, μέσο διατήρησης.
2	4	Καταγραφή ενεργειών που σχετίζονται με την ασφάλεια είναι ενεργοποιημένη κατ΄ελάχιστο στα κρίσιμα συστήματα.
3	1	Καταγραφή ενεργειών που σχετίζονται με την ασφάλεια είναι ενεργοποιημένη σε όλα τα συστήματα.
3	2	Οι εξωτερικές συνδέσεις παρακολουθούνται (logged) αυτόματα από κατάλληλο σύστημα.
3	3	Το σύστημα αυθεντικοποίησης καταγράφει τις επιτυχημένες και απότυχημένες προσπάθειες.
3	4	Στις σχετικές καταγραφές δεν φαίνεται το password ή άλλο μυστικό στοιχείο αυθεντικοποίησης που έχει χρησιμοποιηθεί / εισαχθεί σε κάθε περίπτωση προσπάθειας πρόσβασης.
4	1	Οι ενέργειες πρόσβασης καταγράφονται (logged) ανεξάρτητα του επιπέδου χρήστη.
4	2	Ελέγχονται σε τακτά χρονικά διαστήματα οι καταγραφές (logs) για την επιβεβαίωση της συμμόρφωσης με την πολιτική ελέγχου πρόσβασης και την ανίχνευση πιθανών απόκλίσεων. Όπου είναι δυνατό, η διαδικασίαυλοποιείται αυτόματα.
4	3	Για τους λογαριασμούς που έχουν προνομιακή πρόσβασης σε πόρους, συστήματα και δίκτυα, υλοποιείται παρακολούθηση (logging) και εξασφαλίζεται ότι οι σχετικές καταγραφές δεν μπορούν να τροποιηθούν, απενεργοποιηθούν, διαγραφούν ή αλλοιωθούν από τους λογαριασμούς αυτούς.

4	4	Το χρονικό διάστημα διατήρησης των σχετικών καταγραφών είναι τουλάχιστον για 3 μήνες ανά σύστημα. Σε περίπτωση που αυτό δεν είναι τεχνικά εφικτό, υπάρχει ένας μηχανισμός για την δημιουργία εξαίρεσης από την σχετική πολιτική.
4	5	Η έγκριση της εξαίρεσης ακολουθεί την διαδικασία ελέγχου αλλαγών.
4	6	Η αίτηση για εξαίρεση αναφέρει τους τρόπους με τους οποίους ο σχετικός κίνδυνος μειώνεται μέσω άλλων αντισταθμιστικών μέτρων.
4	7	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Κατάλληλα παραμετροποιημενα συστήματα intrusion detection/prevention και anomaly detection systems έχουν υλοποιηθεί.
5	2	Οι σχετικές καταγραφές διατηρούνται κατ' ελάχιστον ένα έτος.
5	3	Ειδικά κάποιες κατηγορίες (π.χ. χρήση λογαριασμών προνομιακής πρόσβασης σε κρίσιμα συστήματα)αρχειοθετούνται για μεγαλύτερο χρονικό διάστημα, λαμβάνοντας υπόψη και τις απαιτήσεις σχετικής νομοθεσίας όπου υπάρχει.
5	4	Η πρόσβαση στα συστήματα αυτά είναι ελεγχόμενη και περιορισμένη.
5	5	Τα δεδομένα καταγραφών χαρακτηρίζονται εμπιστευτικά σύμφωνα με το σχέση διαβάθμισης πληροφοριών του οργανισμού και χειρίζονται αντίστοιχα.
5	6	Αντίγραφα ασφαλείας των δεδομένων καταγραφών λαμβάνονται σύμφωνα με τις προδιαγραφές της σχετικής πολιτικής αντιγράφων ασφαλείας, της αξιολόγησης διακινδύνευσης και της κρισιμότητας του πόρου.
5	7	Ελέγχονται αυτόματα σε τακτά χρονικά διαστήματα οι καταγραφές (logs) για την επιβεβαίωση της συμμόρφωσης με την πολιτική ελέγχου πρόσβασης και την ανίχνευση πιθανών αποκλίσεων.
5	8	Κατάλληλοι συσχετισμοί / κανόνες και alerts έχουν υλοποιηθεί μέσα στα συστήματα για την έγκαιρη ενημέρωση του οργανισμού.
5	9	Η χρήση γενικών λογαριασμών προνομιακής πρόσβασης παρακολουθείται (logged) ενώ υπάρχει αυτόματο σύστημα το οποίο ενημερώνει το εξουσιοδοτημένο προσωπικό σχετικά με την χρήση του. Τέτοιες περιπτώσεις διαχειρίζονται ως πιθανά περιστατικά ασφαλείας και ενεργοποιείται η αντίστοιχη διαδικασία διαχείρισης περιστατικών ασφαλείας.
5	10	Ανασκοπήσεις των καταγραφών (logs) που προκύπτουν από την λειτουργία των συστημάτων ελέγχου ταυτότητας γίνονται αυτόματα και ενημερώνεται το εξουσιοδοτημένο προσωπικό σε περίπτωση ανίχνευσης κάποιου κινδύνου ή τάσης.
5	11	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	12	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
IAM7		Μέτρο: Διαχείριση του κύκλου ζωής της ταυτότηταςΣτόχος Μέτρου: Να διασφαλιστεί ότι οι ρόλοι και η έγκριση της ταυτότητας αντικατοπτρίζουν τον κύκλο ζωής της ταυτότητας του χρήστη.Περιγραφή Μέτρου: Θέσπιση, εφαρμογή και διατήρηση επαρκών μέτρων διαχείρισης ταυτότητας και πρόσβασης καθ' όλη τη διάρκεια του κύκλου ζωής της ταυτότητας, που περιλαμβάνει μεταξύ άλλων, παροχή, επαλήθευση της ταυτότητας, έγκριση και αφαίρεση ταυτοτήτων. Οι έλεγχοι για τη διαχείριση του κύκλου ζωής της ταυτότητας θα πρέπει να ενσωματωθούν στις διαδικασίες ασφάλειας περί ανθρώπινων πόρων, όπως ορίζεται στο μέτρο [HRS1], προκειμένου να διασφαλιστεί ότι οι ρόλοι πρόσβασης ευθυγραμμίζονται με τον κύκλο ζωής της εργοδότησης των στελεχών μέσα στον οργανισμό. Πηγή:
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Δεν υπάρχει ένας οργανωμένος / δομημένος τρόπος με τον οποίο γίνεται η διαχείριση των χρηστών. Υπάρχουν ανά σύστημα λογαριασμοί πρόσβασης και εκχωρούνται σε χρήστες αλλά δεν υπάρχει κάποια βασική δομή, έλεγχος ή δυνατότητα επιβεβαίωσης για τους λογαριασμούς.
1	1	Η δημιουργία λογαριασμών και η παραχώρηση πρόσβασης σε πόρους του οργανισμού δίνεται μετά από σχετική έγκριση από εξουσιοδοτημένο υπεύθυνο.
1	2	Ο υπεύθυνος τηρεί λίστα με τους λογαριασμούς που έχουν δημιουργηθεί ανά σύστημα.
1	3	Αντίστοιχα σε περίπτωση αποχώρησης, γίνονται κατάλληλες ενέργειες κατάργησης / απενεργοποίησης λογαριασμών από το σχετικά εξουσιοδοτημένο προσωπικό.
2	1	Υπάρχει πολιτική / διαδικασία για την δημιουργία λογαριασμών και την διαχείριση της πρόσβασης σε πόρους του οργανισμού. (Η πολιτική / διαδικασία καλύπτει τόσο στην εγγραφή όσο και την απεγράφη λογαριασμών (registration and deregistration)).

2	2	Υπάρχει σαφής ιδιοκτήτης της πολιτικής και έχουν καθοριστεί τα βήματα που ακολουθούνται για την ενεργοποίηση λογαριασμών και πρόσβασης σε πόρους του οργανισμού.
2	3	Προκειμένου να αποδοθεί πρόσβαση στους πόρους, ακολουθείται διαδικασία έγκρισης από τον αναγνωρισμένο ιδιοκτήτη του πόρου.
2	4	Για κάθε σχετική με λογαριασμούς και δικαιώματα πρόσβασης κίνηση τηρείται η αντίστοιχη καταγραφή.
2	5	Τηρείται μια κεντρική λίστα με τους λογαριασμούς χρηστών στα συστήματα του οργανισμού.
2	6	Υπάρχει αντίστοιχα λίστα και με τα δικαιώματα των λογαριασμών.
3	1	Υπάρχει καταγεγραμμένη πολιτική / διαδικασία για την διαχείριση των λογαριασμών εντός των συστημάτων, των πόρων και των δικτύων.
3	2	Η πολιτική / διαδικασία περιέχει ενέργειες που γίνονται για την δημιουργία, τροποποίηση, ανασκόπηση, απενεργοποίηση και διαγραφή των λογαριασμών.
3	3	Η διαδικασία αναγνωρίζει συγκεκριμένους ρόλους εντός του οργανισμού που διενεργούν τις αντίστοιχες ενέργειες.
3	4	Σύμφωνα με τις απαιτήσεις και τον τρόπο λειτουργίας έχει καθοριστεί ένα σύνολο ρόλων, οι οποίοι στην συνέχεια έχουν συσχετιστεί με δικαιώματα πρόσβασης σε πόρους, συστήματα και δίκτυα.
3	5	Κατά τη διάρκεια της εγγραφής ενός νέου λογαριασμού, στην σχετική αίτηση περιλαμβάνεται: το είδος του λογαριασμού (απλός, προνομιακός, άλλες κατηγορίες σύμφωνα με τις ανάγκες του οργανισμού), ο ιδιοκτήτης του λογαριασμού, η ημερομηνία ενεργοποίησης, ο ρόλος, η διάρκεια (όπου εφαρμόζεται).
3	6	Οι λειτουργίες που αφορούν την διαχείριση λογαριασμών είναι ενσωματωμένες και ευθυγραμμισμένες με τις διαδικασίες ασφάλειας περί ανθρωπίνων πόρων όπως περιγράφονται στο HRS1, ώστε εξασφαλίζεται ότι οι ρόλοι πρόσβασης και οι λογαριασμοί είναι ευθυγραμμισμένοι με τον κύκλο ζωής της εργοδότηρηση των αντίστοιχων οντοτήτων (προσωπικό, εξωτερικοί συνεργάτες κλπ).
3	7	Κάθε φορά που γίνεται αλλαγή (υποβάθμιση, αναβάθμιση, μετακίνηση) ατόμου σε θέση εργασίας, ενεργοποιείται και αλλαγή / ανασκόπηση των δικαιωμάτων πρόσβασης.
3	8	Η ανασκόπηση των λογαριασμών χρηστών γίνεται τουλάχιστον ad-hoc.
4	1	Οι λογαριασμοί που υπάρχουν στα διάφορα συστήματα ανασκοπούνται κατ' ελάχιστο μια φορά το τρίμηνο και μετά από μεγάλες αλλαγές.
4	2	Λογαριασμοί οι οποίοι είναι ανενεργοί για περισσότερες από 90 ημέρες απενεργοποιούνται.
4	3	Οι διαδικασίες για την απενεργοποίηση ή κατάργηση λογαριασμών είναι όσο γίνεται πιο αυτόματες.
4	4	Σε περίπτωση που αναγνωριστεί κάποια απόκλιση, καταγράφεται άμεσα και ενεργοποιείται η διαδικασία ανταπόκρισης σε περιστατικά ασφαλείας.
4	5	Όπου είναι δυνατό,οι λογαριασμοί απενεργοποιούνται μετά από αλλαγή των συνθηματικών πρόσβασης και αφαίρεσης των σχετικών δικαιωμάτων. Σε περίπτωση που αυτό δεν είναι εφικτό, διαγράφονται. (Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor. Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.)
4	6	Οι διαδικασίες της απόδοσης αλλά και της ανασκόπησης λογαριασμών και δικαιωμάτων αφορούν τόσο την λογική όσο και την φυσική πρόσβαση. Λογαριασμοί που ανήκαν ή είχαν αποδοθεί προηγούμενα, δεν εκχωρούνται σε άλλους χρήστες.
4	7	Για κάθε ενέργεια αλλαγής που σχετίζεται με τον κύκλο ζωής ενός λογαριασμού, τηρείται σχετικό ιστορικό και ακριβές timestamp.
4	8	Οι ενέργειες που διενεργούνται στα πλαίσια της διαχείρισης λογαριασμών, υλοποιούνται από ρόλους και άτομα που δεν θα έχουν σύγκρουση συμφερόντων.
4	9	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Η διαδικασία ανασκόπησης και διαχείρισης λογαριασμών είναι αυτοματοποιημένη και συνεχής.
5	2	Τηραούνται τα κατάλληλα τεχνικά μέτρα ώστε το σύνολο του κύκλου ζωής ενός λογαριασμού λειτουργεί με ελάχιστη ανθρώπινη παρέμβαση.
5	3	Τουλάχιστον μια φορά το τρίμηνο, διενεργείται τεχνική αξιολόγηση της απότελεσματικότητας λειτουργίας του αυτοματοποιημένου μηχανισμού διαχείρισης λογαριασμών.
5	4	Οι ενέργειες που διενεργούνται για τους σχετικούς ελέγχους, υλοποιούνται από ρόλους και άτομα που δεν έχουν σύγκρουση συμφερόντων.
5	5	Οι διαδικασίες αφορούν το σύνολο των συστημάτων, δικτύων, πόρων του οργανισμού.

5	6	Σε περίπτωση που δεν μπορεί να ενταχθεί κάποιο σύστημα, δίκτυο ή πόρος στην αυτόματη διαδικασία, υπάρχει μηχανισμός για την δημιουργία εξαίρεσης από την σχετική διαδικασία.
5	7	Η έγκριση της εξαίρεσης ακολουθεί την διαδικασία ελέγχου αλλαγών.
5	8	Η αίτηση για εξαίρεση αναφέρει τους τρόπους με τους οποίους ο σχετικός κίνδυνος μειώνεται μέσω άλλων αντισταθμιστικών μέτρων. .
5	9	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	10	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.

Κατηγορία		ΔΙΑΧΕΙΡΙΣΗ ΕΥΠΑΘΕΙΩΝ ΚΑΙ ΕΝΗΜΕΡΩΣΕΩΝ ΑΣΦΑΛΕΙΑΣ
VM1		Μέτρο: Ανίχνευση και εντοπισμός ευπαθειών Στόχος Μέτρου: Να διασφαλιστεί ότι οι ευπάθειες συστημάτων είναι γνωστές στον οργανισμό, προκειμένου να τύχουν κατάλληλου χειρισμού. Περιγραφή Μέτρου: Κατάρτιση, εφαρμογή και διατήρηση σχεδίου και προσέγγισης βάσει του κινδύνου για τη δοκιμή εφαρμογών, συστημάτων και δικτύων για ευπάθειες και αδυναμίες, οι οποίες θα μπορούσαν να τύχουν εκμετάλλευσης από απειλές. Ο οργανισμός θα πρέπει να εξετάζει την ανίχνευση για τον εντοπισμό ευπαθειών που προκύπτουν από νέες ή τροποποιημένες διαδικασίες ή συστήματα στα πλαίσια επεξεργασίας πληροφοριών. Οι ευπάθειες πρέπει να ανιχνεύονται και να εντοπίζονται στο πλαίσιο των απειλών κατά της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών. Ο οργανισμός θα πρέπει να εξετάζει το ενδεχόμενο διενέργειας δοκιμών διείσδυσης, ως μέσο για την ανίχνευση και τον εντοπισμό ευπαθειών. Τα αποτελέσματα των προσπαθειών ανίχνευσης και εντοπισμού ευπαθειών θα πρέπει να καταγράφονται όπως περιγράφεται στο μέτρο [VM2]. Πηγή:
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν υλοποιεί καμία ενέργεια για την ανίχνευση και εντοπισμό ευπαθειών.
1	1	Υλοποιούνται διορθωτικές ενέργειες έναντι ευπαθειών ως αντίδραση (reactive) και τουλάχιστον ad-hoc τρόπο ή/και συνήθως χωρίς να είναι πρωτοβουλία του οργανισμού (π.χ. εφαρμογή αυτοματοποιημένων security updates).
2	1	Έχουν ενεργοποιηθεί μηχανισμοί και δημιουργηθεί επαφές για την λήψη έγκαιρης πληροφόρησης για την ανίχνευσης και εντοπισμό των ευπαθειών στα κρίσιμα συστήματα.
3	1	Έχει θεσπιστεί, εφαρμόζεται και διατηρείται σχέδιο και προσέγγιση βάσει του κινδύνου για τη δοκιμή εφαρμογών, συστημάτων και δικτύων για ευπάθειες και αδυναμίες, οι οποίες μπορούν να τύχουν εκμετάλλευσης από απειλές.
3	2	Εξετάζεται η ανίχνευση για τον εντοπισμό ευπαθειών που προκύπτουν από νέες ή τροποποιημένες διαδικασίες ή συστήματα στα πλαίσια επεξεργασίας πληροφοριών.
3	3	Οι ευπάθειες ανιχνεύονται και εντοπίζονται στο πλαίσιο των απειλών κατά της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών.
3	4	Τα αποτελέσματα των προσπαθειών ανίχνευσης και εντοπισμού ευπαθειών καταγράφονται όπως περιγράφεται στο μέτρο [VM2].
4	1	Έχουν υιοθετηθεί αυτοματοποιημένες μεθόδοι και εργαλεία για την ανίχνευση και εντοπισμό ευπαθειών.
4	2	Η ανίχνευση και εντοπισμός ευπαθειών στο εσωτερικό του οργανισμού γίνεται τουλάχιστον ανά τρίμηνο, είναι authenticated ή και unauthenticated ενώ τα εργαλεία είναι συμβατά με διεθνείς βέλτιστες πρακτικές όπως είναι το SCAP.
4	3	Η ανίχνευση και εντοπισμός ευπαθειών στα συστήματα του οργανισμού που είναι εκτεθειμένα εξωτερικά, διενεργούνται τουλάχιστον μια φορά το μήνα, ενώ τα εργαλεία είναι συμβατά με διεθνείς βέλτιστες πρακτικές όπως είναι το SCAP.
4	4	Η καταγραφή των ευπαθειών γίνεται σύμφωνα με το [VM2] ενώ η αντιμετώπιση τους γίνεται σύμφωνα με το [VM3].
4	5	Ο οργανισμός έχει εγγραφεί σε υπηρεσίες διαμοιρασμού πληροφοριών σχετικά με τις ευπάθειες προκειμένου να παραμένει ενήμερος για νέα θέματα. Πληροφορίες οι οποίες έχουν ληφθεί με αυτόν τον τρόπο, χρησιμοποιούνται για τον καλύτερο σχεδιασμό και λειτουργία της διαδικασίας και των μηχανισμών ανίχνευσης και εντοπισμού ευπαθειών.
4	6	Τα στοιχεία ευπαθειών αποτελούν εισερχόμενο στην διαδικασία της διαχείρισης κινδύνων.
4	7	Χρησιμοποιούνται έγκυρες πηγές αναγνώρισης ευπαθειών προκειμένου να υπάρχει πρόσβαση σε στοιχεία επαλήθευσης και κατηγοριοποίησης.
4	8	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Ο οργανισμός συμμετέχει και λαμβάνει έγκυρες πληροφορίες Cyber threat intelligence οι οποίες μεταξύ άλλων χρησιμοποιούνται για την επικαιροποίηση του καταλόγου απειλών, ευπαθειών και κινδύνων στους οποίους είναι εκτεθειμένος ο οργανισμός σύμφωνα με το [RM3] και το [VM2].
5	2	Διενεργείται από εξωτερικό ανεξάρτητο μέρος αξιολόγηση ευπαθειών (vulnerability assessment) σε τακτά χρονικά διαστήματα, καλύπτοντας όλα τα κρίσιμα συστήματα του οργανισμού σύμφωνα με την σχετική ανάλυση κρισιμότητας όπως προβλέπεται στο [DS2].

5	3	Διενεργούνται δοκιμές διείσδυσης, ως μέσο για την ανίχνευση και τον εντοπισμό ευπαθειών.
5	4	Τα δεδομένα των vulnerability assessments χρησιμοποιούνται ως σημείο εκκίνησης για την καλύτερη στόχευση των ενεργειών παρείσδυσης.
5	5	Οι δοκιμές παρείσδυσης διενεργούνται εσωτερικά, κατ΄ ελάχιστο μια φορά το χρόνο, σύμφωνα με τον σχετικό σχεδιασμό. Τέτοιου είδους δοκιμές μπορεί να είναι white box ή grey box.
5	6	Λαμβάνοντας υπόψη το πλαίσιο λειτουργίας του οργανισμού, τους στόχους ασφαλείας, την στρατηγική ασφαλείας, τις νομοθετικές, κανονιστικές και συμβατικές απαιτήσεις, καταρτίζεται οργανωμένο σχέδιο (πρόγραμμα) δοκιμών παρείσδυσης.
5	7	Το σχέδιο περιλαμβάνει το πεδίο εφαρμογής των δοκιμών (π.χ. δικτύου, web applications, APIs, hosted υπηρεσίες, μέτρα φυσικής πρόσβασης κα.), τους περιορισμούς (π.χ. τις ώρες που μπορεί να διενεργηθεί, το προσωπικό που πρέπει να ενημερωθεί κ.α), τα είδη των δοκιμών που θα διενεργηθούν και τις σχετικές μεθοδολογίες και πρότυπα, την συχνότητα διενέργειας, τον στόχο, τους ρόλους και αρμοδιότητες, το είδος της τεκμηρίωσης που θα διατηρηθεί και θα παραδοθεί στον οργανισμό, τα σημεία επαφής και ένα πλάνο άμεσων ενεργειών σε περίπτωση ευρήματος.
5	8	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	9	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
VM2		Μέτρο: Καταγραφή και αναφορά ευπαθειών Στόχος Μέτρου: Να διασφαλιστεί ότι οι ευπάθειες καταγράφονται και υποβάλλονται σε σχετικές εκθέσεις, ώστε να είναι δυνατή η λήψη τεκμηριωμένων αποφάσεων από τη διοίκηση όσον αφορά τον χειρισμό τους. Περιγραφή Μέτρου: Θέσπιση, εφαρμογή και διατήρηση διαδικασιών για την καταγραφή και την αναφορά των ευπαθειών που έχουν εντοπιστεί, ώστε να είναι δυνατή η αποκατάσταση και η ενημέρωση συστημάτων και διαδικασιών για τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών. Η καταγραφή ευπαθειών και η υποβολή σχετικών εκθέσεων θα πρέπει να είναι το αποτέλεσμα των προσπαθειών ανίχνευσης και εντοπισμού ευπαθειών, όπως περιγράφεται στο μέτρο [VM1]. Ο οργανισμός πρέπει να εξετάζει το ενδεχόμενο συμπερίληψης στοιχείων για ευπάθειες υψηλού κινδύνου σε γενικές εκθέσεις προς τη διοίκηση, ώστε να εξασφαλίζεται η εκ των άνω προς τα κάτω επίγνωση των ευπαθειών με δυνητικές επιπτώσεις και να προσδιορίζονται τα κατάλληλα μέτρα για την αποκατάσταση και την εφαρμογή διορθωτικών συστημάτων και διαδικασιών, όπως περιγράφεται στο μέτρο [VM3]. Πηγή:
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν υλοποιεί καμία ενέργεια για την ανίχνευση, εντοπισμό, καταγραφή και αναφορά ευπαθειών.
1	1	Υλοποιούνται διορθωτικές ενέργειες έναντι ευπαθειών ως αντίδραση (reactive) και τουλάχιστον ad-hoc τρόπο ή/και συνήθως χωρίς να είναι πρωτοβουλία του οργανισμού (π.χ. εφαρμογή αυτοματοποιημένων security updates) και ίσως χωρίς κάποια καταγραφή της ευπάθειας.
2	1	Έχουν ενεργοποιηθεί μηχανισμοί και δημιουργήθει επαφές για την λήψη έγκαιρης πληροφόρησης για την ανίχνευση και εντοπισμό των ευπαθειών στα κρίσιμα συστήματα.
2	2	Τα στοιχεία των ευπαθειών καταγράφονται σε σχετικά αρχεία και επικοινωνούνται εσωτερικά στον οργανισμό.
3	1	Έχει θεσπιστεί, εφαρμόζεται και διατηρείται διαδικασία για την καταγραφή και την αναφορά των ευπαθειών που έχουν εντοπιστεί, ώστε να είναι δυνατή η αποκατάσταση και η ενημέρωση συστημάτων και διαδικασιών για τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών.
3	2	Η καταγραφή ευπαθειών και η υποβολή σχετικών εκθέσεων είναι το αποτέλεσμα των προσπαθειών ανίχνευσης και εντοπισμού ευπαθειών, όπως περιγράφεται στο μέτρο [VM1].
3	3	Εξετάζεται το ενδεχόμενο συμπερίληψης στοιχείων για ευπάθειες υψηλού κινδύνου σε γενικές εκθέσεις προς τη διοίκηση, ώστε να εξασφαλίζεται η εκ των άνω προς τα κάτω επίγνωση των ευπαθειών με δυνητικές επιπτώσεις και να προσδιορίζονται τα κατάλληλα μέτρα για την αποκατάσταση και την εφαρμογή διορθωτικών συστημάτων και διαδικασιών, όπως περιγράφεται στο μέτρο [VM3].
3	4	Καταγράφονται οι σχετικές ευπάθειες στον κατάλογο απειλών, ευπαθειών και κινδύνων όπως αναφέρεται στο [RM3].
3	5	Αξιολογείται το επίπεδο της ευπάθειας λαμβάνοντας υπόψη την δυνατότητα εκμετάλλευσης (exploitability) την πιθανή επίπτωση της ευπάθειας ανά περίπτωση και ανά κατηγορία στοιχείων ενεργητικού (λαμβάνοντας υπόψη και τα σχετικά μέτρα π.χ. μέτρα σε επίπεδο δικτύου, μέτρα σε επίπεδο στοιχείου ενεργητικού κ.α.).

4	1	Όταν τα εμπλεκόμενα μέρη αναγνωρίσουν ότι αδυναμίες, απειλές ή κίνδυνοι δεν είναι πλέον εφαρμόσιμοι, ο σχετικός κατάλογος επικαιροποιείται υποδεικνύοντας ότι η αντίστοιχη εγγραφή δεν είναι πλέον ενεργή. (Η ιστορικότητα αναγνώρισης διατηρείται και τεκμηριώνεται). Η ενημέρωση των στοιχείων μπορεί να προκύψει από διαφορετικές πηγές όπως αναφέρονται στα [RM3], [VM1].
4	2	Χρησιμοποιούνται έγκυρες πηγές αναγνώρισης ευπαθειών προκειμένου να υπάρχει πρόσβαση σε στοιχεία επαλήθευσης και κατηγοριοποίησης.
4	3	Η κατηγοριοποίηση των ευπαθειών γίνεται σύμφωνα με τις διεθνείς βέλτιστες πρακτικές (π.χ. CVSS).
4	4	Στον κατάλογο ευπαθειών καταγράφονται κατ΄ ελάχιστο ο πόρος ενεργητικού, η ευπάθεια, η απειλή (ή απειλές) που μπορεί να εκμεταλλευτούν την συγκεκριμένη ευπάθεια, ο κίνδυνος που θα δημιουργηθεί, η δυνατότητα εκμετάλλευσης, καθώς και το μέγεθος της ευπάθειας.
4	5	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Χρησιμοποιούνται διεθνείς βέλτιστες πρακτικές και εργαλεία (π.χ. Structured Threat Information Expression (STIX™) και εργαλεία όπως είναι το MISP Threat Sharing Platform) για την δομημένη καταγραφή στοιχείων threat intelligence και την δομημένη υποδοχή ή αποστολή της σχετικής πληροφορίας.
5	2	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	3	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
VM3		Μέτρο: Αποκατάσταση ευπαθειών και ενημερώσεις ασφάλειας Στόχος Μέτρου: Να εξασφαλιστεί η αποκατάσταση των ευπαθειών συστημάτων και η εφαρμογή ενημερώσεων ασφαλείας, κατόπιν απόφασης της διοίκησης Περιγραφή Μέτρου: Θέσπιση, εφαρμογή και διατήρηση διαδικασιών για την αποκατάσταση ευπαθειών και την εισαγωγή ενημερώσεων ασφάλειας για ευπάθειες που εντοπίζονται σε συστήματα, εφαρμογές και στοιχεία δικτύου, και τα οποία απαιτούν μετριασμό ως αποτέλεσμα της αξιολόγησης της διοίκησης. Η αποκατάσταση ευπαθειών και οι ενημερώσεις ασφάλειας πρέπει να είναι το αποτέλεσμα απόφασης της διοίκησης με βάση την καταγραφή ευπαθειών και την υποβολή σχετικών εκθέσεων, όπως περιγράφεται στο μέτρο [VM2]. Πηγή: C2M2 (THREAT, ASSET), NIST 800-53 (SA-22), ISO 27001, ISO 27002
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν υλοποιεί καμία ενέργεια για την αποκατάσταση ευπαθειών.
1	1	Υλοποιούνται διορθωτικές ενέργειες έναντι ευπαθειών ως αντίδραση (reactive) και τουλάχιστον ad-hoc τρόπο ή/και συνήθως χωρίς να είναι πρωτοβουλία του οργανισμού (π.χ. εφαρμογή αυτοματοποιημένων security updates) και ίσως χωρίς κάποια καταγραφή της ευπάθειας.
2	1	Έχουν ενεργοποιηθεί ή εφαρμόζονται πολιτικές για την αποκατάσταση ευπαθειών μόνο στα κρίσιμα συστήματα.
2	2	Δεν γίνεται αυτόματη εγκατάσταση ενημερώσεων. Εξουσιοδοτημένο προσωπικό, ελέγχει πρώτα τις ενημερώσεις και στην συνέχεια διενεργεί τις σχετικές εγκαταστάσεις.
3	1	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται διαδικασίες για την αποκατάσταση ευπαθειών και την εισαγωγή ενημερώσεων ασφάλειας για ευπάθειες που εντοπίζονται σε συστήματα, εφαρμογές και στοιχεία δικτύου, και τα οποία απαιτούν μετριασμό ως αποτέλεσμα της αξιολόγησης της διοίκησης.
3	2	Η αποκατάσταση ευπαθειών και οι ενημερώσεις ασφάλειας είναι το αποτέλεσμα απόφασης της διοίκησης με βάση την καταγραφή ευπαθειών και την υποβολή σχετικών εκθέσεων, όπως περιγράφεται στο μέτρο [VM2].
3	3	Η εφαρμογή ενεργειών για την αποκατάσταση ευπαθειών ακολουθεί την διαδικασία διαχείρισης αλλαγών όπως αναφέρεται στο [CM1].
3	4	Στα πλαίσια των σχετικών διαδικασιών έχει προσδιοριστεί ο τρόπος ανταπόκρισης του οργανισμού σε ευπάθειες συγκεκριμένης κρισιμότητας ανά κατηγορία στοιχείων όπως αυτά αποτυπώνονται στον κατάλογο στοιχείων ενεργητικού [DS2].
3	5	Ο τρόπος αποκατάστασης αναφέρεται στο είδος των ενεργειών που γίνονται αυτόματα, χωρίς κάποια δοκιμή αλλά και στο είδος των ενεργειών που γίνονται αφού έχουν δοκιμαστεί. (Ειδικά για κρίσιμα συστήματα, σε κάθε περίπτωση η εισαγωγή κάποιας ενημέρωσης γίνεται αφού έχει υλοποιηθεί η εγκατάσταση σε δοκιμαστικό / παρόμοιο σύστημα χαμηλού κινδύνου).
3	6	Η σχετική διαδικασία έχει την έγκριση της διοίκησης

3	7	Η διαδικασία παρακολούθησης σε αυτές τις περιπτώσεις ακολουθεί την διαδικασία διαχείρισης αλλαγών [CM1].
4	1	Εφαρμόζονται οι τεχνικές που αναφέρονται στο [VM1] και [VM2] για την ανίχνευση, εντοπισμό και καταγραφή των ευπαθειών.
4	2	Τηρείται σύστημα μέσα από το οποίο ελέγχεται η κατάσταση των διαφόρων στοιχείων ενεργητικού έναντι στις εντοπισμένες ευπάθειες και κατά πόσο έχουν ενσωματωθεί οι τελευταίες ενημερώσεις ασφαλείας.
4	3	Σε περίπτωση που υπάρχουν νέες εκδόσεις προγραμμάτων ή άλλων στοιχείων,εκκινούνται δραστηριότητες για την αξιολόγηση του κόστους / οφέλους της μετάβασης στην νέα έκδοση.
4	4	Ο οργανισμός κατά κανόνα φροντίζει να βρίσκεται στην τελευταία δοκιμασμένη και σταθερή έκδοση των προγραμμάτων που χρησιμοποιεί.
4	5	Λογισμικό ή εξοπλισμός για το οποίο έχει παρέλθει ο κύκλος ζωής του (after end of life) δεν επιτρέπεται εντός του οργανισμού. Σε περίπτωση που δεν γίνεται διαφορετικά, η συγκεκριμένη περίπτωση αναγνωρίζεται ως κίνδυνος και σχεδιάζονται κατάλληλα αντισταθμιστικά μέτρα για την αντιμετώπιση του σχετικού κινδύνου ακολουθώντας τις προδιαγραφές των [RM1-6].
4	6	Όλες οι αναγνωρισμένες ευπάθειες με υψηλή βαθμολογία κρισιμότητας ακολουθούν και καταγράφονται σύμφωνα με την διαδικασία διαχείρισης αλλαγών [CM1].
4	7	Υλοποιούνται λύσεις antimalware με δυνατότητες αναγνώρισης αδυναμιών και φίλτρα anti-exploitation.
4	8	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Μετά την εφαρμογή των μέτρων για την αντιμετώπιση μιας ευπάθειας (μέτρα μπορεί να είναι μια ενημέρωση αλλά ανάλογα με τις ιδιαιτερότητες της ευπάθειας μπορεί να είναι και άλλες ενέργειες διαφορετικής φύσης), ελέγχεται η αποτελεσματικότητα της υλοποίησης των ενεργειών έναντι της ευπάθειας / απειλής.
5	2	Οι τρόποι για την αξιολόγηση της αποτελεσματικότητας αναφέρονται στην καταγραφή της διαχείρισης αλλαγής και μπορεί να είναι διαφορετικών τύπων περιλαμβανομένων δοκιμών, αναλύσεων, advanced threat hunting, active defense κ.α.
5	3	Σε περίπτωση που τα αποτελέσματα της αξιολόγησης της αποτελεσματικότητας είναι αρνητικά, γίνονται κατάλληλες διορθωτικές ενέργειες.
5	4	Οι απαιτήσεις αφορούν λογισμικό τρίτων, ανοικτό λογισμικό ή και λογισμικό που έχει αναπτυχθεί από τον ίδιο τον οργανισμό. Για το τελευταίο ισχύουν και τα στοιχεία του [AS1].
5	5	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	6	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.

Κατηγορία		ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΟΥ
NS1		Μέτρο: Ασφάλεια Περιμέτρου Στόχος Μέτρου: Να διασφαλιστεί ότι η διεπαφή του τοπικού δικτύου με το εξωτερικό δίκτυο προστατεύεται από επιθέσεις, απειλές και άλλες εκούσιες ή ακούσιες ενέργειες με δυνητικά αρνητικές επιπτώσεις. Περιγραφή Μέτρου: Θέσπιση, εφαρμογή και διατήρηση κατάλληλων μέτρων ασφάλειας δικτύου με σκοπό την προστασία της περιμέτρου του δικτύου από εξωτερικές απειλές και τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών που βρίσκονται στο εσωτερικό δίκτυο. Ο οργανισμός θα πρέπει να λαμβάνει υπόψη ότι η ασφάλεια περιμέτρου αποτελεί ένα μόνο συγκεκριμένο επίπεδο σε μια πολυεπίπεδη αρχιτεκτονική άμυνας. Για την προστασία από επιθέσεις στο δίκτυο, ο οργανισμός λαμβάνει υπόψη τις ειδικές για τον οργανισμό, απειλές και τις ειδικές για τον τομέα, απειλές και κινδύνους για το δίκτυο. Ο οργανισμός λαμβάνει υπόψη τα τείχη προστασίας και τα συστήματα ανίχνευσης και πρόληψης εισβολής, όπως περιγράφονται στο μέτρο [NS7]. Ο οργανισμός λαμβάνει εύλογα μέτρα για να διασφαλίσει ότι η κίνηση δεδομένων φιλτράρεται με βάση τις πολιτικές ασφάλειας του οργανισμού. Πηγή: C2M2, NIST 800-53, CIS, ISO 27002
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν εφαρμόζει καθόλου μέτρα για την προστασία της (λογικής) περιμέτρου του οργανισμού.
1	1	Υπάρχει firewall ο οποίος λειτουργεί ως σημείο διεπαφής ανάμεσα στο τοπικό δίκτυο και το εξωτερικό δίκτυο.
1	2	Οι ρυθμίσεις του συγκεκριμένου firewall είναι τουλάχιστον στοιχειώδεις ή/και μπορεί να μην διενεργείται τακτικός και ουσιαστικός έλεγχος και διαχείριση.
2	1	Έχει σχεδιαστεί και υλοποιηθεί μια αρχιτεκτονική δικτύου για την εξασφάλιση του επιθυμητού επιπέδου ασφαλείας δικτύου λαμβάνοντας υπόψη τις πρακτικές και τα μέτρα που αναφέρονται στα [NS2] – [NS7].
2	2	Έχει αποτυπωθεί η αρχιτεκτονική σε διάγραμμα δικτύου, και παρέχει ικανή πληροφορία σχετικά με την διασύνδεση, τον τρόπο λειτουργίας και τα διάφορα επίπεδα προστασίας.
2	3	Έχει αναγνωρισθεί ο εξοπλισμός που εκτελεί δραστηριότητες ασφάλειας σε κάθε επίπεδο.
2	4	Για τον εξοπλισμό που βρίσκεται στην περίμετρο, έχουν εφαρμοστεί πολιτικές και κανόνες ασφαλείας υιοθετώντας αρνητική λογική (όλα κλειστά και ανοίγονται μόνο αν απαιτείται), λογική των ελάχιστων υπηρεσιών (υπηρεσίες που δεν χρειάζονται (περιττές) είναι απενεργοποιημένες), ελεγχόμενη πρόσβαση (σύμφωνα με το [IAM1] και παρακολούθηση των ενεργειών (και τήρηση αρχείων καταγραφής) σύμφωνα με το [IAM2].
2	5	Κατ' ελάχιστο είναι απενεργοποιημένα τα : α) η εισερχόμενη από και εξερχόμενη προς το εξωτερικό δίκτυο επικοινωνία στις παρακάτω θύρες: TCP 445 (SMB), UDP 137 (NetBIOS Name Resolution), UDP 138 (NetBIOS Datagram Service) και TCP 139 (NetBIOS Session Service), β) οι εισερχόμενες SMB συνδέσεις στην TCP θύρα 445 σε όσα στοιχεία δεν φιλοξενούν κοινόχρηστο περιεχόμενο (shares), γ)οι εκδόσεις SMBv1 και v2 στο εσωτερικό δίκτυο,
2	6	Αλλαγές που διενεργούνται στον εξοπλισμό που βρίσκονται στην περίμετρο ακολουθούν την διαδικασία διαχείρισης αλλαγών σύμφωνα με το [CM1].
2	7	Έχουν υλοποιηθεί host-based firewalls ή port filtering tools τα οποία έχουν είτε explicit είτε implicit κανόνα που κάνει drop όλη την κίνηση με εξαίρεση τις υπηρεσίες, τα πρωτόκολλα και τις θύρες που είναι ειδικώς (explicitly) εξουσιοδοτημένα.
3	1	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται μέτρα ασφάλειας δικτύου με σκοπό την προστασία της περιμέτρου του δικτύου από εξωτερικές απειλές και τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών που βρίσκονται στο εσωτερικό δίκτυο.
3	2	Έχει υλοποιήσει μια πολυεπίπεδη αρχιτεκτονική άμυνας, στην οποία ασφάλεια περιμέτρου αποτελεί ένα μόνο συγκεκριμένο επίπεδο.
3	3	Κατά τον σχεδιασμό των κανόνων και των μηχανισμών ασφαλείας που έχουν υιοθετηθεί έχουν ληφθεί υπόψη τα αποτελέσματα της αξιολόγησης κινδύνου καθώς και τις ειδικές για τον οργανισμό, απειλές και τις ειδικές για τον τομέα, απειλές και κινδύνους για το δίκτυο.
3	4	Έχει ορισθεί ένα σύνολο πολιτικών ασφαλείας για την εξασφάλιση ότι η κίνηση φιλτράρεται σε επιθυμητό επίπεδο.
3	5	Υλοποιείται διαχωρισμός δικτύων όπως προβλέπεται στο [NS2]. Σε κάθε περίπτωση στοιχεία τα οποία χρειάζεται να είναι προσβάσιμα από το εξωτερικό δίκτυο, είναι διαχωρισμένα από το εσωτερικό δίκτυο.

3	6	Οι συνδέσεις σε εξωτερικά δίκτυα ή συστήματα γίνονται μόνο από τις διαχειριζόμενες διεπαφές των στοιχείων που έχουν αναγνωριστεί στην λογική περίμετρο (σύμφωνα με την υλοποιημένη αρχιτεκτονική).
3	7	Στα switches είναι ενεργοποιημένη η υπηρεσία port security, ενώ οι θύρες που δεν χρησιμοποιούνται είναι απενεργοποιημένες.
3	8	Στους routers τα interfaces και τα πρωτόκολλα δρομολόγησης είναι απενεργοποιημένα.
3	9	Για την πρόσβαση στο διαχειριστικό περιβάλλον των στοιχείων που απαρτίζουν την περίμετρο χρησιμοποιείται MFA.
3	10	Πρωτόκολλα όπως SMB, SNTP και άλλα τα οποία μπορούν να χρησιμοποιηθούν για την μεταφορά στοιχείων, μηνυμάτων και καταστάσεων χρησιμοποιούνται μόνο αν απαιτείται και μετά από κατάλληλη ανάλυση και παραμετροποίηση. Σχετικά στοιχεία διατηρούνται μέσα από την διαδικασία ελέγχου αλλαγών.
3	11	Έχει καταγραφεί και εφαρμόζει μια πολιτική ασφάλειας δικτύων που περιέχει κατ' ελάχιστο ρόλους και αρμοδιότητες, βασικές αρχές που διέπουν τον σχεδιασμό της αρχιτεκτονικής δικτύου του οργανισμού, βασικές διαδικασίες που σχετίζονται με την διαχείρισης δικτύου, τα σχετικά αρχεία που τηρούνται, τα αρχεία καταγραφής και το χρονικό διάστημα διατήρησής τους και τα μέτρα ασφαλείας που εφαρμόζονται.
3	12	Έχει αποτυπωθεί η αρχιτεκτονική σε διάγραμμα δικτύου, και παρέχει αναλυτική πληροφορία σχετικά τα διάφορα επίπεδα της αρχιτεκτονικής, τα στοιχεία που αποτελούν το κάθε επίπεδο, τα βασικά χαρακτηριστικά τους, πιθανά μοναδικά σημεία αστοχίας, τα σημεία στα οποία είναι ενεργοποιημένη η παρακολούθηση.
3	13	Τα διαγράμματα διαχειρίζονται ως πληροφορία του υψηλότερου επιπέδου διαβάθμισης πληροφοριών (όπως αναφέρεται στο [DS2]).
3	14	Εφεδρικά αντίγραφα ασφαλείας λαμβάνονται για τα αρχεία διαμόρφωσης (configuration files) των εν λόγω στοιχείων σύμφωνα με την σχετική πολιτική του οργανισμού και έκτακτα πριν από κάθε αλλαγή. Το ιστορικό των αντιγράφων διατηρείται.
3	15	Για την πρόσβαση από απόσταση, χρησιμοποιείται VPN (Virtual Private Network) και η σύνδεση γίνεται σε υποδομή AAA (Authentication, Authorization and Accounting) του οργανισμού. (Είναι υποχρεωτική η αυθεντικοποίηση του χρήστη στο κατάλληλο σημείο για την πρόσβαση σε άλλα στοιχεία εντός του οργανισμού).
4	1	Η απομακρυσμένη πρόσβαση χρηστών στο εσωτερικό δίκτυο του γίνεται μέσω VPN (Virtual Private Network), με χρήση αυθεντικοποίησης δύο παραγόντων (2-factor authentication) και των πιο πρόσφατων αλγόριθμων κρυπτογράφησης.
4	2	Οι εργασίες του διαχειριστικού προσωπικού πληροφορικής (administrative tasks) διενεργούνται από στοιχεία που χρησιμοποιούνται αποκλειστικά για αυτό το σκοπό. Κατάλληλα μέτρα για τον διαχωρισμό τους εφαρμόζονται σύμφωνα με το [NS2].
4	3	Υλοποιείται Host-based Intrusion Detection σύμφωνα με τις προδιαγραφές του [NS7].
4	4	Σε όλες τα στοιχεία τα οποία χρησιμοποιούνται εντός του οργανισμού για την προστασία της περιμέτρου αλλά και των άλλων επιπέδων της αρχιτεκτονικής ασφαλείας, εφαρμόζεται παρακολούθηση και καταγραφή σύμφωνα με τα αναγραφόμενα του [AM3]. Ακολούθως γίνεται συλλογή των στοιχείων και ανταπόκριση όπως απαιτείται σύμφωνα με το [AM3] και το [EIM1].
4	5	Είναι ενεργοποιημένη η παρακολούθηση ανάμεσα σε διαφορετικά τμήματα του δικτύου (segments) όπως απαιτείται.
4	6	Σε κάθε σταθμό εργασίας (end-point) αλλά και κάθε άλλο στοιχείου (όπου είναι αυτό δυνατό) είναι ενεργοποιημένο ή υλοποιημένο firewall το οποίο να εμποδίζει κάθε δικτυακή σύνδεση από και προς τη συσκευή με εξαίρεση τις θύρες και υπηρεσίες που απαιτούνται με βάση τις επιχειρησιακές ανάγκες.
4	7	Έχουν υλοποιηθεί σχετικές παραμετροποιήσεις ώστε να αναγνωρίζονται TCP sessions τα οποία διαρκούν ασυνήθιστα μεγάλα χρονικά διαστήματα.
4	8	Οι proxy servers παρακολουθούν και καταγράφουν τα TCP sessions και είναι παραμετροποιημένα ώστε να φιλτράρουν και να εμποδίζουν την πρόσβαση σε συγκεκριμένα URLs, domains, IPs σύμφωνα με τους κανόνες του οργανισμού και τον σχετικό κίνδυνο.
4	9	Έχει προσδιοριστεί ένα μέγιστο χρονικό διάστημα σύνδεσης ανά session και έχουν εφαρμοστεί οι κατάλληλοι τεχνικοί κανόνες και εργαλεία ώστε να τερματίζονται οι συνδέσεις είτε όταν έχει παρέλθει εκείνη η διάρκεια είτε μετά από συγκεκριμένο χρονικό διάστημα αδράνειας. (Η διάρκεια μπορεί να μεταβάλλεται με βάση της κρισιμότητα της πληροφορίας και άλλες συνθήκες).
4	10	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.

4	11	Το σύνολο της δικτυακής κυκλοφορίας από και προς το διαδίκτυο περνά από αυθεντικοποιημένο διακομιστή μεσολάβησης επιπέδου εφαρμογής (application layer (web) proxy server), ο οποίος έχει ρυθμιστεί να απαγορεύει μη εξουσιοδοτημένες συνδέσεις.
5	1	Εφαρμόζονται αρχές Zero trust αρχιτεκτονικής δικτύου σύμφωνα με διεθνείς βέλτιστες πρακτικές (π.χ. NIST 800-207).
5	2	Κατ΄ελάχιστο ικανοποιούνται οι ακόλουθες αρχές: α) Όλα τα δεδομένα και τα συστήματα αποτελούν στοιχεία (πόρους) του οργανισμού, β) Όλες οι επικοινωνίες προστατεύονται ανεξάρτητα από την τοποθεσία δικτύου στην οποία βρίσκονται, γ) Πρόσβαση σε στοιχεία του οργανισμού δίνεται μόνο αν αυστηρά χρειάζεται και σε per-session βάση, δ) Η πρόσβαση στα στοιχεία καθορίζεται από μια δυναμική πολιτική που μπορεί να καθορίζεται από διάφορες παραμέτρους περιλαμβανομένων συμπεριφοράς και περιβαλλοντικούς, ε) Τα μετρά για την ακεραιότητα και την επίδοση / επίπεδο ασφάλειας των στοιχείων παρακολουθούνται, ζ) εφαρμόζονται δυναμικές αυθεντικοποίησης και εξουσιοδότησης, πριν δοθεί η πρόσβαση, η) συλλέγεται όση περισσότερη πληροφορία γίνεται για την τρέχουσα κατάσταση των στοιχείων, της υποδομής δικτύων και των επικοινωνιών και χρησιμοποιείται αυτή η πληροφόρηση για βελτιώση του επιπέδου ασφάλειας.
5	3	Εφαρμόζονται δικτυακά συστήματα ανίχνευσης και πρόληψης εισβολών (network intrusion detection / prevention systems) για την ανίχνευση και πρόληψη επιθέσεων σε κάθε τμήμα / υποδίκτυο του Οργανισμού (π.χ. Network Intrusion Detection System (NIDS) ή αντίστοιχα cloud service provider (CSP) service με τις κατάλληλες εγγυήσεις.)
5	4	Υλοποιείται δίοδος δεδομένων (data diode) σε μορφή hardware, που επιβάλλει τη ροή δεδομένων μόνο προς μία κατεύθυνση με σκοπό την προστασία κρίσιμης πληροφορίας σε τμήματα / υποδίκτυα υψηλών απαιτήσεων ασφάλειας.
5	5	Λαμβάνονται μέτρα για την αποφυγή μη εξουσιοδοτημένης μεταφοράς πληροφορίας (unauthorized exfiltration). Μέτρα που ανήκουν σε αυτή την κατηγορία είναι: 1) προσδιορισμός και περιορισμός σε συγκεκριμένα πρωτόκολλα και τρόπους επικοινωνίας 2) παρακολούθηση πιθανής αποστολής μηνυμάτων από στοιχεία του οργανισμού (π.χ. beaconing) 3) υλοποίηση εργαλείων και προσπάθειας για την αναγνώριση πιθανών περιπτώσεων στεγανογραφίας 4) αποσύνδεση της πρόσβασης σε εξωτερικές διεπαφές όταν δεν χρησιμοποιούνται 5) υλοποίηση ανάλυσης κίνησης για την αναγνώριση της κανονικής / μη κανονικής συμπεριφοράς του συστήματος 6) ανάλυση σε επίπεδο packet headers κ.α. (τέτοιες λύσεις σε ένα βαθμό υλοποιούνται μέσα από deep packet inspection firewalls ή XML gateways.
5	6	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	7	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
NS2		Μέτρο: Διαχωρισμός και τμηματοποίηση του δικτύου Στόχος Μέτρου: Να εξασφαλιστεί ο διαχωρισμός του λογικού δικτύου, σύμφωνα με τις επιχειρηματικές λειτουργίες, και να απόφευχθεί η εξάπλωση κακόβουλων στοιχείων. Περιγραφή Μέτρου: Θέσπιση, εφαρμογή και διατήρηση κατάλληλου διαχωρισμού και τμηματοποίησης του δικτύου, προκειμένου να διασφαλιστεί - λογικός ή/και φυσικός - διαχωρισμός των δικτύων πληροφοριών. Κατά τον σχεδιασμό, την εφαρμογή και τη διατήρηση των μέτρων διαχωρισμού και τμηματοποίησης του δικτύου, ο οργανισμός λαμβάνει υπόψη τους διάφορους τομείς λειτουργικής δραστηριότητας του οργανισμού. Ο οργανισμός λαμβάνει υπόψη τη φύση και την έκταση των δεδομένων που υποβάλλονται σε επεξεργασία στο πλαίσιο συγκεκριμένων επιχειρηματικών δραστηριοτήτων, προκειμένου να διασφαλίζεται επαρκής διαχωρισμός. Ο οργανισμός θα πρέπει να εξετάσει το ενδεχόμενο να υιοθετήσει εικονική τοπική δικτύωση (VLAN) κατά το σχεδιασμό του διαχωρισμού και της αρχιτεκτονικής του δικτύου σε τμήματα. Ο οργανισμός θα πρέπει να εξετάζει τουλάχιστον τον διαχωρισμό των τομέων έρευνας και ανάπτυξης, της διοίκησης, της κεντρικής υποδομής πληροφοριών και των δημόσια διαθέσιμων (στο διαδίκτυο) εφαρμογών και συστημάτων. Πηγή: NIST 800-53 (SC-3), ISO 27001, ISO 27002, PNNL
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν εφαρμόζει καθόλου μέτρα για την προστασία της (λογικής) περιμέτρου του οργανισμού.
1	1	Υπάρχει firewall ο οποίος λειτουργεί ως σημείο διεπαφής ανάμεσα στο τοπικό δίκτυο και το εξωτερικό δίκτυο.
1	2	Οι ρυθμίσεις του συγκεκριμένου firewall είναι τουλάχιστον στοιχειώδεις ή/και μπορεί να μην διενεργείται τακτικός και ουσιαστικός έλεγχος και διαχείριση από την μεριά του οργανισμού. (Ο διαχωρισμός που υλοποιείται δίνατε να αφορά μόνο το εσωτερικό δίκτυο από το εξωτερικό).

2	1	Έχει σχεδιαστεί και υλοποιηθεί μια αρχιτεκτονική δικτύου για την εξασφάλιση του επιθυμητού επιπέδου ασφαλείας δικτύου για τον οργανισμό λαμβάνοντας υπόψη τις πρακτικές και τα μέτρα που αναφέρονται στα [NS2] – [NS7].
2	2	Έχει αποτυπωθεί η αρχιτεκτονική σε διάγραμμα δικτύου, και παρέχει ικανή πληροφορία σχετικά με την διασύνδεση, τον τρόπο λειτουργίας και τα διάφορα επίπεδα προστασίας.
2	3	Κρίσιμα συστήματα προστατεύονται από περισσότερα του ενός επίπεδα.
3	1	Έχει θεσπιστεί, εφαρμόζεται και διατηρείται κατάλληλος διαχωρισμός και τμηματοποίηση του δικτύου, προκειμένου να διασφαλιστεί - λογικός ή/και φυσικός (όπου αυτό είναι εφικτό) - διαχωρισμός των δικτύων πληροφοριών.
3	2	Κατά τον σχεδιασμό, την εφαρμογή και τη διατήρηση των μέτρων διαχωρισμού και τμηματοποίησης του δικτύου, ο οργανισμός λαμβάνονται υπόψη οι διάφοροι τομείς λειτουργικής δραστηριότητας του οργανισμού.
3	3	Λαμβάνεται υπόψη η φύση και η έκταση των δεδομένων που υποβάλλονται σε επεξεργασία στο πλαίσιο συγκεκριμένων επιχειρηματικών δραστηριοτήτων, προκειμένου να διασφαλίζεται επαρκής διαχωρισμός.
3	4	Έχει δημιουργηθεί κατάλογος στοιχείων ενεργητικού όπως αναφέρεται στο [RM2] και έχει γίνει μια σχετική διαβάθμιση σε σχέση με την κρισιμότητά τους όπως αναφέρεται στο [DS2].
3	5	Τα κρίσιμα συστήματα βρίσκονται διαχωρισμένα ώστε να μπορούν να εφαρμόζονται επιπλέον μέτρα προστασίας, υψηλότερου επιπέδου διαχείριση πρόσβασης και παρακολούθηση. Για τα τμήματα αυτά, γίνεται φιλτράρισμα της δικτυακής κίνησης (traffic filtering) μεταξύ των τμημάτων / υποδικτύων για να περιοριστεί η ροή της πληροφορίας στην απολύτως απαραίτητη για τις επιχειρησιακές ανάγκες του οργανισμού.
4	1	Έχει υιοθετηθεί εικονική τοπική δικτύωση (VLAN) κατά το σχεδιασμό του διαχωρισμού και της αρχιτεκτονικής του δικτύου σε τμήματα. Τα VLANs έχουν σχεδιαστεί και υλοποιηθεί λαμβάνοντας υπόψη τις ανάγκες κάθε τμήματος, τους στόχους ασφαλείας, την κρισιμότητα των δεδομένων και άλλα κριτήρια που ο οργανισμός κρίνει ως απαιραίτητα.
4	2	Κατ'ελάχιστο είναι διαχωρισμένοι οι τομείς έρευνας και ανάπτυξης, διοίκησης, κεντρικής υποδομής πληροφοριών και των δημόσια διαθέσιμων (στο διαδίκτυο) εφαρμογών και συστημάτων.
4	3	Οι διαχειριστικές εργασίες πληροφορικής (administrative tasks) διενεργούνται από στοιχεία που χρησιμοποιούνται αποκλειστικά για αυτό το σκοπό. Τυπικά, τα συγκεκριμένα στοιχεία είναι φυσικά ή λογικά διαχωρισμένα από τα υπόλοιπα και δεν έχουν πρόσβαση απευθείας στο διαδίκτυο – ακολουθούνται οι κανόνες του διαχωρισμού και της τμηματοποίησης του δικτύου.
4	4	Διενεργούνται τακτικοί έλεγχοι και δοκιμές για την επιβεβαίωση ότι υλοποιούνται οι σχετικοί κανόνες και υπάρχει ο επιθυμητός διαχωρισμός σε όλα τα επίπεδα.
4	5	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Εφαρμόζονται αρχές Zero trust αρχιτεκτονικής δικτύου σύμφωνα με διεθνείς βέλτιστες πρακτικές (π.χ. NIST 800-207).
5	2	Υλοποιείται διαχωρισμός ανάμεσα στις λειτουργίες ασφάλειας από τις υπόλοιπες με την δημιουργία περιβάλλοντος απομόνωσης (isolation boundary). Αυτό υλοποιείται με τον πιο πρόσφορο τρόπο και μπορεί να κυμαίνεται από την χρήση security kernels via processor rings ή processor modes, ή διαχωρισμό του κώδικα ανάμεσα σε security και non security functions στο δυνατό βαθμό .
5	3	Όπου είναι δυνατό, υλοποιείται φυσικός διαχωρισμός ανάμεσα στα αναγνωρισμένα επίπεδα (αντί απλά για λογικό).
5	4	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	5	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.

NS3		Μέτρο: Προστασία από άρνηση παροχής υπηρεσιών Στόχος Μέτρου: Να διασφαλιστεί η προστασία των οργανωτικών πόρων από επιθέσεις άρνησης παροχής υπηρεσιών, και ότι δεν επηρεάζονται οι νόμιμες δραστηριότητες παροχής υπηρεσιών. Περιγραφή Μέτρου: Θέσπιση, εφαρμογή και διατήρηση επαρκούς προστασίας από άρνηση παροχής υπηρεσιών και διανεμημένη άρνηση παροχής υπηρεσιών, προκειμένου να διασφαλίζεται η έγκαιρη και ποιοτική παροχή της υπηρεσίας σε εξουσιοδοτημένους και επικυρωμένους χρήστες και να διατηρείται σταθερό επίπεδο παραγωγικότητας. Κατά τον σχεδιασμό των σχετικών μέτρων προστασίας, ο οργανισμός θα πρέπει να εξετάσει την ενσωμάτωση ικανοτήτων για τον εντοπισμό νόμιμων χρηστών και εφαρμογών έναντι κακόβουλων προσπαθειών πρόσβασης σε πόρους. Ο οργανισμός θα πρέπει να λαμβάνει υπόψη μέτρα εφεδρείας και υψηλής διαθεσιμότητας, όπως περιγράφονται στο μέτρο [NS6], προκειμένου να εξασφαλίζεται η απρόσκοπτη λειτουργία σε περίπτωση απειλής κατά της διαθεσιμότητας πληροφοριών και υπηρεσιών. Πηγή: NIST 800-53, PNNL
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν εφαρμόζει καθόλου μέτρα για την προστασία της (λογικής) περιμέτρου του οργανισμού.
1	1	Υπάρχει firewall ο οποίος λειτουργεί ως σημείο διεπαφής ανάμεσα στο τοπικό δίκτυο και το εξωτερικό δίκτυο.
1	2	Οι ρυθμίσεις του συγκεκριμένου firewall είναι τουλάχιστον στοιχειώδεις ή/και μπορεί να μην διενεργείται τακτικός και ουσιαστικός έλεγχος και διαχείριση.
2	1	Στα πλαίσια του [RM2] διενεργείται ανάλυση στην οποία κατανοείται ποια είναι τα στοιχεία ενεργητικού που χρησιμοποιούνται προκειμένου να μπορούν να δώθούν οι σχετικές υπηρεσίες.
2	2	Για κάθε ένα από τα κρίσιμα στοιχεία ενεργητικού (όπως αυτά έχουν αναγνωριστεί στο [DS2]), έχουν αναγνωρισθεί και καταγραφεί οι τρόποι με τους οποίους μπορεί να υπερφορτωθεί, καθώς και τα όρια (σε bandwidth, επεξεργαστική ισχύ και αποθηκευτικό χώρο) πέρα από τα οποία η διαθεσιμότητα του στοιχείου διακινδυνεύεται.
2	3	Κίνδυνοι που σχετίζονται με την απώλεια της διαθεσιμότητας των κρίσιμων στοιχείων ενεργητικού περιλαμβάνονται μέσα στην ανάλυση και αξιολόγηση κινδύνων.
2	4	Τα κρίσιμα συστήματα προστατεύονται από περισσότερα του ενός επίπεδα.
3	1	Έχει θεσπιστεί, εφαρμόζεται και διατηρείται επαρκή προστασία από άρνηση παροχής υπηρεσιών και διανεμημένη άρνηση παροχής υπηρεσιών, προκειμένου να διασφαλίζεται η έγκαιρη και ποιοτική παροχή της υπηρεσίας σε εξουσιοδοτημένους και επικυρωμένους χρήστες και να διατηρείται σταθερό επίπεδο παραγωγικότητας.
3	2	Έχουν εφαρμοστεί μέτρα για την εξουσιοδότηση και αυθεντικοποίηση των λογαριασμών που αποκτούν πρόσβαση στον οργανισμό. Δεν επιτρέπεται μη αυθεντικοποιημένη πρόσβαση, όπως αναφέρεται και στο [IAM1].
3	3	Έχει ενεργοποιηθεί παρακολούθηση και καταγραφή ενεργειών σύμφωνα με το [IAM6].
3	4	Λαμβάνονται υπόψη μέτρα εφεδρείας και υψηλής διαθεσιμότητας, όπως περιγράφονται στο μέτρο [NS6] και στο [AM4] προκειμένου να εξασφαλίζεται η απρόσκοπτη λειτουργία σε περίπτωση απειλής κατά της διαθεσιμότητας πληροφοριών και υπηρεσιών.
3	5	Υλοποιείται διαχωρισμός δικτύων όπως προβλέπεται στο [NS2].
3	6	Σε κάθε περίπτωση στοιχεία τα οποία χρειάζεται να είναι προσβάσιμα από το εξωτερικό δίκτυο (και είναι πιθανότερο να στοχοποιηθούν), είναι διαχωρισμένα από το εσωτερικό δίκτυο.
4	1	Υλοποιούνται συστήματα παρακολούθησης της διαθεσιμότητας των κρίσιμων υπηρεσιών του και των στοιχείων ενεργητικού σύμφωνα με το [AM4], που έχουν την δυνατότητα να ανιχνεύουν επιθέσεις άρνησης παροχής υπηρεσιών και να στέλνουν ειδοποίηση σε πραγματικό χρόνο.
4	2	Ειδικά για οργανισμούς που παρέχουν υπηρεσίες μέσω του διαδικτύου, λαμβάνονται ειδικά μέτρα σε σχέση με την υπηρεσία DNS. Ο οργανισμός έχει 2 τουλάχιστον εξυπηρετητές DNS. Οι δυο εξυπηρετητές είναι προστατευμένοι (φυσικά και λογικά) και βρίσκονται σε διαφορετικές τοποθεσίες. Μεταξύ των δυο DNS γίνονται μεταφορές ζώνης τουλάχιστον μια φορά στις 24 ώρες και υλοποιούνται μέτρα για την ανθεκτικότητα έναντι επιθέσεων.
4	3	Η χρήση source routing απαγορεύεται.
4	4	Τα διάφορα κρίσιμα συστήματα έχουν την δυνατότητα να διαχειρίζονται την πλεονάζουσα χωρητικότητα (π.χ. bandwidth, memory κ.α.) προκειμένου να μειώσουν τις επιπτώσεις από μια επίθεση τέτοιου είδους.
4	5	Σε περίπτωση που γίνει αντιληπτή μια σχετική προσπάθεια, το εξουσιοδοτημένο προσωπικό ενημερώνεται άμεσα και να διενεργεί ενέργειες αντιμετώπισης σύμφωνα με το [EIM1].

4	6	Διενεργείται έλεγχος στα στοιχεία της παρακολούθησης σχετικά με την περίληψη στοιχείων που αναφέρονται στο ML3. Μέσω κατάλληλων τεχνικών μέτρων, γίνεται παρακολούθηση της κατάστασης των στοιχείων ενεργητικού όπως προβλέπεται από το [AM6].
4	7	Έχουν τεθεί συγκεκριμένοι κανόνες με όρια (thresholds) για την κατανάλωση συγκεκριμένων δυνατοτήτων των στοιχείων ενεργητικού (π.χ. bandwidth, memory, disk, κ.α.) ώστε να ενημερώνεται άμεσα το διαχειριστικό προσωπικό.
4	8	Το προσωπικό διενεργεί άμεσα αναλύσεις και εξάγει στοιχεία τάσεων ώστε να καθοριστεί ο λόγος για την σχετική συμπεριφορά και ενεργοποιεί την διαδικασία διαχείρισης περιστατικών ασφαλείας σύμφωνα με το [EIM1].
4	9	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
4	10	Εφαρμόζεται η χρήση του domain registrar locking για να εμποδίσει άρνηση παροχής υπηρεσιών λόγω μη εξουσιοδοτημένης διαγραφής, μεταφοράς ή αλλοίωσης της εγγραφής του domain του.
4	11	Χρησιμοποιείται λογισμικό (custom / open / proprietary) το οποίο έχει, κατ' ελάχιστο, λάβει μέτρα προστασίας από προεπιλογή και κατά το σχεδιασμό έναντι των OWASP TOP 10 (για web applications, APIs) και άλλων αντίστοιχων βέλτιστων πρακτικών για τις λοιπές εφαρμογές (OWASP ASVS).
5	1	Η φιλοξενία της δημόσιας πρόσβασης εφαρμογών δίνεται σε εξωτερικό αναγνωρισμένο και υψηλής ασφάλειας παρεχόμενης υπηρεσίας cloud υπηρεσιών (π.χ. τουλάχιστον score 10 στα πλαίσια στου CSA), μετά από ενδελεχή αξιολόγηση και αναζήτηση χαρακτηριστικών όσον αφορά στην ικανότητά του να ανθίσταται σε επιθέσεις άρνησης παροχής υπηρεσιών. Στις σχετικές συμβάσεις λαμβάνονται μέτρα και εγγυήσεις όπως προβλέπεται στην [TPS1].
5	2	Ειδικευμένος πάροχος cloud υπηρεσιών ασφάλειας (security as a service) έχει αναλάβει την παροχή υπηρεσιών προστασίας των δημόσιας πρόσβασης εφαρμογών από κατανεμημένες επιθέσεις άρνησης παροχής υπηρεσιών(π.χ. τουλάχιστον score 10 στα πλαίσια στου CSA), μετά από ενδελεχή αξιολόγηση και αναζήτηση χαρακτηριστικών όσον αφορά στην ικανότητά του να ανθίσταται σε επιθέσεις άρνησης παροχής υπηρεσιών. Στις σχετικές συμβάσεις λαμβάνονται μέτρα και εγγυήσεις όπως προβλέπεται στην [TPS1].
5	3	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	4	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
NS4		Μέτρο: Ασφαλή πρωτόκολλα επικοινωνίας Στόχος Μέτρου: Να διασφαλιστούν κατάλληλα πρωτοκόλλα επικοινωνίας προκειμένου να επιτευχθεί ασφαλής επικοινωνία μεταξύ των πόρων του δικτύου Περιγραφή Μέτρου: Θέσπιση, εφαρμογή και διατήρηση ασφαλών πρωτοκόλλων για τη διευκόλυνση της διακίνησης πληροφοριών μεταξύ σημείων δικτύου, εφαρμογών και συστημάτων, προκειμένου να διασφαλίζεται η εμπιστευτικότητα και η ακεραιότητα των πληροφοριών κατά τη μεταφορά τους, και να αποτρέπονται επιθέσεις και απειλές στο δίκτυο, όπως για παράδειγμα υποκλοπές επικοινωνιών. Ο οργανισμός εξετάζει τα πλέον σύγχρονα πρωτόκολλα επικοινωνίας κατά τη διασφάλιση της μεταφοράς και ανταλλαγής πληροφοριών μέσω δικτύων επικοινωνίας. Ο οργανισμός πρέπει να λαμβάνει υπόψη μέτρα ασφάλειας που υποστηρίζονται από κρυπτογραφικά μέσα, όπως αυτά ορίζονται στο μέτρο [AM5] για την ασφάλεια των επικοινωνιών, χρησιμοποιώντας τεχνολογίες όπως το Hypertext Transfer Protocol Secure (HTTPS), το Internet Protocol security (IPsec), το Transport Layer Security (TLS) / Secure Sockets Layer (SSL), ανάλογα με το επιδιωκόμενο επίπεδο τεχνολογίας Πηγή:
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν εφαρμόζει καθόλου μέτρα για την προστασία της (λογικής) περιμέτρου του οργανισμού.
1	1	Υπάρχει firewall ο οποίος λειτουργεί ως σημείο διεπαφής ανάμεσα στο τοπικό δίκτυο και το εξωτερικό δίκτυο.
1	2	Οι ρυθμίσεις του συγκεκριμένου firewall είναι τουλάχιστον στοιχειώδεις ή/και μπορεί να μην διενεργείται τακτικός και ουσιαστικός έλεγχος και διαχείριση από την μεριά του οργανισμού, σε σχέση με τα επιτρεπόμενα και χρησιμοποιούμενα πρωτόκολλα επικοινωνίας.
2	1	Έχουν αναγνωρισθεί οι διαδικασίες μέσω των οποίων γίνεται ανταλλαγή πληροφοριών υψηλής κρισιμότητας (π.χ. passwords) και χρησιμοποιούνται πρωτόκολλα και τρόποι επικοινωνίας που υλοποιούν κρυπτογράφηση.

2	2	Σε τέτοιες περιπτώσεις άλλα πρωτόκολλα τα οποία δεν υποστηρίζουν ενεργά ισχυρή κρυπτογράφηση χρησιμοποιούνται σε συνδυασμό με δεύτερο μέτρο (π.χ. telnet, virtual network computing, remote desk protocol πάνω από SSL ή Internet Protocol Security (IPsec)).
3	1	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται ασφαλή πρωτόκολλα για τη διευκόλυνση της διακίνησης πληροφοριών μεταξύ σημείων δικτύου, εφαρμογών και συστημάτων, προκειμένου να διασφαλίζεται η εμπιστευτικότητα και η ακεραιότητα των πληροφοριών κατά τη μεταφορά τους, και να αποτρέπονται επιθέσεις και απειλές στο δίκτυο, όπως για παράδειγμα υποκλοπές επικοινωνιών.
3	2	Εξετάζονται τα πλέον σύγχρονα πρωτόκολλα επικοινωνίας κατά τη διασφάλιση της μεταφοράς και ανταλλαγής πληροφοριών μέσω δικτύων επικοινωνίας.
3	3	Λαμβάνονται υπόψη μέτρα ασφάλειας που υποστηρίζονται από κρυπτογραφικά μέσα, όπως αυτά ορίζονται στο μέτρο [AM5] για την ασφάλεια των επικοινωνιών, χρησιμοποιώντας τεχνολογίες όπως το Hypertext Transfer Protocol Secure (HTTPS), το Internet Protocol security (IPsec), το Transport Layer Security (TLS) / Secure Sockets Layer (SSL), ανάλογα με το επιδιωκόμενο επίπεδο τεχνολογίας
3	4	Ειδικά για τα κρίσιμα ή ευαίσθητα δεδομένα, υλοποιείται κρυπτογράφηση κατά την ανταλλαγή ή μεταφορά. Παραδείγματα τέτοιας υλοποίησης περιλαμβάνει (Transport Layer Security (TLS) and Open Secure Shell (OpenSSH) κα.).
3	5	Τα δεδομένα που μεταφέρονται με φυσικά μέσα, πρώτα κρυπτογραφούνται κατάλληλα και μετά αποστέλλονται. Τα κλειδιά κρυπτογράφησης μεταφέρονται χωριστά, με άλλο μέσο (ή τρόπο) χωρίς επισήμανση της χρήσης τους.
3	6	Για σύγχρονη μεταφορά χρησιμοποιούνται πρωτόκολλα των πιο πρόσφατων σταθερών εκδόσεων πρωτοκόλλων όπως είναι το SFTP ή HTTPS.
3	8	Γίνονται ανασκόπηση και αναλύονται τα διάφορα συστήματα και στοιχεία προκειμένου να αναγνωρίζονται ποια πρωτοκόλλα, πόρτες και υπηρεσίες απαιτούνται για την ορθή και αποτελεσματική λειτουργία τους. Οτιδήποτε δεν προκύπτει ότι απαιτείται απενεργοποιείται. (Αυτό αφορά και πρωτόκολλα και μεθόδους όπως είναι το Bluetooth, FTP, peer-to-peer κ.α.)
4	1	Για την ανταλλαγή πληροφοριών μέσω APIs, γίνεται κατάλληλος σχεδιασμός, παραμετροποίηση, υλοποίηση και λειτουργίας ώστε να συμμορφώνεται με το επίπεδο ασφάλειας του οργανισμού.
4	2	Εφαρμόζονται βέλτιστες διεθνείς πρακτικές (π.χ. API OWASP Top Ten) .
4	3	Η εμπιστευτικότητα των δεδομένων εξασφαλίζεται είτε με κρυπτογράφηση σε επίπεδο καναλιού είτε με κρυπτογράφηση σε επίπεδο δεδομένων όταν γίνεται μεταφορά σε διαφορετικά δίκτυα ακόμα και εντός του ίδιου οργανισμού.
4	4	Για την κίνηση προς το εξωτερικό του οργανισμού (outgoing web, FTP, SSL) γίνεται δρομολόγηση μέσω (τουλάχιστον) ενός proxy σε ένα DMZ δίκτυο. Ο proxy υποστηρίζει παρακολούθηση των TCP sessions, και αποκλείει πρόσβαση σε συγκεκριμένα URLs, domain names και IPs.
4	5	Έχει απενεργοποιηθεί η αποστολή στοιχείων ανατροφοδότησης (τουλάχιστον όσο αφορά πληροφορία που δεν έχει ήδη ο αιτών) σε περίπτωση που γίνεται κάποιο λάθος επικύρωσης (feedback to senders on protocol format validation failure).
4	6	Χρησιμοποιείται secure routing protocols ή static routes προκειμένου να μην φαίνεται η εσωτερική δομή του.
4	7	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Έχουν ενεργοποιηθεί περιορισμοί σε σχέση με το VOIP.
5	2	Συγκεκριμένα, χρήση VOIP γίνεται μόνο για συγκεκριμένες εξουσιοδοτημένες χρήσεις και μόνο μέσω συγκεκριμένων dedicated τμημάτων του δικτύου.
5	3	Υλοποιούνται ρυθμίσεις για την προστασία της σχετικής λειτουργίας και την εξασφάλιση υψηλού επιπέδου ασφάλειας επικοινωνιών.
5	4	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	5	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.

NS5		Μέτρο: Έλεγχος πρόσβασης στο δίκτυοΣτόχος Μέτρου: Να εξασφαλιστεί ότι η πρόσβαση στο λογικό δίκτυο από εξωτερικά και εσωτερικά συστήματα ασφαλίζεται κατάλληλα, ώστε μόνο τα εξουσιοδοτημένα πρόσωπα να μπορούν να έχουν πρόσβαση σε οργανωτικούς πόρους.Περιγραφή Μέτρου: Θέσπιση, εφαρμογή και διατήρηση μέτρων ελέγχου πρόσβασης στο δίκτυο, ώστε να διασφαλίζεται η λογική πρόσβαση στο δίκτυο του οργανισμού και στους πόρους πληροφοριών, και να αποτρέπεται η μη εξουσιοδοτημένη πρόσβαση. Ο οργανισμός θα πρέπει να εξετάζει συγκεκριμένα τεχνικά και οργανωτικά μέτρα, όπως τους μηχανισμούς επαλήθευσης ταυτότητας για πρόσβαση στο δίκτυο, προκειμένου να διευκολύνει τη λειτουργία του εν λόγω μέτρου. Ο οργανισμός θα πρέπει να εξετάζει το ενδεχόμενο ελέγχου πρόσβασης στο δίκτυο για ενσύρματη, ασύρματη και άλλου είδους σύνδεση με το δίκτυο. Ο οργανισμός θα πρέπει να εξετάσει το ενδεχόμενο ενσωμάτωσης του ελέγχου της πρόσβασης στο δίκτυο με κεντρικά διαπιστευτήρια και με διαδικασίες διαχείρισης της ταυτότητας και της πρόσβασης, όπως ορίζεται στο μέτρο [IAM5]. Πηγή:
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν διαχειρίζεται καθόλου την πρόσβαση στα συστήματά του (λογικά ή φυσικά).
1	1	Υπάρχουν συστήματα για την διαχείριση πρόσβασης στο δίκτυό.
2	1	Υπάρχει μια πολιτική ελέγχου πρόσβασης η οποία καλύπτει όλα τα στοιχεία ενεργητικού και τα κτήρια του οργανισμού όπως εμφανίζονται στο κατάλογο στοιχείων ενεργητικού σύμφωνα με το [AM2].
2	2	Η πολιτική ελέγχου πρόσβασης καλύπτει τουλάχιστον την πρόσβαση σε εφαρμογές, δίκτυα, πόρους και κτήρια.
3	1	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται μέτρα ελέγχου πρόσβασης στο δίκτυο, ώστε να διασφαλίζεται η λογική πρόσβαση στο δίκτυο του οργανισμού και στους πόρους πληροφοριών, και να αποτρέπεται η μη εξουσιοδοτημένη πρόσβαση.
3	2	Υλοποιούνται συγκεκριμένα τεχνικά και οργανωτικά μέτρα, όπως τους μηχανισμούς επαλήθευσης ταυτότητας για πρόσβαση στο δίκτυο, προκειμένου να διευκολύνται η λειτουργία του εν λόγω μέτρου.
3	3	Υλοποιούνται μέτρα για τον έλεγχο πρόσβασης στο δίκτυο για ενσύρματη, ασύρματη και άλλου είδους σύνδεση με το δίκτυο.
3	4	Σε περίπτωση παροχής πρόσβασης σε ασύρματα δίκτυα για δημόσια πρόσβαση, αυτά είναι διαχωρισμένα από το υπόλοιπο δίκτυο.
3	5	Σε κάθε περίπτωση οι διαδικασίες που αναφέρονται στο [IAM1] ισχύουν.
4	1	Η ασύρματη δικτυακή κυκλοφορία κρυπτογραφείται με τον αλγόριθμο Advanced Encryption Standard (AES) με χρήση κλειδιού μήκους 256 bits.
4	2	Χρησιμοποιείται ασύρματο σύστημα ανίχνευσης εισβολών (wireless intrusion detection system, WIDS) για την ανίχνευση μη εγκεκριμένων ασύρματων σημείων πρόσβασης (wireless access points) συνδεδεμένων στο δίκτυο.
4	3	Για την πρόσβαση μέσω ασύρματου δικτύου χρησιμοποιούνται κατάλληλα πρωτοκόλλα αυθεντικοποίησης όπως είναι extensible authentication protocol-transport layer security.
4	4	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Απενεργοποιείται η ασύρματη πρόσβαση σε διάφορα στοιχεία που έχουν την συγκεκριμένη δυνατότητα αλλά δεν απαιτείται για την σωστή και αποτελεσματική τους λειτουργία.
5	2	Υλοποιούνται σχετικές τεχνικές διαδικασίες και εργαλεία για την εξουσιοδότηση της χρήσης ασύρματων δικτύων ενώ υπάρχει αυστηρή πολιτική για το ποιος χρήστης έχει δικαίωμα να παραμετροποιεί wireless networking capabilities.
5	3	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	4	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.

NS6		Μέτρο: Εφεδρεία και υψηλή διαθεσιμότητα Στόχος Μέτρου: Να εξασφαλιστεί της η διαθεσιμότητα πληροφοριών και δικτύων πληροφοριών με την επίτευξη επαρκούς διαθεσιμότητας πόρων, εφεδρικού εξοπλισμού, συστημάτων και συνδέσεων υψηλής διαθεσιμότητας. Περιγραφή Μέτρου: Θέσπιση, εφαρμογή και διατήρηση επαρκών μέτρων για να διασφαλίζεται ένα εύλογο επίπεδο εφεδρείας και υψηλής διαθεσιμότητας, ιδίως για τα συστήματα, τις υπηρεσίες και τις εφαρμογές ζωτικής σημασίας που επεξεργάζονται διαβαθμισμένες ή/και επιχειρησιακές πληροφορίες. Ο οργανισμός πρέπει να εξετάζει το ενδεχόμενο εφεδρείας και υψηλής διαθεσιμότητας σε όλα τα επίπεδα τεχνολογίας, μεταξύ άλλων, αποθήκευσης, επικοινωνίας και επεξεργασίας. Ο οργανισμός λαμβάνει υπόψη τεχνολογίες εφεδρείας και υψηλής διαθεσιμότητας όπως είναι τα συστήματα εναλλακτικής σύνδεσης ή εφεδρείας, Redundant Arrays of Independent Disks (RAID), και εγκαταστάσεις αποθήκευσης δεδομένων σε cold, warm και hot. Πηγή:
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν έχει λάβει μέτρα για την εξασφάλιση της διαθεσιμότητας των δικτύων και συστημάτων πληροφορικής.
1	1	Υπάρχει κάποιος εξοπλισμός σε εφεδρεία που μπορεί να χρησιμοποιηθεί σε περίπτωση αστοχίας ενός στοιχείου ενεργητικού.
2	1	Έχουν αναγνωρισθεί τα κρίσιμα στοιχεία ενεργητικού.
2	2	Για τα συγκεκριμένα στοιχεία υπάρχει τουλάχιστον ένα ακόμα στοιχείο σε εφεδρεία (μπορεί να είναι το ίδιο ή αντίστοιχης ικανότητας).
2	3	Τα στοιχεία αυτά περιέχονται μέσα στον κατάλογο στοιχείων ενεργητικού.
3	1	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται επαρκή μέτρα για να διασφαλίζεται ένα εύλογο επίπεδο εφεδρείας και υψηλής διαθεσιμότητας, ιδίως για τα συστήματα, τις υπηρεσίες και τις εφαρμογές ζωτικής σημασίας που επεξεργάζονται διαβαθμισμένες ή/και επιχειρησιακές πληροφορίες.
3	2	Εξασφαλίζεται εφεδρεία και υψηλή διαθεσιμότητα σε όλα τα επίπεδα τεχνολογίας, μεταξύ άλλων, αποθήκευσης, επικοινωνίας και επεξεργασίας.
3	3	Λαμβάνονται υπόψη τεχνολογίες εφεδρείας και υψηλής διαθεσιμότητας όπως είναι τα συστήματα εναλλακτικής σύνδεσης ή εφεδρείας, Redundant Arrays of Independent Disks (RAID), και εγκαταστάσεις αποθήκευσης δεδομένων σε cold, warm και hot.
3	4	Κατ΄ ελάχιστο ο εξοπλισμός που βρίσκεται στον οργανισμό διαθέτει εφεδρείες σε σχέση με την ενέργεια, την χωρητικότητα, το δίκτυο και τον τρόπο διασύνδεσης. Δεν υπάρχει κρίσιμος εξοπλισμός που δεν έχει εφεδρικό εντός του ίδιου χώρου σε ενεργή ή και ανενεργή λειτουργία.
3	5	Υπάρχει εξοπλισμός σε δευτερεύον σημείο, ο οποίος έχει σχετικά μελετηθεί ώστε να μπορεί να χρησιμοποιηθεί για να ανακάμψουν οι βασικές δραστηριότητες του οργανισμού ενός συγκεκριμένου χρονικού διαστήματος και σε συγκεκριμένο επίπεδο.
3	6	Τηρούνται εφεδρικά αντίγραφα ασφαλείας όπως αναφέρονται στο [DS3].
3	7	Έχουν τεθεί συγκεκριμένοι κανόνες με όρια (thresholds) για την κατανάλωση συγκεκριμένων δυνατοτήτων των στοιχείων ενεργητικού (π.χ. bandwidth, memory, disk, κ.α.) ώστε να ενημερώνεται άμεσα το διαχειριστικό προσωπικό. Το προσωπικό διενεργεί άμεσα αναλύσεις και εξάγει στοιχεία τάσεων ώστε να καθοριστεί ο λόγος για την σχετική συμπεριφορά και ενεργοποιεί την διαδικασία διαχείρισης περιστατικών ασφαλείας σύμφωνα με το [EIM1].
4	1	Έχει υλοποιηθεί ο σχεδιασμός και τα μέτρα που απαιτούνται για την ορθή και αποτελεσματική λειτουργία του Σχεδίου επιχειρησιακής συνέχειας και του Σχεδίου αποκατάστασης από καταστροφή όπως αναφέρονται στα [BCR1-4].
4	2	Υπάρχει τουλάχιστον μια δεύτερη εγκατάσταση αποθήκευσης δεδομένων με τον κρίσιμο εξοπλισμό σε κατάσταση που μπορεί να χαρακτηριστεί ως warm.
4	3	Υπάρχουν εφεδρικά καλώδια (δικτύου, ρεύματος, και ότι άλλο απαιτείται) από διαφορετικές (φυσικά διαχωρισμένες) οδεύσεις, λαμβάνοντας υπόψη τους σχετικούς κινδύνους.
4	4	Διενεργούνται δοκιμές για την αξιολόγηση της ύπαρξης και δυνατότητας ορθής και αποτελεσματικής λειτουργίας του εν λόγω εξοπλισμού αν απαιτηθεί. Σε περίπτωση αναγνώρισης προβλημάτων, αυτά διορθώνονται άμεσα και τηρούνται καταγραφές σύμφωνα με την διαδικασία διαχείρισης αλλαγών [CM1].
4	5	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Υπάρχει τουλάχιστον μια δεύτερη εγκατάσταση αποθήκευσης δεδομένων με τον κρίσιμο εξοπλισμό σε κατάσταση που μπορεί να χαρακτηριστεί ως hot.

5	2	Οι διαδικασίες για την μετάβαση μεταξύ των δυο εγκαταστάσεων είναι αυτόματες με την ελάχιστη δυνατή ανθρώπινη παρέμβαση. (Οι σχετικές εγκαταστάσεις αποθήκευσης και λειτουργίας ακολουθούν διεθνείς βέλτιστες πρακτικές για την διαθεσιμότητα και ανθεκτικότητα – π.χ. επιπέδου τουλάχιστον Tier III Uptime institute.)
5	3	Διενεργούνται δοκιμές για την αξιολόγηση της ύπαρξης και δυνατότητας ορθής και αποτελεσματικής λειτουργίας του εν λόγω εξοπλισμού όταν απαιτηθεί.
5	4	Σε περίπτωση αναγνώρισης προβλημάτων, αυτά διορθώνονται άμεσα και να τηρούνται καταγραφές σύμφωνα με την διαδικασία διαχείρισης αλλαγών [CM1].
5	5	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	6	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
NS7		Μέτρο: Ανίχνευση και πρόληψη εισβολώνΣτόχος Μέτρου: Να διασφαλιστεί η ανίχνευση και η πρόληψη από εξωτερικές απόπειρες εισβολής και επιθέσεις ασφάλειας.Περιγραφή Μέτρου: Θέσπιση, εφαρμογή και διατήρηση επαρκών μέτρων για τον εντοπισμό και την πρόληψη εισβολών στο δίκτυο και τους πόρους του οργανισμού. Ο οργανισμός θα πρέπει να λαμβάνει υπόψη τα συστήματα ανίχνευσης εισβολών (IDS) και τα συστήματα πρόληψης εισβολών (IPS) για τον μετριασμό του κινδύνου απόπειρας εξωτερικής εισβολής. Ο οργανισμός εξετάζει το ενδεχόμενο δημιουργίας κονσόλας διαχείρισης για την παρακολούθηση του δικτύου με στόχο την καταχώρηση όλων των απόπειρών εισβολής για περαιτέρω ανάλυση. Στα πλαίσια σχεδιασμού των διαδικασιών ανίχνευσης και πρόληψης εισβολών, ο οργανισμός πρέπει να εξετάσει το ενδεχόμενο αυτόματης ενεργοποίησης μοχλών για την αντιμετώπιση συμβάντων, όπως ορίζεται στο [EIM2]. Ο οργανισμός πρέπει να λαμβάνει υπόψη τις λύσεις για τη διαχείριση συμβάντων και περιστατικών ασφάλειας (SIEM) για την υποστήριξη των διαδικασιών πρόληψης και ανίχνευσης εισβολών. Πηγή:
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν εφαρμόζει καθόλου μέτρα για την προστασία της (λογικής) περιμέτρου του οργανισμού.
1	1	Υπάρχει firewall ο οποίος λειτουργεί ως σημείο διεπαφής ανάμεσα στο τοπικό δίκτυο και το εξωτερικό δίκτυο.
1	2	Οι ρυθμίσεις του συγκεκριμένου firewall είναι τουλάχιστον στοιχειώδεις ή/και μπορεί να μην διενεργείται τακτικός και ουσιαστικός έλεγχος και διαχείριση.
2	1	Για τα κρίσιμα στοιχεία ενεργητικού, όπως αυτά αποτυπώνονται στον σχετικό κατάλογο [AM2 / RM2], έχει ενεργοποιηθεί κατ'ελάχιστο μη αυτοπατοποιημένη παρακολούθηση.
2	2	Η παρακολούθηση περιλαμβάνει κατ’ ελάχιστο τις ενέργειες των ατόμων, αντικειμένων και οντοτήτων όταν αποκτούν πρόσβαση ή χρησιμοποιούν τα στοιχεία ενεργητικού, τα γεγονότα που μπορεί να διαταράξουν την ομαλή λειτουργία μιας δραστηριότητας, τις αλλαγές των στοιχείων ενεργητικού που οδηγούν σε διαφοροποίηση από το security baseline, στοιχεία ενεργητικού που συνδέονται (μη-αναμενόμενα) στα δίκτυα του οργανισμού και οποιαδήποτε άλλη ύποπτη δραστηριότητα.
3	1	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται επαρκή μέτρα για τον εντοπισμό και την πρόληψη εισβολών στο δίκτυο και τους πόρους του οργανισμού.
3	2	Έχουν υλοποιηθεί και διατηρούνται συστήματα ανίχνευσης εισβολών (IDS) και συστήματα πρόληψης εισβολών (IPS) για τον μετριασμό του κινδύνου απόπειρας εξωτερικής εισβολής.
3	3	Σε περίπτωση αναγνώρισης μη τυπικής (anomalous) συμπεριφορά, ενεργοποιείται η διαδικασία ανταπόκρισης περιστατικών ασφαλείας και απομονώνονται τα σχετικά στοιχεία μέχρι να διερευνηθεί πλήρως η κατάσταση.
3	4	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται δυνατότητες παρακολούθησης των στοιχείων ενεργητικού, ώστε ο οργανισμός να είναι σε θέση να εντοπίζει ανωμαλίες σε σχέση με κανονικές συνθήκες (π.χ. τοποθεσία, χρήση) και/ή τη λειτουργία των στοιχείων αυτών σύμφωνα με το [AM3].
4	1	Χρησιμοποιείται κονσόλα διαχείρισης για την παρακολούθηση του δικτύου με στόχο την καταχώρηση όλων των απόπειρών εισβολής για περαιτέρω ανάλυση.
4	2	Στα πλαίσια σχεδιασμού των διαδικασιών ανίχνευσης και πρόληψης εισβολών, υλοποιείται αυτόματη ενεργοποίηση μοχλών για την αντιμετώπιση συμβάντων, όπως ορίζεται στο [EIM2].
4	3	Χρησιμοποιείται ασύρματο σύστημα ανίχνευσης εισβολών (wireless intrusion detection system, WIDS) για την ανίχνευση μη εγκεκριμένων ασύρματων σημείων πρόσβασης (wireless access points) συνδεδεμένων στο δίκτυο του οργανισμού.
4	4	Έχει υλοποιηθεί IDS εντός της DMZ για ανάλυση της πληροφορίας που ανταλλάσσεται με το εξωτερικό δίκτυο.

4	5	Έχουν υλοποιηθεί IDS sensors στο εξωτερικό δίκτυο αλλά και σε δίκτυα που είναι εκτεθειμένα, για πιο άμεσο εντοπισμό σχετικών επιθέσεων με την χρήση υπογραφών, ανάλυσης κυκλοφορίας ή και άλλων μηχανισμών.
4	6	Η πληροφορία που εξάγεται από τα διάφορα εργαλεία και επίπεδα παρακολούθησης και καταγραφής ενεργειών αναλύεται και τα συμπεράσματα χρησιμοποιούνται στην εκπαίδευση των σχετικών εργαλείων με σκοπό την μείωση των false positives, την μείωση των false negatives και το γενικό fine tuning τους.
4	7	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Έχει τεθεί σε λειτουργία σύστημα SIEM το οποίο συγκεντρώνει τα στοιχεία παρακολούθησης από το σύνολο των στοιχείων ενεργητικού του οργανισμού.
5	2	Έχουν παραμετροποιηθεί κανόνες και έχουν δημιουργηθεί ενημερώσεις (notifications & alerts) στο κατάλληλο προσωπικό σε περίπτωση ενεργοποίησης κάποιου κανόνα. Για την δημιουργία των κανόνων έχουν ληφθεί υπόψη βασικές μέθοδοι επίθεσης.
5	3	Το SIEM λειτουργεί κατ΄ ελάχιστον σύμφωνα με τους κανόνες και τις άλλες προδιαγραφές που αναφέρονται στο [AM3].
5	4	Έχει υλοποιηθεί network based IPS, τα οποία σε συνεργασία με τα IDS, αποτρέπουν συγκεκριμένη κίνηση, συμπεριφορά ή άλλο.
5	5	Τα IPS είναι παραμετροποιημένα (όπως και οι άλλες συσκευές δικτύου όπως αναφέρονται στο [NS1] να παρακολουθούν και να καταγράφουν όλη την κίνηση.
5	6	Έχει δημιουργηθεί μια διασύνδεση ανάμεσα στο IDS και στα εργαλεία ελέγχου πρόσβασης ώστε να μπορούν να ενεργοποιηθούν άμεσα μηχανισμοί για την λήψη κατάλληλων ενεργειών απαγόρευσης πρόσβασης σε περίπτωση σχετικής επίθεσης.
5	7	Το SIEM είναι παραμετροποιημένο ώστε να στέλνει ενημερώσεις σε κατάλληλα εξουσιοδοτημένες και εκπαιδευμένες ομάδες ατόμων, σε περίπτωση αναγνώρισης κάποιου πιθανού security related event.
5	8	Το SIEM συνδυάζει την πληροφορία που έρχεται από διαφορετικές πηγές (όχι μόνο από το IDS/IPS) προκειμένου να δώσει τα βέλτιστα δυνατά αποτελέσματα (σχετικά συστήματα είναι: firewalls, routers, anti-virus software, servers κ.α.). Αν είναι δυνατό, ο οργανισμός επεκτείνει τις πηγές πληροφορίας του SIEM και σε δεδομένα από την φυσική παρακολούθηση ή από την εφοδιαστική αλυσίδα.
5	9	Έχει ανατεθεί σε κατάλληλο εσωτερικό ή εξωτερικό προσωπικό η παρακολούθηση 24x7x365 των σχετικών εργαλείων και στοιχείων, για όσο πιο έγκαιρη προειδοποίηση και όσο πιο άμεση ανταπόκριση γίνεται.
5	10	Διενεργούνται δοκιμές για τον έλεγχο των εργαλείων IDS, IPS και SIEM καθώς και της ετοιμότητας και ικανότητας του σχετικού προσωπικού σε τακτική βάση.
5	11	Έχουν ληφθεί υπόψη κατά το σχεδιασμό και την υλοποίηση των συγκεκριμένων εργαλείων (θέση στο δίκτυο, τύπος του εργαλείου, είδη κανόνων κ.α.) οι ανάγκες για παρακολούθηση και οι ανάγκες για προστασία (π.χ. encryption).
5	12	Υλοποιούνται μέτρα για τον έλεγχο της πληροφορίας που εξέρχεται από το δίκτυό του όπως αναφέρεται στο [NS1].
5	13	Αναγνωρίζονται Indicators of Compromise για ανταπόκριση με μεγαλύτερη ταχύτητα και μειώση της επίπτωσης μιας σχετικής επίθεσης στον οργανισμό.
5	14	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	15	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.

Κατηγορία		ΑΣΦΑΛΕΙΑ ΣΥΣΤΗΜΑΤΩΝ
SS1		Μέτρο: Καταπολέμηση κακόβουλου λογισμικού Στόχος Μέτρου: Να διασφαλιστεί ότι δεν θα επηρεαστούν οργανωτικοί πόροι από κακόβουλο λογισμικό και κώδικα. Περιγραφή Μέτρου: Θέσπιση, εφαρμογή και διατήρηση επαρκών μέτρων για την προστασία των συστημάτων από μολύνσεις από κακόβουλο λογισμικό και κώδικα, προκειμένου να διασφαλίζεται η εμπιστευτικότητα, η ακεραιότητα, η διαθεσιμότητα και η αυθεντικότητα των πληροφοριών. Ο οργανισμός εξετάζει σειρά μέτρων για την καταπολέμηση κακόβουλου λογισμικού, μεταξύ άλλων, λειτουργικά συστήματα, συστήματα και υπηρεσίες δικτύου, λειτουργικά συστήματα εξοπλισμού δικτύου, τερματικά σημεία χρηστών και κινητές συσκευές, καθώς και φορητές συσκευές περιεχομένου. Ο οργανισμός πρέπει να διασφαλίζει ότι τα μέτρα καταπολέμησης του κακόβουλου λογισμικού βασίζονται σε ενημερωμένα δεδομένα με σκοπό τον εντοπισμό και την επίλυση απειλών από κακόβουλο λογισμικό. Πηγή:
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν έχει υλοποιήσει κανένα μέτρο για την προστασία από κακόβουλο λογισμικό / κώδικα.
1	1	Έχει εγκατασταθεί και χρησιμοποιείται λογισμικό για την προστασία από κακόβουλο λογισμικό / κώδικα σε κάποια από τα end-point devices.
2	1	Έχει εγκατασταθεί και χρησιμοποιείται λογισμικό για την προστασία από κακόβουλο λογισμικό / κώδικα σε όλα τα end-point devices.
2	2	Η εγκατάσταση του λογισμικού προστασίας γίνεται με συστηματικό τρόπο με κεντρική διαχείριση.
3	1	Έχει θεσπιστεί, εφαρμόζεται και διατηρείται διαδικασία / πολιτική και μέτρα για την προστασία των συστημάτων από μολύνσεις από κακόβουλο λογισμικό και κώδικα, προκειμένου να διασφαλίζεται η εμπιστευτικότητα, η ακεραιότητα, η διαθεσιμότητα και η αυθεντικότητα των πληροφοριών.
3	2	Εφαρμόζεται μια σειρά μέτρων για την καταπολέμηση κακόβουλου λογισμικού, μεταξύ άλλων, λειτουργικά συστήματα, συστήματα και υπηρεσίες δικτύου, λειτουργικά συστήματα εξοπλισμού δικτύου, τερματικά σημεία χρηστών και κινητές συσκευές, καθώς και φορητές συσκευές περιεχομένου.
3	3	Διασφαλίζεται ότι τα μέτρα καταπολέμησης του κακόβουλου λογισμικού βασίζονται σε ενημερωμένα δεδομένα με σκοπό τον εντοπισμό και την επίλυση απειλών από κακόβουλο λογισμικό.
3	4	Το λογισμικό προστασίας θα είναι παραμετροποιημένο με τέτοιο τρόπο ώστε να: (α) Διενεργεί αυτόματα scan (autoprotect) σε οποιοδήποτε εισερχόμενο, (β) Διενεργεί scan και να μπλοκάρει συνημμένα ηλεκτρονικών επικοινωνιών που περιέχουν κακόβουλο κώδικα ή τύπους αρχείων που ενέχουν αυξημένο κίνδυνο, (γ) Διενεργούν τακτικούς ελέγχους στα σημεία αποθήκευσης πληροφοριών για την αναγνώριση αρχείων ή άλλων στοιχείων που σχετίζονται με κακόβουλο κώδικα, (δ) Δεν επιτρέπουν την αυτόματη έναρξη λογισμικών (auto-run) από διάφορα μέσα, (ε) Ειδοποιεί το χρήστη σε περίπτωση αναγνώρισης κάποιας απειλής, (ζ) Αυτόματα διενεργεί ενέργειες για την διαγραφή ή απομόνωση της απειλής και (η) Αυτόματα διενεργεί ενημερώσεις τόσο των υπογραφών όσο και της λειτουργικότητας
3	5	Υλοποιείται προστασία τόσο σε επίπεδο συσκευής όσο και σε επίπεδο δικτύου (π.χ. σχετικές υλοποιήσεις σε επίπεδο firewall, proxy κλπ).
3	6	Διενεργούνται εκπαιδεύσεις σε θέματα που σχετίζονται με την προστασία από malware, τεχνικές επίθεσης, phishing & social engineering.
4	1	Χρησιμοποιούνται αυτόματα και κεντρικοποιημένα συστήματα για την συνεχή παρακολούθησης σε σχέση με την προστασία από κακόβουλο κώδικα / λογισμικό όλων των στοιχείων. (workstations, servers, mobile devices, firewalls, IPS κλπ). Τα κεντρικά συστήματα παρέχουν την δυνατότητα στο εξουσιοδοτημένο προσωπικό να βλέπουν την κατάσταση προστασίας από κακόβουλο κώδικά / λογισμικό για όλα τα στοιχεία (ανεξάρτητα του είδους και του λειτουργικού συστήματος). Σε περίπτωση που κάποιο στοιχείο δεν λαμβάνει ενημερώσεις θα πρέπει να γίνονται κατάλληλες ενέργειες.
4	2	Υλοποιούνται λύσεις antimalware με δυνατότητες αναγνώρισης αδυναμιών και φίλτρα anti-exploitation.
4	3	Όπου που υπάρχει αναγνώριση σχετικής απειλής εμφανίζεται σχετικό μήνυμα τόσο στο σημείο αναγνώρισης όσο και κεντρικά και το κατάλληλο προσωπικό ενημερώνεται άμεσα ώστε να υλοποιηθούν οι απαραίτητες ενέργειες. Σε κάθε περίπτωση τα εργαλεία είναι παραμετροποιημένα με default ενέργειες σε περίπτωση ανίχνευσης απειλής (π.χ. quarantine, delete) και σε σχετικούς συνδυασμούς σε περίπτωση αποτυχίας.

4	4	Υλοποιούνται δοκιμές και ασκήσεις για τον έλεγχο της αποτελεσματικότητας της σχετικής εκπαίδευσης και την ετοιμότητα και ανθεκτικότητα του προσωπικού έναντι των σχετικών απειλών.
4	5	Υλοποιούνται μηχανισμοί anti-tampering protection ώστε να μην μπορεί να γίνει απενεργοποίηση της σχετικής προστασίας από μη εξουσιοδοτημένα άτομα.
4	6	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Τηρείται και εφαρμόζεται λίστα με επιτρεπόμενο λογισμικό.
5	2	Διενεργούνται σε τακτική βάση έλεγχοι ακεραιότητας των δεδομένων (integrity monitoring) για την αναγνώριση πιθανών μη εξουσιοδοτημένων αλλαγών και την ύπαρξη σχετικών απειλών εντός του οργανισμού.
5	3	Διασφαλίζεται (με οργανωτικά ή τεχνικά μέσα) ότι ακόμα και όταν στοιχεία βρίσκονται εκτός δικτύου, υπάρχει δυνατότητα λήψης των σχετικών ενημερώσεων και πολιτικών ασφαλείας με ασφάλεια.
5	4	Διενεργούνται δοκιμές για την αξιολόγηση της αποτελεσματικότητας των λύσεων προστασίας από κακόβουλο κώδικα / λογισμικό.
5	5	Εξετάζεται ειδικά η προστασία από επίκαιρες απειλές, με την χρήση μηχανισμών ανίχνευσης που δεν στηρίζονται στην ταυτοποίηση υπογραφών (signature based).
5	6	Ειδικά για κρίσιμα συστήματα και πριν την ενσωμάτωση νέου λογισμικού ή αλλαγής, γίνεται ανάλυση σε επίπεδο ασφάλειας (π.χ. δοκιμές ανάλυσης κώδικα για ανίχνευση παράνομων διεργασιών μέσα σε ελεγχόμενο περιβάλλον κ.α.)
5	7	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	8	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
SS2		Μέτρο: Θωράκιση συστημάτων και συσκευών και βασικές απαιτήσεις ασφάλειας Στόχος Μέτρου: Να ελαχιστοποιηθεί, στο μέτρο του δυνατού, η επιφάνεια επίθεσης των συστημάτων πληροφοριών, μέσω της μείωσης της λειτουργικότητας και των χαρακτηριστικών τους. Περιγραφή Μέτρου: Θέσπιση, εφαρμογή και διατήρηση διαδικασίας για τη θωράκιση συστημάτων και συσκευών με βάση καθορισμένες βασικές απαιτήσεις ασφάλειας, ώστε να αποτρέπεται η μη εξουσιοδοτημένη πρόσβαση και χρήση των πόρων και των υπηρεσιών του συστήματος. Ο οργανισμός εξετάζει τα λειτουργικά συστήματα, τις εφαρμογές και κάθε άλλο λογισμικό που είναι εγκατεστημένο σε συσκευές που εμπίπτουν στο πεδίο εφαρμογής της διαδικασίας θωράκισης. Ο οργανισμός πρέπει να εξετάζει τις κατευθυντήριες γραμμές και τα έγγραφα για τη θωράκιση συστημάτων που παρέχονται από τους προμηθευτές λογισμικού και υλισμικού, καθώς και τις κατευθυντήριες γραμμές και τις βέλτιστες πρακτικές που δημοσιεύονται από ομάδες συστημάτων τεχνολογίας, ρυθμιστικές αρχές και άλλες διεθνείς βέλτιστες πρακτικές ή πλαίσια. Ο οργανισμός πρέπει να λαμβάνει υπόψη, τουλάχιστον, τα default configurations και την κατάργηση των μη αναγκαίων προκαθορισμένων λογαριασμών, την εξασφάλιση ενιαίων πρωτογενών λειτουργιών ανά διακομιστή για την αποφυγή λειτουργιών με διαφορετικά επίπεδα ασφάλειας στον ίδιο εξυπηρετητή, παρέχοντας μόνο τις απαραίτητες υπηρεσίες, τα πρωτόκολλα και τους daemons, χρησιμοποιώντας παραμέτρους για την ασφάλεια του συστήματος με στόχο την πρόληψη της κατάχρησης, και την αφαίρεση κάθε περιττής λειτουργίας, όπως των scripts, των drivers, των χαρακτηριστικών και των υποσυστημάτων, προκειμένου να ελαχιστοποιηθεί η επιφάνεια επίθεσης του συστήματος. Ο οργανισμός θα πρέπει να εξετάσει το ενδεχόμενο εφαρμογής τείχων προστασίας στο επίπεδο συστημάτων (firewalls), προκειμένου να αποτρέπονται οι επιπτώσεις από κακόβουλο κώδικα στην ασφάλεια των πληροφοριών που αποθηκεύονται στο τελικό σημείο. Πηγή:
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν εφαρμόζει μέτρα για την αναγνώριση και εφαρμογή ελάχιστου προφίλ ασφαλείας για τα στοιχεία.
1	1	Διενεργούνται τουλάχιστον βασικές λειτουργίες για την παραμετροποίηση συσκευών.
1	2	Οι απαιτήσεις ασφαλείας που ενσωματώνονται στις συσκευές γίνονται τουλάχιστον ad-hoc και δύναται να μην είναι πλήρης.
2	1	Έχουν αναγνωρισθεί βασικά στοιχεία που πρέπει να είναι περιορισμένα σε συγκεκριμένες κατηγορίες στοιχείων.
2	2	Τα στοιχεία αυτά δύναται να ενσωματώνονται είτε κατά την εγκατάσταση είτε κατόπιν αυτής.

3	1	Έχει θεσπιστεί, εφαρμόζεται και διατηρείται διαδικασία για τη θωράκιση συστημάτων και συσκευών με βάση καθορισμένες βασικές απαιτήσεις ασφάλειας, ώστε να αποτρέπεται η μη εξουσιοδοτημένη πρόσβαση και χρήση των πόρων και των υπηρεσιών του συστήματος.
3	2	Τα λειτουργικά συστήματα, οι εφαρμογές και κάθε άλλο λογισμικό που είναι εγκατεστημένο σε συσκευές που εμπίπτουν στο πεδίο εφαρμογής της διαδικασίας θωράκισης εξετάζεται.
3	3	Εξετάζονται οι κατευθυντήριες γραμμές και τα έγγραφα για τη θωράκιση συστημάτων που παρέχονται από τους προμηθευτές λογισμικού και υλισμικού, καθώς και οι κατευθυντήριες γραμμές και οι βέλτιστες πρακτικές που δημοσιεύονται από ομάδες συστημάτων τεχνολογίας, ρυθμιστικές αρχές και άλλες διεθνείς βέλτιστες πρακτικές ή πλαίσια.
3	4	Λαμβάνονται υπόψη, τουλάχιστον, τα default configurations και η κατάργηση των μη αναγκαίων προκαθορισμένων λογαριασμών, την εξασφάλιση ενιαίων πρωτογενών λειτουργιών ανά διακομιστή για την αποφυγή λειτουργιών με διαφορετικά επίπεδα ασφάλειας στον ίδιο εξυπηρετητή, παρέχοντας μόνο τις απαραίτητες υπηρεσίες, τα πρωτόκολλα και τους daemons, χρησιμοποιώντας παραμέτρους για την ασφάλεια του συστήματος με στόχο την πρόληψη της κατάχρησης, και την αφαίρεση κάθε περιττής λειτουργίας, όπως των scripts, των drivers, των χαρακτηριστικών και των υποσυστημάτων, προκειμένου να ελαχιστοποιηθεί η επιφάνεια επίθεσης του συστήματος, σύμφωνα με τις απαιτήσεις [IAM1].
3	5	Εξετάζεται το ενδεχόμενο εφαρμογής τείχων προστασίας στο επίπεδο συστημάτων (firewalls), προκειμένου να αποτρέπονται οι επιπτώσεις από κακόβουλο κώδικα στην ασφάλεια των πληροφοριών που αποθηκεύονται στο τελικό σημείο σύμφωνα με τις απαιτήσεις του [NS1].
3	6	Εγκατάσταση λογισμικού γίνεται από ειδικά εξουσιοδοτημένο προσωπικό.
4	1	Για κάθε λειτουργικό σύστημα έχει δημιουργηθεί ένα αρχείο (ανάλογα με τον τρόπο με τον οποίο γίνεται το deployment – container, vm, image κλπ) που αντιστοιχεί στην πιο επίκαιρη, σταθερή και ασφαλή παραμετροποίηση του.
4	2	Η παραμετροποίηση ακολουθεί τις προτάσεις του κατασκευαστή ή άλλων αξιόπιστων πηγών και έχει το επιθυμητό επίπεδο θωράκισης (hardened).
4	3	Οι βασικές αρχές που έχουν αναφερθεί στα σχετικά [IAM1], [NS1], [AM1-4] εφαρμόζονται. Κατ' ελάχιστον καλύπτονται τα στοιχεία του ML3 καθώς και τα ακόλουθα: μη χρησιμοποιούμενες θύρες, θύρες που χρησιμοποιούνται για διαγνωστικούς σκοπούς, μη επιθυμητά πρωτόκολλα, απενεργοποίηση μη χρησιμοποιούμενων λογαριασμών, υλοποίηση λύσεων προστασίας από κακόβουλο λογισμικό, ενεργοποίηση λογισμικού firewall, IDS και IPS όπου αυτά βρίσκουν εφαρμογή κ.α.
4	4	Γίνεται διαχείριση των αλλαγών στα αρχεία αυτά μέσω της διαδικασίας διαχείρισης αλλαγών [CM1]. (Αλλαγές πρέπει να γίνονται για την επικαιροποίηση των updates / patches, στην αλλαγή ρυθμίσεων βάσει στοιχείων περιστατικών ή ενημέρωσης από άλλα αξιόπιστα ενδιαφερόμενα μέρη κ.α.). Σε περίπτωση που υπάρχει κάποιο πρόβλημα με κάποιο στοιχείο, αντικαθίσταται με καθαρή υλοποίηση από το αρχείο (baseline).
4	5	Κάθε στοιχείο εντός του δικτύου του οργανισμού είναι μοναδικά αναγνωρίσιμο και περιέχεται μέσα στον κατάλογο στοιχείων ενεργητικού όπως αναφέρεται στο [DS1/RM2].
4	6	Αντίστοιχες διαδικασίες και οδηγίες υπάρχουν και για διαφορετικού είδους λογισμικά όπως είναι εφαρμογές, βάσεις δεδομένων κ.α.
4	7	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Τηρείται και εφαρμόζεται λίστα με επιτρεπόμενο λογισμικό για κάθε περίπτωση λογισμικού που αναγνωρισμένα υποστηρίζει τις επιχειρησιακές λειτουργίες του οργανισμού.
5	2	Για κάθε λογισμικό (περιλαμβανομένου και του λειτουργικού) έχουν αναγνωριστεί και καταγραφεί οι επιτρεπτές εκδόσεις σε συμφωνία με τους στόχους του οργανισμού και τον σχετικό κίνδυνο.
5	3	Όσα στοιχεία έχουν έμμεσα ή άμεσα πρόσβαση σε πληροφορία, είναι απενεργοποιημένα τα: peer-to-peer wireless network capabilities και το wireless peripheral access to devices (περιλαμβανομένου του Bluetooth) – εκτός των περιπτώσεων που έχει υλοποιηθεί τεχνικός τρόπος ώστε να γίνεται σύνδεση με συγκεκριμένες – εξουσιοδοτημένες από τον οργανισμό συσκευές.
5	4	Τα προηγούμενα αρχεία (baselines) διατηρούνται για λόγους ιστορικότητας και δυνατότητας roll back σε περίπτωση ανάγκης.
5	5	Τηρούνται αρχεία (baseline) και για τα συστήματα που χρησιμοποιούνται για την ανάπτυξη και δοκιμή, διακριτά από αυτά που χρησιμοποιούνται για την παραγωγή.
5	6	Διενεργούνται έλεγχοι και δοκιμές για την αξιολόγηση της ανθετικότητας των baseline αρχείων. Σε περίπτωση που διαπιστωθούν αδυναμίες, λαμβάνονται άμεσα μέτρα και ακολουθείται η διαδικασία διαχείρισης αλλαγών.

5	7	Διενεργούνται τακτικοί έλεγχοι για τον έλεγχο της συμμόρφωσης της παραμετροποίησης και της λειτουργίας των στοιχείων προς τις αναγνωρισμένες βέλτιστες πρακτικές θωράκισης. Μέτρα λαμβάνονται άμεσα και διαχειρίζονται μέσα από την διαδικασία διαχείρισης αλλαγών ή / και την διαχείριση περιστατικών ασφαλείας όπως απαιτείται.
5	8	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	9	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
SS3		Μέτρο: Ασφάλεια κινητών συσκευών Στόχος Μέτρου: Να εξασφαλιστεί η κατάλληλη ασφάλεια των κινητών συσκευών που έχουν πρόσβαση σε οργανωτικούς πόρους. Περιγραφή Μέτρου: Θέσπιση, εφαρμογή και διατήρηση μέτρων ασφάλειας κινητών συσκευών προκειμένου να διασφαλίζεται η εμπιστευτικότητα, η ακεραιότητα, η διαθεσιμότητα και η αυθεντικότητα των κινητών συστημάτων που χρησιμοποιούνται από τα στελέχη για να συνδέονται, αλληλοεπιδρούν ή επεξεργάζονται οργανωτικά στοιχεία υποδομής και πόρους. Ο οργανισμός πρέπει να εξετάζει τη διαχείριση κινητών συσκευών, μέτρα ασφαλούς αποθήκευσης και κρυπτογράφησης, όπως ορίζονται στο μέτρο [DS5], ισχυρή επαλήθευση ταυτότητας, όπως ορίζεται στο μέτρο [IAM4], και μέτρα ασφαλούς επικοινωνίας και δικτύωσης, όπως ορίζονται στο μέτρο [NS4]. Ο φορέας διασφαλίζει την επαρκή προστασία των κινητών συσκευών και των πληροφοριών που διατηρούνται σε κινητές συσκευές έναντι κλοπής και απώλειας. Ο οργανισμός πρέπει να εξετάζει τη δυνατότητα εξ αποστάσεως καθαρισμού και του εντοπισμού της γεωγραφικής θέσης. Πηγή:
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν λαμβάνει μέτρα για την ασφάλεια κινητών συσκευών.
1	1	Λαμβάνονται κάποια μέτρα για την ασφάλεια κινητών συσκευών, σε μέρος ή στο σύνολο των συσκευών, τουλάχιστον με ad-hoc τρόπο.
2	1	Έχουν αναγνωρισθεί στα πλαίσια του καταλόγου στοιχείων όπως αναφέρεται στο [DS2/RM2] τα στοιχεία που είναι μεταφερόμενες – κινητές συσκευές.
2	2	Έχουν αναγνωρισθεί οι κίνδυνοι όπως προβλέπεται από τα [RM1/RM3] που σχετίζονται με την ύπαρξη και λειτουργία μεταφερόμενων / κινητών συσκευών.
2	3	Για αυτά τα στοιχεία εφαρμόζεται κρυπτογράφηση σε επίπεδο συσκευής (σύμφωνα με τα αναγραφόμενα του [AM5].
3	1	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται μέτρα ασφάλειας κινητών συσκευών προκειμένου να διασφαλίζεται η εμπιστευτικότητα, η ακεραιότητα, η διαθεσιμότητα και η αυθεντικότητα των κινητών συστημάτων που χρησιμοποιούνται από τα στελέχη για να συνδέονται, αλληλοεπιδρούν ή επεξεργάζονται οργανωτικά στοιχεία υποδομής και πόρους.
3	2	Εξετάζονται η διαχείριση κινητών συσκευών, μέτρα ασφαλούς αποθήκευσης και κρυπτογράφησης, όπως ορίζονται στο μέτρο [DS5], ισχυρή επαλήθευση ταυτότητας, όπως ορίζεται στο μέτρο [IAM4], και μέτρα ασφαλούς επικοινωνίας και δικτύωσης, όπως ορίζονται στο μέτρο [NS4].
3	3	Διασφαλίζεται η επαρκή προστασία των κινητών συσκευών και των πληροφοριών που διατηρούνται σε κινητές συσκευές έναντι κλοπής και απώλειας.
3	4	Αλλαγές στις συσκευές υλοποιούνται από εξουσιοδοτημένους χρήστες σύμφωνα με την διαδικασία [IAM1].
4	1	Εφαρμόζεται σύστημα για την διαχείριση φορητών συσκευών (MDM). Η παραμετροποίηση του MDM δίνει στον οργανισμό την δυνατότητα: να αναγνωρίζει την συσκευή, την τοποθεσία της συσκευής, τον αναγνωρισμένο χρήστη της συσκευής, να εφαρμόζει τις πολιτικές του οργανισμού σε σχέση με την ασφάλεια (αποθήκευση δεδομένων, κρυπτογράφηση, δυνατότητα διασύνδεσης, επιτρεπόμενο λογισμικό, επιτρεπόμενα πρωτόκολλα, υπηρεσίες και θύρες και να διενεργεί άμεσες ενέργειες ασφαλούς διαγραφής σε περίπτωση που αυτό κρίνεται απαραίτητο.
4	2	Υπάρχει σχετική συμμόρφωση της συγκεκριμένης πρακτικής με την κείμενη νομοθεσία και κανονισμούς για την προστασία δεδομένων προσωπικού χαρακτήρα.
4	3	Όπου απαιτείται για την αποτελεσματική λειτουργία του οργανισμού δίνεται η απο απόσταση ανάθεση προνομιακών δικαιωμάτων και στην οποία εφαρμόζονται τεχνικά μέτρα (οι συγκεκριμένες εφαρμογές στηρίζονται σε ένα event based authorization χωρίς να υπάρχει αποκάλυψη προνομιακών κωδικών πρόσβασης σε μη εξουσιοδοτημένες οντότητες).
4	4	Η εξ αποστάσεως δυνατότητα καθορίζει και εντοπίζει τη γεωγραφική θέση.
4	5	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.

5	1	Έχει διενεργηθεί ανάλυση και έχουν προσδιορισθεί οι κατασκευαστές και οι συσκευές που προμηθεύονται και χρησιμοποιούνται στον οργανισμό.
5	2	Όπου είναι εφικτό, διενεργούνται σχετικές επικοινωνίες με τις εν λόγω εταιρίες ώστε η προμήθεια των συσκευών να γίνεται με secure out-of-the box configuration (προ παραμετροποιημένο λαμβάνοντας υπόψη τις απαιτήσεις ασφαλείας).
5	3	Διενεργούνται σε τακτική βάση έλεγχοι για την συμμόρφωση των φορητών συσκευών προς τις απαιτήσεις του οργανισμού.
5	4	Διενεργούνται έλεγχοι και δοκιμές για τον προσδιορισμό της αποτελεσματικότητας των εφαρμοζόμενων μέτρων ανά περίπτωση. Σε περίπτωση απόκλισης λαμβάνονται άμεσες ενέργειες οι οποίες διαχειρίζονται μέσα από την διαδικασία διαχείρισης αλλαγών ή αντιμετώπισης περιστατικών ασφαλείας όπως απαιτείται.
5	5	Κάθε νέο μέσο ή στοιχείο, κρυπτογραφείται με αυτοματοποιημένο τρόπο όπου αυτό είναι δυνατό, πριν ή κατά την εισαγωγή του στον οργανισμό.
5	6	Για την διαγραφή δεδομένων, σε περίπτωση που αυτή υλοποιείται μέσω λογισμικού, χρησιμοποιούνται επιπλέον μέτρα σε φυσικό επίπεδο (π.χ. degaussing). (όπως προβλέπεται στο [DS1]).
5	7	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	8	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
SS4		Μέτρο: Διαχείριση διαμόρφωσης εφαρμογών Στόχος Μέτρου: Να διασφαλιστεί η κατάλληλη διαχείριση των εφαρμογών που χρησιμοποιούνται για την πρόσβαση ή επεξεργασία οργανωτικών πόρων. Περιγραφή Μέτρου: Θέσπιση, εφαρμογή και διατήρηση μέτρων διαχείρισης της διαμόρφωσης εφαρμογών με σκοπό την πρόληψη της μη επιτρεπόμενης και κακόβουλης εγκατάστασης, της διαμόρφωσης ή της τροποποίησης εφαρμογών και του λογισμικού σε οργανωτικά στοιχεία και συσκευές. Ο οργανισμός πρέπει να εξετάσει το ενδεχόμενο δημιουργίας κεντρικής διεπαφής για τη διαχείριση και διαμόρφωση εφαρμογών ώστε να εξασφαλίζεται ότι όλες οι οργανωτικές συσκευές υπόκεινται σε κεντρική διαχείριση, ενώ η διαμόρφωση και οι ενημερώσεις λογισμικού μπορούν να προωθηθούν στις τελικές συσκευές. Αυτή η κεντρική διεπαφή διαχείρισης πρέπει να επιτρέπει στον οργανισμό να θεσπίζει κατάλογο ορισμένων επιτρεπόμενων ή μη επιτρεπόμενων τύπων εφαρμογών. Πηγή:
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν εφαρμόζει κάποια μέτρα ή έλεγχο για την εγκατάσταση εφαρμογών.
1	1	Εφαρμόζονται κάποια μέτρα για την εγκατάσταση εφαρμογών στα κρίσιμα συστήματα όπως είναι οι servers.
1	2	Τα μέτρα επιλέγονται και εφαρμόζονται τουλάχιστον σε ad-hoc βάση.
2	1	Για τα κρίσιμα στοιχεία ενεργητικού, όπως αυτά αποτυπώνονται στον σχετικό κατάλογο [AM2 / RM2], έχει ενεργοποιηθεί παρακολούθηση.
2	2	Έχει δημιουργηθεί μια πολιτική ελέγχου πρόσβασης η οποία καλύπτει όλα τα στοιχεία ενεργητικού και τα κτήρια του οργανισμού όπως εμφανίζονται στον κατάλογο στοιχείων ενεργητικού σύμφωνα με το [AM2].
2	3	Δεν υπάρχει η δυνατότητα σε όλους τους χρήστες να κάνουν αλλαγές ή να εγκαθιστούν λογισμικού σε κρίσιμα συστήματα του οργανισμού.
3	1	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται μέτρα διαχείρισης της διαμόρφωσης εφαρμογών με σκοπό την πρόληψη της μη επιτρεπόμενης και κακόβουλης εγκατάστασης, της διαμόρφωσης ή της τροποποίησης εφαρμογών και του λογισμικού σε οργανωτικά στοιχεία και συσκευές.
3	2	Για κάθε στοιχείο λογισμικού έχει αναγνωριστεί ιδιοκτήτης ο οποίος σε συνεργασία με το λοιπό τεχνικό προσωπικό, προσδιορίζει τους ρόλους για τους οποίους απαιτείται πρόσβαση (στο λογισμικό) καθώς και το επίπεδο της πρόσβασης.
3	3	Αλλαγές στις συσκευές υλοποιούνται από εξουσιοδοτημένους χρήστες σύμφωνα με την διαδικασία [IAM1].
4	1	Έχει δημιουργηθεί κεντρική διεπαφή για τη διαχείριση και διαμόρφωση εφαρμογών ώστε να εξασφαλίζεται ότι όλες οι οργανωτικές συσκευές υπόκεινται σε κεντρική διαχείριση, ενώ η διαμόρφωση και οι ενημερώσεις λογισμικού μπορούν να προωθηθούν στις τελικές συσκευές.
4	2	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.

5	1	Τηρείται και εφαρμόζεται λίστα με επιτρεπόμενο λογισμικό για κάθε περίπτωση λογισμικού που αναγνωρισμένα υποστηρίζει τις επιχειρησιακές λειτουργίες του οργανισμού μέσω της κεντρικής διεπαφή διαχείρισης.
5	2	Για κάθε λογισμικό (περιλαμβανομένου και του λειτουργικού) έχουν αναγνωριστεί και καταγραφεί οι επιτρεπτές εκδόσεις σε συμφωνία με τους στόχους του οργανισμού και τον σχετικό κίνδυνο.
5	3	Τηρούνται λίστες και μέτρα για τα επιτρεπόμενα components λογισμικού.
5	4	Διενεργούνται τακτικοί έλεγχοι για τον έλεγχο της συμμόρφωσης της παραμετροποίησης και της λειτουργίας των στοιχείων προς τις αναγνωρισμένες βέλτιστες πρακτικές θωράκισης.
5	5	Όπου απαιτείται τα μέτρα που λαμβάνονται είναι άμεσα και διαχειρίζονται μέσα από την διαδικασία διαχείρισης αλλαγών ή / και την διαχείριση περιστατικών ασφαλείας όπως απαιτείται.
5	6	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	7	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.

Κατηγορία		ΑΣΦΑΛΕΙΑ ΕΦΑΡΜΟΓΩΝ
AS1		Μέτρο: Ασφαλής κύκλος ζωής ανάπτυξης λογισμικού Στόχος Μέτρου: Να διασφαλιστούν επαρκή μέτρα ασφάλειας στο πλαίσιο των δραστηριοτήτων ανάπτυξης λογισμικού που αναπτύσσει ο οργανισμός Περιγραφή Μέτρου: Θέσπιση, εφαρμογή και διατήρηση ασφαλών πρακτικών ανάπτυξης λογισμικού σε παραδοσιακές διαδικασίες κύκλου ζωής ανάπτυξης λογισμικού, ώστε να διασφαλίζεται ότι η ασφάλεια είναι ενσωματωμένη στο σχεδιασμό στο πλαίσιο των δραστηριοτήτων ανάπτυξης εφαρμογών και λογισμικού. Ο οργανισμός πρέπει να εξετάσει το ενδεχόμενο εφαρμογής, τουλάχιστον, μιας αξιολόγησης κινδύνου στο αρχικό στάδιο του έργου, διενέργειας δοκιμών ασφάλειας και εξέτασης κώδικα στα στάδια ανάπτυξης του έργου, και διενέργεια αξιολόγησης ασφάλειας και ασφαλούς διαμόρφωσης στην παράδοση του έργου. Ο οργανισμός πρέπει να διασφαλίζει ότι εφαρμόζονται κατάλληλα μέτρα για τον διαχωρισμό των περιβαλλόντων ανάπτυξης λογισμικού από το επιχειρησιακό περιβάλλον παραγωγής. Ο οργανισμός διασφαλίζει ότι τα δεδομένα που χρησιμοποιούνται για τη διενέργεια δοκιμών είναι ανώνυμα και δεν συνδέονται με εμπιστευτικές και ευαίσθητες πληροφορίες στο πλαίσιο αναπτυξιακών δραστηριοτήτων. Πηγή:
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν λαμβάνει μέτρα για την ασφαλή ανάπτυξη λογισμικού.
1	1	Κατά την ανάπτυξη λογισμικού τίθονται περιοδικά και όχι κατ'ανάγκη με συστηματικό τρόπο, κάποιες προδιαγραφές ασφαλείας και κάποιες σχετικές δοκιμές.
2	1	Δημιουργείται χωριστό έργο (project) για ανάπτυξη λογισμικού που πρέπει να διενεργηθεί.
2	2	Έχει δημιουργηθεί μια διαδικασία διαχείρισης του κύκλου ανάπτυξης λογισμικού (SDLC).
2	3	Στα αρχικά βήματα του κύκλου ζωής, περιλαμβάνεται η αναγνώριση απαιτήσεων ασφαλείας.
2	4	Στα τελευταία βήματα της ανάπτυξης και πριν την εφαρμογή στην παραγωγή έχουν προβλεφθεί και γίνονται δοκιμές για την αποδοχή του συστήματος έναντι των κριτηρίων και απαιτήσεων ποιότητας, λειτουργικότητας και ασφάλειας.
3	1	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται ασφαλείς πρακτικές ανάπτυξης λογισμικού σε παραδοσιακές διαδικασίες κύκλου ζωής ανάπτυξης λογισμικού, ώστε να διασφαλίζεται ότι η ασφάλεια είναι ενσωματωμένη στο σχεδιασμό στο πλαίσιο των δραστηριοτήτων ανάπτυξης εφαρμογών και λογισμικού.
3	2	Εφαρμόζονται κατάλληλα μέτρα για τον διαχωρισμό των περιβαλλόντων ανάπτυξης λογισμικού από το επιχειρησιακό περιβάλλον παραγωγής.
3	3	Τα δεδομένα που χρησιμοποιούνται για τη διενέργεια δοκιμών είναι ανώνυμα και δεν συνδέονται με εμπιστευτικές και ευαίσθητες πληροφορίες στο πλαίσιο αναπτυξιακών δραστηριοτήτων.
3	4	Στη περίπτωση που η ανάπτυξη εφαρμογών δίνεται σε τρίτα μέρη, δίνονται τουλάχιστον προδιαγραφές ασφαλείας που χρειάζεται να ικανοποιεί η εφαρμογή και ζητούνται επαρκείς εγγυήσεις, διαβεβαιώσεις και στοιχεία ότι καλύπτονται πριν την αποδοχή ή την λειτουργία τους.
3	6	Διενεργείται risk assessment ή threat profiling κατά τη διάρκεια του σχεδιασμού ενός λογισμικού. Κατάλληλα μέτρα ασφαλείας ενσωματώνονται στην εφαρμογή σύμφωνα με τα αποτελέσματα των διαδικασιών αυτών.
3	7	Αλλαγές στο λογισμικό ελέγχονται μέσα από την διαδικασία διαχείρισης αλλαγών [CM1].
3	8	Δεξιότητες και γνώσεις σχετικά με την ασφαλή ανάπτυξη λογισμικού αναγνωρίζονται στις σχετικές θέσεις εργασίας ως προαπαιτούμενο.
3	9	Έχουν ενταχθεί απαιτήσεις για ασφάλεια και ιδωτικότητα από προεπιλογή και από σχεδιασμό σύμφωνα με τις απαιτήσεις κανονισμών, νομοθεσίας και βέλτιστων σχετικών πρακτικών.
4	1	Διενεργείται, τουλάχιστον, μια αξιολόγηση κινδύνου στο αρχικό στάδιο του έργου, δοκιμές ασφάλειας και εξέταση κώδικα στα στάδια ανάπτυξης του έργου, και αξιολόγηση ασφάλειας και ασφαλούς διαμόρφωσης στην παράδοση του έργου.
4	2	Στην εκκίνηση του σχεδιασμού το περιβάλλον καθορίζεται το περιβάλλον στο οποίο γίνεται η ανάπτυξη.
4	3	Το περιβάλλον καθορίζεται σύμφωνα με τις απαιτήσεις ασφαλείας του λογισμικού προς ανάπτυξη αλλά και την προσδοκώμενη χρήση του (intended use).
4	4	Το περιβάλλον ανάπτυξης αποτελείται από την γλώσσα προγραμματισμού, το χρησιμοποιούμενο framework, τα εργαλεία ανάπτυξης, τα εργαλεία δοκιμών και τα εργαλεία διαχείρισης και αποθήκευσης του κώδικα. Σε κάθε περίπτωση επιλέγεται και η έκδοση των εν λόγω στοιχείων, λαμβάνοντας υπόψη τις δυνατότητες αλλά και τις ανοιχτές αδυναμίες σύμφωνα με έγκυρες σχετικές πηγές.

4	5	Τα αποτελέσματα των δοκιμών διατηρούνται και ενεργοποιούν και διαδικασίες διόρθωσης όπως απαιτείται σύμφωνα με την διαδικασία διαχείρισης αλλαγών [CM1].
4	6	Υπάρχει πλήρης διαχωρισμός καθηκόντων ανάμεσα στο προσωπικό το οποίο διενεργεί την ανάπτυξη, το προσωπικό που διενεργεί τις δοκιμές και το προσωπικό που είναι υπεύθυνο για την παραγωγική λειτουργία των συστημάτων.
4	7	Στη περίπτωση που το λογισμικό λαμβάνεται από τρίτο μέρος, εξετάζεται ότι η διαδικασία ανάπτυξης καλύπτει τις απαιτήσεις που θα είχε ο οργανισμός αν υλοποιούσε μόνος του την ανάπτυξη. Επίσης, εξετάζεται η ιστορικότητα (σε σχέση με περιστατικά, με ενημερώσεις, με ανοιχτές ευπάθειες) του τρίτου μέρους και οι διαδικασίες για ανταπόκριση σε αναγνωρισμένες ευπάθειες.
4	8	Έχει δημιουργηθεί μια σειρά από οδηγίες (υποχρεωτικής εφαρμογής) για την ασφαλή ανάπτυξη λογισμικού. Οι οδηγίες είναι εξειδικευμένες ανά γλώσσα ή περιβάλλον ανάπτυξης και είναι σύμφωνες με τις διεθνείς βέλτιστες πρακτικές και τις οδηγίες του αντίστοιχου vendor.
4	9	Αντίστοιχες διαδικασίες και οδηγίες υπάρχουν και για διαφορετικού είδους λογισμικά όπως είναι εφαρμογές, βάσεις δεδομένων κ.α.
4	10	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Εντάσσονται αυτόματα εργαλεία για static analysis του κώδικα σε επίπεδο ασφάλειας κατά την ανάπτυξη του λογισμικού.
5	2	Διενεργούνται συγκεκριμένα τεστ, τα οποία γίνονται σε κάθε περίπτωση ανάπτυξης ή αλλαγής με αυτόματους ή ημιαυτόματους τρόπους με την χρήση κατάλληλων εργαλείων. Ειδικά για κρίσιμα συστήματα και πριν την ενσωμάτωση νέου λογισμικού ή αλλαγής, γίνεται ανάλυση σε επίπεδο ασφάλειας (π.χ. δοκιμές ανάλυσης κώδικα για ανίχνευση παράνομων διεργασιών μέσα σε ελεγχόμενο περιβάλλον κ.α.)
5	3	Σε περίπτωση που είναι εφικτό, ο οργανισμόςδέχεται εξωτερικό έλεγχο ή και πιστοποίηση από ανεξάρτητο εργαστήριο για την ασφάλεια του λογισμικού, πριν την εφαρμογή στην παραγωγή και χρήση του.
5	4	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	5	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.

Κατηγορία		ΑΣΦΑΛΕΙΑ ΑΝΘΡΩΠΙΝΩΝ ΠΟΡΩΝ
HRS1		Μέτρο: Κύκλος ζωής της εργοδότησης Στόχος Μέτρου: Να υλοποιούνται επαρκή μέτρα για την εξασφάλιση ότι τα στελέχη που εργάζονται για λογαριασμό του οργανισμού, τα οποία έχουν πρόσβαση σε οργανωτικούς πόρους, υποστηρίζουν την πολιτική ασφάλειας πληροφοριών και τους στόχους του οργανισμού. Περιγραφή Μέτρου: Κατάρτιση, εφαρμογή και διατήρηση σχεδίου για να διασφαλιστεί ότι η ασφάλεια πληροφοριών είναι ενσωματωμένη καθ' όλη τη διάρκεια του κύκλου ζωής της εργοδότησης (δηλαδή πριν, κατά τη διάρκεια και μετά την εργοδότηση των εργαζομένων) και να καταβάλει κάθε εύλογη προσπάθεια προκειμένου να διασφαλίσει ότι οι εργαζόμενοι κατανοούν τις ευθύνες τους σε σχέση με την ασφάλεια πληροφοριών. Το σχέδιο περιλαμβάνει κατάλληλα μέτρα ασφάλειας πληροφοριών σε κάθε φάση της εργοδότησης, π.χ. έλεγχοι ιστορικού πριν την πρόσληψη, κατάρτιση και ευαισθητοποίηση των εργαζομένων, ενσωμάτωση επαρκών προνοιών στις συμβάσεις εργασίας, κατάρτιση πολιτικής αποδεκτή ς χρήσης, επιστροφή των συσκευών των εργαζομένων που περιέχουν κρίσιμες πληροφορίες, και αφαίρεση της πρόσβασης σε συστήματα και εφαρμογές σύμφωνα με τον κύκλο ζωής της διαχείρισης ταυτότητας, όπως ορίζεται στο μέτρο [IAM7]. Πηγή: 27002, PNNL
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν λαμβάνει μέτρα ώστε να διασφαλίσει ότι η ασφάλεια πληροφοριών είναι ενσωματωμένη καθ' όλη τη διάρκεια του κύκλου ζωής της εργοδότησης.
1	1	Διενεργείται επαλήθευση των υποχρεωτικών ακαδημαϊκών και επαγγελματικών προσόντων μέσω της λήψης και της εξέτασης των σχετικών εγγράφων.
1	2	Τα αποτελέσματα του ελέγχου τα οποία αφορούν προσωπικά δεδομένα, προστατεύονται σύμφωνα με το υψηλότερο επίπεδο ταξινόμησης.
2	1	Διενεργούνται έλεγχοι ιστορικού για βασικό προσωπικό και εξωτερικούς εργολάβους, όταν χρειάζεται και επιτρέπεται από το νόμο.
2	2	Ζητούνται σχετικές αναφορές που επαληθεύουν την ύπαρξη των επιθυμητών χαρακτηριστικών που έχει δηλώσει ο υποψήφιος.
2	3	Έχει θεσπιστεί μία βασική διαδικασία σχετικά με τον έλεγχο ιστορικού για τους υποψήφιους υπαλλήλους.
3	1	Έχει θεσπιστεί, εφαρμόζεται και διατηρείται μια διαδικασία που διασφαλίζει ότι η ασφάλεια πληροφοριών είναι ενσωματωμένη καθ' όλη τη διάρκεια του κύκλου ζωής της εργοδότησης και καταβάλει κάθε εύλογη προσπάθεια προκειμένου να διασφαλίσει ότι οι εργαζόμενοι κατανοούν τις ευθύνες τους σε σχέση με την ασφάλεια πληροφοριών.
3	2	Η διαδικασία περιλαμβάνει κατάλληλα μέτρα ασφάλειας πληροφοριών σε κάθε φάση της εργοδότησης, π.χ. έλεγχοι ιστορικού πριν την πρόσληψη, κατάρτιση και ευαισθητοποίηση τους.
4	1	Έχει θεσπιστεί διαδικασία ελέγχων επαλήθευσης που περιγράφει λεπτομερώς τα κριτήρια και τους περιορισμούς για τους ελέγχους επαλήθευσης, π.χ. ποιος είναι κατάλληλος για τον έλεγχο ατόμων και πώς, πότε και γιατί διενεργούνται έλεγχοι επαλήθευσης.
4	2	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Υπάρχει συνεργασία με τρίτο μέρος το οποίο έχει αναλάβει να υλοποιεί τους ελέγχους ιστορικού και σύμφωνα με τις απαιτήσεις της σχετικής νομοθεσίας.
5	2	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	3	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
HRS2		Μέτρο: Παρακολούθηση εργαζομένων Στόχος Μέτρου: Να εξασφαλιστεί ότι τα στελέχη που εργάζονται για λογαριασμό του οργανισμού συμμορφώνονται με την πολιτική ασφάλειας πληροφοριών και τηρούν τις ευθύνες ασφάλειας τους καθ' όλη τη διάρκεια του κύκλου ζωής της απασχόλησης. Περιγραφή Μέτρου: Θέσπιση, εφαρμογή και διατήρηση σχεδίου για την παρακολούθηση της συμμόρφωσης των εργαζομένων με τις υποχρεώσεις και τις ευθύνες τους όσον αφορά την ασφάλεια πληροφοριών, καθ' όλη τη διάρκεια του κύκλου ζωής της απασχόλησης. Πηγή:
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου

0	1	Ο οργανισμός δεν εφαρμόζει μέτρα σχετικά με την παρακολούθηση της συμμόρφωσης των εργαζομένων με τις υποχρεώσεις και τις ευθύνες τους όσον αφορά την ασφάλεια πληροφοριών, καθ' όλη τη διάρκεια του κύκλου ζωής της απασχόλησης.
1	1	Είναι δυνατό και αναγνωρίζεται ότι υπάρχει κάποια μη συμμόρφωση προσωπικού σε σχέση με πολιτικές, διαδικασίες ή μέτρα κατά τη διάρκεια σχετικής διερεύνησης περιστατικού ασφαλείας.
2	1	Έχει γίνει καταγραφή των ρόλων και αρμοδιοτήτων και έχουν ανατεθεί στο αντίστοιχο προσωπικό.
2	2	Το προσωπικό έχει ενημερωθεί σχετικά με τις σχετικές υποχρεώσεις του.
2	3	Γίνονται κάποιοι έλεγχοι τουλάχιστον ad-hoc στο προσωπικό ως προς τη συμμόρφωσή τους προς τις σχετικές υποχρεώσεις.
3	1	Έχει θεσπιστεί, εφαρμόζεται και διατηρείται διαδικασία για την παρακολούθηση της συμμόρφωσης των εργαζομένων με τις υποχρεώσεις και τις ευθύνες τους όσον αφορά την ασφάλεια πληροφοριών, καθ' όλη τη διάρκεια του κύκλου ζωής της απασχόλησης.
3	2	Σχετικοί έλεγχοι περιλαμβάνουν και δοκιμές που σχετίζονται με τον έλεγχο της αποτελεσματικότητας της εκπαίδευσης του προσωπικού όπως αναφέρεται στο [DS5] και [SS1].
4	1	Έχουν δημιουργηθεί συγκεκριμένα πλάνα ελέγχου (εσωτερικά και εξωτερικά) που περιλαμβάνουν (στο πεδίο εφαρμογής τους) και ελέγχους συμμόρφωσης του προσωπικού προς τις πολιτικές, διαδικασίες και μέτρα ασφαλείας του οργανισμού.
4	2	Τα στοιχεία των ελέγχων αναλύονται και εξάγονται συμπεράσματα για την συμμόρφωση του ανθρώπινου δυναμικού προς τις σχετικές απαιτήσεις. Σε περίπτωση που έχει αναγνωριστεί κάποια απόκλιση, γίνεται ενεργοποίηση της διαδικασίας ανταπόκρισης περιστατικών ασφαλείας [EIM1] και την διαδικασία για τα πειθαρχικά μέτρα [HRS3].
4	3	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Έχουν εφαρμοστεί αυτοματοποιημένα μέτρα για τον έλεγχο της συμμόρφωσης του προσωπικού με τις πολιτικές, διαδικασίες και μέτρα ασφαλείας του οργανισμού (όπου είναι αυτό εφικτό). (π.χ. υλοποίηση MDM για την διαχείριση και εφαρμογή πολιτικών στις κινητές συσκευές, υλοποίηση DLP για τον έλεγχο της διαχείρισης της πληροφορίας εντός του οργανισμού, παρακολούθηση και καταγραφή ενεργειών – logs τα οποία συγκεντρώνονται και αναλύονται κ.α.).
5	2	Τα στοιχεία από τα αυτοματοποιημένα εργαλεία, καθώς και τα στοιχεία των άλλων ελέγχων που προβλέπονται αναλύονται και εξάγονται συμπεράσματα για την συμμόρφωση του ανθρώπινου δυναμικού προς τις σχετικές απαιτήσεις. Σε περίπτωση που έχει αναγνωριστεί κάποια απόκλιση, γίνεται ενεργοποίηση της διαδικασίας ανταπόκρισης περιστατικών ασφαλείας [EIM1] και την διαδικασία για τα πειθαρχικά μέτρα [HRS3].
5	3	Συλλέγονται στοιχεία για την συμμόρφωση του προσωπικού προς τις απαιτήσεις και προδιαγραφές των διαδικασιών και των πολιτικών του οργανισμού σε συμφωνία με την κείμενη νομοθεσία.
5	4	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	5	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
HRS3		Μέτρο: Πειθαρχικά μέτρα και επιβολή Στόχος Μέτρου: Να εξασφαλιστεί ότι τα στελέχη που εργάζονται για λογαριασμό του οργανισμού, είναι υπεύθυνα για τις εκούσιες ή ακούσιες δραστηριότητες που επηρεάζουν τους στόχους ασφάλειας πληροφοριών του οργανισμού. Περιγραφή Μέτρου: Θέσπιση, εφαρμογή και διατήρηση σειράς πειθαρχικών μέτρων προκειμένου να διασφαλιστεί η συμμόρφωση των στελεχών με τις υποχρεώσεις και τις ευθύνες τους όσον αφορά την ασφάλεια πληροφοριών και την ανάληψη δράσης σε περίπτωση παραβίασης των υποχρεώσεων και των ευθυνών αυτών. Ο οργανισμός πρέπει να εξετάσει το ενδεχόμενο θέσπισης επίσημης διαδικασίας επιβολής κυρώσεων για στελέχη που δεν συμμορφώνονται με τις υποχρεώσεις και τις ευθύνες τους στον τομέα της ασφάλειας πληροφοριών. Η μη συμμόρφωση με τις υποχρεώσεις και τις ευθύνες όσον αφορά την ασφάλεια πληροφοριών εντοπίζεται μέσω των διαδικασιών παρακολούθησης των εργαζομένων [HRS2]. Πηγή: 27002
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου

0	1	Ο οργανισμός δεν υλοποιεί μέτρα και δεν έχει δημιουργήσει διαδικασία επιβολής κυρώσεων προκειμένου να διασφαλιστεί η συμμόρφωση των στελεχών με τις υποχρεώσεις και τις ευθύνες τους όσον αφορά την ασφάλεια πληροφοριών και την ανάληψη δράσης σε περίπτωση παραβίασης των υποχρεώσεων και των ευθυνών αυτών.
1	1	Στις περιπτώσεις πειθαρχικού παραπτώματος σε σχέση με την ασφάλεια πληροφοριών, το εμπλεκόμενο προσωπικό απομακρύνεται με τουλάχιστον ad-hoc τρόπο.
2	1	Έχει θεσπίστει πειθαρχική διαδικασία για τη λήψη μέτρων κατά των εργαζομένων που έχουν διαπράξει παραβίαση της ασφάλειας των πληροφοριών.
3	1	Έχει θεσπιστεί, εφαρμόζεται και διατηρείται σειρά πειθαρχικών μέτρων μέσω πειθαρχικής διαδικασίας προκειμένου να διασφαλιστεί η συμμόρφωση των στελεχών με τις υποχρεώσεις και τις ευθύνες τους όσον αφορά την ασφάλεια πληροφοριών και την ανάληψη δράσης σε περίπτωση παραβίασης των υποχρεώσεων και των ευθυνών αυτών.
3	2	Η πειθαρχική διαδικασία διασφαλίζει τη σωστή και δίκαιη μεταχείριση των εργαζομένων που είναι ύποπτοι για παραβιάσεις της ασφάλειας των πληροφοριών.
3	3	Η πειθαρχική διαδικασία προβλέπει μια σταδιακή απάντηση που λαμβάνει υπόψη παράγοντες όπως η φύση και η σοβαρότητα της παράβασης και ο αντίκτυπός της στην επιχείρηση, είτε πρόκειται για πρώτο ή επαναλαμβανόμενο παράπτωμα είτε όχι, είτε ο παραβάτης ήταν κατάλληλα εκπαιδευμένος είτε όχι, επιχειρηματικές συμβάσεις και άλλους παράγοντες όπου απαιτείται.
3	4	Έχει κοινοποιηθεί η πειθαρχική διαδικασία στο σύνολο του προσωπικού.
3	5	Έχει εξεταστεί το ενδεχόμενο θέσπισης επίσημης διαδικασίας επιβολής κυρώσεων για στελέχη που δεν συμμορφώνονται με τις υποχρεώσεις και τις ευθύνες τους στον τομέα της ασφάλειας πληροφοριών.
3	6	Η μη συμμόρφωση με τις υποχρεώσεις και τις ευθύνες όσον αφορά την ασφάλεια πληροφοριών εντοπίζεται μέσω των διαδικασιών παρακολούθησης των εργαζομένων [HRS2].
4	1	Έχει θεσπίστει επίσημη διαδικασία επιβολής κυρώσεων για στελέχη που δεν συμμορφώνονται με τις υποχρεώσεις και τις ευθύνες τους στον τομέα της ασφάλειας πληροφοριών.
4	2	Η μη συμμόρφωση με τις υποχρεώσεις και τις ευθύνες όσον αφορά την ασφάλεια πληροφοριών εντοπίζεται μέσω των διαδικασιών παρακολούθησης των εργαζομένων [HRS2].
4	3	Η διαδικασία επιβολής κυρώσεων έχει κοινοποιηθεί στο σύνολο του προσωπικού του οργανισμού.
4	4	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Συλλέγονται στοιχεία για την συμμόρφωση του προσωπικού προς τις απαιτήσεις και προδιαγραφές των διαδικασιών και των πολιτικών του οργανισμού σε συμφωνία με την κείμενη νομοθεσία.
5	2	Τα στοιχεία της παρακολούθησης όπως αναφέρεται στο [HRS2] ενεργοποιούν την διαδικασία των πειθαρχικών μέτρων.
5	3	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	4	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
HRS4		Μέτρο: Εξωτερικοί συνεργάτες Στόχος Μέτρου: Να εξασφαλιστεί ότι οι εξωτερικοί συνεργάτες που εργάζονται για λογαριασμό του οργανισμού τηρούν την πολιτική ασφάλειας πληροφοριών και τους στόχους ασφάλειας του οργανισμού. Περιγραφή Μέτρου: Θέσπιση, εφαρμογή και διατήρηση μέτρων για την ασφάλεια πληροφοριών σε σχέση με το εξωτερικό εργατικό δυναμικό, π.χ. με τους αναδόχους συμβάσεων, προκειμένου να διασφαλίζεται η δέουσα προστασία των πληροφοριών που ανταλλάσσονται με εξωτερικούς συνεργάτες. Πηγή: 27002
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν έχει θεσπίσει και δεν εφαρμόζει μέτρα για την ασφάλεια πληροφοριών σε σχέση με το εξωτερικό εργατικό δυναμικό.
1	1	Στους εξωτερικούς συνεργάτες αναφέρονται βασικά μέτρα σε σχέση με την ασφάλεια πληροφοριών τα οποία μπορεί να μην αποτυπώνονται στις συμβάσεις μεταξύ των 2 μερών.
2	1	Περιλαμβάνονται μέτρα στις συμβατικές συμφωνίες με βασικά εξωτερικά μέρη αλλά όχι κατ'ανάγκη στο σύνολο, σε σχέση με την ασφάλεια πληροφοριών.

2	2	Στις συμβατικές συμφωνίες περιέχονται οι νομικές ευθύνες και δικαιώματα του αναδόχου, π.χ. σχετικά με τους νόμους περί πνευματικών δικαιωμάτων ή τη νομοθεσία περί προστασίας δεδομένων.
3	1	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται για την ασφάλεια πληροφοριών σε σχέση με το εξωτερικό εργατικό δυναμικό προκειμένου να διασφαλίζεται η δέουσα προστασία των πληροφοριών που ανταλλάσσονται με εξωτερικούς συνεργάτες.
3	2	Στις συμβατικές συμφωνίες υπάρχει σχετικό παράρτημα που ενημερώνει τους εξωτερικούς συνεργάτες σχετικά με την πολιτική ασφάλειας πληροφοριών του οργανισμού και την υποχρέωση για την τήρηση αυτής.
3	3	Ο οργανισμός συνάπτει συμβατική συμφωνία με το εκάστοτε εξωτερικό εργατικό δυναμικό που περιλαμβάνει μέτρα σε σχέση με την ασφάλεια πληροφοριών.
3	4	Οι συμβατικές συμφωνίες περιέχουν μια σαφή δήλωση ότι όλοι οι εργολάβοι στους οποίους παρέχεται πρόσβαση σε εμπιστευτικές πληροφορίες υπογράφουν συμφωνία εμπιστευτικότητας ή μη αποκάλυψης προτού τους δοθεί πρόσβαση σε εγκαταστάσεις επεξεργασίας πληροφοριών. Το NDA θα μπορούσε να είναι μέρος της συμβατικής συμφωνίας.
3	5	Η συμβατική συμφωνία περιλαμβάνει τις ευθύνες για την ταξινόμηση των πληροφοριών και τη διαχείριση οργανωτικών περιουσιακών στοιχείων που σχετίζονται με πληροφορίες, εγκαταστάσεις επεξεργασίας πληροφοριών και υπηρεσίες πληροφοριών που διαχειρίζεται ο ανάδοχος, καθώς και τις ευθύνες του αναδόχου για τη διαχείριση πληροφοριών που λαμβάνονται από άλλες εταιρείες ή εξωτερικά μέρη.
4	1	Έχει θεσπιστεί συγκεκριμένη διαδικασία σε σχέση με το εξωτερικό εργατικό δυναμικό.
4	2	Η συμβατική συμφωνία περιέχει ενέργειες που πρέπει να γίνουν εάν ο ανάδοχος αγνοήσει τις απαιτήσεις ασφάλειας του οργανισμού.
4	3	Στις συμβατικές συμφωνίες υπάρχει σχετικό παράρτημα που ενημερώνει τους εξωτερικούς συνεργάτες σχετικά με τους στόχους ασφάλειας του οργανισμού και την υποχρέωση για την τήρηση τους.
4	4	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Ένας κώδικας δεοντολογίας χρησιμοποιείται για να δηλώσει τις ευθύνες ασφάλειας πληροφοριών του αναδόχου σχετικά με το απόρρητο, την προστασία δεδομένων, τη δεοντολογία, την κατάλληλη χρήση του εξοπλισμού και των εγκαταστάσεων του οργανισμού, καθώς και αξιόπιστες πρακτικές που αναμένει ο οργανισμός. Ένα εξωτερικό μέρος, με το οποίο συνδέεται ένας ανάδοχος, μπορεί να κληθεί να συνάψει συμβατικές ρυθμίσεις για λογαριασμό του συμβαλλόμενου ατόμου.
5	2	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	3	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
HRS5		Μέτρο: Προστασία από απειλές που προέρχονται από εσωτερικά πρόσωπα Στόχος Μέτρου: Να εξασφαλιστεί η προστασία από απειλές κατά της ασφάλειας δικτύων και πληροφοριών από το εσωτερικό του οργανισμού. Περιγραφή Μέτρου: Θέσπιση, εφαρμογή και διατήρηση κατάλληλων μέτρων για την πρόληψη, τον εντοπισμό και την παρακολούθηση των επιθέσεων από εσωτερικά πρόσωπα, από άγνοια, αμέλεια, ή κακόβουλες ή επαγγελματικές προθέσεις. Ο οργανισμός πρέπει να εκπαιδεύει και να ευαισθητοποιεί τους εργαζόμενους σχετικά με τις πρακτικές ασφάλειας των πληροφοριών εντός του οργανισμού, σύμφωνα με το μέτρο [TA2], να διενεργεί επαρκή έλεγχο των υποψηφίων σύμφωνα με το μέτρο [HRS1], και να παρακολουθεί τους εργαζόμενους [HRS2], ώστε να μειώνεται η πιθανότητα να υπάρξουν εσωτερικές επιθέσεις. Πηγή:
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν παίρνει κάποιο μέτρο για την προστασία από απειλές που προέρχονται από εσωτερικά πρόσωπα.
1	1	Όπου υπάρχει κάποια μη συμμόρφωση προσωπικού σε σχέση με πολιτικές, διαδικασίες ή μέτρα κατά τη διάρκεια σχετικής διερεύνησης περιστατικού ασφαλείας, αυτή αναγνωρίζεται. Σε αυτή την περίπτωση λαμβάνονται μέτρα για την ανταπόκριση στο συγκεκριμένο περιστατικό.
2	1	Ακολουθείται μια καθορισμένη μέθοδος (διαδικασία) για εντοπισμό κινδύνων που προκύπτουν από το εσωτερικό του οργανισμού.
2	3	Έχουν αναγνωρισθεί και κάποιοι κίνδυνοι που σχετίζονται με απειλές που προέρχονται από εσωτερικά πρόσωπα.

3	1	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται κατάλληλα μέτρα για την πρόληψη, τον εντοπισμό και την παρακολούθηση των επιθέσεων από εσωτερικά πρόσωπα, από άγνοια, αμέλεια, ή κακόβουλες ή επαγγελματικές προθέσεις.
3	2	Οι εργαζόμενοι εκπαιδεύονται και ευαισθητοποιούνται σχετικά με τις πρακτικές ασφάλειας των πληροφοριών εντός του οργανισμού, σύμφωνα με το μέτρο [TA2], διενεργείται επαρκής έλεγχος των υποψηφίων σύμφωνα με το μέτρο [HRS1], και οι εργαζόμενοι παρακολουθούνται [HRS2], ώστε να μειώνεται η πιθανότητα να υπάρξουν εσωτερικές επιθέσεις.
4	1	Οι κίνδυνοι καλύπτουν όλες τις πιθανές κατηγορίες πηγών κινδύνων (risk sources) ανεξάρτητα από το αν είναι υπό τον έλεγχο του οργανισμού.
4	2	Έχουν κατ' ελάχιστο αναγνωριστεί πηγές κινδύνων που σχετίζονται με τον ανθρώπινο παράγοντα.
4	3	Επίσης περιλαμβάνονται απειλές όπως remote spying, theft of equipment, theft of information or media, retrieval of recycled or discarded media, data input from untrustworthy sources, incorrect use of devices, illegal processing of data, sending or distributing of malware, abuse of rights κ.α.
4	4	Αντίστοιχα περιλαμβάνονται αδυναμίες όπως είναι ελλιπείς πόροι προσωπικού, προσωπικό που διενεργεί ενέργειες με conflict of interest / απουσία διαχωρισμού καθηκόντων, έλλειψη παρακολούθησης και εποπτείας, μερικός ορισμός πολιτικών, αδυναμία εφαρμογής τεχνικών μέτρων επιβολής πολιτικών και διαδικασιών, κ.α.
4	5	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Τα στοιχεία από την παρακολούθηση του προσωπικού όπως αναφέρεται στο [HRS2] και τα στοιχεία από την διαχείριση περιστατικών ασφαλείας όπως αναφέρεται στο [EIM1] τροφοδοτούν την διαδικασία διαχείρισης διακινδύνευσης. Συγκεκριμένα, ελέγχεται αν υπάρχει σχετικός κίνδυνος που χρειάζεται να επικαιροποιηθεί ή αν δεν υπάρχει, να γίνει η σχετική προσθήκη ακολουθώντας το σύνολο της διαδικασίας όπως αναφέρεται στο [RM1-RM4]. Σε κάθε περίπτωση διενεργείται διαδικασία διάγνωσης για τους λόγους για τους οποίους δεν είχε αναγνωριστεί σωστά ή ελλιπώς κάποιος κίνδυνος. Σε περίπτωση που έχει αναγνωριστεί κάποια συστηματική απόκλιση ή παράλειψη διενεργείται εκ νέου η διαδικασία διαχείρισης διακινδύνευσης είτε συνολικά είτε στο μέρος που άμεσα ή έμμεσα επηρεάζεται.
5	2	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	3	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
HRS6		Μέτρο: Συμφωνίες εργοδότησης και αποδεκτή χρήσηΣτόχος Μέτρου: Να διασφαλιστεί ότι οι ευθύνες που αφορούν την ασφάλεια πληροφοριών και την αποδεκτή χρήση των στοιχείων ενεργητικού, ενσωματώνονται στις συμφωνίες εργοδότησης και στις διαδικασίες έναρξης απασχόλησης, για την επίτευξη υπευθυνότητας και ευαισθητοποίησης.Περιγραφή Μέτρου: Θέσπιση, εφαρμογή και διατήρηση μιας αποδεκτής πολιτικής χρήσης, η οποία προσδιορίζει τις χρήσεις που ο οργανισμός θεωρεί αποδεκτές χρήσεις των συστημάτων πληροφοριών που τίθενται στη διάθεση των στελεχών, ώστε να εξασφαλίζεται ότι τα στελέχη γνωρίζουν τι αναμένεται από αυτούς όσον αφορά τη χρήση, π.χ., ηλεκτρονικών υπολογιστών και κινητών συσκευών. Ο οργανισμός θα πρέπει να εξετάζει το ενδεχόμενο να ελέγχει την επίγνωση σχετικά με την πολιτική αποδεκτής χρήσης. Ο οργανισμός θα πρέπει επίσης να συνάπτει επαρκείς συμφωνίες εργοδότησης, στις οποίες να αναφέρονται με σαφήνεια οι υποχρεώσεις και οι ευθύνες του εργαζομένου όσον αφορά την ασφάλεια πληροφοριών. Πηγή:
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν έχει θεσπίσει πολιτική αποδεκτής χρήσης η οποία προσδιορίζει τις χρήσεις που ο οργανισμός θεωρεί αποδεκτές χρήσεις των συστημάτων πληροφοριών που τίθενται στη διάθεση των στελεχών, ώστε να εξασφαλίζεται ότι τα στελέχη γνωρίζουν τι αναμένεται από αυτούς όσον αφορά τη χρήση.
1	1	Το προσωπικό ενημερώνεται για την αποδεκτή χρήση των πόρων ή/και των πληροφοριών, χωρίς κατ'ανάγκη αυτό να είναι καταγεγραμμένο ή/και να υλοποιείται συστηματικά.
2	1	Έχουν προσδιορισθεί και εφαρμόζονται βασικούς κανόνες για την αποδεκτή χρήση πληροφοριών και περιουσιακών στοιχείων που σχετίζονται με πληροφορίες κρίσιμες για τον οργανισμό.
2	2	Στα βασικά στοιχεία περιέχονται τα ακόλουθα: (α) Περιορισμοί σε σχέση με τον τρόπο πλοήγησης στο διαδίκτυο, (β) Χρήση των υπολογιστών και άλλων πόρων που έχουν εκχωρηθεί για την διενέργεια εταιρικών εργασιών, (γ) Απαγόρευση της χρήσης των υπολογιστών και άλλων πόρων που έχουν εκχωρηθεί για την διενέργεια εταιρικών εργασιών για προσωπική χρήση.

3	1	Έχει θεσπιστεί, εφαρμόζεται και διατηρείται μία πολιτική αποδεκτής χρήσης η οποία προσδιορίζει τις χρήσεις που ο οργανισμός θεωρεί αποδεκτές χρήσεις των συστημάτων πληροφοριών που τίθενται στη διάθεση των στελεχών, ώστε να εξασφαλίζεται ότι τα στελέχη γνωρίζουν τι αναμένεται από αυτούς όσον αφορά τη χρήση.
3	2	Συνάπτονται επαρκείς συμφωνίες εργοδότησης, στις οποίες αναφέρονται με σαφήνεια οι υποχρεώσεις και οι ευθύνες του εργαζομένου όσον αφορά την ασφάλεια πληροφοριών.
3	3	Η πολιτική αποδεκτή χρήσης κοινοποιείται σε όλο το προσωπικό και γίνεται αποδεκτή μέσω των συμφωνιών εργοδότησης.
3	4	Το προσωπικό του οργανισμού έχει λάβει σχετική εκπαίδευση για την πολιτική αποδεκτής χρήσης.
3	5	Η πολιτική αποδεκτής χρήσης καθορίζει ότι: (α) Τα στοιχεία του οργανισμού χρησιμοποιούνται μόνο από εξουσιοδοτημένα άτομα, (β) Οι κωδικοί ή άλλα μέσα αυθεντικοποίησης της πρόσβασης δεν διαμοιράζονται με οποιονδήποτε άλλο, (γ) Το προσωπικό να οφείλει να εφαρμόζει μέτρα ανάλογα με την κρισιμότητα της πληροφορίας σύμφωνα με τις προδιαγραφές του [DS2], (δ) Γίνεται χρήση μόνο αδειοδοτημένου λογισμικού, (ε) Σε περίπτωση περιστατικού ασφαλείας χρειάζεται ενημέρωση, μαζί με τα σχετικά στοιχεία και λεπτομέρειες (ζ) Υπάρχει αποδεκτή χρήση για μεταφερόμενα μέσα (περιλαμβανομένης της αποθήκευσης on transit, της μετακίνησης κ.α.), η οποία περιγράφεται.
3	6	Γενικά η πολιτική περιέχει αναμενόμενες και μη αποδεκτές συμπεριφορές και χειρισμό εντός του οργανισμού και σε σχέση με τον χειρισμό των πληροφοριών και πόρων του οργανισμού. Επιπλέον στην πολιτική αναφέρονται και οι τρόποι παρακολούθησης (monitoring & logging) που έχει υλοποιήσει ο οργανισμός.
4	1	Η επίγνωση σχετικά με την πολιτική αποδεκτής χρήσης, ελέγχεται μέσω ερωτηματολογίων που συμπληρώνονται από το προσωπικό σε ετήσια βάση.
4	2	Οι συγκεκριμένοι κανόνες και πολιτικές αφορούν τόσο προσωπικό που εργοδοτείται από τον οργανισμό και αυτούς που παρέχουν υπηρεσία στον οργανισμό μέσω τρίτων μερών ή μπορεί να επηρεάσουν την ασφάλεια του οργανισμού.
4	3	Οι πολιτικές που έχουν δημιουργηθεί καλύπτουν: (α) Την πρόσβαση στο διαδίκτυο και το σχετικό φιλτράρισμα που γίνεται από τον οργανισμό (Web Access and filtering Policy), (β) Την χρήση μεταφερόμενων συσκευών (Mobile computing policy), (γ) Την χρήση μεταφερόμενων μέσων (Media policy), (δ) Την εργασία από απόσταση (Teleworking policy), (ε) Την πολιτική ελέγχου πρόσβασης με έμφαση στο κάθε επίπεδο διαβάθμισης όπως αναφέρονται στο [AM1] και στο [DS2], (ζ) Οδηγίες σε σχέση με την συντήρηση και την αποθήκευση των πόρων από το προσωπικό βάσει του ρόλου τους, (η) Πολιτική για την ασφαλή διαγραφή και απόσυρση πληροφοριών και πόρων (Secure erasure & disposal policy).
4	4	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Υλοποιούνται τεχνικά μέτρα ώστε να ενημερώνεται το προσωπικό κάθε φορά που πρόκειται να αποκτήσει πρόσβαση στα συστήματα του οργανισμού για τις οδηγίες αποδεκτής χρήσης.
5	2	Για κάθε περίπτωση πρόσβασης, ζητείται ενεργητική κίνηση από το σχετικό προσωπικό για την ανάγνωση των οδηγιών και τηρούνται τα σχετικά στοιχεία (χρόνος και τοποθεσία) της κίνησης.
5	3	Οι συγκεκριμένες ενέργειες και οδηγίες γίνονται σε συμφωνία με την κείμενη νομοθεσία ειδικά για θέματα προσωπικών δεδομένων.
5	4	Σε περίπτωση χρήσης cloud services, οι σχετικές οδηγίες και πολιτικές εφαρμόζονται και για τους συγκεκριμένους πόρους τόσο από το προσωπικό του οργανισμού όσο και από τον cloud provider (το τελευταίο εξασφαλίζεται μέσα από τις σχετικές συμβάσεις / συμφωνίες).
5	5	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	6	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.

Κατηγορία		ΦΥΣΙΚΗ ΑΣΦΑΛΕΙΑ
PS1		Μέτρο: Περιβαλλοντικά μέτρα Στόχος Μέτρου: Να εξασφαλιστούν επαρκή μέτρα για την προστασία του οργανισμού από τις επιπτώσεις φυσικών καταστροφών, όπως οι πλημμύρες, οι σεισμοί και οι πυρκαγιές. Περιγραφή Μέτρου: Θέσπιση, εφαρμογή και διατήρηση κατάλληλων μέτρων για την προστασία του οργανισμού από τις επιπτώσεις φυσικών καταστροφών, όπως οι πλημμύρες, οι σεισμοί και οι πυρκαγιές. Ο οργανισμός πρέπει να λαμβάνει υπόψη τη γεωγραφική θέση κατά τη δημιουργία της υποδομής δικτύου και να εξασφαλίζει ότι τα κρίσιμα στοιχεία υποδομής και συστήματα είναι γεωγραφικά διάσπαρτα. Πηγή: ENISA
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν λαμβάνει μέτρα για την προστασία του οργανισμού από τις επιπτώσεις φυσικών καταστροφών.
1	1	Έχουν ληφθεί τουλάχιστον κάποια βασικά μέτρα σχετικά με την προστασία του οργανισμού από τις επιπτώσεις φυσικών καταστροφών, όπως οι πλημμύρες, σεισμοί και πυρκαγιές.
1	2	Έχει συνταχθεί και υλοποιηθεί ο κατάλληλος σχεδιασμός για την πυροπροστασία του κτηρίου όπως προβλέπουν οι κανονισμοί πυροπροστασίας.
2	1	Διενεργούνται δοκιμές εκκένωσης σε τακτική βάση για σχετικά σενάρια κινδύνων.
2	2	Τα στοιχεία από τις δοκιμές λαμβάνονται υπόψη στον σχεδιασμό των σχεδίων επιχειρησιακής συνέχειας και ανάκαμψης από καταστροφή.
3	1	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται κατάλληλα μέτρα για την προστασία του οργανισμού από τις επιπτώσεις φυσικών καταστροφών, όπως οι πλημμύρες, οι σεισμοί και οι πυρκαγιές.
3	2	Λαμβάνεται υπόψη η γεωγραφική θέση κατά τη δημιουργία της υποδομής δικτύου και εξασφαλίζεται ότι τα κρίσιμα στοιχεία υποδομής και συστήματα είναι γεωγραφικά διάσπαρτα.
3	3	Εξασφαλίζεται ότι οι βασικές παροχές (π.χ. ρεύμα, δίκτυο) και οι κρίσιμες διασυνδέσεις με τρίτα μέρη, όπου απαιτούνται, έχουν τουλάχιστον 2 διαφορετικές οδεύσεις και αν είναι δυνατό, διαφορετικούς παρόχους.
3	4	Έχουν καταγραφεί και επικαιροποιηθεί, όπως απαιτείται, σχετικά σχέδια που αποτυπώνουν τις σχετικές οδεύσεις.
4	1	Το(α) κτήριο(α) που στεγάζει, λειτουργεί, εξυπηρετεί μέρος ή ολόκληρες τις κρίσιμες λειτουργίες και προσωπικό του οργανισμού έχει σχεδιαστεί και δομηθεί σύμφωνα με τα πρότυπα, τους κώδικες πρακτικής και τον αντισεισμικό κώδικα όπως ίσχυε στην ημερομηνία ανέγερσής του.
4	2	Το(α) κτήριο(α) έχουν σχετική έγκυρη άδεια σύμφωνα με την χρήση τους.
4	3	Έχει διενεργηθεί αξιολόγηση κινδύνου σε σχέση με τους περιβαλλοντικούς κινδύνους (π.χ. σεισμός, πλημμύρα, πυρκαγιά).
4	4	Για τους κινδύνους αυτούς έχει γίνει ανάλυση και σχεδιασμός βασικών προληπτικών μέτρων τόσο στο εξωτερικό του κτηρίου όσο και στο εσωτερικό όπως αναφέρεται στο [PS5], λαμβάνοντας υπόψη ιστορικά στοιχεία και διαθέσιμες μελέτες ανά περιοχή. (Ειδικά μέτρα θα πρέπει να ληφθούν αν το(α) κτήριο(α) βρίσκονται σε περιοχές που έχουν αναγνωριστεί ως Περιοχές Δυνητικού Σημαντικού Κινδύνου Πλημμύρας σύμφωνα με την Οδηγία 2007/60/ΕΚ.
4	5	Έχει θεσπιστεί, εφαρμόζεται και διατηρείται πολιτική για μέτρα φυσικής ασφάλειας και περιβαλλοντικούς ελέγχους.
4	6	Στο χώρο του computer room έχει τοποθετηθεί σύστημα το οποίο ενημερώνει σε περίπτωση πλημμύρας.
4	7	Στο χώρο του computer room έχει τοποθετηθεί αυτόματο σύστημα πυρανίχνευσης και πυρόσβεσης.
4	8	Έχει δημιουργηθεί σχετικό σχέδιο για την αντιμετώπισης των αντίστοιχων κινδύνων.
4	9	Έχει πραγματοποιηθεί μελέτη για τα περιβαλλοντικά μέτρα που υλοποιήθηκαν.
4	10	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Διενεργείται τακτική επιθεώρηση κτηρίων όσο αφορά τη δομοστατική τους επάρκεια από κατάλληλα εξουσιοδοτημένο και έμπειρο προσωπικό. Σε περίπτωση που προκύπτουν αποκλίσεις, υλοποιούνται τα κατάλληλα διορθωτικά μέτρα.
5	2	Τηρούνται κατάλληλες διασυνδέσεις και επαφές με αξιόπιστες πηγές (π.χ. εθνικές αρχές, ομάδες ενδιαφέροντος, παρατηρητήρια κ.α.) για την λήψη έγκυρης και έγκαιρης ενημέρωσης σχετικά με περιβαλλοντικούς κινδύνους.

5	3	Η σχετική πληροφορία που λαμβάνεται, αξιολογείται ώστε να εξασφαλίζεται η υψηλότερη ετοιμότητα του οργανισμού έναντι των συγκεκριμένων κινδύνων. Ο οργανισμός τηρεί δομημένα σχέδια ανταπόκρισης σε καταστάσεις κρίσεων σύμφωνα με τα [BCR1-4].
5	4	Τα σχέδια δοκιμάζονται τακτικά με την συμμετοχή των κατάλληλων αρχών και εθνικών ομάδων αντιμετώπισης.
5	5	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	6	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
PS2		Μέτρο: Έλεγχος περιμετρικής πρόσβασηςΣτόχος Μέτρου: Να διασφαλιστεί η φυσική περίμετρος του οργανισμού, με την εξασφάλιση και αποτροπή της μη εξουσιοδοτημένης πρόσβασης.Περιγραφή Μέτρου: Θέσπιση, εφαρμογή και διατήρηση φυσικής περιμέτρου ασφάλειας με σκοπό την προστασία των εγκαταστάσεων επεξεργασίας πληροφοριών. Ο οργανισμός πρέπει να καθιερώσει κατάλληλα μέτρα ελέγχου της περιμετρικής πρόσβασης με την εφαρμογή φυσικών συνόρων, όπως φράχτες, πόρτες και τοίχοι. Ο οργανισμός απαιτεί επίσης από τους υπαλλήλους και τους επισκέπτες να αποδεικνύουν την ταυτότητά τους στους φρουρούς ασφαλείας προκειμένου να εισέλθουν (σε κάποιο μέρος) του οργανισμού. Ο οργανισμός θα πρέπει να εξετάσει την εγκατάσταση καμερών κλειστού κυκλώματος με σκοπό τον εντοπισμό εισβολέων στα όρια του οργανισμού. Πηγή: NIST
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν λαμβάνει μέτρα για την ασφάλεια της φυσικής περιμέτρου του οργανισμού.
1	1	Τηρούνται τουλάχιστον κάποια βασικά μέτρα σχετικά με την περιμετρική ασφάλεια του οργανισμού, όπως το κλείδωμα όλων των κεντρικών εισόδων και ο έλεγχος στην είσοδο των ατόμων που εισέρχονται στο οργανισμό, χωρίς όμως να γίνεται καταγραφή.
2	1	Διατηρείται λίστα στην είσοδο των εγκαταστάσεων με τα άτομα που εισέρχονται στον οργανισμό.
2	2	Έχει τοποθετηθεί κάμερα μόνο στην κεντρική είσοδο του οργανισμού.
3	1	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται μέτρα για την ασφάλεια της περιμέτρου του οργανισμού με σκοπό την προστασία των εγκαταστάσεων επεξεργασίας πληροφοριών.
3	2	Έχουν καθιερωθεί κατάλληλα μέτρα ελέγχου της περιμετρικής πρόσβασης με την εφαρμογή φυσικών συνόρων, όπως φράχτες, πόρτες και τοίχους.
3	3	Έχει εγκατασταθεί σύστημα συναγερμού στις εγκαταστάσεις του.
3	4	Έχει εγκατασταθεί σύστημα access control για την είσοδο του προσωπικού στις εγκαταστάσεις του οργανισμού.
3	5	Οι επισκέπτες του οργανισμού συνοδεύονται καθ' όλη τη διάρκεια της παρουσίας τους στις εγκαταστάσεις του οργανισμού.
4	1	Έχει θεσπιστεί, εφαρμόζεται και διατηρείται διαδικασία και πολιτική σχετικά με την ασφάλεια της περιμέτρου του οργανισμού και την είσοδο στις εγκαταστάσεις.
4	2	Έχει εγκατασταθεί σύστημα καμερών κλειστού κυκλώματος με σκοπό τον εντοπισμό εισβολέων στα όρια του οργανισμού.
4	3	Διατηρούνται logs σχετικά με την καταγραφή των καμερών σύμφωνα με τη σχετική νομοθεσία για τα προσωπικά δεδομένα.
4	4	Διατηρούνται Logs από το σύστημα access control και ενημερώνεται μέσω ειδοποιήσεων για τυχόν παραβιάσεις.
4	5	Παρακολουθείται το σύστημα συναγερμού και το σύστημα καμερών κλειστού κυκλώματος και λαμβάνονται σχετικές ενημερώσεις σε περίπτωση που παρουσιαστεί οποιαδήποτε κίνηση.
4	6	Εκτελούνται έλεγχοι ασφαλείας στο φυσικό όριο της εγκατάστασης του οργανισμού για τη μη εξουσιοδοτημένη πρόσβαση και εξαγωγή πληροφοριών.
4	7	Ανασκοπούνται τουλάχιστον σε ετήσια βάση τα δικαιώματα και τις προσβάσεις του προσωπικού όσον αφορά το συναγερμό και το access control.
4	8	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Υπάρχει σύμβαση με εταιρεία που έχει αναλάβει τη φύλαξη των εγκαταστάσεων του οργανισμού και την παρακολούθηση του κλειστού κυκλώματος καμερών σε 24ώρη βάση.

5	2	Πραγματοποιούνται σε ετήσια βάση, δοκιμές παρείσδυσης που περιλαμβάνουν απροειδοποίητες προσπάθειες παράκαμψης ή παράκαμψης ελέγχων ασφαλείας που σχετίζονται με τα φυσικά σημεία πρόσβασης στην εγκατάσταση.
5	3	Έχουν υλοποιηθεί για την είσοδο στις εγκαταστάσεις του οργανισμού 2 επίπεδα ελέγχου, ο πρώτος έλεγχος πραγματοποιείται στην περίμετρο των εγκαταστάσεων και ο δεύτερος στην είσοδο του κτιρίου.
5	4	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	5	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
PS3		Μέτρο: Έλεγχος εσωτερικής πρόσβασης Στόχος Μέτρου: Να εξασφαλιστεί ο έλεγχος της πρόσβασης σε εσωτερικούς χώρους εργασίας και τις εγκαταστάσεις, ώστε να διασφαλίζεται ότι η φυσική πρόσβαση περιορίζεται κατόπιν ανάγκης. Περιγραφή Μέτρου: Θέσπιση, εφαρμογή και διατήρηση εσωτερικών μέτρων πρόσβασης, ευθυγραμμισμένων με τους ρόλους που περιγράφονται στο [IAM1], προκειμένου να διασφαλιστεί ότι μόνο τα στελέχη με έννομο συμφέρον έχουν πρόσβαση σε (συγκεκριμένα μέρη) του οργανισμού, π.χ. με τη δημιουργία ειδικών σαρωτών ταυτότητας για την πρόσβαση σε ένα μέρος του οργανισμού. Πηγή: 27002, NIST
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν λαμβάνει μέτρα για την εσωτερική πρόσβαση.
1	1	Τα άτομα που εισέρχονται και εξέρχονται από τις εγκαταστάσεις του οργανισμού ελέγχονται, αλλά δύναται να μη πραγματοποιείται η καταγραφή τους.
2	1	Διατηρείται λίστα στην είσοδο των εγκαταστάσεων με τα άτομα που έχουν εισέλθει στον οργανισμό.
3	1	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται εσωτερικά μέτρα πρόσβασης, τα οποία είναι ευθυγραμμισμένα με τους ρόλους που περιγράφονται στο [IAM1], προκειμένου να διασφαλιστεί ότι μόνο τα στελέχη με έννομο συμφέρον έχουν πρόσβαση σε (συγκεκριμένα μέρη) του οργανισμού.
3	2	Έχει εγκατασταθεί και χρησιμοποιείται σύστημα access control για την είσοδο του προσωπικού στις εγκαταστάσεις του οργανισμού.
3	3	Οι επιμέρους προσβάσεις σε χώρους ορίζονται σύμφωνα με τον ρόλο του εκάστοτε υπαλλήλου.
3	4	Για τους επισκέπτες δίδονται κάρτες που έχουν πρόσβαση μόνο στην κεντρική είσοδο. Κατά τη διάρκεια παραμονής τους στις εγκαταστάσεις συνοδεύονται υποχρεωτικά.
4	1	Έχει θεσπιστεί, εφαρμόζεται και διατηρείται διαδικασία και πολιτική σχετικά με τον έλεγχο της εσωτερικής πρόσβασης σε χώρους εργασίας.
4	2	Εκτελούνται έλεγχοι ασφαλείας στις εγκαταστάσεις του οργανισμού για μη εξουσιοδοτημένη πρόσβαση.
4	3	Οι προσβάσεις και τα δικαιώματα που δίδονται στο προσωπικό σε σχέση με το access control ανασκοπούνται τουλάχιστον μία φορά το χρόνο.
4	4	Διατηρούνται Logs από το σύστημα access control και ενημερώνεται μέσω ειδοποιήσεων για τυχόν παραβιάσεις.
4	5	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Για την είσοδο στις εγκαταστάσεις του οργανισμού, υλοποιούνται 2 επίπεδα ελέγχου, ο πρώτος έλεγχος πραγματοποιείται στην περίμετρο των εγκαταστάσεων και ο δεύτερος στην είσοδο του κτιρίου.
5	2	Πραγματοποιείούνται σε ετήσια βάση, δοκιμές παρείσδυσης που περιλαμβάνουν απροειδοποίητες προσπάθειες παράκαμψης ή παράκαμψης ελέγχων ασφαλείας που σχετίζονται με τα φυσικά σημεία πρόσβασης στην εγκατάσταση.
5	3	Χρησιμοποιούνται αυτοματοποιημένοι μηχανισμοί για να διευκολύνει τον έλεγχο των αρχείων πρόσβασης επισκεπτών και προσωπικού.
5	4	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	5	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.

PS4		Μέτρο: Ασφάλεια καλωδίωσης, εξοπλισμού και εγκαταστάσεων Στόχος Μέτρου: Να εξασφαλιστεί ότι για την καλωδίωση και τον εξοπλισμό που υποστηρίζουν την επεξεργασία των πληροφοριών, εξασφαλίζεται η φυσική προστασία από παρεμβολές, υποκλοπή ή ζημιά Περιγραφή Μέτρου: Θέσπιση, εφαρμογή και διατήρηση κατάλληλων μέτρων προκειμένου να προστατεύει την καλωδίωση και τον λοιπό εξοπλισμό από παρεμβολές, υποκλοπή ή ζημιά, οι οποίες θα προκαλούσαν διακοπή στις υπηρεσίες του οργανισμού. Ο οργανισμός πρέπει να εξασφαλίζει ότι τα καλώδια που παρέχουν ηλεκτρική ενέργεια σε κρίσιμες υποδομές προστατεύονται δεόντως και να εκπαιδεύει τους υπαλλήλους σύμφωνα με το μέτρο [TA2], ώστε να γνωρίζουν τη σημασία του εξοπλισμού που υποστηρίζει τις δραστηριότητες επεξεργασίας πληροφοριών. Η φυσική πρόσβαση στα λογικά δίκτυα θα πρέπει επίσης να προστατεύεται με κατάλληλα μέτρα ώστε να αποτρέπεται η μη εξουσιοδοτημένη φυσική πρόσβαση στο λογικό εξοπλισμό και το δίκτυο του οργανισμού. Ο φορέας εξετάζει κατάλληλα μέτρα πρόσβασης στο δίκτυο, όπως ορίζονται στο [NS5]. Ο οργανισμός διασφαλίζει τη φυσική ακεραιότητα και την τακτική συντήρηση των εγκαταστάσεων στις οποίες είναι εγκατεστημένος ο εξοπλισμός δικτύου, καθώς και την ορθή λειτουργία των μέτρων ασφάλειας. Πηγή: 27002, NIST
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν εφαρμόζει κάποια μέτρα σχετικά με ασφάλεια της καλωδίωσης και τη φυσική πρόσβαση στα λογικά δίκτυα.
1	1	Υπάρχει προστασία στα καλώδια τροφοδοσίας και τηλεπικοινωνιών που μεταφέρουν δεδομένα ή υπηρεσίες υποστήριξης πληροφοριών από υποκλοπές, παρεμβολές ή ζημιές.
1	2	Ο εξοπλισμός συντηρείται σύμφωνα με τα προτεινόμενα διαστήματα συντήρησης και τις προδιαγραφές του προμηθευτή.
2	1	Οι γραμμές ηλεκτρικού ρεύματος και τηλεπικοινωνιών στις εγκαταστάσεις επεξεργασίας πληροφοριών είναι υπόγειες, όπου είναι δυνατόν.
2	2	Χρησιμοποιείται μόνο εξουσιοδοτημένο προσωπικό συντήρησης για τις επισκευές και τον πιθανό εξοπλισμό συντήρησης.
3	1	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται κατάλληλα μέτρα προκειμένου να προστατεύεται η καλωδίωση και ο λοιπός εξοπλισμός από παρεμβολές, υποκλοπή ή ζημιά, οι οποίες θα προκαλούσαν διακοπή στις υπηρεσίες του οργανισμού.
3	2	Εξασφαλίζεται ότι τα καλώδια που παρέχουν ηλεκτρική ενέργεια σε κρίσιμες υποδομές προστατεύονται δεόντως και οι υπαλληλοι εκπαιδεύονται σύμφωνα με το μέτρο [TA2], ώστε να γνωρίζουν τη σημασία του εξοπλισμού που υποστηρίζει τις δραστηριότητες επεξεργασίας πληροφοριών.
3	3	Τα καλώδια τροφοδοσίας διαχωρίζονται από τα καλώδια επικοινωνίας για την αποφυγή παρεμβολών.
3	4	Η φυσική πρόσβαση στα λογικά δίκτυα προστατεύεται με κατάλληλα μέτρα ώστε να αποτρέπεται η μη εξουσιοδοτημένη φυσική πρόσβαση στο λογικό εξοπλισμό και το δίκτυο του οργανισμού.
3	5	Ασφαλίζονται (π.χ racks που κλειδώνουν) οι χώροι όπου υπάρχει πιθανότητα πρόσβασης στα patch panels ή σε οποιοδήποτε δικτυακό εξοπλισμό.
3	6	Ο φορέας εξετάζει κατάλληλα μέτρα πρόσβασης στο δίκτυο, όπως ορίζονται στο [NS5].
3	7	Διασφαλίζεται η φυσική ακεραιότητα και η τακτική συντήρηση των εγκαταστάσεων στις οποίες είναι εγκατεστημένος ο εξοπλισμός δικτύου, καθώς και η ορθή λειτουργία των μέτρων ασφάλειας.
3	8	Τηρούνται αρχεία για όλες τις βλάβες και για κάθε προληπτική και διορθωτική συντήρηση.
3	9	Η απομακρυσμένη συντήρηση των περιουσιακών στοιχείων του οργανισμού εγκρίνεται, καταγράφεται και εκτελείται με τρόπο που αποτρέπει τη μη εξουσιοδοτημένη πρόσβαση.
3	10	Εφαρμόζονται έλεγχοι όταν ο εξοπλισμός προγραμματίζεται για συντήρηση, λαμβάνοντας υπόψη εάν αυτή η συντήρηση εκτελείται από προσωπικό στο χώρο του οργανισμού ή εκτός αυτού. Όπου είναι απαραίτητο, οι εμπιστευτικές πληροφορίες διαγράφονται από τον εξοπλισμό.
4	1	Έχει θεσπιστεί, εφαρμόζεται και διατηρείται διαδικασία και πολιτική σχετικά με την ασφάλεια καλωδίωσης, εξοπλισμού και εγκαταστάσεων.
4	2	Έχει εγκατασταθεί για την προστασία των καλωδίων επικοινωνίας θωρακισμένος αγωγός καλωδίωσης.
4	3	Πραγματοποιούνται τεχνικές σαρώσεις και φυσικές επιθεωρήσεις για μη εξουσιοδοτημένες συσκευές που συνδέονται στα καλώδια.
4	4	Ο εξοπλισμός ελέγχεται πριν τεθεί ξανά σε λειτουργία ότι δεν έχει παραβιαστεί και ότι δεν παρουσιάζει δυσλειτουργία.

4	5	Τηρούνται από τους προμηθευτές όλες οι απαιτήσεις που επιβάλλονται από τα ασφαλιστήρια συμβόλαια.
4	6	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Γίνεται χρήση ηλεκτρομαγνητικής θωράκισης για την προστασία των καλωδίων.
5	2	Χρησιμοποιούνται μηχανισμοί ελέγχου ακεραιότητας για την επαλήθευση της ακεραιότητας του υλικού.
5	3	Κατά τη διάρκεια των εργασιών συντήρησης οι μηχανικοί υποχρεούνται να χρησιμοποιούν ιμάντα καρπού ηλεκτροστατικής εκκένωσης (ESD) ώστε να αποφευχθεί η συσσώρευση στατικού ηλεκτρισμού κοντά σε ευαίσθητα ηλεκτρονικά.
5	4	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	5	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
PS5		Μέτρο: Εσωτερικά περιβαλλοντικά μέτρα Στόχος Μέτρου: Να εξασφαλιστεί ότι οι εσωτερικοί χώροι και οι εγκαταστάσεις του οργανισμού προστατεύονται από φυσικές ζημιές Περιγραφή Μέτρου: Θέσπιση, εφαρμογή και διατήρηση μέτρων φυσικής ασφάλειας και προστασίας, ώστε να αποφεύγεται η φυσική ζημία στους εσωτερικούς χώρους και τις εγκαταστάσεις του οργανισμού. Κατά την εφαρμογή εσωτερικών περιβαλλοντικών μέτρων, ο οργανισμός θα πρέπει να εξετάζει τους κινδύνους που σχετίζονται με τη φωτιά και τη θερμοκρασία, την υγρασία, την ηλεκτρική ενέργεια, τη χρήση του νερού και άλλα στοιχεία που θα μπορούσαν να επηρεάσουν αρνητικά τη φυσική ασφάλεια των στοιχείων ενεργητικού. Ο οργανισμός πρέπει να εξετάζει την πυρόσβεση, τον έλεγχο της υγρασίας και άλλα μέτρα ανάλογα με τα χαρακτηριστικά των εσωτερικών φυσικών χώρων, όπως είναι τα κέντρα δεδομένων ή άλλους χώρους όπου βρίσκεται εξοπλισμός επεξεργασίας πληροφοριών. Πηγή:
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν έχει λάβει κανένα μέτρο για την προστασία των εσωτερικών χώρων και των εγκαταστάσεων του οργανισμού από φυσικές ζημιές.
1	1	Τα κρίσιμα στοιχεία του οργανισμού, όπως έχουν αναγνωριστεί στο [DS2] και στο [AM2], φιλοξενούνται σε διακριτούς χώρους που εφαρμόζεται έλεγχος πρόσβασης, έστω χωρίς να γίνεται σχετική καταγραφή.
1	2	Έχουν ληφθεί τουλάχιστον κάποια βασικά μέτρα σχετικά με την προστασία του χώρου, του εξοπλισμού και των πληροφοριών που στεγάζονται εκεί από τις επιπτώσεις φυσικών καταστροφών, όπως οι πλημμύρες, οι σεισμοί και οι πυρκαγιές. (Π.χ. υπάρχει τουλάχιστον ένας πυροσβεστήρας έξω από τον χώρο, ο εξοπλισμός είναι τοποθετημένος σε σημείο που δεν μπορεί να μετακινηθεί εύκολα σε περίπτωση σεισμού κλπ).
2	1	Παρακολουθούνται (έστω και χειροκίνητα) οι συνθήκες θερμοκρασίας και υγρασίας στους χώρους που φιλοξενούν τα κρίσιμα στοιχεία του οργανισμού.
2	2	Έχει οριστεί τουλάχιστον ένα άτομο εντός του οργανισμού που είναι υπεύθυνο για την παρακολούθηση των σχετικών στοιχείων και την ενημέρωση αρμόδιου προσωπικού σε περίπτωση που βρεθούν εκτός των προδιαγεγραμμένων αποδεκτών ορίων.
2	3	Υλοποιούνται κατάλληλα μέτρα (τουλάχιστον μια μονάδα κλιματισμού) προκειμένου να διασφαλίζεται ένα σταθερό επίπεδο θερμοκρασίας στους συγκεκριμένους χώρους.
3	1	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται μέτρα φυσικής ασφάλειας και προστασίας, ώστε να αποφεύγεται η φυσική ζημία στους εσωτερικούς χώρους και τις εγκαταστάσεις του οργανισμού.
3	2	Κατά την εφαρμογή εσωτερικών περιβαλλοντικών μέτρων, ο οργανισμός έχει εξετάσει τους κινδύνους που σχετίζονται με τη φωτιά και τη θερμοκρασία, την υγρασία, την ηλεκτρική ενέργεια, τη χρήση του νερού και άλλα στοιχεία που μπορούν να επηρεάσουν αρνητικά τη φυσική ασφάλεια των στοιχείων ενεργητικού.
3	3	Εξετάζεται η πυρόσβεση, ο έλεγχος της υγρασίας και άλλα μέτρα ανάλογα με τα χαρακτηριστικά των εσωτερικών φυσικών χώρων, όπως είναι τα κέντρα δεδομένων ή άλλους χώρους όπου βρίσκεται εξοπλισμός επεξεργασίας πληροφοριών.
3	4	Παρακολουθούνται με αυτόματα μέσα οι συνθήκες θερμοκρασίας και υγρασίας στους χώρους που φιλοξενούνται τα κρίσιμα στοιχεία του οργανισμού.
3	5	Έχουν οριστεί σχετικοί κανόνες για την ενημέρωση του κατάλληλου προσωπικού σε περίπτωση που οι τιμές βρεθούν εκτός των προδιαγεγραμμένων αποδεκτών ορίων.

3	6	Τα ελάχιστα μέτρα περιλαμβάνουν: (α) Αυτόματο σύστημα πυρανίχνευσης, (β) Το σύνολο του εξοπλισμού βρίσκεται τοποθετημένο εντός rack τα οποία έχουν ελεγχόμενη πρόσβαση, (γ) Αποτυπωμένο σχέδιο του χώρου με αναγνώριση των σημείων που βρίσκεται ο εξοπλισμός, (δ) Σήμανση, μεγάφωνο και κουμπί εκκένωσης καθώς και κατάλληλο φωτισμό ασφαλείας, (ε) Υπερυψωμένο πάτωμα, (ζ) Στους χώρους πρέπει να απαγορεύεται η φορτοεκφόρτωση και η είσοδος μη εξουσιοδοτημένου προσωπικού και (η) Για τους χώρους της γεννήτριας και του σημείου αποθήκευσης καυσίμου θα πρέπει να υπάρχουν κατάλληλα μέτρα πυρανίχνευσης όπου απαιτείται (π.χ εσωτερικούς χώρους) και πυρόσβεσης.
4	1	Έχει δημιουργηθεί ένα πλάνο και μια διαδικασία για τον διαχωρισμό και διαβάθμιση των χώρων επεξεργασίας πληροφοριών.
4	2	Η διαβάθμιση των χώρων λαμβάνει υπόψη την κρισιμότητα των διεργασιών που εκτελούνται εντός τους σύμφωνα με τα στοιχεία που έχουν εξαχθεί από το Business Impact Analysis [BCR1], την κρισιμότητα και ευαισθησία των πληροφοριών που επεξεργάζονται όπως περιγράφεται στο [DS2] και τα αποτελέσματα της διαδικασίας διαχείρισης διακινδύνευσης.
4	3	Έχουν καταγραφεί τα μέτρα που εφαρμόζονται για την κάθε κατηγορία χώρου.
4	4	Ειδικά για τους χώρους που ανήκουν στην υψηλότερη κατηγορία κατ' ελάχιστο εφαρμόζονται τα ακόλουθα μέτρα: (α) Αυτόματο σύστημα πυρόσβεσης με κατάλληλο μέσο ώστε να εξασφαλίζεται η μικρότερη επίπτωση επί των ανθρώπων, του εξοπλισμού ή των πληροφοριών, (β) Διπλά (εφεδρικά) συστήματα για την διατήρηση της σταθερής θερμοκρασίας εντός των χώρων, (γ) Εφεδρικές διασυνδέσεις σε επίπεδο ενέργειες και δικτύου, (δ) ΄Υπαρξη τουλάχιστον 3 ειδών παροχής ενέργειας (δίκτυο, UPS, γεννήτρια), (ε) Κατάλληλα μέτρα προστασίας για φυσική προστασία των καλωδίων από τρωκτικά και άλλους παράγοντες, (ζ) Ειδικά power strips για κάθε rack το οποίο φιλοξενεί εξοπλισμό τα οποία συνδέονται με τουλάχιστον 2 διακριτές πηγές ενέργειας, (η) Προσωπικό που είναι εξουσιοδοτημένο για την παρακολούθηση, συντήρηση, ορθή λειτουργία και άμεση ανταπόκριση σε σχέση με τα φυσικά μέσα προστασίας, (θ) Σύστημα αναγνώρισης και σήμανσης σχετικών καλωδίων, (ι) Υπάρχει μελέτη και σχεδιασμός του χώρου και του πατώματος σχετικά με το μέγιστο βάρος που μπορεί να αντέξει και την σχετική κατανομή του, (κ) Σε περίπτωση ενεργοποίησης της γεννήτριας, εξασφαλίζεται παροχή ρεύματος και στα συστήματα ελέγχου θερμοκρασίας, στα συστήματα φωτισμού και ελέγχου πρόσβασης καθώς και σε όλα τα σημεία δικτύου που απαιτούνται για την λειτουργική διασύνδεση και παροχή των κρίσιμων υπηρεσιών, (λ) Τηρείται διαδικασία για την συντήρηση, τον έλεγχο και την δοκιμή των στοιχείων που παρέχουν ενέργεια σε τακτική βάση, (μ) Έχει μετρηθεί ο χρόνος και ο τρόπος με τον οποίο εκκινείται η γεννήτρια και έχει ενσωματωθεί στον σχετικό σχεδιασμό για την ικανότητα του UPS και για την αυτοματοποίηση των ενεργειών, (ν) Υπάρχει αυτοματοποιημένο σύστημα by-pass για την απομόνωση στοιχείων ενέργειας σε περίπτωση που γίνεται συντήρηση, αντικατάσταση στοιχείων ή μπαταριών ή υπάρχει κάποια αστοχία, (ξ) Τηρείται διαδικασία για την συντήρηση, τον έλεγχο και την δοκιμή των στοιχείων πυροπροστασίας και διατήρησης θερμοκρασίας σε τακτική βάση, (ο) Υπάρχει κατάλληλη σήμανση και ανιχνευτές που υποδεικνύουν ότι στο χώρο έχει απελευθερωθεί αέριο που δεν είναι κατάλληλο για ανθρώπους, (π) Επαρκή μέτρα έχουν ληφθεί για την γείωση του συνόλου της εγκατάστασης ή του εξοπλισμού. Όλα τα παραπάνω μέτρα τηρούνται και στις περιπτώσεις που ο οργανισμός χρησιμοποιεί χώρους και εγκαταστάσεις τρίτων για την φιλοξενία του σχετικού εξοπλισμού.
4	5	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Οι σχετικές εγκαταστάσεις αποθήκευσης και λειτουργίας ακολουθούν διεθνείς βέλτιστες πρακτικές για την ανθεκτικότητα – π.χ. επιπέδου τουλάχιστον Tier III Uptime institute.
5	2	Διενεργούνται δοκιμές για την αξιολόγηση της ύπαρξης και δυνατότητας ορθής και αποτελεσματικής λειτουργίας του εν λόγω εξοπλισμού. Σε περίπτωση αναγνώρισης προβλημάτων, αυτά διορθώνονται άμεσα και τηρούνται καταγραφές σύμφωνα με την διαδικασία διαχείρισης αλλαγών [CM1].

5	3	Έχουν καταγραφεί τα μέτρα που εφαρμόζονται για την κάθε κατηγορία χώρου. Ειδικά για τους χώρους που ανήκουν στην υψηλότερη κατηγορία κατ' ελάχιστο εφαρμόζονται τα ακόλουθα μέτρα: (α) Ειδικό σχεδιασμό για την εξασφάλιση της μέγιστης απόδοσης σε επίπεδο θερμότητας και διατήρησης θερμοκρασίας (θερμοί και ψυχροί διάδρομοι κ.α.), (β) Διασυνδέσεις δικτύου για το core δίκτυο και για τα κρίσιμα συστήματα με οπτική ίνα, (γ) Σε περίπτωση που κάποια από τα racks δεν χρησιμοποιούνται τοποθετούνται σχετικά στοιχεία ώστε να επιτυγχάνεται ο έλεγχος πρόσβασης αλλά ταυτόχρονα να μην επηρεάζεται η λειτουργία και αποτελεσματικότητα των ψυχρών και θερμών διαδρόμων, (δ) Αυτόματο σύστημα παρακολούθησης των περιεχομένων των rack, της κατανάλωσης ενέργειας και της κατάστασης, (ε) Τα μηχανήματα είναι παραμετροποιημένα ώστε να ενεργοποιείται graceful shutdown σε περίπτωση επικείμενης ολικής απώλειας ενέργειας. Σε αυτές τις περιπτώσεις τα UPS αντέχουν το συνολικό φορτίο για τουλάχιστον 30 λεπτά, (ζ) Έχει υλοποιηθεί ένα battery monitoring σύστημα για τα UPS στα οποία παρακολουθείται, καταγράφεται και αναλύεται η επίδοση και οι τάσεις λειτουργίας των μπαταριών, (η) Υπάρχει κατάλληλος εξοπλισμός εκτός των συγκεκριμένων χώρων για εξοπλισμό για το προσωπικό όπως μάσκες / αναπνευστήρες / φακοί / κουβέρτες φωτιάς κ.α. , (θ) Για το χώρο που είναι αποθηκευμένα τα UPS και οι σχετικές μπαταρίες θα πρέπει να υπάρχουν μέτρα προστασίας – πρόσβασης, υγρασίας και θερμοκρασίας, (ι) Υπάρχει σύστημα για την αντικεραυνική προστασία, (κ) Έχει εφαρμοσθεί ένα BMS για την συνολική παρακολούθηση και λειτουργία των μηχανολογικών, ηλεκτρικών μέτρων καθώς και των μέτρων πυρασφάλειας
5	4	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	5	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.

Κατηγορία		ΔΙΑΧΕΙΡΙΣΗ ΣΥΜΒΑΝΤΩΝ ΚΑΙ ΠΕΡΙΣΤΑΤΙΚΩΝ
EIM1		Μέτρο: Ετοιμότητα και εντοπισμός συμβάντων και περιστατικών Στόχος Μέτρου: Να διασφαλίζει ότι ο οργανισμός είναι σε θέση να εντοπίζει συμβάντα και περιστατικά που ενδέχεται να συνιστούν απειλή για τους στόχους της ασφάλειας πληροφοριών του οργανισμού και να ενεργοποιεί τις αντίστοιχες διαδικασίες αντιμετώπισης περιστατικών. Περιγραφή Μέτρου: Θέσπιση, εφαρμογή και διατήρηση σχεδίου διαχείρισης και αντιμετώπισης συμβάντων και περιστατικών προκειμένου να διασφαλιστεί ότι ο οργανισμός είναι έτοιμος να αντιδράσει σε περίπτωση σοβαρού συμβάντος ή περιστατικού που αφορά την ασφάλεια πληροφοριών. Ο οργανισμός εξετάζει το ενδεχόμενο ευθυγράμμισης των διαδικασιών του για την αντιμετώπιση συμβάντων και περιστατικών με γενικές δυνατότητες παρακολούθησης και ειδικές λειτουργίες παρακολούθησης της ασφάλειας, όπως τις υπηρεσίες ανίχνευσης και πρόληψης εισβολών που περιγράφονται στο μέτρο [NS7]. Πηγή: NIST
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν έχει θεσπίσει σχέδιο διαχείρισης και αντιμετώπισης συμβάντων και περιστατικών προκειμένου να διασφαλιστεί ότι ο οργανισμός είναι έτοιμος να αντιδράσει σε περίπτωση σοβαρού συμβάντος ή περιστατικού που αφορά την ασφάλεια πληροφοριών.
1	1	Η διαχείριση για τα περιστατικά και τα συμβάντα γίνεται τουλάχιστον ad-hoc και χωρίς κατ'ανάγκη να έχει θεσπιστεί σχέδιο διαχείρισης και αντιμετώπισης συμβάντων και περιστατικών.
2	1	Έχει θεσπιστεί και εφαρμόζεται ένα βασικό σχέδιο διαχείρισης και αντιμετώπισης συμβάντων και περιστατικών.
3	1	Έχει θεσπιστεί, εφαρμόζεται και διατηρείται σχέδιο διαχείρισης και αντιμετώπισης συμβάντων και περιστατικών προκειμένου να διασφαλιστεί ότι ο οργανισμός είναι έτοιμος να αντιδράσει σε περίπτωση σοβαρού συμβάντος ή περιστατικού που αφορά την ασφάλεια πληροφοριών.
3	2	Το σχέδιο αντιμετώπισης συμβάντων και περιστατικών θα πρέπει να: (α) Παρέχει στον οργανισμό έναν οδικό χάρτη για την εφαρμογή της ικανότητας απόκρισης συμβάντων (β) Περιγράφει τη δομή και την οργάνωση της ικανότητας απόκρισης σε περιστατικό. (γ) Παρέχει μία high level προσέγγιση για τον τρόπο με τον οποίο η ικανότητα απόκρισης περιστατικού ταιριάζει στο σύνολο του οργανισμού. (δ) Πληροί τις μοναδικές απαιτήσεις του οργανισμού, οι οποίες σχετίζονται με την αποστολή, το μέγεθος, τη δομή και τις λειτουργίες. (ε) Καθορίζει τα περιστατικά ασφάλειας για τα οποία θα πρέπει να συμπληρώνονται σχετικές αναφορές. (ζ) Παρέχει KPI's για τη μέτρηση της ικανότητας απόκρισης περιστατικού εντός του οργανισμού. (η) Καθορίζει τους πόρους και τη διοικητική υποστήριξη που απαιτούνται για την αποτελεσματική διατήρηση και ωρίμανση της ικανότητας απόκρισης σε περιστατικά.
3	3	Εξετάζεται το ενδεχόμενο ευθυγράμμισης των διαδικασιών του για την αντιμετώπιση συμβάντων και περιστατικών με γενικές δυνατότητες παρακολούθησης και ειδικές λειτουργίες παρακολούθησης της ασφάλειας, όπως τις υπηρεσίες ανίχνευσης και πρόληψης εισβολών που περιγράφονται στο μέτρο [NS7].
3	4	Ο οργανισμός διανέμει αντίγραφα του σχεδίου αντιμετώπισης συμβάντων και περιστατικών σε όλους τους εμπλεκόμενους (εσωτερικούς ή/και εξωτερικούς) και διατηρεί σχετική λίστα.
3	5	Το σχέδιο αντιμετώπισης συμβάντων και περιστατικών εγκρίνεται από τη διοίκηση του οργανισμού.
4	1	Οι διαδικασίες του για την αντιμετώπιση συμβάντων και περιστατικών είναι ευθυγραμμισμένες με γενικές δυνατότητες παρακολούθησης και ειδικές λειτουργίες παρακολούθησης της ασφάλειας, όπως τις υπηρεσίες ανίχνευσης και πρόληψης εισβολών που περιγράφονται στο μέτρο [NS7].
4	2	Οι αλλαγές του σχεδίου αντιμετώπισης συμβάντων και περιστατικών επικοινωνούνται σε όλους τους εμπλεκόμενους (εσωτερικούς ή/και εξωτερικούς).
4	3	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Το σχέδιο αντιμετώπισης συμβάντων και περιστατικών προστατεύεται από μη εξουσιοδοτημένη αποκάλυψη και μη εξουσιοδοτημένη/ελεγχόμενη τροποποίηση.

5	2	Έγκυρες πληροφορίες Cyber threat intelligence λαμβάνονται έγκαιρα και μεταξύ άλλων χρησιμοποιούνται για την επικαιροποίηση του καταλόγου απειλών, ευπαθειών και κινδύνων στους οποίους είναι εκτεθειμένος ο οργανισμός.
5	3	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	4	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
EIM2		Μέτρο: Ανάλυση και αξιολόγηση συμβάντων και περιστατικώνΣτόχος Μέτρου: Να διασφαλιστεί ότι ο οργανισμός είναι σε θέση να αναλύει και να αξιολογεί συμβάντα και περιστατικά που αφορούν την ασφάλεια πληροφοριών, ούτως ώστε να ενεργοποιεί κατάλληλες διαδικασίες περιορισμού και ανάκτησης.Περιγραφή Μέτρου: Θέσπιση, εφαρμογή και διατήρηση διαδικασιών που επιτρέπουν την ανάλυση και την αξιολόγηση συμβάντων και περιστατικών, ώστε να είναι σε θέση ο οργανισμός να λαμβάνει αιτιολογημένες αποφάσεις σχετικά με τις δράσεις και τα μέτρα που πρέπει να ληφθούν για την αντιμετώπιση ή την αποκατάσταση από συμβάντα και περιστατικά που αφορούν την ασφάλεια. Ο οργανισμός εξετάζει τον αντίκτυπο στα υποκείμενα δεδομένων, στις επιχειρηματικές δραστηριότητες, στα εξωτερικά μέρη και στο οικοσύστημα των φορέων. Ο οργανισμός διασφαλίζει ότι η ανάλυση και αξιολόγηση συμβάντων και περιστατικών διεκπεραιώνεται σε συνεννόηση με την ανώτατη διοίκηση για τη σύνδεση συμβάντων και περιστατικών με σενάρια υψηλού κινδύνου.
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν αναλύει και δεν αξιολογεί συμβάντα και περιστατικά που αφορούν την ασφάλεια πληροφοριών. Δεν έχει θεσπίσει διαδικασίες για την ανάλυση και την αξιολόγηση συμβάντων και περιστατικών.
1	1	Τα συμβάντα και περιστατικά αξιολογούνται και αναλύονται τουλάχιστον με ad-hoc τρόπο, χωρίς κατ' ανάγκη να έχει δημιουργήθεί σχετική διαδικασία.
2	1	Έχει θεσπίστεί μία διαδικασία η οποία αφορά τον τρόπο που πραγματοποιείται η ανάλυση και η αξιολόγηση συμβάντων και περιστατικών.
3	1	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται διαδικασίες που επιτρέπουν την ανάλυση και την αξιολόγηση συμβάντων και περιστατικών, ώστε ο οργανισμός να λαμβάνει αιτιολογημένες αποφάσεις σχετικά με τις δράσεις και τα μέτρα για την αντιμετώπιση ή την αποκατάσταση από συμβάντα και περιστατικά που αφορούν την ασφάλεια.
3	2	Εξετάζεται ο αντίκτυπος στα υποκείμενα δεδομένων, στις επιχειρηματικές δραστηριότητες, στα εξωτερικά μέρη και στο οικοσύστημα των φορέων.
3	3	Διασφαλίζεται ότι η ανάλυση και αξιολόγηση συμβάντων και περιστατικών διεκπεραιώνεται σε συνεννόηση με την ανώτατη διοίκηση για τη σύνδεση συμβάντων και περιστατικών με σενάρια υψηλού κινδύνου.
3	4	Γίνεται καταγραφή των αποτελεσμάτων της ανάλυσης και της αξιολόγησης των εκάστοτε συμβάντων ή περιστατικών που έχουν εντοπιστεί από τον οργανισμό.
3	5	Τα περιστατικά ασφάλειας πληροφοριών ταξινομούνται κατά σοβαρότητα χρησιμοποιώντας την κλίμακα: (α) Πληροφορίες: κανένα αντίκτυπο, αλλά η ανάλυση θα μπορούσε να χρησιμοποιηθεί για τη βελτίωση των πολιτικών, διαδικασιών ή ελέγχων ασφάλειας πληροφοριών, (β) Προειδοποίηση: χαμηλό αντίκτυπο, (γ) Κρίσιμο: μέτριο αντίκτυπο, και (δ) Έκτακτη ανάγκη: σοβαρό αντίκτυπο, ή αντίστοιχο 'πολυεπιπεδές σχήμα ταξινόμησης'.
3	6	Σύμφωνα με τους παραπάνω παράγοντες ταξινόμησης, αυτή η προσέγγιση ταξινομεί τα συμβάντα ασφάλειας πληροφοριών σε τέσσερις κατηγορίες: (α) Πολύ σοβαρά, (β) Σοβαρά, (γ) Λιγότερο σοβαρά, και (δ) Μικρά ή αντίστοιχο' πολυεπιπεδές σχήμα ταξινόμησης. (α) Πολύ σοβαρά περιστατικά είναι αυτά που ενεργούν σε κρίσιμα συστήματα πληροφοριών και οδηγούν σε ιδιαίτερα σοβαρή επιχειρησιακή απώλεια, ή οδηγούν σε ιδιαίτερα σημαντικό κοινωνικό αντίκτυπο. (β) Σοβαρά περιστατικά είναι αυτά που ενεργούν σε κρίσιμα συστήματα πληροφοριών ή σημαντικά συστήματα πληροφοριών και οδηγούν σε σοβαρή επιχειρησιακή απώλεια ή οδηγούν σε σημαντικό κοινωνικό αντίκτυπο. (γ) Λιγότερο σοβαρά περιστατικά είναι αυτά που ενεργούν σε σημαντικά συστήματα πληροφοριών ή συστήματα πληροφοριών που δεν έχουν μεγάλο αντίκτυπο για τον οργανισμό και οδηγούν σε σημαντική επιχειρησιακή απώλεια, ή οδηγούν σε σημαντικό κοινωνικό αντίκτυπο. (δ) Μικρά περιστατικά είναι αυτά που ενεργούν σε συστήματα πληροφοριών που δεν έχουν μεγάλο αντίκτυπο για τον οργανισμό και οδηγούν σε μικρή επιχειρησιακή απώλεια ή καμία επιχειρησιακή απώλεια, ή οδηγούν σε μικρό κοινωνικό αντίκτυπο ή χωρίς κοινωνικό αντίκτυπο.

3	7	Έχει ορισθεί σημείο επαφής (εσωτερικά του οργανισμού) το οποίο αξιολογεί κάθε συμβάν ασφάλειας πληροφοριών χρησιμοποιώντας τη συμφωνημένη κλίμακα ταξινόμησης περιστατικών και αποφασίζει εάν το συμβάν πρέπει να ταξινομηθεί ως περιστατικό ασφάλειας πληροφοριών.
4	1	Υπάρχει ομάδα αντιμετώπισης περιστατικών ασφάλειας πληροφοριών (ISIRT).
4	2	Διαβιβάζεται η αξιολόγηση και η απόφαση ενός περιστατικού ή/και συμβάντος για επιβεβαίωση ή επανεκτίμηση ανάλογα με τη σοβαρότητα.
4	3	Η ομάδα αντιμετώπισης περιστατικών ασφάλειας πληροφοριών αναλύει τα περιστατικά που έχουν εντοπιστεί με σκοπό την κατανόηση των μεθόδων και των στόχων της επίθεσης.
4	4	Υπάρχει συνεργασία με πάροχο υπηρεσιών για τη διαχείριση περιστατικών.
4	5	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Υπάρχει σύμβαση με τρίτο μέρος το οποίο εκτελεί ψηφιακή εγκληματολογία για τον οργανισμό σε περίπτωση σχετικού περιστατικού ασφαλείας ή συμβάντος.
5	2	Υπάρχει συμμετοχή σε εσωτερικές ή και εξωτερικές ασκήσεις για την αξιολόγηση της αποτελεσματικότητας και επίγνωσης του προσωπικού σχετικά με την ανάλυση και αξιολόγηση περιστατικών.
5	3	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	4	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
EIM3		Μέτρο: Περιορισμός και ανάκτηση από συμβάντα και περιστατικά Στόχος Μέτρου: Να εξασφαλιστεί επαρκής περιορισμός και αποκατάσταση από συμβάντα και περιστατικά ασφάλειας που επηρεάζουν αρνητικά τους στόχους ασφάλειας πληροφοριών του οργανισμού. Περιγραφή Μέτρου: Θέσπιση, εφαρμογή και διατήρηση διαδικασιών για τον περιορισμό και την ανάκτηση από συμβάντα και περιστατικά, ώστε να περιορίζονται στο ελάχιστο οι επιπτώσεις στα συστήματα, τις εφαρμογές, τα δίκτυα και τα δεδομένα, καθώς και να διασφαλίζονται, στο μέτρο του δυνατού, οι κρίσιμες λειτουργίες του οργανισμού. Ο οργανισμός εξετάζει τους στόχους αποκατάστασης από συμβάντα και περιστατικά, λαμβάνοντας υπόψη τον στόχο του σημείου ανάκτησης (RPO) και τον χρόνο αποκατάστασης (RTO), προκειμένου να προσδιορίσει τη στοχοθετημένη διάρκεια και το επίπεδο των υπηρεσιών εντός των οποίων πρέπει να αποκατασταθεί μια επιχειρηματική διαδικασία μετά από κάποιο περιστατικό. Πηγή:
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν έχει θεσπίσει και δεν εφαρμόζει διαδικασίες για τον περιορισμό και την αποκατάσταση από συμβάντα και περιστατικά.
1	1	Η αντίδραση στα περιστατικά ασφαλείας γίνεται τουλάχιστον με ad-hoc τρόπο.
2	1	Έχουν αναγνωρισθεί κάποιοι ρόλοι σε σχέση με την ανταπόκριση σε περιστατικά ασφαλείας και έχει ενημερωθεί το λοιπό προσωπικό και τα συγκεκριμένα άτομα σχετικά με τις υποχρεώσεις τους σε σχέση με πιθανά περιστατικά ασφαλείας.
3	1	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται διαδικασίες για τον περιορισμό και την αποκατάσταση (ανάκαμψη) από συμβάντα και περιστατικά, ώστε να περιορίζονται στο ελάχιστο οι επιπτώσεις στα συστήματα, τις εφαρμογές, τα δίκτυα και τα δεδομένα, καθώς και να διασφαλίζονται, στο μέτρο του δυνατού, οι κρίσιμες λειτουργίες του οργανισμού.
3	2	Οι στόχοι αποκατάστασης από συμβάντα και περιστατικά εξετάζονται, λαμβάνοντας υπόψη τον στόχο του σημείου ανάκτησης (RPO) και τον χρόνο αποκατάστασης (RTO), προκειμένου να προσδιορισθεί η στοχοθετημένη διάρκεια και το επίπεδο των υπηρεσιών εντός των οποίων πρέπει να αποκατασταθεί μια επιχειρηματική διαδικασία μετά από κάποιο περιστατικό.
3	3	Ακολουθείται η κατηγοριοποίηση περιστατικών που αναλύεται στο [EIM2].
4	1	Έχουν δημιουργηθεί συγκεκριμένα σχέδια στα οποία περιγράφονται τρόποι λειτουργίας, μέτρα και βήματα σε περίπτωση συγκεκριμένων τύπων περιστατικών.
4	2	Τα δεδομένα των σχεδίων έχουν προκύψει από την σχετική αξιολόγηση κινδύνων και να καλύπτουν τα κυριότερα είδη απειλών / επιθέσεων σύμφωνα με διεθνείς αναφορές και στοιχεία.

4	3	Κατ΄ ελάχιστο τέτοια σχέδια περιλαμβάνουν περιπτώσεις όπως: (α) Ransomware, b) Malware, c) Social engineering attack, d) Denial of Service , e) Supply chain availability attack, f) Physical security attack, g) Theft of media / device / information.
4	4	Λαμβάνεται υπόψη ο στόχος του σημείου ανάκτησης (RPO) και του χρόνο αποκατάστασης (RTO), προκειμένου να προσδιορίσει η στοχοθετημένη διάρκεια και το επίπεδο των υπηρεσιών εντός των οποίων πρέπει να αποκατασταθεί μια επιχειρηματική διαδικασία μετά από κάποιο περιστατικό.
4	5	Οι ενέργειες που προβλέπονται για τον περιορισμό των επιπτώσεων του οργανισμού είναι κατάλληλες ανάλογα με την κρισιμότητα του περιστατικού και τις πληροφορίες ή λειτουργίες που επηρεάζονται ή δύναται να επηρεαστούν. Ο οργανισμός στα πλαίσια του περιορισμού και της ανταπόκρισης μπορεί να ζητήσει την συνδρομή από τις σχετικές αρχές.
4	6	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Έχουν προδιαγραφεί συγκεκριμένες διαδικασίες σχετικά με τον χειρισμό και την διατήρηση δεδομένων σε περίπτωση περιστατικού ασφαλείας.
5	2	Υλοποιούνται κατάλληλες ενέργειες ώστε κατάλληλα εξουσιοδοτημένοι ρόλοι να αναλάβουν την ασφαλή λήψη (με διατήρηση του chain of custody) στοιχείων ώστε να μπορούν να χρησιμοποιηθούν στην συνέχεια από τις αρμόδιες αρχές ή άλλα ειδικά εξουσιοδοτημένα μέρη.
5	3	Διενεργούνται τακτικές ασκήσεις και δοκιμές για να εξασφαλισθεί ότι το προσωπικό έχει επίγνωση των σχετικών σχεδίων, ότι οι προβλέψεις τους είναι ορθές και αποτελεσματικές και έχουν την δυνατότητα να επιτύχουν το επίπεδο ασφάλειας και λειτουργίας που επιθυμεί ο οργανισμός ακόμα και σε περίπτωση περιστατικού.
5	4	Υπάρχει απίτηση από τους συνεργάτες και υπεργολάβους του (που απαρτίζουν το supply chain των κρίσιμων λειτουργιών) να έχουν αντίστοιχες καταγεγραμμένες και ελεγμένες διαδικασίες ανταπόκρισης στα περιστατικά ασφαλείας και να δεσμεύονται για την άμεση συνδρομή τους σε περίπτωση που απαιτείται από τον οργανισμό.
5	5	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	6	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
EIM4		Μέτρο: Δραστηριότητες μετά το συμβάν και το περιστατικό. Στόχος Μέτρου: Να διασφαλιστεί ότι ο οργανισμός μαθαίνει από συμβάντα και περιστατικά ασφάλειας, προκειμένου να αποτρέπονται παρόμοια συμβάντα και περιστατικά στο μέλλον. Περιγραφή Μέτρου: Θέσπιση, εφαρμογή και διατήρηση διαδικασιών μετά την εκδήλωση συμβάντων και περιστατικών, προκειμένου να αποτυπωθούν τα διδάγματα που έχουν αντληθεί από τα συμβάντα και περιστατικά ασφάλειας πληροφοριών και να προσδιορίζουν κατά πόσον πρέπει να θεσπιστούν πρόσθετα μέτρα ασφάλειας για την πρόληψη παρόμοιων συμβάντων και περιστατικών. Ο οργανισμός εξετάζει το ενδεχόμενο θέσπισης εκ των υστέρων διαδικασίας, η οποία περιλαμβάνει συνάντηση για την αξιολόγηση του συμβάντος ή περιστατικού με τους επηρεαζόμενους ιδιοκτήτες του συστήματος, τους διαχειριστές δεδομένων και άλλα ενδιαφερόμενα μέρη που συμμετείχαν στην αντιμετώπιση του περιστατικού, με σκοπό την ανταλλαγή διδαγμάτων και τον προσδιορισμό προληπτικών μέτρων. Πηγή: 27002, 27035
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν έχει θεσπίσει διαδικασίες ώστε μετά την εκδήλωση συμβάντων και περιστατικών να αποτυπωθούν τα διδάγματα από τα συμβάντα και περιστατικά ασφάλειας πληροφοριών και να προσδιορίζουν κατά πόσον πρέπει να θεσπιστούν πρόσθετα μέτρα ασφάλειας για την πρόληψη παρόμοιων συμβάντων και περιστατικών.
1	1	Μετά από συμβάν ή περιστατικό ασφαλείας οι διαθέσιμες πληροφορίες συλλέγονται τουλάχιστον με ad-hoc τρόπο, ώστε να κατανοηθεί το περιστατικό ή το συμβάν.
2	1	Έχει θεσπιστεί διαδικασία σχετικά με τα βήματα που πρέπει να ακολουθούνται μετά από ένα περιστατικό ώστε ο οργανισμός να αξιολογεί το επίπεδο ασφάλειάς του και να αποτρέπονται παρόμοια συμβάντα και περιστατικά στο μέλλον.

3	1	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται διαδικασίες μετά την εκδήλωση συμβάντων και περιστατικών, προκειμένου να αποτυπωθούν τα διδάγματα που έχουν αντληθεί από τα συμβάντα και περιστατικά ασφάλειας πληροφοριών και να προσδιορίζουν κατά πόσον πρέπει να θεσπιστούν πρόσθετα μέτρα ασφάλειας για την πρόληψη παρόμοιων συμβάντων και περιστατικών.
3	2	Για τη φάση των διδαγμάτων, εκτελούνται οι ακόλουθες δραστηριότητες οι οποίες αποτυπώνονται και στη διαδικασία: (α) Ο οργανισμός εντοπίζει τα διδάγματα που αντλήθηκαν από συμβάντα και τρωτά σημεία ασφάλειας πληροφοριών, (β) Αναγνώριση, επανεξέταση και πραγματοποίηση βελτιώσεων στην εφαρμογή μέτρων ασφάλειας πληροφοριών, (γ) Επανεξέταση και βελτίωση στην αξιολόγηση κινδύνου για την ασφάλεια των πληροφοριών, (δ) Εξέταση της αποτελεσματικότητας των διαδικασιών, των πολιτικών, των εμπλεκόμενων με το περιστατικό (π.χ. Ομάδα ανταπόκρισης), την ανάλυση και την ανάκτηση από περιστατικό και την αντιμετώπιση τρωτών σημείων σε σχέση με την ασφάλεια πληροφοριών. Με βάση τα διδάγματα που αντλήθηκαν, εντοπίζονται και πραγματοποιούνται βελτιώσεις στο σχέδιο διαχείρισης συμβάντων ασφάλειας πληροφοριών.
3	3	Χρησιμοποιούνται οι πληροφορίες που λαμβάνονται από την αξιολόγηση των συμβάντων ή περιστατικών ασφάλειας πληροφοριών για τον επαναλαμβανόμενων ή υψηλού αντίκτυπου συμβάντων.
3	4	Εξετάζεται το ενδεχόμενο θέσπισης εκ των υστέρων διαδικασίας, η οποία περιλαμβάνει συνάντηση για την αξιολόγηση του συμβάντος ή περιστατικού με τους επηρεαζόμενους ιδιοκτήτες του συστήματος, τους διαχειριστές δεδομένων και άλλα ενδιαφερόμενα μέρη που συμμετείχαν στην αντιμετώπιση του περιστατικού, με σκοπό την ανταλλαγή διδαγμάτων και τον προσδιορισμό προληπτικών μέτρων.
4	1	Έχει θεσπιστεί και εφαρμόζεται διαδικασία η οποία περιλαμβάνει συνάντηση για την αξιολόγηση του συμβάντος ή περιστατικού με τους επηρεαζόμενους ιδιοκτήτες του συστήματος, τους διαχειριστές δεδομένων και άλλα ενδιαφερόμενα μέρη που συμμετείχαν στην αντιμετώπιση του περιστατικού, με σκοπό την ανταλλαγή διδαγμάτων και τον προσδιορισμό προληπτικών μέτρων.
4	2	Μετά από ένα περιστατικό ή ένα συμβάν αξιολογείται η αποτελεσματικότητα και η σωστή ανταπόκριση της ομάδας αντιμετώπισης περιστατικών ασφάλειας πληροφοριών.
4	3	Χρησιμοποιούνται στοιχεία από πραγματικά περιστατικά ασφαλείας πληροφοριών που μπορούν να συμπεριληφθούν στην εκπαίδευση του προσωπικού ως παραδείγματα για το τι θα μπορούσε να συμβεί, πώς να αντιδράσετε σε τέτοια περιστατικά και πώς να τα αποφύγετε στο μέλλον.
4	4	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Ελέγχεται εάν οι πληροφορίες του περιστατικού, οι σχετικοί φορείς επίθεσης και τα τρωτά σημεία μπορούν να κοινοποιηθούν με συνεργαζόμενους οργανισμούς για να βοηθήσουν στην αποτροπή εμφάνισης ίδιων περιστατικών στο περιβάλλον τους.
5	2	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	3	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
EIM5		Μέτρο: Ρυθμιστικές υποχρεώσεις κοινοποίησης συμβάντος και συνεργασίας. Στόχος Μέτρου: Να διασφαλίσει ότι ο οργανισμός ενημερώνει τα σχετικά ενδιαφερόμενα μέρη στην περίπτωση συμβάντων ή περιστατικών ασφάλειας, όπως περιγράφεται σε νομικές και ρυθμιστικές υποχρεώσεις. Περιγραφή Μέτρου: Θέσπιση, εφαρμογή και διατήρηση διαδικασιών για τη διασφάλιση της συμμόρφωσης με ρυθμιστικές και νομοθετικές απαιτήσεις όσον αφορά την κοινοποίηση περιστατικών. Ο οργανισμός διασφαλίζει ότι υπάρχουν επαρκείς διαδικασίες κοινοποίησης και υποβολής εκθέσεων για συμβάντα και περιστατικά ασφάλειας πληροφοριών σε αρμόδιες ρυθμιστικές αρχές, όπως την ΑΨΑ. Στο πλαίσιο των δεδομένων προσωπικού χαρακτήρα, ο οργανισμός διασφαλίζει τη συμμόρφωση με τις σχετικές νομοθετικές και ρυθμιστικές διατάξεις που αφορούν την προστασία των δεδομένων προσωπικού χαρακτήρα και επικοινωνεί, όπου είναι απαραίτητο, με την αρμόδια αρχή προστασίας δεδομένων. Πηγή:
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν έχει θεσπίσει διαδικασία για τη διασφάλιση της συμμόρφωσης με ρυθμιστικές και νομοθετικές απαιτήσεις όσον αφορά την κοινοποίηση περιστατικών.
1	1	Τα σχετικά ενδιαφερόμενα μέρη στην περίπτωση συμβάντων ή περιστατικών ασφάλειας ενημερώνονται τουλάχιστον με τρόπο ad-hoc.

2	1	Έχουν καταγραφεί σε λίστα τα σχετικά στοιχεία επικοινωνίας και τα ενδιαφερόμενα μέρη τα οποία πρέπει να ενημερωθούν στην περίπτωση συμβάντων ή περιστατικών ασφάλειας.
2	2	Στην λίστα έχει καταγραφεί επίσης, το χρονικό διάστημα στο οποίο πρέπει να γίνει η ενημέρωση, το είδος του περιστατικού που αφορά η ενημέρωση και το υπεύθυνο άτομο από την μεριά του οργανισμού.
3	1	Έχει θεσπιστεί, εφαρμόζεται και διατηρείται διαδικασία για τη διασφάλιση της συμμόρφωσης με ρυθμιστικές και νομοθετικές απαιτήσεις όσον αφορά την κοινοποίηση περιστατικών.
3	2	Διασφαλίζεται ότι υπάρχουν επαρκείς διαδικασίες κοινοποίησης και υποβολής εκθέσεων για συμβάντα και περιστατικά ασφάλειας πληροφοριών σε αρμόδιες ρυθμιστικές αρχές, όπως την ΑΨΑ.
3	3	Στο πλαίσιο των δεδομένων προσωπικού χαρακτήρα,διασφαλίζεται η συμμόρφωση με τις σχετικές νομοθετικές και ρυθμιστικές διατάξεις που αφορούν την προστασία των δεδομένων προσωπικού χαρακτήρα και επικοινωνεί, όπου είναι απαραίτητο, με την αρμόδια αρχή προστασίας δεδομένων.
3	4	Έχουν ορισθεί συγκεκριμένες αρμοδιότητες και υπευθυνότητες σε σχέση με την γνωστοποίηση των περιστατικών στις ρυθμιστικές αρχές και έχουν ανατεθεί εγγράφως στα αντίστοιχα άτομα ή ρόλους. Σε αυτά περιλαμβάνονται και οι αρμοδιότητες του Υπεύθυνου ασφάλειας δικτύων και πληροφοριών όπως αναφέρεται στο [GOV1].
4	1	Έχουν σχεδιασθεί και διενεργούνται σε προκαθορισμένους χρόνους ασκήσεις προσομοίωσης περιστατικών ασφαλείας, με σκοπό την αποτύπωση και τον έλεγχο του χρόνου κοινοποίησης και υποβολής εκθέσεων για συμβάντα και περιστατικά ασφάλειας πληροφοριών σε αρμόδιες ρυθμιστικές αρχές ώστε να υπάρχει συμμόρφωση με τις ρυθμιστικές και νομοθετικές απαιτήσεις όσον αφορά την κοινοποίηση περιστατικών.
4	2	Έχουν δημιουργηθεί σχετικές πρότυπες φόρμες συμπληρώνονται από το αρμόδιο προσωπικό σε περίπτωση περιστατικού ανά είδος και ανά σχετική αρχή.
4	3	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Έχει δημιουργηθεί μια σειρά από αναλυτικές οδηγίες / οδηγούς που περιέχουν τα βήματα που πρέπει να ακολουθηθούν σε διακριτές χρονικές στιγμές από το αρμόδιο προσωπικό για την ορθή, έγκαιρη και αποτελεσματική πληροφόρηση των ανά περίπτωση εμπλεκόμενων αρχών. (Οι οδηγοί περιέχουν χρονικά διαστήματα, ρόλους, πρακτικά, οδηγίες για ψηφιακά πειστήρια, οδηγούς για τον προσδιορισμό ποιοι πρέπει να είναι οι αποδέκτες της ενημέρωσης – π.χ. σε περίπτωση περιστατικού που αφορά δεδομένα προσωπικού χαρακτήρα αν απαιτείται να ενημερωθούν και τα υποκείμενα -, πρότυπα κείμενα ενημέρωσης κ.α.)
5	2	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	3	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
EIM6		Μέτρο: Επικοινωνία με ενδιαφερόμενους φορείς για συμβάντα και περιστατικά.Στόχος Μέτρου: Να εξασφαλίζει ότι ο οργανισμός κοινοποιεί πληροφορίες σχετικά με συμβάντα και περιστατικά ασφάλειας δικτύων και πληροφοριών σε εσωτερικούς και εξωτερικούς ενδιαφερόμενους φορείς.Περιγραφή Μέτρου: Θέσπιση, εφαρμογή και διατήρηση διαδικασιών για τη διασφάλιση σχετικής επικοινωνίας όσον αφορά συμβάντα και περιστατικά ασφάλειας πληροφοριών προς εξωτερικούς και εσωτερικούς αποδέκτες, προκειμένου να εξασφαλίζεται η επίγνωση του συμβάντος ή περιστατικού και να παρέχεται στους εξωτερικούς και εσωτερικούς ενδιαφερόμενους φορείς η δυνατότητα να καθορίζουν κατάλληλα μέτρα αντίδρασης, εάν αυτό είναι απαραίτητο. Ο οργανισμός πρέπει να εξετάζει το ενδεχόμενο συνεργασίας με εξωτερικούς και εσωτερικούς ενδιαφερόμενους φορείς όσον αφορά τον περιορισμό συμβάντων και περιστατικών, προκειμένου να ελαχιστοποιούνται οι σχετικές επιπτώσεις και οι εκ των υστέρων δραστηριότητες προκειμένου να καθορίζονται προληπτικά μέτρα, όπως με την ΑΨΑ και τις υπηρεσίες έκτακτης ανάγκης. Πηγή:
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν πραγματοποιεί επικοινωνία με ενδιαφερόμενους φορείς για συμβάντα και περιστατικά.
1	1	Πραγματοποιείται τουλάχιστον ad-hoc και όχι κατ' ανάγκη συστηματικά, επικοινωνία με ενδιαφερόμενους φορείς για συμβάντα και περιστατικά ασφαλείας.
2	1	Διατηρείται λίστα με ενδιαφερόμενους φορείς με τους οποίους επικοινωνεί συστηματικά προκειμένου να εξασφαλίζεται η επίγνωση του συμβάντος.
3	1	Έχει θεσπιστεί, εφαρμόζεται και διατηρείται διαδικασία για τη διασφάλιση σχετικής επικοινωνίας όσον αφορά συμβάντα και περιστατικά ασφάλειας πληροφοριών προς εξωτερικούς και εσωτερικούς αποδέκτες, προκειμένου να εξασφαλίζεται η επίγνωση του

		συμβάντος ή περιστατικού και να παρέχεται στους εξωτερικούς και εσωτερικούς ενδιαφερόμενους φορείς η δυνατότητα να καθορίζουν κατάλληλα μέτρα αντίδρασης, εάν αυτό είναι απαραίτητο.
3	2	Εξετάζεται το ενδεχόμενο συνεργασίας με εξωτερικούς και εσωτερικούς ενδιαφερόμενους φορείς όσον αφορά τον περιορισμό συμβάντων και περιστατικών, προκειμένου να ελαχιστοποιούνται οι σχετικές επιπτώσεις και οι εκ των υστέρων δραστηριότητες προκειμένου να καθορίζονται προληπτικά μέτρα, όπως με την ΑΨΑ και τις υπηρεσίες έκτακτης ανάγκης.
4	1	Υπάρχει συνεργασία με εξωτερικούς και εσωτερικούς ενδιαφερόμενους φορείς όσον αφορά τον περιορισμό συμβάντων και περιστατικών, προκειμένου να ελαχιστοποιούνται οι σχετικές επιπτώσεις και οι εκ των υστέρων δραστηριότητες προκειμένου να καθορίζονται προληπτικά μέτρα, όπως με την ΑΨΑ και τις υπηρεσίες έκτακτης ανάγκης.
4	2	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Χρησιμοποιούνται αυτοματοποιημένοι μηχανισμοί για να αυξηθεί η διαθεσιμότητα πληροφοριών και υποστήριξης που σχετίζονται με την αντιμετώπιση περιστατικών. (π.χ. Να υπάρχει η δυνατότητα να λαμβάνει ο οργανισμός αυτοματοποιημένες πληροφορίες μέσω μηνυμάτων ή emails ως μέρος της αυξανόμενης κατανόησης των τρεχουσών δυνατοτήτων απόκρισης και υποστήριξης.)
5	2	Λαμβάνονται αλλά και διαμοιράζονται έγκυρες πληροφορίες Cyber threat intelligence μέσω σχετικών επαφών με σχετικούς οργανισμούς (όπως είναι sector specific ISAC's, CSIRTs, coallitions κλπ).
5	3	Υπάρχουν διαδικασίες που αποτυπώνουν τα μέτρα και βήματα που διενεργεί ο οργανισμός σε περίπτωση που ανταλλάσσει σχετικές πληροφορίες ώστε να μπορούν να μεταφερθούν αποτελεσματικά, να μπορούν να αναγνωστούν αποτελεσματικά και να μην εκθέσουν εσωτερικές εμπιστευτικές πληροφορίες του οργανισμού σε άλλα μη εξουσιοδοτημένα μέρη. Στα πλαίσια των διαδικασιών αυτών θα προσδιορίζει και πρωτόκολλα, εργαλεία και δομή της πληροφορίας.
5	4	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	5	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.

Κατηγορία		ΕΠΙΧΕΙΡΗΣΙΑΚΗ ΣΥΝΕΧΕΙΑ ΚΑΙ ΑΝΘΕΚΤΙΚΟΤΗΤΑ
BCR1		Μέτρο: Ανάλυση επιχειρησιακών επιπτώσεων Στόχος Μέτρου: Να εξασφαλιστεί ότι ο οργανισμός έχει αναλύσει και αξιολογήσει τις κρίσιμες επιχειρηματικές διαδικασίες που πρέπει να ληφθεί υπόψη στο σχέδιο επιχειρησιακής συνέχειας, ώστε να μπορέσει ο οργανισμός να αποκαταστήσει τις επιχειρηματικές διαδικασίες σε αποδεκτό επίπεδο, το συντομότερο δυνατόν, σε περίπτωση συμβάντος ή περιστατικού. Περιγραφή Μέτρου: Θέσπιση, εφαρμογή και διατήρηση διαδικασίας ανάλυσης επιχειρησιακών επιπτώσεων προκειμένου να προσδιορίσει όλα τα κρίσιμα περιουσιακά στοιχεία εντός του οργανισμού. Η ανάλυση των επιχειρησιακών επιπτώσεων θα επιτρέψει στον οργανισμό να ιεραρχήσει τις λειτουργίες και τα συστήματα με βάση την αναγκαιότητα παροχής επιχειρησιακών υπηρεσιών. Η ανάλυση των επιχειρησιακών επιπτώσεων διενεργείται βάσει συστήματος ταξινόμησης που λαμβάνει υπόψη καθορισμένα επίπεδα κρισιμότητας και εξετάζει εάν κρίσιμες λειτουργίες ή συστήματα λειτουργούν αυτόνομα ή συνδέονται με άλλη λειτουργία ή σύστημα του οργανισμού. Πηγή: 22313
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν έχει διενεργήσει ανάλυση επιχειρησιακών επιπτώσεων.
1	1	Ο οργανισμός έχει κάνει μια ανάλυση των βασικών υπηρεσιών που παρέχει και έχει αναγνωρίσει κάποιες από τις επιχειρησιακές του δραστηριότητες αλλά δύναται ο τρόπος αναγνώρισης να μην είναι συστηματικός.
2	1	Έχει δημιουργηθεί, έστω μια απλή, διαδικασία για την αναγνώριση των κρίσιμων επιχειρησιακών δραστηριοτήτων.
2	2	Τα αποτελέσματα της διενέργειας της συγκεκριμένης διαδικασίας καταγράφονται στα πλαίσια του κατάλογου στοιχείων ενεργητικού, συστημάτων και διαδικασιών εντός του οργανισμού όπως αναφέρεται στο [RM2].
2	3	Έχουν ανατεθεί ρόλοι και αρμοδιότητες σε σχέση με την συγκεκριμένη διαδικασία σε κατάλληλο προσωπικό.
2	4	Η διαδικασία διενεργείται τουλάχιστον μια φορά το χρόνο.
3	1	Έχει θεσπιστεί, εφαρμόζεται και διατηρείται διαδικασία ανάλυσης επιχειρησιακών επιπτώσεων προκειμένου να προσδιορίσει όλα τα κρίσιμα περιουσιακά στοιχεία εντός του οργανισμού.
3	2	Η ανάλυση των επιχειρησιακών επιπτώσεων επιτρέπει στον οργανισμό να ιεραρχήσει τις λειτουργίες και τα συστήματα με βάση την αναγκαιότητα παροχής επιχειρησιακών υπηρεσιών.
3	3	Η ανάλυση των επιχειρησιακών επιπτώσεων διενεργείται βάσει συστήματος ταξινόμησης που λαμβάνει υπόψη καθορισμένα επίπεδα κρισιμότητας και εξετάζει εάν κρίσιμες λειτουργίες ή συστήματα λειτουργούν αυτόνομα ή συνδέονται με άλλη λειτουργία ή σύστημα του οργανισμού.
3	4	Η διαδικασία περιλαμβάνει: (α) τον καθορισμό κριτηρίων αξιολόγησης σχετικά με το πλαίσιο του οργανισμού, συμπεριλαμβανομένου των τύπων επιπτώσεων και χρονικά πλαίσια, (β) τον εντοπισμό δραστηριοτήτων που υποστηρίζουν την παράδοση των προϊόντων και των υπηρεσιών του οργανισμού, (γ) χρήση των κριτηρίων αξιολόγησης για την αξιολόγηση των αναμενόμενων επιπτώσεων με την πάροδο του χρόνου που προκύπτουν από τη διακοπή αυτών των δραστηριοτήτων, (δ) εκτίμηση του χρόνου εντός του οποίου οι επιπτώσεις από τη μη επανέναρξη των δραστηριοτήτων θα γίνουν μη αποδεκτές, (ε) καθορισμό χρονικών πλαισίων εντός του χρόνου που προσδιορίζεται παραπάνω για την επανέναρξη των δραστηριοτήτων σε καθορισμένες ελάχιστες αποδεκτές λειτουργικότητες, (ζ) τον προσδιορισμό των δραστηριοτήτων με προτεραιότητα, (η) εντοπισμό των εξαρτήσεων των δραστηριοτήτων με προτεραιότητα, συμπεριλαμβανομένων των ανθρώπων, των πληροφοριών και των δεδομένων, των κτιρίων, των χώρων εργασίας και των σχετικών υπηρεσιών κοινής ωφέλειας, του εξοπλισμού και των αναλώσιμων, των συστημάτων ICT, μεταφορές και logistics, χρηματοδότηση και συνεργάτες και εφοδιαστική αλυσίδα.
3	5	Υλοποιείται σχετική διαδικασία και εξάγονται αποτελέσματα σε σχετική αναφορά η οποία παρουσιάζεται στην διοίκηση από την οποία και εγκρίνεται.
3	6	Η αναφορά περιέχει κατ' ελάχιστον τα στοιχεία για τα RTO, MAO/MTPD, RPO και MBCO που έχει αναγνωρίσει ο οργανισμός ανά διεργασία ή/και δραστηριότητα.
4	1	Διενεργούνται workshops και συναντήσεις με αντιπροσωπευτικό μέρος του προσωπικού ανά εμπλεκόμενο τμήμα ή διεργασία για την λήψη των στοιχείων για την ανάλυση επιχειρησιακών επιπτώσεων.

4	2	Στα πλαίσια της ανάλυσης, το προσωπικό αναγνωρίζει, αναλύει και αξιολογεί κινδύνους που μπορεί να οδηγήσουν στην διακύβευσης της δυνατότητας του οργανισμού να συνεχίσει την λειτουργία του συγκεκριμένου τμήματος / διεργασίας / υπηρεσίας.
4	3	Οι κλίμακες που χρησιμοποιούνται για την αξιολόγηση των αναμενόμενων επιπτώσεων αλλά και για την ανάλυση και αξιολόγηση κινδύνων είναι εγκεκριμένα από την διοίκηση και εκφρασμένα με τέτοιο τρόπο ώστε να είναι κατανοητά από το σύνολο του εμπλεκόμενου προσωπικού (ακόμα και από αυτό που δεν έχει κάποια ειδική γνώση σε σχέση με την πληροφορική ή την επιχειρησιακή συνέχεια).
4	4	Τα κριτήρια σε κάθε περίπτωση λαμβάνουν υπόψη και είναι ευθυγραμμισμένα με τις προδιαγραφές της σχετικής εφαρμόσιμης νομοθεσίας.
4	5	Η αξιολόγηση της επίπτωσης γίνεται τουλάχιστον σε επίπεδο: επίπτωσης στην συμμόρφωση του οργανισμού, επίπτωση στην επίτευξη των στόχων του οργανισμού, οικονομική επίπτωση, επίπτωση στην φήμη, επίπτωση στην υγεία, ασφάλεια και ευμάρεια του προσωπικού και επίπτωση στην υγεία, ασφάλεια και ευμάρεια των χρηστών των υπηρεσιών.
4	6	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Χρησιμοποιείται αυτοματοποιημένο εργαλείο για την υποστήριξη της υλοποίησης της διαδικασίας ανάλυσης των επιχειρησιακών επιπτώσεων. Μέσα από το εργαλείο, ο οργανισμός έχει την δυνατότητα να αποτυπώνει τις εξαρτήσεις ανάμεσα στους πόρους (άτομα, εξοπλισμό, IT διεργασίες, αρχεία κ.α.) αλλά και μεταξύ των διαφόρων διεργασιών. Ο οργανισμός διενεργεί επικαιροποίηση των στοιχείων της ανάλυσης επιχειρησιακών επιπτώσεων μια φορά το χρόνο (κατ΄ελάχιστο) και σε περίπτωση σημαντικών αλλαγών.
5	2	Διενεργούνται σχετικές δοκιμές, αναλύσεις και ασκήσεις για έλεγχο της εγκυρότητας των στοιχείων της ανάλυσης επιχειρησιακών επιπτώσεων. Σε περίπτωση αναγνωρισμένης απόκλισης, διενεργεί άμεσα κατάλληλες ενέργειες για την αντιμετώπιση της αιτίας της απόκλισης και την διόρθωση του προβλήματος.
5	3	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	4	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
BCR2		Μέτρο: Σχέδιο επιχειρησιακής συνέχειας Στόχος Μέτρου: Να εξασφαλιστεί ότι ο οργανισμός διαθέτει σχέδιο για τη διατήρηση της συνέχειας των κρίσιμων επιχειρηματικών διαδικασιών και την αποκατάσταση κατά τη διάρκεια συμβάντος ή περιστατικού και μετά από αυτό. Περιγραφή Μέτρου: Θέσπιση, εφαρμογή και διατήρηση σχεδίου επιχειρησιακής συνέχειας προκειμένου να διασφαλιστεί ότι ο οργανισμός μπορεί να ανταποκρίνεται σε καταστάσεις έκτακτης ανάγκης με άμεσο και κατάλληλο τρόπο, και είναι σε θέση να διατηρεί επιχειρηματικές λειτουργίες ελαχιστοποιώντας τις συνέπειες και τις ζημίες που προκύπτουν από ένα περιστατικό. Το σχέδιο επιχειρησιακής συνέχειας περιλαμβάνει το σχέδιο αποκατάστασης από καταστροφή, όπως περιγράφεται στο μέτρο [BCR4] και λαμβάνει υπόψη την ανάλυση των επιχειρησιακών επιπτώσεων. Πηγή:
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν έχει καταρτίσει σχέδιο επιχειρησιακής συνέχειας.
1	1	Έχουν προσδιορισθεί κάποιες εναλλακτικές λύσεις σε περίπτωση περιστατικού διαταραχής (disruptive) οι οποίες μπορεί όμως να είναι περιστασιακές και μπορεί να μην στηρίζονται στην ανάλυση επιχειρησιακών επιπτώσεων, χωρίς κατ'ανάγκη να είναι και πλήρως κατεγραμμένες.
2	1	Έχουν δομηθεί σχέδια επιχειρησιακής συνέχειας για τις κρίσιμες δραστηριότητες.
2	2	Τα συγκεκριμένα σχέδια είναι καταγεγραμμένα αλλά μπορεί και να μην στηρίζονται σε δομημένα στοιχεία Business Impact Analysis.
2	3	Στα σχέδια περιέχονται στοιχεία σε σχέση με τον επιθυμητό χρόνο ανάκαμψης ανά δραστηριότητα καθώς και ενέργειες που πρέπει να υλοποιηθούν σε περίπτωση διαταραχής.
3	1	Έχει θεσπιστεί, εφαρμόζεται και διατηρείται σχέδιο επιχειρησιακής συνέχειας προκειμένου να διασφαλιστεί ότι ο οργανισμός μπορεί να ανταποκρίνεται σε καταστάσεις έκτακτης ανάγκης με άμεσο και κατάλληλο τρόπο, και είναι σε θέση να διατηρεί επιχειρηματικές λειτουργίες ελαχιστοποιώντας τις συνέπειες και τις ζημίες που προκύπτουν από ένα περιστατικό.
3	2	Το σχέδιο επιχειρησιακής συνέχειας περιλαμβάνει το σχέδιο αποκατάστασης από καταστροφή, όπως περιγράφεται στο μέτρο [BCR4] και λαμβάνει υπόψη την ανάλυση των επιχειρησιακών επιπτώσεων [BCR1].

3	3	Έχει δημιουργηθεί ένα (ή πολλαπλά) σχέδια επιχειρησιακής συνέχειας με έμφαση στις επιπτώσεις που μπορεί να αντιμετωπίσει ένας οργανισμός ως αποτέλεσμα μιας διαταραχής και όχι τον/ τους λόγο/λόγους που μπορεί να οδηγήσουν στις επιπτώσεις αυτές.
3	4	Το/ τα σχέδιο/α περιλαμβάνουν:(α) το σκοπό, το πεδίο εφαρμογής και τους στόχους του κάθε σχεδίου,(β) τις παραδοχές και τις εξαιρέσεις του σχεδίου,(γ) τους ρόλους και τις ευθύνες της ομάδας που θα εφαρμόσει το σχέδιο,(δ) τα βήματα και τις λεπτομέρειες τους που θα κάνουν οι ομάδες προκειμένου να συνεχίζουν ή ανακτήσουν τις επιχειρησιακές δραστηριότητες σε προκαθορισμένο επίπεδο και εντός προσυμφωνημένου και αποδεκτού χρονικού διαστήματος,(ε) παρακολουθήσουν τις επιπτώσεις του περιστατικού και ανταποκριθούν σε αυτές ώστε να μειώσουν την έκτασή του στους ανθρώπους και στον οργανισμό όσο γίνεται περισσότερο.λαμβάνοντας υπόψη την υγεία και ασφάλεια των ατόμων, τον περιορισμό της επέκτασης της επίπτωσης της διαταραχής και την μείωση των σχετικών επιπτώσεων, την επίπτωση στο περιβάλλον και στην κοινωνία,(ε) τα RTO/ RPO / MAO-MTPD ανά διεργασία / υπηρεσία και αν είναι εφικτό δραστηριότητα,(ζ) την διαδικασία και τις αρμοδιότητες σε σχέση με την ενημέρωση, διάγνωση, απόφαση για ενεργοποίηση και υλοποίηση του σχεδίου, (η) τις εσωτερικές και εξωτερικές αλληλεξαρτήσεις και τις προβλέψεις που έχουν γίνει για την συνέχειά τους,(θ) τις απαιτήσεις πόρων,(ι) τους τρόπους και τα στοιχεία επικοινωνίας μεταξύ των ενδιαφερόμενων μερών,(κ) την ανάλυση των απαιτούμενων ανθρώπινων πόρων συναρτήσει του χρόνου, (λ) την σχετική τεκμηρίωση που θα τηρείται σε περίπτωση ενεργοποίησης και (μ) την διαδικασία υπαναχώρησης (standing down)
3	5	Κάθε σχέδιο επιχειρησιακής συνέχειας είναι γνωστό στο εμπλεκόμενο προσωπικό και είναι διαθέσιμο όταν το χρειάζονται.
4	1	Αναλύονται οι δυνατές στρατηγικές επιχειρησιακής συνέχειας και ανάκαμψης από καταστροφή και ξεχωρίζουν και καταγράφονται εκείνες που ανά διεργασία / ανά είδος επίπτωσης / ανά RTO /MAO έχουν την δυνατότητα να επιτρέψουν στον οργανισμό να ανακάμψει τις επιχειρησιακές του δραστηριότητες σε προδιαγεγραμμένο αποδεκτό χρόνο και σε προκαθορισμένο επίπεδο.
4	2	Οι επιλογές των στρατηγικών καταγράφονται και παρουσιάζονται στην διοίκηση του οργανισμού, συνοδευόμενες και από στοιχεία κόστους οφέλους (Cost Benefit analysis).
4	3	Ο διοίκηση του οργανισμού εγκρίνει τις αποδεκτές στρατηγικές.
4	4	Καταρτίζονται σχέδια επιχειρησιακής συνέχειας και ανάκαμψης από καταστροφή σύμφωνα με τις αποδεκτές και εγκεκριμένες από τη διοίκηση στρατηγικές.
4	5	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Κάθε σχέδιο επιχειρησιακής συνέχειας έχει έναν ιδιοκτήτη, ο οποίος είναι υπεύθυνος για την παρακολούθησή του καθ' όλο τον κύκλο ζωής του.
5	2	Ο Υπεύθυνος δημιουργεί πλάνο ενεργειών για την υλοποίηση των προβλέψεων του κάθε σχεδίου επιχειρησιακής συνέχειας.
5	3	Το πλάνο ενεργειών περιλαμβάνει ενέργειες όπως: συντονισμός και διαθεσιμότητα των σχετικών πόρων, εκπαίδευση προσωπικού, δημιουργία σχετικών οδηγιών, δημιουργία πλάνου δοκιμών για τον έλεγχο της αποτελεσματικότητας του σχεδίου, ενέργειες για την ασφαλή αποθήκευση του σχεδίου όπου χρειάζεται και την κατάλληλη διαθεσιμότητά του όταν χρειαστεί, τον συντονισμό για την καταγραφή και την επικαιροποίηση των call trees όπου απαιτείται, αναγνώριση ρόλων για την ανταπόκριση, την λειτουργία, την ενεργοποίηση και τον έλεγχο του σχεδίου κ.α.
5	4	Ο υπεύθυνος παρακολουθεί τις ενέργειες για την ετοιμότητα του οργανισμού ανά πλάνο επιχειρησιακής συνέχειας και αναφέρει στην διοίκηση το βαθμό ετοιμότητας και την επίδοσή του.
5	5	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	6	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.

BCR3		Μέτρο: Ασκήσεις και προσομοιώσεις επιχειρησιακής συνέχειαςΣτόχος Μέτρου: Να διασφαλιστεί ότι ο οργανισμός και τα στελέχη του γνωρίζουν τις ευθύνες τους κατά τη διάρκεια ενός συμβάντος ή περιστατικού που ενεργοποιεί το σχέδιο επιχειρησιακής συνέχειας.Περιγραφή Μέτρου: Θέσπιση, εφαρμογή και διατήρηση μέτρων για τον έλεγχο, την αναθεώρηση και τη βελτίωση του σχεδίου επιχειρησιακής συνέχειας μέσω ασκήσεων όπου προσομοιώνονται συμβάντα και περιστατικά στον οργανισμό, με σκοπό τον έλεγχο της ανταπόκρισης του οργανισμού σε παρόμοια συμβάντα και περιστατικά, και τη βελτίωση των διαδικασιών επιχειρησιακής συνέχειας. Οι ασκήσεις και οι προσομοιώσεις επιχειρησιακής συνέχειας θα πρέπει να παρέχουν στον οργανισμό τη δυνατότητα να εντοπίζει ευκαιρίες βελτίωσης και να επιτυγχάνει καλύτερα αποτελέσματα με την πάροδο του χρόνου. Ο οργανισμός θα πρέπει να εξετάσει το ενδεχόμενο να συνδέσει το σχέδιο επιχειρησιακής συνέχειας με τις διαδικασίες διαχείρισης αλλαγών, όπως περιγράφονται στο [CM1], προκειμένου να λαμβάνονται υπόψη στο σχέδιο επιχειρησιακής συνέχειας οι συνέπειες από όποιες αλλαγές εντός του οργανισμού. Ο οργανισμός θα πρέπει να διενεργεί ασκήσεις και προσομοιώσεις επιχειρησιακής συνέχειας σε τακτά χρονικά διαστήματα, προκειμένου οι εργαζόμενοι να είσαι σε επαγρύπνηση για συμβάντα και περιστατικά που θα μπορούσαν να βλάψουν τον οργανισμό. Κατά την κατάρτιση του σχεδίου επιχειρησιακής συνέχειας, ο οργανισμός εξετάζει και την αποκατάσταση από καταστροφή, όπως ορίζεται στο μέτρο [BCR4]. Πηγή:
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν έχει καταρτίσει σχέδιο επιχειρησιακής συνέχειας.
1	1	Έχουν προσδιορισθεί κάποιες εναλλακτικές λύσεις σε περίπτωση περιστατικού διαταραχής (disruptive) οι οποίες μπορεί όμως να είναι περιστασιακές και μπορεί να μην στηρίζονται στην ανάλυση επιχειρησιακών επιπτώσεων, χωρίς κατ'ανάγκη να είναι πλήρως κατεγραμμένες και να εξασκούνται με συστηματικό τρόπο.
2	1	Έχουν δομηθεί σχέδια επιχειρησιακής συνέχειας για τις κρίσιμες δραστηριότητες.
2	2	Τα συγκεκριμένα σχέδια είναι καταγεγραμμένα αλλά μπορεί και να μην στηρίζονται σε δομημένα στοιχεία Business Impact Analysis.
2	3	Στα σχέδια περιέχονται στοιχεία σε σχέση με τον επιθυμητό χρόνο ανάκαμψης ανά δραστηριότητα καθώς και ενέργειες που πρέπει να υλοποιηθούν για την επίτευξή τους σε περίπτωση διαταραχής.
2	4	Έχει γίνει τουλάχιστον μια δοκιμή των σχεδίων επιχειρησιακής συνέχειας κατά τη διάρκεια των δυο τελευταίων ετών.
3	1	Έχουν θεσπιστεί, εφαρμόζονται και διατηρούνται μέτρα για τον έλεγχο, την αναθεώρηση και τη βελτίωση του σχεδίου επιχειρησιακής συνέχειας μέσω ασκήσεων όπου προσομοιώνονται συμβάντα και περιστατικά στον οργανισμό, με σκοπό τον έλεγχο της ανταπόκρισης του οργανισμού σε παρόμοια συμβάντα και περιστατικά, και τη βελτίωση των διαδικασιών επιχειρησιακής συνέχειας.
3	2	Οι ασκήσεις και οι προσομοιώσεις επιχειρησιακής συνέχειας παρέχουν στον οργανισμό τη δυνατότητα να εντοπίζει ευκαιρίες βελτίωσης και να επιτυγχάνει καλύτερα αποτελέσματα με την πάροδο του χρόνου.
3	3	Διενεργούνται ασκήσεις και προσομοιώσεις επιχειρησιακής συνέχειας σε τακτά χρονικά διαστήματα, προκειμένου οι εργαζόμενοι να είσαι σε επαγρύπνηση για συμβάντα και περιστατικά που θα μπορούσαν να βλάψουν τον οργανισμό. Κατά την κατάρτιση του σχεδίου επιχειρησιακής συνέχειας, ο οργανισμός εξετάζει και την αποκατάσταση από καταστροφή, όπως ορίζεται στο μέτρο [BCR4].
3	4	Οι δοκιμές και οι ασκήσεις γίνονται τουλάχιστον μια φορά το χρόνο και καλύπτουν το σύνολο των προβλέψεων επιχειρησιακής συνέχειας τουλάχιστον μια φορά και με έναν τουλάχιστον τρόπο (ακόμα και αν είναι table top).
4	1	Έχει δημιουργηθεί σχέδιο / πρόγραμμα ασκήσεων και δοκιμών.
4	2	Το πρόγραμμα εξασφαλίζει ότι διενεργούνται ασκήσεις και δοκιμές που είναι συμβατές με τους στόχους του οργανισμού για επιχειρησιακή συνέχεια, στηρίζονται σε κατάλληλα σενάρια (τα οποία είναι ξεκάθαρα και καταγεγραμμένα, κάθε ένα εκ των οποίων χει συγκεκριμένο στόχο), στοχεύουν σε συγκεκριμένες πτυχές των σχεδίων (π.χ. επικοινωνία, τεχνολογική ετοιμότητα, συνεργατικότητα, αποτελεσματικότητα κ.α.) και ότι όταν συνδυάζονται όλες οι ασκήσεις και δοκιμές στο διάστημα ενός ολόκληρου έτους, καταφέρουν να δοκιμάσουν το σύνολο των προβλέψεων επιχειρησιακής συνέχειας του οργανισμού με μια ποικιλία μεθόδων.
4	3	Για τις ασκήσεις και τις δοκιμές τηρούνται καταγεγραμμένα πρακτικά τα οποία αναφέρουν το ιστορικό της δοκιμής, τους χρόνους ανά βήμα σύμφωνα με το εφαρμόσιμο σχέδιο ή μέρος του σχεδίου, και πιθανές παρατηρήσεις.

4	4	Έχει συνδεθεί το σχέδιο επιχειρησιακής συνέχειας με τις διαδικασίες διαχείρισης αλλαγών, όπως περιγράφονται στο [CM1], προκειμένου να λαμβάνονται υπόψη στο σχέδιο επιχειρησιακής συνέχειας οι συνέπειες από όποιες αλλαγές εντός του οργανισμού.
4	5	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Έχει δημιουργηθεί σχέδιο / πρόγραμμα ασκήσεων και δοκιμών.
5	2	Το πρόγραμμα εξασφαλίζει ότι διενεργούνται ασκήσεις και δοκιμές που είναι συμβατές με τους στόχους του οργανισμού για επιχειρησιακή συνέχεια και στο σύνολό τους στο διάστημα ενός ολόκληρου έτους, καταφέρουν να δοκιμάσουν το σύνολο των προβλέψεων επιχειρησιακής συνέχειας του οργανισμού με μια ποικιλία μεθόδων.
5	3	Στα πλαίσια του πλάνου προβλέπεται και υλοποιείται τουλάχιστον σε ετήσια βάση μια πλήρης δοκιμή του/των σχεδίων επιχειρησιακής συνέχειας και του σχεδίου αποκατάστασης από καταστροφή. Σε περίπτωση λόγω της ιδιομορφίας του περιβάλλοντος του οργανισμού δεν είναι δυνατή η πλήρης δοκιμή, γίνεται καταγραφή της σχετικής αιτιολόγησης και δημιουργούνται τόσες ασκήσεις προσομοίωσης ή μικρότερες δοκιμές ώστε να είναι δυνατός ο έλεγχος του συνόλου τον προβλέψεων.
5	4	Στο βαθμό που είναι δυνατό, ζητείται η συμμετοχή σχετικών αρχών στην υλοποίηση των σχετικών δοκιμών. Σε περίπτωση που αυτό είναι εφικτό, ο οργανισμός διενεργεί προσομοιώσεις περιστατικών σε περιβάλλοντα digital tweens.
5	5	Διενεργείται σχετική ανάλυση και αξιολόγηση κινδύνου για τον προσδιορισμό του βαθμού ενημέρωσης που θα έχει το προσωπικό σχετικά με την υλοποίηση των δοκιμών, λαμβάνοντας και ως γνώμονα την υγεία και ασφάλεια του προσωπικού.
5	6	Διενεργούνται συζητήσεις και συναντήσεις μετά τις δοκιμές για την αξιολόγηση της επίδοσης των επιμέρους μερών των σχεδίων, την ανάδειξη προβλημάτων και την αναγνώριση σημείων βελτίωσης.
5	7	Οι δοκιμές και οι συζητήσεις συντονίζονται και παρακολουθούνται από ανεξάρτητο παρατηρητή (μπορεί να είναι εσωτερικό άτομο του οργανισμού αλλά πρέπει να μην συμμετέχει στην διαδικασία της ανάκαμψης, αντιμετώπισης και λειτουργίας).
5	8	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	9	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.
BCR4		Μέτρο: Σχέδιο αποκατάστασης από καταστροφή Στόχος Μέτρου: Να εξασφαλιστεί ότι ο οργανισμός διαθέτει σχέδιο για την αποκατάσταση των συστημάτων κρίσιμων πληροφοριών σε αποδεκτό επίπεδο κατά τη διάρκεια ή μετά από περιστατικό. Περιγραφή Μέτρου: Θέσπιση, εφαρμογή και διατήρηση σχεδίου αποκατάστασης από καταστροφή, προκειμένου να διασφαλίζεται η αποκατάσταση και η ανάκτηση όλων των κρίσιμων διαδικασιών των συστημάτων πληροφορικής και των υποστηρικτικών στοιχείων ενεργητικού, όπως η παροχή ηλεκτρικής ενέργειας, μετά την ύπαρξη ενός περιστατικού. Το σχέδιο αποκατάστασης από καταστροφή θα πρέπει να περιλαμβάνει σαφείς οδηγίες για το προσωπικό πληροφορικής, ώστε να εξασφαλίζεται έγκαιρη και αποτελεσματική αντίδραση σε όλα τα περιστατικά που επηρεάζουν το περιβάλλον πληροφορικής του οργανισμού. Στο σχέδιο αποκατάστασης από καταστροφή θα πρέπει να καθορίζεται ο στόχος του σημείου ανάκτησης (RPO) και ο στόχος για τον χρόνο αποκατάστασης (RTO), ώστε να αποφεύγονται μη αποδεκτές συνέπειες για τον οργανισμό. Πηγή:
Επίπεδο Ωριμότητας	Επιμέρους	Περιγραφή Ελέγχου
0	1	Ο οργανισμός δεν έχει καταρτίσει σχέδιο αποκατάστασης από καταστροφή
1	1	Έχουν προσδιορισθεί κάποια βήματα για να εκτελούνται σε περίπτωση καταστροφής, τα οποία μπορεί όμως να είναι περιστασιακά, μπορεί να μην στηρίζονται στην ανάλυση επιχειρησιακών επιπτώσεων και μπορεί να μην είναι πλήρως κατεγραμμένα.
2	1	Έχει δομηθεί σχέδιο αποκατάστασης από καταστροφή για τις κρίσιμες δραστηριότητες.
2	2	Το συγκεκριμένο σχέδιο είναι καταγεγραμμένο αλλά μπορεί και να μην στηρίζεται σε δομημένα στοιχεία Business Impact Analysis.
2	3	Το σχέδιο στηρίζεται στην ύπαρξη εφεδρικών αντιγράφων ασφαλείας και στην χρήση τους για την ανάκαμψη στον ίδιο ή σε διαφορετικό χώρο σε περίπτωση καταστροφής.
3	1	Έχει θεσπιστεί, εφαρμόζεται και διατηρείται σχέδιο αποκατάστασης από καταστροφή, προκειμένου να διασφαλίζεται η αποκατάσταση και η ανάκτηση όλων των κρίσιμων διαδικασιών των συστημάτων πληροφορικής και των υποστηρικτικών στοιχείων ενεργητικού, όπως η παροχή ηλεκτρικής ενέργειας, μετά την ύπαρξη ενός περιστατικού.

3	2	Το σχέδιο αποκατάστασης από καταστροφή περιλαμβάνει σαφείς οδηγίες για το προσωπικό πληροφορικής, ώστε να εξασφαλίζεται έγκαιρη και αποτελεσματική αντίδραση σε όλα τα περιστατικά που επηρεάζουν το περιβάλλον πληροφορικής του οργανισμού.
3	3	Στο σχέδιο αποκατάστασης από καταστροφή καθορίζεται ο στόχος του σημείου ανάκτησης (RPO) και ο στόχος για τον χρόνο αποκατάστασης (RTO), ώστε να αποφεύγονται μη αποδεκτές συνέπειες για τον οργανισμό.
3	4	Το σχέδιο αποκατάστασης από καταστροφή περιλαμβάνει όλους τους πόρους που χρειάζονται και έχουν αναγνωριστεί κατά την ανάλυση επιχειρησιακών επιπτώσεων ότι απαιτούνται για την ορθή λειτουργία των κρίσιμων διεργασιών εντός προκαθορισμένου χρονικού διαστήματος.
3	5	Το προσωπικό που εμπλέκεται στην λειτουργία του σχεδίου αποκατάστασης από καταστροφή είναι πλήρως ενημερωμένο σχετικά με τις αρμοδιότητες και τις υπευθυνότητές του.
3	6	Γίνεται δοκιμή του σχεδίου σύμφωνα με το [BCR3].
3	7	Διενεργούνται ενημερώσεις και αλλαγές σύμφωνα με την διαδικασία διαχείρισης αλλαγών [CM1].
4	1	Το σχέδιο αποκατάστασης από καταστροφή προβλέπει την ύπαρξη κατάλληλου αδειοδοτημένου λογισμικού για την ανάκτηση των στοιχείων από τα σχετικά αντίγραφα ασφαλείας.
4	2	Τα αρχεία εφεδρικών αντιγράφων κρυπτογραφούνται με την χρήση αλγορίθμων όπως προβλέπεται από το [AM1].
4	3	Έχει γίνει πρόβλεψη ώστε να υπάρχει δυνατότητα πρόσβασης και ανάκτησης των δεδομένων όπως απαιτείται από τα εφεδρικά αντίγραφα (π.χ. υπάρχει δυνατότητα λήψης, εγκατάστασης ή χρήσης του λογισμικού αντιγράφων ασφαλείας και υπάρχει διαθεσιμότητα των σχετικών κλειδιών).
4	4	Τα σχέδια αποκατάστασης από καταστροφή αποθηκεύονται σε ασφαλή τοποθεσία, προστατεύονται με τα κατάλληλα μέτρα ώς πληροφορία του υψηλότερου επιπέδου διαβάθμισης και εξασφαλίζεται ότι είναι διαθέσιμα σε περίπτωση καταστροφής της κύριας εγκατάστασης.
4	5	Τα σχετικά έγγραφα ανασκοπούνται για την καταλληλότητα τους τουλάχιστον μια φορά το χρόνο. Σε περίπτωση αλλαγών η διαδικασία που ακολουθείται είναι αυτή της διαχείρισης αλλαγών.
5	1	Έχουν εφαρμοσθεί λύσεις συγχρονισμού (replication) σε εναλλακτικό χώρο για τα κρίσιμα συστήματα όπως αυτά έχουν αναγνωριστεί σύμφωνα με την ανάλυση επιχειρησιακών επιπτώσεων και τις σχετικές στρατηγικές.
5	2	Τα σχέδια εξασκούνται τουλάχιστον ετησίως και αξιολογείται η δυνατότητα ορθής και αποτελεσματικής εφαρμογής τους.
5	3	Διενεργούνται συζητήσεις και συναντήσεις μετά τις δοκιμές για την αξιολόγηση της επίδοσης των επιμέρους μερών των σχεδίων, την ανάδειξη προβλημάτων και την αναγνώριση σημείων βελτίωσης.
5	4	Οι δοκιμές και οι συζητήσεις συντονίζονται και παρακολουθούνται από ανεξάρτητο παρατηρητή (μπορεί να είναι εσωτερικό άτομο του οργανισμού αλλά πρέπει να μην συμμετέχει στην διαδικασία της ανάκαμψης, αντιμετώπισης και λειτουργίας).
5	5	Έχουν αναγνωριστεί οι δεξιότητες / ικανότητες και γνώσεις που απαιτούνται για την λειτουργία της συγκεκριμένης διαδικασίας από τους προς τούτο εξουσιοδοτημένους ρόλους.
5	6	Ο οργανισμός εξασφαλίζει ότι οι συγκεκριμένες γνώσεις υπάρχουν ήδη από το αρμόδιο προσωπικό διαφορετικά μεριμνά ώστε να δίνονται.

ΠΑΡΑΡΤΗΜΑ ΣΤ: ΠΛΑΙΣΙΟ ΕΓΓΡΑΦΗΣ ΕΛΕΓΚΤΩΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

ΠΕΡΙΕΧΟΜΕΝΑ

➔ Ορισμοί και όροι που χρησιμοποιούνται στο παρόν Παράρτημα και στα Προσαρτήματα αυτού, έχουν την έννοια που αποδίδει σε αυτούς ο Νόμος και η παρούσα Απόφαση.

1. Εισαγωγή

Η επιτακτική ανάγκη της αγοράς για εξειδίκευση σε ορισμένους επαγγελματικούς κλάδους, σε συνδυασμό με την τάση για διασφάλιση ενός ελάχιστου επιπέδου ποιότητας των παρεχόμενων υπηρεσιών από τους επαγγελματίες, είναι οι αιτίες που οδηγούν στη δημιουργία προτύπων, προδιαγραφών και κατ' επέκταση Πλαισίων Πιστοποίησης που θα διασφαλίζουν την παροχή αυτών των υπηρεσιών.

Η έγκριση προσώπων παρέχει εν γένει τα εχέγγυα ότι ο εγκεκριμένος πληροί τις απαιτήσεις του παρόντος Πλαισίου, βάσει του οποίου εγκρίθηκε.

Στο πλαίσιο αυτό η Αρχή ανέπτυξε το παρόν Πλαίσιο.

2. Πεδίο Εφαρμογής- Σκοπός

Το πεδίο εφαρμογής του Πλαισίου αφορά στην αξιολόγηση και πιστοποίηση Γνώσεων, Δεξιοτήτων και Ικανοτήτων στον κλάδο των ελεγκτών.

Η συνολική διαχείριση του Πλαισίου και η έγκριση των ελεγκτών, ικανοποιεί τις απαιτήσεις:

- των προνοιών του Νόμου 89(Ι)/2020 και της δευτερογενούς νομοθεσίας που εκδίδεται δυνάμει αυτού, ως εκάστοτε τροποποιούνται·
- του προτύπου ISO/IEC 17024, κατά την ημερομηνία συγγραφής του Πλαισίου·
- του μοντέλου ωριμότητας κυβερνοασφάλειας (cybersecurity maturity model)· και
- άλλα έγγραφα και έντυπα που αφορούν το παρόν Πλαίσιο.

Σκοπός του Πλαισίου είναι να παρέχει πληροφόρηση προς τον κάθε ενδιαφερόμενο σχετικά με:

- τις προϋποθέσεις που πρέπει να πληρούνται ώστε να συμμετάσχει στις εξετάσεις,
- την παρουσίαση της διαδικασίας που ακολουθείται για την πραγματοποίηση και αξιολόγησή της εξέτασης,
- τις συνθήκες χορήγησης και διατήρησης της έγκρισης, και
- τα δικαιώματα και τις υποχρεώσεις των εγκεκριμένων ελεγκτών.

Σύμφωνα με το παρόν Πλαίσιο, ο ελεγκτής διενεργεί ανεξάρτητους ελέγχους βάσει των απαιτήσεων του ΠΑΡΑΡΤΗΜΑΤΟΣ ΙΙΙ: ΠΛΑΙΣΙΟ ΜΕΤΡΩΝ ΑΣΦΑΛΕΙΑΣ της Απόφασης Κ.Δ.Π 389/2020 και βάσει του μοντέλου ωριμότητας κυβερνοασφάλειας (cybersecurity maturity model), όπως αυτός έχει καθοριστεί από την Αρχή.

3. Ανάπτυξη του Πλαισίου

3.1 Κυβερνοασφάλεια και Οδηγία (ΕΕ) 2016/1148 (Οδηγία NIS)

Τα συστήματα και οι υπηρεσίες δικτύων και πληροφοριών διαδραματίζουν ζωτικό ρόλο στην κοινωνία. Η αξιοπιστία και η ασφάλειά τους είναι ουσιώδους σημασίας για τις οικονομικές και κοινωνικές δραστηριότητες και ιδίως για τη λειτουργία της εσωτερικής αγοράς[2].

Το μέγεθος, η συχνότητα και ο αντίκτυπος των συμβάντων ασφάλειας αυξάνονται και συνιστούν μείζονα απειλή για τη λειτουργία των συστημάτων δικτύου και πληροφοριών. Τα συστήματα αυτά μπορούν επίσης να αποτελέσουν στόχο σκόπιμων επιζήμιων ενεργειών που έχουν σκοπό να προκαλέσουν βλάβες στα συστήματα ή να διακόψουν τη λειτουργία τους. Τέτοια συμβάντα μπορούν να παρεμποδίσουν την άσκηση οικονομικών δραστηριοτήτων, να προκαλέσουν σημαντικές οικονομικές ζημιές, να υπονομεύσουν την εμπιστοσύνη των χρηστών και να προκαλέσουν σημαντική ζημιά στην οικονομία της χώρας ή και της Ευρωπαϊκής Ένωσης (ανάλογα με το περιστατικό, την έκταση και τη διασυνοριακή επίδραση).

Τα συστήματα δικτύου και πληροφοριών, και κυρίως το διαδίκτυο, διαδραματίζουν ένα ουσιώδη ρόλο στη διευκόλυνση της (εντός της χώρας και της διασυνοριακής) κυκλοφορίας αγαθών, υπηρεσιών και προσώπων. Λόγω του εκτεταμένου τους χαρακτήρα, ενδεχόμενη σημαντική διατάραξη των συστημάτων αυτών, εσκεμμένη ή μη, και ανεξαρτήτως του τόπου όπου εκδηλώνεται, μπορεί να επηρεάσει ατομικά κράτη μέλη και την Ένωση στο σύνολό της. Επομένως, η ασφάλεια των συστημάτων δικτύου και πληροφοριών είναι ουσιώδης για την ομαλή λειτουργία της εσωτερικής αγοράς. Στον κόσμο της συνεχούς αναπτυσσόμενης ψηφιακής τεχνολογίας, η κυβερνοασφάλεια αναδεικνύεται ως κομβικός τομέας στην προστασία της πληροφορίας και των ψηφιακών υποδομών. Κεντρικός στόχος της είναι η διασφάλιση της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητας των δεδομένων και των συστημάτων. Η κυβερνοασφάλεια καλύπτει ένα ευρύ φάσμα θεμάτων, από την πρόληψη εισβολών και επιθέσεων στα δίκτυα, μέχρι τη διαχείριση των κυβερνο-απειλών και την ανάκτηση από περιστατικά παραβίασης της ασφάλειας.

[2] Οδηγία (ΕΕ) 2016/1148 (Οδηγία NIS): https://eur-lex.europa.eu/legalcontent/EL/TXT/HTML/?uri=CELEX:32016L1148

Η Οδηγία (ΕΕ) 2016/1148 (Οδηγία NIS) ανέδειξε τη σημαντικότητα ύπαρξης από όλα τα κράτη μέλη ενός ελάχιστου επιπέδου ικανοτήτων και μια στρατηγική που θα εξασφαλίζει υψηλό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών στην επικράτειά τους. Επιπλέον, αποσκοπούσε στην ανάπτυξη ικανοτήτων κυβερνοασφάλειας σε ολόκληρη την Ένωση, στον μετριασμό των απειλών για τα συστήματα δικτύου και πληροφοριών που χρησιμοποιούνται για την παροχή βασικών υπηρεσιών σε σημαντικούς τομείς και στη διασφάλιση της συνέχειας των υπηρεσιών αυτών κατά την αντιμετώπιση περιστατικών, ώστε να συμβάλει στην ασφάλεια και την αποτελεσματική λειτουργία της οικονομίας και της κοινωνίας της Ένωσης. Μετά την έναρξη ισχύος της Οδηγίας NIS, έχει σημειωθεί σημαντική πρόοδος στην αύξηση του επιπέδου κυβερνοανθεκτικότητας της Ένωσης και διασφαλίστηκε η ολοκλήρωση των εθνικών πλαισίων για την ασφάλεια των συστημάτων δικτύου και πληροφοριών, με τη θέσπιση εθνικών στρατηγικών για την ασφάλεια των συστημάτων δικτύου και πληροφοριών, τη θέσπιση εθνικών ικανοτήτων και με την εφαρμογή ρυθμιστικών μέτρων τα οποία καλύπτουν βασικές υποδομές και οντότητες που προσδιορίζονται από κάθε κράτος μέλος. Περαιτέρω, συνέβαλε στη συνεργασία σε επίπεδο Ένωσης μέσω της σύστασης της ομάδας συνεργασίας και του δικτύου εθνικών ομάδων αντιμετώπισης περιστατικών ασφάλειας υπολογιστικών συστημάτων και προσδιόρισε ότι τα κράτη μέλη εξασφαλίζουν ότι οι φορείς εκμετάλλευσης βασικών υπηρεσιών λαμβάνουν κατάλληλα και αναλογικά τεχνικά και οργανωτικά μέτρα για τη διαχείριση των κινδύνων, όσον αφορά την ασφάλεια των συστημάτων δικτύου και πληροφοριών που χρησιμοποιούν στις δραστηριότητές τους. Λαμβάνοντας υπόψη τις πλέον πρόσφατες τεχνικές δυνατότητες, τα μέτρα αυτά διασφαλίζουν επίπεδο ασφάλειας των συστημάτων δικτύου και πληροφοριών ανάλογο προς τον εκάστοτε κίνδυνο.

Ως εκ των ανωτέρω, η Αρχή εξέδωσε την Απόφαση Κ.Δ.Π. 389/2020 με την οποία καθορίζονται ελάχιστες απαιτήσεις και υποχρεώσεις σχετικά με την ασφάλεια δικτύων και συστημάτων πληροφοριών, τις οποίες πρέπει να τηρούν οι Φορείς στην Κυπριακή Δημοκρατία. Σκοπός των ρυθμιστικών υποχρεώσεων που επιβάλλονται στους Φορείς από την Απόφαση Κ.Δ.Π. 389/2020, είναι η ενίσχυση της ασφάλειας και της ανθεκτικότητας των υποδομών και των υπηρεσιών τους, η αντιμετώπιση περιστατικών παραβίασης ασφάλειας και η διασφάλιση της επιχειρησιακής συνέχειας των δικτύων, των συστημάτων πληροφοριών και των υπηρεσιών τους σε περίπτωση καταστρεπτικής βλάβης ή σε περίπτωση ανωτέρας βίας.

3.2 Έλεγχος και εποπτεία

Σύμφωνα με το άρθρο 16 της Απόφασης Κ.Δ.Π. 389/2020 που προνοεί:

16.(1) Με την επιφύλαξη των γενικών εξουσιών και καθηκόντων ελέγχου/έρευνας που έχει σύμφωνα με την ισχύουσα νομοθεσία και ιδιαίτερα τα άρθρα 17(ιζ)(ιη)(ιθ) και 20(1)(α) του Νόμου και τις δυνάμει του Νόμου εκδοθείσες Αποφάσεις, η Αρχή δύναται κατά την κρίση της να ελέγχει την ορθή εκτέλεση των υποχρεώσεων που απορρέουν από τη παρούσα Απόφαση και τα σχετικά παραρτήματα, καθώς επίσης και την ακρίβεια των πληροφοριών που του παρέχονται σύμφωνα με τη παρούσα Απόφαση.

(2) Σε περίπτωση κατά την οποία ο προβλεπόμενος στο εδάφιο (1) έλεγχος από την Αρχή απαιτεί σύμβαση παροχής υπηρεσιών από τεχνικούς συμβούλους ή άλλα πρόσωπα, η Αρχή λαμβάνει εύλογα μέτρα για την εξασφάλιση της ανεξαρτησίας τους καθώς και για την τήρηση εκ μέρους τους εμπιστευτικότητας και αμεροληψίας.

(3) Για την άσκηση των αρμοδιοτήτων της η Αρχή δύναται να διεξάγει έρευνα σύμφωνα με το άρθρο 23 του Νόμου και να επιβάλλει διορθωτικά μέτρα έχοντας την εξουσία να:

(α) Δίνει εντολή σε φορέα να της παρέχει όλα τα σχετικά έγγραφα σύμφωνα με το άρθρο 13.

(β) Εκδίδει κατευθυντήριες γραμμές και δεσμευτικές οδηγίες προς τους φορείς όσον αφορά την παροχή εγγράφων και πληροφοριών στην Αρχή και τη μορφή τους.

(γ) Διενεργεί ελέγχους ασφάλειας πληροφοριών προκειμένου να αξιολογήσει κατά πόσον ο φορέας συμμορφώνεται με τις υποχρεώσεις του, όπως αυτές περιγράφονται στο παρόν Πλαίσιο.

(δ) Εκδίδει κατευθυντήριες γραμμές και δεσμευτικές οδηγίες όσον αφορά τους φορείς που δεν εκπληρώνουν τις υποχρεώσεις τους σύμφωνα με αυτό το Πλαίσιο. Επιπλέον, η Αρχή έχει την εξουσία να εκδίδει επίσημες γνωμοδοτήσεις και κατευθυντήριες γραμμές για να βοηθά τους φορείς στην εφαρμογή συγκεκριμένων μέτρων που καθορίζονται στα Παραρτήματα της παρούσας Απόφασης.,

η Αρχή, κατ' εφαρμογή της παραγράφου (γ) του εδαφίου (3) του άρθρου 16 της Απόφασης Κ.Δ.Π. 389/2020 προχώρησε στη δημιουργία ενός μοντέλου ωριμότητας κυβερνοασφάλειας (cybersecurity maturity model), με σκοπό την εξειδίκευση των απαιτήσεων της Απόφασης Κ.Δ.Π. 389/2020 και αντιστοίχισή τους προς διακριτά επίπεδα ωριμότητας ασφάλειας. Το μοντέλο ωριμότητας κυβερνοασφάλειας (cybersecurity maturity model) καλύπτει το πλήρες εύρος των απαιτήσεων ασφαλείας που προνοούνται στην Απόφαση Κ.Δ.Π. 389/2020 και στους τρείς σχετικούς πυλώνες, δηλαδή στους πυλώνες της προετοιμασίας (Prepare), προστασίας και εντοπισμού (Protect and Detect) και ανταπόκρισης (Respond). Το μοντέλο ωριμότητας κυβερνοασφάλειας (cybersecurity maturity model) βασίζεται σε διεθνείς βέλτιστες πρακτικές και πρότυπα και περιέχει πέντε (5) διακριτά επίπεδα ωριμότητας κυβερνοασφάλειας. Το επίπεδο τρία (3) περιέχει τις ακριβείς απαιτήσεις της Απόφασης Κ.Δ.Π. 389/2020 και δύναται να αναγνωρίσει το επίπεδο των Φορέων που συμμορφώθηκαν με τις απαιτήσεις της Απόφασης Κ.Δ.Π. 389/2020, καθώς και των Φορέων που ακόμη να συμμορφωθούν.

Περαιτέρω, χρησιμοποιείται ως βάση για τη διενέργεια των ελέγχων και αξιολογεί το επίπεδο συμμόρφωσης του Φορέα με τις απαιτήσεις της Απόφασης Κ.Δ.Π. 389/2020. Επίσης, δύναται να αποτελέσει χρήσιμο εργαλείο αυτοαξιολόγησης και σχεδιασμού για τον Φορέα, όπου δύναται να τον βοηθήσει να βελτιώσει σημαντικά τη θέση του στον κυβερνοχώρο σε ένα διαρκώς εξελισσόμενο τοπίο απειλών.

Ειδικότερα, η Αρχή επιθυμεί, μέσα από τους ελέγχους ως προς τις προδιαγραφές του μοντέλου ωριμότητας κυβερνοασφάλειας (cybersecurity maturity model), να αναγνωρίζει το επίπεδο ωριμότητας των Φορέων έναντι των

απαιτήσεων της Απόφασης Κ.Δ.Π. 389/2020, να ενημερώνεται σχετικά με το επίπεδο των Φορέων, πέραν από τα οριζόμενα της Απόφασης Κ.Δ.Π. 389/2020 και να μπορεί (με την χρήση της εξερχόμενης αναφοράς) να ζητήσει από τους Φορείς να θέσουν πλάνο ενεργειών για τη συμμόρφωσή τους σύμφωνα με τις πρόνοιες της Απόφασης Κ.Δ.Π. 389/2020 ή τη βελτίωση του επιπέδου ασφαλείας τους.

Μερικά από τα πλεονεκτήματα της χρήσης του μοντέλου ωριμότητας κυβερνοασφάλειας (cybersecurity maturity model) είναι τα ακόλουθα:

i. εντοπίζει τα δυνατά και αδύνατα σημεία επιτρέποντας στοχευμένες βελτιώσεις·
ii. βοηθά στην ευθυγράμμιση των επενδύσεων ασφάλειας με τις πραγματικές ανάγκες·
iii. ενσωματώνει βέλτιστες πρακτικές από διεθνή, ευρωπαϊκά και εθνικά πρότυπα·
iv. παρέχει έναν πρακτικό χάρτη για τη συνεχή ενίσχυση της ανθεκτικότητας στον κυβερνοχώρο.

4. Το σκεπτικό της ανάπτυξης του Πλαισίου

Στην Κυπριακή Δημοκρατία η Οδηγία NIS εναρμονίστηκε με τον Νόμο 89(Ι)/2020, Νόμος ο οποίος αποτέλεσε ορόσημο στην προσπάθεια για αυξημένη κυβερνοασφάλεια στην Κυπριακή Δημοκρατία. Η Αρχή, ως η αρμόδια εθνική αρχή για την εφαρμογή των διατάξεων του Νόμου 89(Ι)/2020, ως εκάστοτε τροποποιείται ή αντικαθίσταται, κατά την άσκηση των αρμοδιοτήτων και εξουσιών της, ενεργεί κατά τρόπο ο οποίος προάγει την επίτευξη επιπέδου ασφάλειας δικτύων και συστημάτων πληροφοριών, συμπεριλαμβανομένων όλων των βασικών υπηρεσιών/ κρίσιμων υποδομών πληροφοριών της Δημοκρατίας και των ψηφιακών υπηρεσιών που υπάγονται στην αρμοδιότητά της. Περαιτέρω, προάγει τη διατήρηση της ακεραιότητας και ασφάλειας των δικτύων ηλεκτρονικών επικοινωνιών και της ασφάλειας των πληροφοριών, συμπεριλαμβανομένης της προστασίας των κρίσιμων υποδομών πληροφοριών.

Ως εκ των ανωτέρω, η Αρχή εξέδωσε την Απόφαση Κ.Δ.Π. 389/2020 με την οποία καθορίζεται το πλαίσιο των ελάχιστων μέτρων ασφάλειας δικτύων και συστημάτων πληροφοριών και το οποίο έχει ως στόχο να βοηθήσει τους Φορείς να συμμορφωθούν με τις απαιτήσεις και τις υποχρεώσεις του Νόμου 89(Ι)/2020, ως εκάστοτε τροποποιείται ή αντικαθίσταται, και της Οδηγίας (ΕΕ) 2016/1148.

Στο πλαίσιο αυτών των εξελίξεων, και για να υπάρξει μια συστηματοποιημένη προσέγγιση στην αξιολόγηση της ωριμότητας κυβερνοασφάλειας των Φορέων, η Αρχή ανέπτυξε ένα μοντέλο ωριμότητας (cybersecurity maturity model), με το οποίο επιδιώκει να καθοδηγήσει τους Φορείς ώστε να υλοποιήσουν τις απαιτήσεις της Απόφασης Κ.Δ.Π. 389/2020 και να κατατάξει την ωριμότητά τους σε διακριτά επίπεδα.

Το παρόν Πλαίσιο αποτελεί το επόμενο βήμα για την πιο πάνω διαδικασία. Συγκεκριμένα, το Πλαίσιο προορίζεται να εγκρίνει επαγγελματίες ικανούς να διεξάγουν τις αξιολογήσεις ωριμότητας κυβερνοασφάλειας των Φορέων και διασφαλίζει ότι διαθέτουν την απαραίτητη τεχνική εμπειρία και γνώση. Οι εγκεκριμένοι ελεγκτές θα αξιολογούν την κατάσταση σχετικά με την κυβερνοασφάλεια των Φορέων, εστιάζοντας στην πληρότητα και την αποτελεσματικότητα των υφιστάμενων πολιτικών και μέτρων. Μέσω του Πλαισίου, η Αρχή επιδιώκει να διασφαλίσει ένα συνεπές και αξιόπιστο επίπεδο εμπειρίας και εξειδίκευσης στο πεδίο ελέγχου της κυβερνοασφάλειας, ενισχύοντας την επιβλεπόμενη και αξιόπιστη αξιολόγηση των μέτρων ασφαλείας. Οι εγκεκριμένοι ελεγκτές εφόσον παρακολουθήσουν συγκεκριμένες και εξειδικευμένες εκπαιδεύσεις και εφόσον αξιολογηθούν βάσει αυστηρών κριτηρίων, θα είναι επαρκώς εξοπλισμένοι για να εκτιμήσουν την κυβερνοασφάλεια των Φορέων, να αναλύσουν τις υπάρχουσες πρακτικές και, όπου απαιτείται, να προτείνουν βελτιώσεις.

Μέσω αυτού του Πλαισίου, η Αρχή επιδιώκει να ενισχύσει την κυβερνοανθεκτικότητα των Φορέων, να αυξήσει την επίγνωση για τις κυβερνοαπειλές και να ενθαρρύνει τη συνεχή βελτίωση των μεθόδων ασφάλειας στις υποδομές των Φορέων. Επιπλέον, συμβάλλει στην εδραίωση μιας κουλτούρας ασφάλειας στο ψηφιακό περιβάλλον της Κυπριακής Δημοκρατίας. Με την έγκριση επαγγελματιών που είναι κατάλληλα εκπαιδευμένοι και ενημερωμένοι, η Κυπριακή Δημοκρατία ενισχύει την ικανότητά της να προστατεύει τις κρίσιμες ψηφιακές υποδομές και τις πληροφορίες της, γεγονός που είναι ιδιαίτερα σημαντικό σε μιαν περίοδο που η ψηφιακή ασφάλεια αποτελεί και εθνικό αλλά και διεθνές ζήτημα. Τέλος, σε μια εποχή όπου οι κυβερνοαπειλές μπορούν να έχουν εκτεταμένες συνέπειες στην οικονομική και κοινωνική ζωή, το Πλαίσιο συμβάλλει στη διαμόρφωση ενός ασφαλέστερου ψηφιακού περιβάλλοντος για τους πολίτες, τις επιχειρήσεις και τον δημόσιο τομέα.

4.1 Χαρακτηριστικά Ελεγκτών Κυβερνοασφάλειας

Οι ελεγκτές είναι αρμόδιοι να διενεργούν τους ελέγχους με τη χρήση του μοντέλου ωριμότητας κυβερνοασφάλειας (cybersecurity maturity model) της Αρχής, το οποίο είναι δομημένο και καλύπτει τις απαιτήσεις του ΠΑΡΑΡΤΗΜΑΤΟΣ ΙΙΙ: ΠΛΑΙΣΙΟ ΜΕΤΡΩΝ ΑΣΦΑΛΕΙΑΣ της Απόφασης Κ.Δ.Π. 389/2020. Περαιτέρω, αποτελούν το κύριο εργαλείο για την ορθή εφαρμογή του μοντέλου ωριμότητας κυβερνοασφάλειας και ως εκ τούτου απαιτείται να έχουν συγκεκριμένες γνώσεις και δεξιότητες για την αποτελεσματική αξιολόγηση της κυβερνοασφάλειας στους Φορείς.

Για τον σκοπό αυτόν, η Αρχή δημιούργησε ένα προφίλ για τον ελεγκτή. Το συγκεκριμένο προφίλ περιλαμβάνει τις βασικές γνώσεις και δεξιότητες που υποχρεούται να διαθέτει ο ελεγκτής προκειμένου να διενεργήσει με αποτελεσματικότητα τον έλεγχο και εντός των παρεχόμενων χρονικών πλαισίων.

Τα προσόντα, οι γνώσεις, οι δεξιότητες και τα καθήκοντα που απαιτείται να διαθέτει και να κατέχει ο ελεγκτής αναλύονται και προνοούνται στα άρθρα 28, 29 και 30 της παρούσας Απόφασης.

4.2 Τήρηση και προστασία αρχείων τα οποία προνοούνται από το Πλαίσιο και την Τράπεζα Θεμάτων Εξέτασης

Όλες οι πληροφορίες, τα έγγραφα, τα αρχεία ανάπτυξης του παρόντος Πλαισίου, συμπεριλαμβανομένης της τράπεζας θεμάτων της εξέτασης, των δεδομένων, των αποτελεσμάτων, της επιβεβαίωση και της επικύρωσης, των ανασκοπήσεων, αξιολογήσεων, τροποποιήσεων, ενέργειες βελτίωσης κλπ. τηρούνται ως ηλεκτρονικά αρχεία από τον Διαχειριστή Τράπεζας Θεμάτων Εξέτασης. Η Αρχή αναγνωρίζει και αναθέτει τον ρόλο του Διαχειριστή Τράπεζας Θεμάτων Εξέτασης, σε οργανισμό ο οποίος θα φέρει την ευθύνη για τα ακόλουθα:

- Τη Διαχείριση: Οργάνωση, αποθήκευση και ασφαλή τήρηση της Τράπεζας Θεμάτων Εξέτασης.
- Την Εισαγωγή Θεμάτων: Επεξεργασία και καταχώριση νέων θεμάτων, λαμβάνοντας υπόψη διάφορες παραμέτρους, μετά από την σχετική εντολή της Αρχής.
- Τη Διανομή Θεμάτων: Διανομή των εξεταστικών θεμάτων για εξετάσεις στους εγκεκριμένους εξεταστικούς φορείς.
- Την Επικαιροποίηση: Αναθεώρηση των θεμάτων βάσει ανατροφοδότησης (feedback), μετά από τη σχετική εντολή της Αρχής, διασφαλίζοντας την επικαιρότητα και την αποτελεσματικότητά τους.
- Την Επίλυση Προβλημάτων: Αναγνώριση και διόρθωση τυχόν σφαλμάτων ή ασαφειών στα θέματα, μετά από τη σχετική εντολή της Αρχής.

Επιπρόσθετα, ο Διαχειριστής της Τράπεζας Θεμάτων Εξέτασης οφείλει να τηρεί τα ακόλουθα:

- Κρυπτογράφηση: Εφαρμογή ισχυρών αλγόριθμων κρυπτογράφησης για την ασφάλεια και εμπιστευτικότητα των δεδομένων, τόσο κατά την αποθήκευση όσο και κατά τη μεταφορά.
- Ακεραιότητα Δεδομένων: εφαρμογή μέτρων ασφαλείας για τη διασφάλιση της ακεραιότητας και της διαθεσιμότητας της βάσης δεδομένων των ερωτήσεων και εφαρμογή ελέγχων πρόσβασης και μηχανισμών αντιγράφων ασφαλείας (onsite και offsite) για την προστασία από μη εξουσιοδοτημένες τροποποιήσεις ή απώλεια δεδομένων. Η πρόσβαση θα πρέπει να γίνεται μόνο από περιορισμένο σε αριθμό εξουσιοδοτημένο προσωπικό της Αρχής ή/και του Διαχειριστή Τράπεζας Θεμάτων Εξέτασης.
- Ιστορικό Αλλαγών: Διατήρηση λεπτομερούς ιστορικού ιχνηλασιμότητα ενεργειών (audit log) για κάθε αλλαγή στα θέματα (full accounting and traceability of changes), επιτρέποντας την ιχνηλασιμότητα και την αναίρεση τυχόν σφαλμάτων. Το ιστορικό των ενεργειών θα πρέπει να διατηρείται για τουλάχιστον ένα (1) έτος.
- Εφαρμογή ελέγχου εκδόσεων (Version Control): παρακολούθηση των αλλαγών και των ενημερώσεων των ερωτήσεων με την τήρηση εκδόσεων.
- Διαχείριση Κρίσεων: Εκπόνηση και εφαρμογή σχεδίου αντιμετώπισης κρίσεων και επιχειρησιακής συνέχειας για τυχόν περιστατικά όπως διαρροή θεμάτων, μη διαθεσιμότητα συστημάτων κ.α.

5. Συνολική διαδικασία

Το παρακάτω διάγραμμα αποτυπώνει τα επιμέρους βήματα και τα εμπλεκόμενα μέρη της διαδικασίας έγκρισης του ελεγκτή.

Βήμα Διαδικασίας	Υλοποιητής	Εξερχόμενο
1. ΕΚΠΑΙΔΕΥΣΗ Παρακολούθηση εκπαίδευσης 40 ωρών στο γνωστικό αντικείμενο	Αρχή Ψηφιακής Ασφάλειας ή εξουσιοδοτημένος αντιπρόσωπος από την Αρχή	Βεβαίωση Παρακολούθησης
2. ΑΙΤΗΣΗ ΚΑΙ ΣΥΜΜΕΤΟΧΗ ΣΕ ΕΞΕΤΑΣΕΙΣ Ο υποψήφιος υποβάλλει αίτηση για συμμετοχή σε εξετάσεις, οι οποίες διεξάγονται σε συγκεκριμένο χρόνο και τόπο	Εξεταστικός φορέας	Πιστοποιητικό επιτυχίας σε εξετάσεις
3. ΥΠΟΒΟΛΗ ΑΙΤΗΣΗΣ ΓΙΑ ΕΓΓΡΑΦΗ ΣΤΟ ΜΗΤΡΩΟ ΕΛΕΓΚΤΩΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ Ο Υποψήφιος υποβάλλει όλα τα απαραίτητα αποδεικτικά στοιχεία μαζί με τη σχετική αίτηση στον Κυπριακό Οργανισμό Τυποποίησης (CYS)	Κυπριακός Οργανισμός Τυποποίησης (CYS)	Εγγραφή στο Μητρώο Ελεγκτών Κυβερνοασφάλειας

Όπως παρουσιάζεται και στον πιο πάνω πίνακα η διαδικασία έγκρισης περιλαμβάνει τα ακόλουθα **τρία βήματα**:

1. Εκπαίδευση:

- Ο υποψήφιος οφείλει να παρακολουθήσει 40 ώρες εκπαίδευσης στο γνωστικό αντικείμενο.
- Η εκπαίδευση παρέχεται από την Αρχή ή από εξουσιοδοτημένο αντιπρόσωπο από την Αρχή.
- Μετά την ολοκλήρωση της εκπαίδευσης, ο υποψήφιος λαμβάνει βεβαίωση παρακολούθησης.

2. Αίτηση και συμμετοχή σε εξετάσεις:

- Σε οποιανδήποτε χρονική στιγμή, ο υποψήφιος υποβάλλει αίτηση για συμμετοχή στις εξετάσεις σε εξεταστικό φορέα.
- Η αίτηση γίνεται μέσω του τρόπου που υποδεικνύεται από τον εξεταστικό φορέα.
- Ο υποψήφιος συμμετέχει στις εξετάσεις όπως αυτές ορίζονται από τον εξεταστικό φορέα.
- Οι εξετάσεις διεξάγονται σε εγκεκριμένα εξεταστικά κέντρα, με φυσική παρουσία. Το σύστημα των εξετάσεων είναι ψηφιακό και λαμβάνει τα θέματα από τον Διαχειριστή Τράπεζας Θεμάτων Εξέτασης.
- Ο εξεταστικός φορέας αξιολογεί την επίδοση στις εξετάσεις και, σε περίπτωση επιτυχίας, εκδίδει σχετικό πιστοποιητικό επιτυχίας με ισχύ 3 έτη.

3. Υποβολή αίτησης για Εγγραφή στο Μητρώο Ελεγκτών Κυβερνοασφάλειας:

- Ο υποψήφιος συλλέγει τα αποδεικτικά στοιχεία για όλα τα απαιτούμενα τα οποία ορίζονται στο παρόν Πλαίσιο.
- Συμπληρώνει και υποβάλλει την αίτηση εγγραφής μαζί με τα απαραίτητα αποδεικτικά στοιχεία στον Κυπριακό Οργανισμό Τυποποίησης (CYS).
- Το Πιστοποιητικό επιτυχίας στην εξέταση θα πρέπει να έχει ληφθεί εντός ενός (1) έτους από την ημερομηνία υποβολής της αίτησης
- Γίνεται έλεγχος της πληρότητας και της εγκυρότητας των προαπαιτούμενων όπως αυτά καταγράφονται στη παράγραφο 6.1 και 6.2.
- Εφόσον ο Κυπριακός Οργανισμός Τυποποίησης (CYS) ελέγξει την πληρότητα και εγκυρότητα των προ απαιτούμενων εγγράφων/δικαιολογητικών, καταχωρεί το όνομα του εγκεκριμένου ελεγκτή στο σχετικό Μητρώο Ελεγκτών Κυβερνοασφάλειας

6 Μητρώο Ελεγκτών Κυβερνοασφάλειας

6.1. Κριτήρια εγγραφής στο Μητρώο Ελεγκτών Κυβερνοασφάλειας ως ελεγκτής

Για την εγγραφή στο Μητρώο Ελεγκτών Κυβερνοασφάλειας, θα πρέπει ο υποψήφιος ελεγκτής να πληροί/κατέχει τα ακόλουθα προσόντα και επαγγελματική πείρα:

Εκπαιδευτικά Προσόντα	α) Πανεπιστημιακό Δίπλωμα ή τίτλο ή ισότιμο προσόν σ' ένα από τα πιο κάτω αντικείμενα ή συνδυασμό των αντικειμένων αυτών ή σε κάποιο άλλο συναφές με την Πληροφορική ή την ασφάλεια πληροφοριών/κυβερνοασφάλεια: 1. Επιστήμης των Ηλεκτρονικών Υπολογιστών ή/και της Πληροφορικής και της Διοίκησης Πληροφοριακών Συστημάτων (περιλαμβανομένων των Software Engineering, Information Technology, Computer Engineering, Electronic Engineering, Electrical Engineering, Data Communications, Computer Science, Digital Engineering, Electronic Imaging, Management Information Systems, Web Development, Visual Communications, Web Optimisation, Animation, Multimedia, Web applications, Graphics, Web Design) 2. Πληροφορικής και Τηλεπικοινωνιών 3. Ηλεκτρολογικής Μηχανικής και Μηχανικής Υπολογιστών 4. Εφαρμοσμένης Πληροφορικής 5. Ηλεκτρολογικής Μηχανικής & Τεχνολογίας Υπολογιστών 6. Μηχανικής Ηλεκτρονικών/Υπολογιστών και Πληροφορικής 7. Επιστήμης Υπολογιστών 8. Μηχανικής Πληροφοριακών και Επικοινωνιακών Συστημάτων, Μηχανικής Ηλεκτρονικών Υπολογιστών, Τηλεπικοινωνιών και Δικτύων 9. Επιστήμης και Τεχνολογίας Υπολογιστών 10. Επιστήμης και Τεχνολογίας Τηλεπικοινωνιών 11. Διδακτικής της Τεχνολογίας και Ψηφιακών Συστημάτων

	12. Επιστημών και Πολιτισμού – Κατεύθυνση Η/Υ (Π.Σ.Ε.) 13. Πληροφορικής στην Εκπαίδευση 14. Electronic Systems Engineering, Telematics (Communications with software) 15. Τεχνολογίες διαδικτύου και ασφάλεια 16. Ψηφιακών Συστημάτων 17. Διοίκησης επιχειρήσεων και πληροφοριακών συστημάτων 18. Θεμελιώσεις Πληροφορικής και Εφαρμογές 19. Πληροφοριακών συστήματα 20. Εξειδίκευση στα πληροφοριακά συστήματα 21. Μηχανικής Λογισμικού για διαδικτυακές & φορητές εφαρμογές, πληροφορικής και τηλεματικής 22. Μικροηλεκτρονικής 23. Επιστήμης και Τεχνολογίας Υπολογιστών 24. Ολοκληρωμένα συστήματα υλικού και λογισμικού 25. Συστήματα Επεξεργασίας Σημάτων και Επικοινωνιών 26. Επιστήμης Υπολογιστών 27. Ηλεκτρονικής Μηχανικής και Μηχανικής Υπολογιστών 28. Πληροφοριακών συστημάτων και ψηφιακής καινοτομίας, κυβερνοασφάλειας και Επιστήμης Δεδομένων 29. Ανάπτυξης και Ασφάλειας Πληροφοριακών Συστημάτων 30. Προηγμένων Τεχνολογιών Πληροφορικής 31. Επιστήμης και Μηχανικής Δεδομένων 32. Ηλεκτρολογικής Μηχανικής και Εφαρμοσμένης Πληροφορικής • Ο όρος Πανεπιστημιακός τίτλος καλύπτει και μεταπτυχιακό τίτλο. β) Σε περίπτωση απουσίας σχετικού τίτλου σπουδών, ως αναφέρεται ανωτέρω, γίνονται δεκτοί και άλλοι κάτοχοι Πανεπιστημιακών Διπλωμάτων με άλλους τίτλους σπουδών, υπό την προϋπόθεση ότι η επαγγελματική εμπειρία που καταγράφεται στην ενότητα Επαγγελματική Πείρα, αντίστοιχα μετατρέπεται ως εξής: - Δεκαετής (10) τουλάχιστον εργασιακή εμπειρία πλήρους απασχόλησης στον τομέα της Τεχνολογίας Πληροφοριών, εκ των οποίων τουλάχιστον 5 χρόνια σε θέση που σχετίζεται με την ασφάλεια των πληροφοριών ή Κυβερνοασφάλεια (π.χ. Δίκτυα και Ασφάλεια Πληροφοριακών Συστημάτων, Αρχιτεκτονική Δικτύων, Πρωτόκολλα Μεταφοράς, Δίκτυα Επικοινωνιών, Διαχείριση Υποδομών Πληροφορικής και Τηλεπικοινωνιών, Ασφάλεια Πληροφοριακών Συστημάτων, υπολογιστών και δικτύων, Εφαρμογές Διαδικτύου και Κρυπτογραφία, Διαχείριση Κινδύνων Ασφάλειας Πληροφοριακών και Επικοινωνιακών Συστημάτων, Έλεγχος Ασφάλειας Πληροφοριακών ή/και Επικοινωνιακών Συστημάτων κ.α.)

	γ) Πολύ καλή γνώση της Ελληνικής και Αγγλικής γλώσσας, σύμφωνα με τα τεκμήρια γνώσης γλωσσών της Επιτροπής Δημόσιας Υπηρεσίας (βλ. http://www.psc.gov.cy/psc/psc.nsf/page31_gr/page31_gr?OpenDocument). δ) Εκπαίδευση 40 ωρών στο «Πρόγραμμα Κατάρτισης Ελεγκτών Ωριμότητας Κυβερνοασφάλειας». ε) Επιτυχία στις εξετάσεις Ελεγκτή Κυβερνοασφάλειας.
Επαγγελματική Πείρα	α) Απαιτείται τουλάχιστον τετραετής (4) πλήρης εργασιακή εμπειρία στον τομέα της Τεχνολογίας Πληροφοριών, εκ των οποίων τουλάχιστον τα δύο (2) χρόνια σε θέση που σχετίζεται με την ασφάλεια των πληροφοριών ή Κυβερνοασφάλεια (όπως είναι: Δίκτυα και Ασφάλεια Πληροφοριακών Συστημάτων, Αρχιτεκτονική Δικτύων, Πρωτόκολλα Μεταφοράς, Δίκτυα Επικοινωνιών, Διαχείριση Υποδομών Πληροφορικής και Τηλεπικοινωνιών, Ασφάλεια Πληροφοριακών Συστημάτων, υπολογιστών και δικτύων, Εφαρμογές Διαδικτύου και Κρυπτογραφία, Διαχείριση Κινδύνων Ασφαλείας Πληροφοριακών και Επικοινωνιακών Συστημάτων, Έλεγχος Ασφάλειας Πληροφοριακών ή/και Επικοινωνιακών Συστημάτων κ.α.) β) Απαιτείται ενεργό πιστοποιητικό CISA ή/και ISO27001-Lead Auditor και τουλάχιστον τρείς (3) ελέγχους συστημάτων τρίτου μέρους (third party audits[3]) συνολικής διάρκειας είκοσι (20) ημερών, που διενεργήθηκαν τα τελευταία πέντε (5) χρόνια. Η διάρκεια θα ελέγχεται από log book ή από βεβαίωση που θα προσκομίσει ο αιτητής και η οποία θα είναι υπογεγραμμένη από διαπιστευμένο φορέα πιστοποίησης ή από κρατική υπηρεσία. γ) Νοείται ότι, σε περίπτωση απουσίας του πιστοποιητικού όπως αναφέρεται στα σημεία ανωτέρω, ή/και της διάρκειας ελέγχων ως προνοείται στο παρόν, και εφόσον ο υποψήφιος για ελεγκτής επιτύχει στην εξέταση θα εγγράφεται στο Μητρώο Ελεγκτών Κυβερνοασφάλειας ως εκπαιδευόμενος ελεγκτής και οφείλει να συνοδεύσει άλλον εγκεκριμένο ελεγκτή και να παρακολουθήσει δύο (2) ολοκληρωμένους ελέγχους με ελάχιστη συνολική διάρκεια δέκα (10) ημερών από εγκεκριμένο ελεγκτή, ως προνοείται στην παρούσα Απόφαση. Ακολούθως, η κατάσταση του στο Μητρώο Ελεγκτών Κυβερνοασφάλειας θα αλλάζει σε δόκιμο (junior) ελεγκτή. Ο δόκιμος (junior) ελεγκτής θα μπορεί να επιλεχθεί για έλεγχο ωριμότητας ΜΟΝΟ από Φορέα με επίπεδο κρισιμότητας «Μέτριο» και «Χαμηλό» και θα συνοδεύεται από την Αρχή για επιτήρηση. Αν η επιτήρησή του είναι επιτυχής τότε η κατάστασή του στο Μητρώο Ελεγκτών Κυβερνοασφάλειας θα αλλάζει από δόκιμο (junior) σε εγκεκριμένο ελεγκτή.

6.2. Αίτηση Εγγραφής στο Μητρώο Ελεγκτών Κυβερνοασφάλειας

Κάθε υποψήφιος που επιθυμεί να εγγραφεί στο Μητρώο Ελεγκτών Κυβερνοασφάλειας, μπορεί να υποβάλει σχετική αίτηση εγγραφής, ανεξαρτήτως φύλου, ηλικίας, εθνικότητας, ιθαγένειας, θρησκείας, σωματικής ή άλλης αναπηρίας (Άτομα με Αναπηρία- ΑμεΑ) εντός των πλαισίων και εξαιρέσεων που προνοεί η ισχύουσα νομοθεσία.

Αποτελεί ουσιαστική και καθοριστική επαγγελματική προϋπόθεση, ο υποψήφιος που επιθυμεί να εγγραφεί ως ελεγκτής στο Μητρώο Ελεγκτών Κυβερνοασφάλειας να είναι σε θέση να παρατηρεί και να βλέπει κατά τη διενέργεια των ελέγχων.

Η διαδικασία εγγραφής στο Μητρώο Ελεγκτών Ωριμότητας Κυβερνοασφάλειας περιλαμβάνει τα ακόλουθα στάδια:

1. Ο υποψήφιος Ελεγκτής υποβάλλει την αίτησή του, μαζί με τα απαραίτητα έγκυρα (και όπου χρειάζεται πιστοποιημένα) έγγραφα/δικαιολογητικά στα γραφεία του Κυπριακού Οργανισμού Τυποποίησης (CYS), είτε ταχυδρομικώς, είτε μέσω ηλεκτρονικού ταχυδρομείου και με τρόπο που διασφαλίζει την επιτυχή παράδοση του,

[3] παράγραφος 3.1 από το ISO 19011:2018, ως εκάστοτε αναθεωρείται.

καταβάλλοντας αντίστοιχο ποσό τέλους, το ύψος του οποίου καθορίζεται από τον Κυπριακό Οργανισμό Τυποποίησης (CYS) κατόπιν συνεννόησής με την Αρχή.

1. Η αίτηση περιλαμβάνει κατ΄ ελάχιστον τα συγκεκριμένα πεδία:
    i. Ονοματεπώνυμο, ημερομηνία γέννησης, διεύθυνση, τηλέφωνο, διεύθυνση ηλεκτρονικού ταχυδρομείου, αριθμό δελτίου ταυτότητας (ΑΔΤ)
    ii. Αιτούμενη ειδικότητα (πάντα Ελεγκτές Ωριμότητας Κυβερνοασφάλειας)
    iii. Αποδεικτικά στοιχεία/έγγραφα αναφορικά με τις απαιτήσεις σύμφωνα με τη περιγραφή της εργασίας του Ελεγκτή
    iv. Δέσμευση υποψηφίου και υποχρεώσεις του Ελεγκτή
    v. Δήλωση του υποψηφίου για τη συμμόρφωσή του με τις απαιτήσεις του Πλαισίου.
    vi. Συναίνεση του υποψηφίου για τη δημοσιοποίηση των προσωπικών του στοιχείων [όνομα, επίθετο, όνομα εταιρείας (σε περίπτωση που είναι νομικό πρόσωπο), τηλέφωνο, διεύθυνση ηλεκτρονικού ταχυδρομείου (email), και αριθμός στο Μητρώο] στο Μητρώο Ελεγκτών Κυβερνοασφάλειας και αποδοχή των όρων διαχείρισης προσωπικών δεδομένων
    vii. Αποδοχή της συμμόρφωσης προς τους δεοντολογικούς κανόνες επαγγέλματος, σύμφωνα με το ΠΡΟΣΑΡΤΗΜΑ 1.
    viii. Δέσμευση του υποψηφίου για αυστηρή τήρηση εμπιστευτικότητας του συνόλου των πληροφοριών και την διατήρηση της αμεροληψίας του στα πλαίσια των ελέγχων
    ix. Ημερομηνία συμπλήρωσης αίτησης και υπογραφή υποψηφίου.

Η αίτηση συνοδεύεται απαραιτήτως από:

- ακριβές αντίγραφο δικαιολογητικού που πιστοποιεί τα προσωπικά στοιχεία του υποψηφίου (φωτοτυπία των δύο όψεων του δελτίου ταυτότητας ή της σχετικής προσωρινής βεβαίωσης της αρμόδιας αρχής ή του διαβατήριου ή αδείας παραμονής κ.λπ.), και

- πρωτότυπο Πιστοποιητικό Λευκού Ποινικού Μητρώου από την Κυπριακή Δημοκρατία ή τη χώρα διαμονής του υποψηφίου, δεόντως επικυρωμένο, με ημερομηνία έκδοσης ενός (1) μηνός πριν από την ημερομηνία υποβολής της αίτησης.

2. Ο Κυπριακός Οργανισμός Τυποποίησης (CYS) προβαίνει σε έλεγχο της εγκυρότητας και πληρότητας της αίτησης και των εγγράφων/πιστοποιητικών (δικαιολογητικών) που συνοδεύουν την αίτηση, σύμφωνα με τη διαδικασία που είναι αναρτημένη στην ιστοσελίδα του. Σε περίπτωση που όλα τα στοιχεία είναι πλήρη και σύμφωνα με τις απαιτήσεις (προαπαιτούμενα ενότητα 6.1), ο Κυπριακός Οργανισμός Τυποποίησης (CYS) ενημερώνει τον υποψήφιο ότι η αίτηση του είναι αποδεκτή. Αν όχι, ο CYS ενημερώνει ότι εκκρεμεί η υποβολή εγγράφων και ότι ο αιτητής εντός τεσσάρων (4) μηνών υποχρεούται να τα υποβάλει στον Κυπριακό Οργανισμό Τυποποίησης (CYS). Κατά την περίοδο αυτήν, η αίτηση θα έχει την κατάσταση «Εκκρεμής» -"Pending".

3. Σε περίπτωση απουσίας στοιχείων ή δικαιολογητικών ή μη κάλυψης απαιτήσεων μετά την έλευση των πιο πάνω, στο σημείο 2, τεσσάρων (4) μηνών, ο Κυπριακός Οργανισμός Τυποποίησης (CYS) απορρίπτει την αίτηση οριστικά. Ο υποψήφιος έχει τη δυνατότητα να υποβάλει νέα αίτηση όποτε το επιθυμεί, καταβάλλοντας εκ νέου το αντίστοιχο ποσό τέλους, το ύψος του οποίου καθορίζεται από τον Κυπριακό Οργανισμό Τυποποίησης (CYS) κατόπιν συνεννόησης με την Αρχή.

6.3. Διαχείριση του Μητρώου Ελεγκτών Κυβερνοασφάλειας

Όταν η αίτηση για εγγραφή στο Μητρώο Ελεγκτών Κυβερνοασφάλειας γίνει αποδεκτή, τότε ακολουθούνται τα εξής βήματα:

1. Ο Κυπριακός Οργανισμός Τυποποίησης (CYS) προχωρά στην επαλήθευση και καταχώρηση των στοιχείων του ελεγκτή στο ηλεκτρονικό σύστημα του Μητρώου Ελεγκτών Κυβερνοασφάλειας.

2. Ο Κυπριακός Οργανισμός Τυποποίησης (CYS) εκδίδει την ταυτότητα του ελεγκτή, η οποία αναγράφει όλα τα απαραίτητα στοιχεία και είναι πλαστικοποιημένη για μεγαλύτερη ανθεκτικότητα. Η φωτογραφία του υποψηφίου θα σφραγίζεται από τον Κυπριακό Οργανισμό Τυποποίησης (CYS) για επιπλέον επικύρωση.

3. Ο ελεγκτής λαμβάνει απόδειξη πληρωμής και τιμολόγιο για το ποσό που κατέβαλε για την εγγραφή στο Μητρώο Ελεγκτών Κυβερνοασφάλειας και την έκδοση της ταυτότητας.

4. Τα στοιχεία του ελεγκτή [όνομα, επίθετο, όνομα εταιρείας (σε περίπτωση που είναι νομικό πρόσωπο), τηλέφωνο, διεύθυνση ηλεκτρονικού ταχυδρομείου και αριθμός στο Μητρώο] θα αναρτηθούν στο Μητρώο Ελεγκτών Κυβερνοασφάλειας εντός δυο (2) εργάσιμων ημερών από την έγκριση της αίτησης, διασφαλίζοντας την προστασία των προσωπικών τους δεδομένων, σύμφωνα με την ισχύουσα νομοθεσία περί ιδιωτικότητας και προστασίας δεδομένων.

5. Σε περίπτωση απώλειας, κλοπής ή φθοράς της ταυτότητας, ο ελεγκτής δύναται να ζητήσει αντικατάσταση, καταβάλλοντας το αντίστοιχο ποσό τέλους, το ύψος του οποίου καθορίζεται από τον Κυπριακό Οργανισμό Τυποποίησης (CYS) κατόπιν συνεννόησής με την Αρχή.

6. Η ταυτότητα του ελεγκτή θα έχει ισχύ τρία (3) έτη από την ημερομηνία έκδοσής της, και μπορεί να ανανεωθεί με την προσκόμιση των απαραίτητων δικαιολογητικών και με την πληρωμή του αντίστοιχου τέλους, το ύψος του οποίου καθορίζεται από τον Κυπριακό Οργανισμό Τυποποίησης (CYS), κατόπιν συνεννόησής με την Αρχή και νοουμένου ότι πληροί τις προϋποθέσεις της παραγράφου 8.8.

Οι ελεγκτές υποχρεούνται να ακολουθούν τις διαδικασίες επιτήρησης και επικαιροποίησης, όσον αφορά την εγγραφή τους στο Μητρώο Ελεγκτών Κυβερνοασφάλειας.

Σε περίπτωση που υπάρξει καταγγελία από τρίτους καθώς και ανάρμοστη συμπεριφορά από τον ελεγκτή, όπως είναι η παραβίαση των δεοντολογικών κανόνων του επαγγέλματος, η Αρχή θα αξιολογεί και θα διερευνά τις καταγγελίες και δύναται να ζητά γραπτώς από τον Κυπριακό Οργανισμό Τυποποίησης (CYS) τη διαγραφή ή αναστολή ή ανάκληση της εγγραφής του ελεγκτή από το Μητρώο Ελεγκτών Κυβερνοασφάλειας.

Τα κριτήρια για την εγγραφή στο Μητρώο Ελεγκτών Κυβερνοασφάλειας θα επανεξετάζονται και θα ενημερώνονται σε τακτική βάση από την Αρχή, ώστε να αντανακλούν τις τρέχουσες απαιτήσεις και προκλήσεις στον τομέα της κυβερνοασφάλειας.

7. Εκπαίδευση στο γνωστικό αντικείμενο

Το πρόγραμμα της εκπαίδευσης και όλα όσα περιλαμβάνει η εκπαίδευση αναφέρονται λεπτομερώς στο ΠΡΟΣΑΡΤΗΜΑ 2.

Για την υλοποίηση της εκπαίδευσης των 40 ωρών στο «Πρόγραμμα Κατάρτισης Ελεγκτών Ωριμότητας Κυβερνοασφάλειας», οι εκπαιδευτές του προγράμματος πρέπει να πληρούν αυστηρά τα ακόλουθα κριτήρια:

Εμπειρία: Να κατέχουν αποδεδειγμένη διδακτική εμπειρία άνω των 100 ωρών στο αντικείμενο της κυβερνοασφάλειας.

Γνώσεις:

- Να διαθέτουν πολύ καλή γνώση:
    - Της ισχύουσας εθνικής νομοθεσίας αναφορικά με τα θέματα της κυβερνοασφάλειας και ασφάλειας δικτύων και συστημάτων πληροφοριών.
    - Του ευρωπαϊκού νομοθετικού πλαισίου αναφορικά με τα θέματά της που άπτεται της κυβερνοασφάλειας και ασφάλειας δικτύων και συστημάτων πληροφοριών.
    - Του μοντέλου ωριμότητας κυβερνοασφάλειας (cybersecurity maturity model) που υιοθετεί η Αρχή.

Επαγγελματική εμπειρία:

- Τουλάχιστον δεκαετή (10) εμπειρία στη διενέργεια ελέγχων στον τομέα της κυβερνοασφάλειας.
- Να διαθέτουν πενταετή τουλάχιστον πρακτική εμπειρία στον χώρο της πληροφορικής και της κυβερνοασφάλειας.

Εκπαίδευση:

- Να κατέχουν ακαδημαϊκό τίτλο σπουδών σε τομέα της πληροφορικής, εξασφαλίζοντας στέρεες γνώσεις θεμελιωδών αρχών.

Το πιστοποιητικό παρακολούθησης της εκπαίδευσης γίνεται αποδεκτό όταν χορηγείται από την Αρχή ή από τον εξουσιοδοτημένο αντιπρόσωπό της.

8. Εξετάσεις – Πιστοποιητικό επιτυχούς εξέτασης του υποψήφιου Ελεγκτή Κυβερνοασφάλειας

8.1. Αίτηση συμμετοχής στις εξετάσεις

Κάθε υποψήφιος που το επιθυμεί δύναται να υποβάλει αίτηση για συμμετοχή στις εξετάσεις. Κάθε εξεταστικός φορέας που έχει υιοθετήσει το συγκεκριμένο Πλαίσιο έχει την δυνατότητα να δέχεται συνεχώς αιτήσεις συμμετοχής σε εξετάσεις ή να προκαθορίζει συγκεκριμένο χρονικό διάστημα αιτήσεων. Σε περίπτωση που ισχύει το δεύτερο, οι εξεταστικοί φορείς οφείλουν να ενημερώσουν με άμεσο, κατανοητό και αποτελεσματικό τρόπο το κοινό σχετικά με το χρονικό διάστημα στο οποίο θα γίνονται αποδεκτές οι σχετικές αιτήσεις.

Το έντυπο αίτησης Συμμετοχής στις εξετάσεις περιλαμβάνει κατ' ελάχιστον τις εξής πληροφορίες και δεδομένα που οφείλει να συμπληρώσει ο κάθε υποψήφιος:

- Ονοματεπώνυμο, ημερομηνία γέννησης, διεύθυνση, τηλέφωνο, διεύθυνση ηλεκτρονικού ταχυδρομείου (email), αριθμό δελτίου ταυτότητας (ΑΔΤ)
- Αιτούμενη ειδικότητα (ήτοι Ελεγκτές Ωριμότητας Κυβερνοασφάλειας)
- Αποδεικτικά πληρωμής του τέλους συμμετοχής στις εξετάσεις

- Επιθυμητή ημερομηνία και τόπος συμμετοχής στις εξετάσεις. Συγκεκριμένα, ο εξεταστικός φορέας δύναται σε συγκεκριμένο σημείο της αίτησης να δίνει τη δυνατότητα στον υποψήφιο να επιλέγει τη χρονική περίοδο και το εξεταστικό κέντρο στο οποίο επιθυμεί να συμμετέχει στη διαδικασία των εξετάσεων.
- Ειδικές συνθήκες που πρέπει να ληφθούν υπόψη για την ασφαλή και ισότιμη συμμετοχή του υποψηφίου στις εξετάσεις, όπως για παράδειγμα αν ο υποψήφιος είναι άτομο με αναπηρία ή διαμένει στο εξωτερικό, με σκοπό να δοθεί εύλογο χρονικό διάστημα για να συμμετέχει στις εξετάσεις
- Δήλωση σχετικά με την ύπαρξη / μη ύπαρξη παραγόντων που μπορεί να επηρεάσουν την αμεροληψία της εξεταστικής διαδικασίας
- Ημερομηνία συμπλήρωσης αίτησης
- Υπογραφή υποψηφίου (μόνο σε περίπτωση έντυπης μορφής)
- Πιστό αντίγραφο επικυρωμένο, του δικαιολογητικού που πιστοποιεί τα προσωπικά στοιχεία του υποψηφίου (αντίγραφο των δύο όψεων του δελτίου ταυτότητας ή της σχετικής προσωρινής βεβαίωσης της αρμόδιας αρχής ή του διαβατήριου ή αδείας παραμονής κ.λπ.)

Με σκοπό να εξασφαλιστεί ότι όλη η απαιτούμενη πληροφόρηση έχει υποβληθεί σωστά, η λήψη και ο έλεγχος της αίτησης αποτελεί ευθύνη του εξεταστικού φορέα. Ο έλεγχος της αίτησης επικεντρώνεται στην πληρότητά, την ορθότητα καθώς και την εγκυρότητα των δηλωθέντων στοιχείων/ δικαιολογητικών σε σχέση με τις ελάχιστες τυπικές προϋποθέσεις συμμετοχής.

Ο έλεγχος της αίτησης αφορά στα ακόλουθα:

1. Έλεγχος των πεδίων υποχρεωτικής συμπλήρωσης
2. Ταυτοποίηση στοιχείων αίτησης και προσκομισθέντων εγγράφων/δικαιολογητικών
3. Ύπαρξη ιδιόχειρης υπογραφής (μόνο σε περίπτωση έντυπης μορφής)
4. Έλεγχος στοιχείων αμεροληψίας που έχουν υποβληθεί από τον υποψήφιο, καθώς και έλεγχος για ύπαρξη εργασιακής ή άλλης σχέσης με τον εξεταστικό φορέα ή την ύπαρξη βαθμού συγγένειας έως τρίτου βαθμού με άτομα του εξεταστικού φορέα που συμμετέχουν στη διαδικασία πιστοποίησης
5. Αποδοχή των όρων διαχείρισης προσωπικών δεδομένων
6. Αποδοχή των όρων του εξεταστικού φορέα από τον αιτούντα, όσον αφορά στη διεξαγωγή των εξετάσεων

Η αίτηση που δεν ικανοποιεί στο σύνολο της τα προαπαιτούμενά απορρίπτεται. Στην περίπτωση που διαπιστωθεί οποιοδήποτε πρόβλημα, και πριν τη διεξαγωγή των εξετάσεων, ο υποψήφιος ενημερώνεται για την απόρριψη της αίτησής του. Με σκοπό να αποτραπεί ο αποκλεισμός του υποψηφίου από τις εξετάσεις, ο υποψήφιος, πριν τη διενέργεια των εξετάσεων και μέχρι την λήξη της προθεσμίας για την υποβολή αιτήσεων για συμμετοχή σε εξετάσεις, έχει τη δυνατότητα να προσκομίσει τα ορθά έγγραφα στον εξεταστικό φορέα.

Όλοι οι υποψήφιοι των οποίων οι αιτήσεις έχουν ελεγχθεί και εγκριθεί από τον εξεταστικό φορέα έχουν δικαίωμα συμμετοχής στις εξετάσεις. Δεν υπάρχει κανένας περιορισμός ή προϋπόθεση για τη συμμετοχή στις εξετάσεις, εκτός των προαπαιτήσεων που δύναται να απαιτούνται από το Πλαίσιο.

8.2. Προγραμματισμός Εξετάσεων

Ο εξεταστικός φορέας ανακοινώνει το πρόγραμμα των εξετάσεων είτε μετά τη λήξη της προθεσμίας για την υποβολή αιτήσεων για συμμετοχή σε εξετάσεις από τους ενδιαφερόμενους, είτε σε προκαθορισμένα διαστήματα (σε περίπτωση που δέχεται συνεχώς αιτήσεις συμμετοχής). Κατά τη διαδικασία κατάρτισης του προγράμματος εξετάσεων λαμβάνει υπόψη το πλήθος, τη γεωγραφική κατανομή και τις ειδικές συνθήκες των αιτήσεων.

Ειδικότερα, ο εξεταστικός φορέας συντάσσει αναλυτικό πρόγραμμα εξετάσεων το οποίο περιλαμβάνει πληροφορίες για την εξέταση, όπως την ημερομηνία που θα διεξαχθεί, την τοποθεσία/ χώρο διενέργειας και τη διάρκεια της εξέτασης.

Η ενημέρωση των ενδιαφερόμενων για την ημερομηνία των εξετάσεων γίνεται τουλάχιστον δεκαπέντε (15) μέρες πριν από τη διεξαγωγή τους.

Η ενημέρωση πραγματοποιείται από την επίσημη διαδικτυακή ιστοσελίδα του εξεταστικού φορέα, με αναφορά:

- στο εξεταστικό/ά κέντρο/α Ε.Κ. (διεύθυνση, τηλέφωνο επικοινωνίας, υπεύθυνος επικοινωνίας),
- στην ημερομηνία και ακριβή ώρα εξέτασης,
- σε πληροφορίες σχετικά με ΑμεΑ,
- σε οτιδήποτε άλλο κρίνεται απαραίτητο.

Ο ενδιαφερόμενος θα δικαιούται να αιτηθεί και να διευθετήσει ημερομηνία εξέτασης με το εξεταστικό κέντρο, μετά την ολοκλήρωση της πιο πάνω διαδικασίας.

8.3 Πληροφορίες για τη διαδικασία εξετάσεων Ελεγκτών Κυβερνοασφάλειας

Η επιτυχής ολοκλήρωση των απαιτούμενων εξετάσεων που διεξάγει ο εξεταστικός φορέας παράγει αντίστοιχο πιστοποιητικό επιτυχίας στην εξέταση. Για τη χορήγηση του πιστοποιητικού απαιτείται η επιτυχής ολοκλήρωση των εξετάσεων, με βάση επιτυχίας το **75%**.

Το πιστοποιητικό επιτυχίας στην εξέταση πιστοποιεί ότι ο εξεταζόμενος διαθέτει την απαιτούμενη επάρκεια γνώσεων στα συγκεκριμένα γνωστικά αντικείμενα που καλύπτει το Πλαίσιο και αφορά αποκλειστικά τον εξεταζόμενο στον οποίο χορηγήθηκε.

Ο εξεταστικός φορέας οφείλει να δημοσιοποιεί σε εμφανές σημείο, όπως για παράδειγμα την ιστοσελίδα του, τις πληροφορίες σχετικά με το Πλαίσιο, την ημερομηνία διεξαγωγής της εξέτασης, όλη τη διαδικασία έγκρισης, τα δικαιώματα του αιτούντος και τις υποχρεώσεις ενός εγκεκριμένου ελεγκτή.

Οι υποψήφιοι δύναται να επικοινωνούν με τον εξεταστικό φορέα προκειμένου να ενημερωθούν για οτιδήποτε αφορά στις εξετάσεις και την έκδοση και χορήγηση πιστοποιητικού επιτυχίας στην εξέταση.

Κατά κανόνα, οι εξετάσεις υλοποιούνται σε ηλεκτρονική μορφή, μέσω ηλεκτρονικών υπολογιστών που βρίσκονται στον χώρο του εξεταστικού φορέα, με φυσική παρουσία του υποψηφίου και φυσική επίβλεψη από προσωπικό του εξεταστικού φορέα. Τα θέματα των εξετάσεων επιλέγονται και αποστέλλονται, με ασφαλή τρόπο, απευθείας από τον Διαχειριστή Τράπεζας Θεμάτων Εξέτασης και σύμφωνα με τις προδιαγραφές του παρόντος Πλαισίου. Η συγκεκριμένη διαδικασία μπορεί να γίνεται είτε μέσω σχετικού λογισμικού του Διαχειριστή Τράπεζας Θεμάτων Εξέτασης είτε μέσω διεπαφής του κατάλληλου λογισμικού του εξεταστικού φορέα και του Διαχειριστή Τράπεζας Θεμάτων Εξέτασης.

Κατ' εξαίρεση, και μόνο σε περίπτωση ανωτέρας βίας, οι εξετάσεις δύναται να υλοποιηθούν με συμβατικό τρόπο. Σε αυτήν την περίπτωση ο Διαχειριστής Τράπεζας Θεμάτων Εξέτασης αποστέλλει, με ασφαλή τρόπο, τα θέματα των εξετάσεων στον εξεταστικό φορέα, τα οποία διατηρούνται με ασφάλεια από τον εξεταστικό φορέα και λίγο πριν την έναρξη των εξετάσεων, ο εξεταστικός φορέας οφείλει να τα εκτυπώσει για να δοθούν στους υποψήφιους.

8.4 Εξεταστικό σύστημα

Το εξεταστικό σύστημα του εξεταστικού φορέα βασίζεται στη θεωρητική εξέταση του υποψηφίου μέσω «κλειστού τύπου» ερωτήσεων πολλαπλών επιλογών (multiple choice), οι οποίες επιλέγονται τυχαία από την Τράπεζα Θεμάτων μέσω ψηφιακού συστήματος που διασφαλίζει αφενός την τυχαιότητα της επιλογής των ερωτήσεων και αφετέρου τη διαφορετική σειρά κατάταξης της ορθής απάντησης μεταξύ των επιλέξιμων. Το πλήθος, το είδος των ερωτήσεων και η αναλογία των ερωτήσεων που θα αντλούνται από κάθε Θεματική Ενότητα, θα αναπροσαρμόζονται ώστε να διασφαλίζεται διαρκώς η απαιτούμενη συνέπεια με την εξεταστέα ύλη, όπως αυτή εκάστοτε θα επικαιροποιείται.

Η θεωρητική εξέταση διεξάγεται δια ζώσης, με φυσική παρουσία, στο εξεταστικό κέντρο, υλοποιείται με ηλεκτρονικό τρόπο (πρόσβαση σε ειδική εφαρμογή Η/Υ), όπου δεν απαιτούνται εξεταστές, καθώς η βαθμολόγηση των γραπτών γίνεται αυτόματα από το διαχειριστικό πρόγραμμα του εξεταστικού φορέα. Κατά τη διάρκεια διεξαγωγής των εξετάσεων απαιτείται η ύπαρξη επιτηρητή/ών, για μέγιστο αριθμό δεκαπέντε (15) εξεταζόμενων.

Σε περιπτώσεις ανωτέρας βίας, δύναται οι απαντήσεις των ερωτήσεων να καταγράφονται και σε τετράδιο εξέτασης, όπου αποκρύπτονται τα στοιχεία του υποψηφίου για διασφάλιση της αμεροληψίας και το οποίο βαθμολογείται από εξεταστές. Κατά τη διάρκεια διεξαγωγής των εξετάσεων απαιτείται η φυσική παρουσία επιτηρητή/ών, για μέγιστο αριθμό δεκαπέντε (15) εξεταζόμενων.

Η εξέταση αποτελείται από 65 ερωτήσεις πολλαπλής επιλογής ίδιας βαρύτητας, στις οποίες αντιστοιχεί μία μόνο σωστή απάντηση. Ο υποψήφιος έχει στη διάθεσή του 120 λεπτά (2 ώρες) για να ολοκληρώσει την εξέταση. Τα θέματα εξέτασης συντάσσονται στην ελληνική γλώσσα (με χρήση και ξενόγλωσσων όρων, όπου απαιτείται).

Στο ΠΡΟΣΑΡΤΗΜΑ 3 «ΠΕΡΙΕΧΟΜΕΝΟ ΕΞΕΤΑΣΗΣ ΠΙΣΤΟΠΟΙΗΣΗΣ» παρατίθενται οι λεπτομέρειες σχετικά με την εξέταση, όπως είναι για παράδειγμα τα μέρη στα οποία υποδιαιρείται η εξέταση, το πλήθος των θεμάτων εξέτασης ανά γνωστικό αντικείμενο, ο διαθέσιμος χρόνος υλοποίησης των απαντήσεων σε αυτά, ο βαθμός αξιολόγησης που νοείται ως ελάχιστος για να θεωρηθεί επιτυχής η εξέταση πιστοποίησης κ.ά.. Το εξεταστικό σύστημα που ακολουθεί ο εξεταστικός φορέας πρέπει να διασφαλίζει τα παρακάτω:

- Ακεραιότητα και αξιοπιστία των διενεργούμενων εξετάσεων με τη βοήθεια των επιτηρητών.
- Σωματική ακεραιότητα κάθε εξεταζόμενου μέσω προληπτικών μέτρων ασφαλείας που λαμβάνονται κατά τη διάρκεια διεξαγωγής της εξέτασης, τόσο για τον ίδιον όσο και για τον χώρο που διεξάγεται η εξέταση.
- Δυνατότητα συνεχούς αναβάθμισης των θεμάτων εξέτασης και εμπλουτισμού τους με νέα, όπως αυτά θα ετοιμάζονται από το Διαχειριστή Τράπεζας Θεμάτων Εξέτασης.
- Αποστολή διαφορετικού συνόλου θεμάτων εξέτασης για κάθε εξεταζόμενο ή ομάδα εξεταζόμενων (ανάλογα με τη φύση της πιστοποίησης).
- Αποστολή διαφορετικών θεμάτων εξέτασης απ' αυτά που ανεπιτυχώς εξετάστηκε κάποιος εξεταζόμενος.
- Απ' ευθείας αποστολή των απαντήσεων του εξεταζόμενου στα θέματα εξέτασης, αμέσως μετά την ολοκλήρωση αυτών, μέσω Διαδικτύου, από τον Η/Υ του εξεταζόμενου προς τον κεντρικό διακομιστή εξετάσεων, χωρίς την ενδιάμεση παρεμβολή τρίτου μέρους, διασφαλίζοντας την ασφαλή και κρυπτογραφημένη επικοινωνία. Σε περίπτωση αδυναμίας πρόσβασης στο Διαδίκτυο, στην πρώτη περίπτωση, ο επιτηρητής της εξέτασης πιστοποίησης αναζητά άλλη βιώσιμη σύνδεση με το Διαδίκτυο ώστε να αποστείλει τα κρυπτογραφημένα ηλεκτρονικά αρχεία στον Υπεύθυνο Εξετάσεων Πιστοποίησης του ΕΦ, ενώ (στην εξαιρετική περίπτωση της χρήσης ατομικών τετραδίων εξέτασης) είναι υπεύθυνος για την ασφαλή παράδοση εντός σφραγισμένου

φακέλου των αντίστοιχων έντυπων ατομικών δελτίων αξιολόγησης στον Υπεύθυνο Εξετάσεων του εξεταστικού φορέα.
- Προστασία του κεντρικού διακομιστή εξετάσεων, ο οποίος φυλάσσει τα αποτελέσματα της αξιολόγησης των απαντήσεων/επιδόσεων των εξεταζόμενων.

Σε κάθε περίπτωση, ο εξεταστικός φορέας είναι ανεξάρτητος και αμερόληπτος και φροντίζει για τη διεξαγωγή αξιόπιστων εξετάσεων, είτε αυτές διεξάγονται στις εγκαταστάσεις του είτε σε συνεργαζόμενα εξεταστικά κέντρα. Οι εξετάσεις προγραμματίζονται και διαρθρώνονται κατά τρόπον ώστε να εξασφαλίζεται ότι καλύπτουν τις ελάχιστες δεξιότητες και γνώσεις που προνοούνται στην παρούσα Απόφαση και τα Παραρτήματα αυτής.

8.5. Αξιολόγηση Απαντήσεων/Επιδόσεων

Η αξιολόγηση των απαντήσεων βασίζεται στο τελικό αποτέλεσμα, χωρίς να λαμβάνεται υπόψη ο χρόνος που χρειάστηκε ο υποψήφιος για να απαντήσει σε κάθε ερώτηση, νοουμένου ότι δεν έγινε υπέρβαση του συνολικού χρόνου της εξέτασης. Η βάση επιτυχίας της θεωρητικής εξέτασης είναι η επιτυχής κάλυψη του **75%** της μέγιστης δυνατής βαθμολογίας. Ειδικότερα, επειδή οι εξετάσεις διεξάγονται μέσω ηλεκτρονικής πλατφόρμας και είναι κλειστού τύπου, πολλαπλών επιλογών, το αποτέλεσμα της εξέτασης εξάγεται αυτόματα από την πλατφόρμα. Στην εξαιρετική περίπτωση που για λόγους ανωτέρας βίας οι εξετάσεις δεν δύναται να διεξαχθούν πλήρως ηλεκτρονικά, τότε τα τετράδια απαντήσεων συλλέγονται από τον εξεταστικό φορέα, ο οποίος φροντίζει να εξάγει το τελικό αποτέλεσμα.

Ο κεντρικός διακομιστής(server) εξετάσεων, ο οποίος φυλάσσει τα αποτελέσματα της αξιολόγησης των απαντήσεων/επιδόσεων των εξεταζόμενων, προστατεύεται μέσω της εφαρμογής κατάλληλων τεχνικών και οργανωτικών μέτρων και με δικαίωμα εισόδου μόνο από τα αρμοδίως εξουσιοδοτημένα στελέχη.

Ο εξεταστικός φορέας οφείλει να λαμβάνει όλα τα απαραίτητα μέτρα ασφαλείας έτσι ώστε να εξασφαλίζεται το αδιάβλητο των αξιολογήσεων. Στο πλαίσιο αυτό, διαθέτει διαδικασίες υποβολής εκθέσεων και τηρεί αρχεία για να καταστεί δυνατή η τεκμηρίωση των ατομικών και των συνολικών αποτελεσμάτων της επιτυχίας και να διασφαλίζεται η ιχνηλασιμότητα κάθε απόφασης επιτυχίας. Για τον ίδιο λόγο, θεσπίζει διαδικασίες για την ασφαλή διαχείριση των τεκμηρίων εξέτασης.

Τα τεκμήρια εξέτασης και τα έντυπα / έγγραφα / αρχεία του εξεταστικού μηχανισμού που συγκεντρώνονται μετά από κάθε εξεταστική διαδικασία διασφαλίζουν την ιχνηλασιμότητα και τον συσχετισμό του κάθε εξεταζόμενου υποψηφίου με το αποτέλεσμα της εξέτασης / αξιολόγησής του, προκειμένου να είναι εφικτή η διερεύνηση και ο χειρισμός κάποιου παραπόνου ή ένστασης. Όλα αυτά διατηρούνται για περίοδο έξι (6) χρόνων.

8.6. Έκδοση Αποτελεσμάτων Αξιολόγησης της Εξέτασης

Ο εξεταστικός φορέας υποχρεούται να ανακοινώσει τα αποτελέσματα εντός δεκαπέντε (15) ημερών από την τελευταία ημέρα της εξέτασης. Τα αποτελέσματα για κάθε υποψήφιο ανακοινώνονται γραπτώς και προσωπικά στον υποψήφιο με τη μορφή «επιτυχής εξέταση» ή «όχι επιτυχής εξέταση» (PASS/ FAIL).

Ο εξεταστικός φορέας χορηγεί πιστοποιητικό επιτυχίας στην εξέταση σε κάθε υποψήφιο, σύμφωνα με το οποίο τεκμηριώνεται επιτυχές αποτέλεσμα και ότι δεν υπάρχει κάποιο άλλο κώλυμα (πιθανές αναφορές από τον επιτηρητή κλπ).

Σε κάθε περίπτωση, ο εξεταστικός φορέας οφείλει να λαμβάνει όλα τα απαραίτητα μέτρα για την προστασία των προσωπικών δεδομένων των εξεταζομένων κατά την ανακοίνωση της βαθμολογίας / αποτελεσμάτων των εξετάσεων, σύμφωνα με την ισχύουσα ενωσιακή και εθνική νομοθεσία.

Δεν υπάρχει περιορισμός αναφορικά με τη δυνατότητα συμμετοχής σε εξετάσεις. Οι ενδιαφερόμενοι μπορούν να λάβουν μέρος σε εξετάσεις όσες φορές θέλουν μέχρι να επιτύχουν και καταβάλλοντας το αντίστοιχο ποσό τέλους σε κάθε ξεχωριστή περίπτωση.

8.7 Χορήγηση πιστοποιητικού επιτυχίας στην εξέταση

Το πιστοποιητικό επιτυχίας στην εξέταση που χορηγεί ο εξεταστικός φορέας, πιστοποιεί ότι ο εξεταζόμενος διαθέτει την απαιτούμενη επάρκεια γνώσεων/δεξιοτήτων ή/και ικανοτήτων στα συγκεκριμένα γνωστικά αντικείμενα. Το εν λόγω πιστοποιητικό αφορά αποκλειστικά τον εξεταζόμενο στον οποίο χορηγήθηκε και μόνο για τα γνωστικά αντικείμενα που αυτό καλύπτει.

Για τη χορήγηση του πιστοποιητικού απαιτείται η επιτυχής συμμετοχή στις εξετάσεις, σύμφωνα με την καθορισμένη βάση επιτυχίας. Όλα τα έγγραφα, τα οποία χορηγούνται από τον εξεταστικό φορέα και αποτελούν μέρος της διαδικασίας, αποτελούν ιδιοκτησία του εξεταστικού φορέα.

Ένα πιστοποιητικό εκδίδεται κατόπιν απόφασης του αρμόδιου οργάνου του εξεταστικού φορέα, στο οποίο αναγράφεται η ημερομηνία έκδοσης. Το πιστοποιητικό που εκδίδεται έχει μοναδική αρίθμηση και είναι υπογεγραμμένο από τον Διαχειριστή - Νόμιμο Εκπρόσωπο του εξεταστικού φορέα.

Το εν λόγω πιστοποιητικό αποτελεί απόδειξη του υποψηφίου και πρέπει να επιδεικνύεται κατόπιν οποιασδήποτε σχετικής απαίτησης, όπου αυτό κρίνεται απαραίτητο. Το πιστοποιητικό συνιστά ιδιοκτησία του εξεταστικού φορέα και κατόπιν σχετικής απαίτησης του πρέπει να επιστρέφεται σε αυτόν.

Σύμφωνα με το πρότυπο ISO 17024, τα πιστοποιητικά οφείλουν να περιλαμβάνουν κατ' ελάχιστον τα ακόλουθα στοιχεία:

1. Ονοματεπώνυμο Επιτυχόντος: Το πλήρες όνομα του ατόμου που χορηγήθηκε το πιστοποιητικό.
2. Αριθμός Πιστοποιητικού: Μοναδικό αριθμό αναγνώρισης που αντιστοιχεί στο πιστοποιητικό.
3. Ονομασία Εξεταστικού Φορέα: Το όνομα του εξεταστικού φορέα που χορήγησε το πιστοποιητικό.
4. Αναφορά στο Πλαίσιο Εγγραφής Ελεγκτών Κυβερνοασφάλειας: Αναφορά στον παρόν Πλαίσιο και στην έκδοσή του που ίσχυε κατά την περίοδο χορήγησης του πιστοποιητικού.
4. Πεδίο Εφαρμογής: Την εξής ονομασία της πιστοποίησης «Ελεγκτής Ωριμότητας Κυβερνοασφάλειας»
5. Ημερομηνία Έκδοσης: Την ημερομηνία κατά την οποία εκδόθηκε το πιστοποιητικό.

Προαιρετικά Στοιχεία:
Εκτός από τα απαραίτητα στοιχεία, τα πιστοποιητικά μπορεί να φέρουν και:

- Λογότυπο του Εξεταστικού Φορέα: Το επίσημο λογότυπο του εξεταστικού φορέα που εξέδωσε και χορήγησε το πιστοποιητικό.
- Υπογραφή: Την υπογραφή του αρμόδιου εκπροσώπου του εξεταστικού φορέα.
- Σφραγίδα: Την επίσημη σφραγίδα του εξεταστικού φορέα.
- Στοιχεία Επικοινωνίας: Πληροφορίες επικοινωνίας του εξεταστικού φορέα (π.χ. ιστοσελίδα, διεύθυνση ηλεκτρονικού ταχυδρομείου).

Μέτρα Ασφάλειας:
Για την αποφυγή παραχάραξης, τα πιστοποιητικά δύναται να ενσωματώνουν:

- QR Codes: Κωδικούς QR που οδηγούν σε ηλεκτρονική επαλήθευση της γνησιότητας του πιστοποιητικού.
- Υδατογραφήματα: Ειδικά μοτίβα ενσωματωμένα στο χαρτί του πιστοποιητικού που δύναται να ανιχνευθούν οπτικά.
- Ολογράμματα: Ειδικά αυτοκόλλητα με οπτικά εφέ που δύναται να επαληθεύσουν την αυθεντικότητα του πιστοποιητικού.

Όλες οι πιστοποιήσεις καταχωρούνται στο σχετικό Μητρώο που τηρεί ο εξεταστικός φορέας και το οποίο υποχρεούται να ενημερώνει συστηματικά.

Υπόδειγμα πιστοποιητικού επιτυχίας στην εξέταση παρατίθεται στο ΠΡΟΣΑΡΤΗΜΑ 4**.**

8.8 Διαδικασία Ανανέωσης Πιστοποιητικού

Σύμφωνα με το παρόν Πλαίσιο, ο κάτοχος του πιστοποιητικού επιτυχίας στην εξέταση, που εκδίδεται δυνάμει της παραγράφου 8.7 πιο πάνω, υποχρεούται να επικαιροποιεί τις γνώσεις του στο αντικείμενο της κυβερνοασφάλειας, συμμετέχοντας σε κατάλληλες δράσεις ενημέρωσης και επιμόρφωσης διάρκειας κατ' ελάχιστο 21 ωρών[4], εντός 3 ετών από την αρχική έγκριση. Υπεύθυνη για την υλοποίησή τους είναι η Αρχή. Επιπρόσθετα, θα πρέπει να έχει διενεργήσει τουλάχιστον δύο (2) ολοκληρωμένους ελέγχους με ελάχιστη συνολική διάρκεια δέκα (10) ημερών.

8.9 Προθεσμία Ανανέωσης Πιστοποιητικού

Η προθεσμία ανανέωσης του πιστοποιητικού είναιεντός τριών (3) μηνών πριν την ημερομηνία λήξης ισχύος του πιστοποιητικού επιτυχίας στην εξέταση.

8.10 Έλεγχος Ισχύος/Εγκυρότητας Πιστοποιητικών της Εξέτασης

Όλα τα πιστοποιητικά επιτυχίας στην εξέταση υπόκεινται και σε πιθανή ανάκλησή τους (εφόσον υπάρχουν λόγοι που το επιβάλλουν), σύμφωνα με την Αντικανονική Χρήση Πιστοποιητικών, χάνοντας σ' αυτήν την περίπτωση οριστικά την εγκυρότητά τους. Στην περίπτωση αυτήν ο εξεταστικός φορέας δεν αναλαμβάνει ουδεμία ευθύνη για ενέργειες που υποστηρίχθηκαν από μη έγκυρα πιστοποιητικά που εξέδωσε.

Για τον έλεγχο της εγκυρότητας των πιστοποιητικών επιτυχίας της εξέτασης που έχει χορηγήσει, ο εξεταστικός φορέας έχει δημιουργήσει την υποδομή όπου, με την καταχώρηση του μοναδικού κωδικού που αναγράφεται στο πιστοποιητικό, ενημερώνεται ο κάθε ενδιαφερόμενος για την ισχύ και την εγκυρότητα ή την πλαστότητα του πιστοποιητικού.

[4] Ως ώρα νοείται η διδακτική ώρα – 45 λεπτά.

8.11 Χρήση πιστοποιητικού επιτυχίας στην εξέταση- Υποχρεώσεις

Τα πιστοποιητικά που εκδίδονται και χορηγούνται από τον εξεταστικό φορέα και τα αντίγραφα που προκύπτουν από αυτά δύνανται να χρησιμοποιηθούν μόνο για να αποδεικνύεται το επίπεδο των γνώσεων, δεξιοτήτων και ικανοτήτων του πιστοποιηθέντος προσώπου, όπως αυτό τεκμηριώνεται στο πιστοποιητικό. Τα πιστοποιητικά προορίζονται για κάθε νόμιμη χρήση, κατά την οποία απαιτείται επίσημη απόδειξη πιστοποίησης στο συγκεκριμένο γνωστικό αντικείμενο.

Ο κάτοχος πιστοποιητικού επιτυχίας σε εξέταση υποχρεούται να:

- δηλώνει ότι κατέχει πιστοποιητικό, το οποίο θα προβάλλει μόνο για τα γνωστικά αντικείμενα για τα οποία έχει πιστοποιηθεί,
- μην χρησιμοποιεί το πιστοποιητικό και να μην κάνει οποιαδήποτε δήλωση που αφορά στην πιστοποίηση με τρόπο που μπορεί να εκληφθεί ως παραπλανητικός,
- διακόψει άμεσα κάθε χρήση και αναφορά στο πιστοποιητικό, εάν αυτό ανασταλεί για οποιοδήποτε λόγο,
- επιστρέψει άμεσα στον εξεταστικό φορέα οποιοδήποτε έγγραφο πιστοποίησης εάν το χορηγηθέν πιστοποιητικό ανακληθεί για οποιονδήποτε λόγο,
- επιτηρεί το πιστοποιητικό του στο αντίστοιχο της πιστοποίησης χρονικό διάστημα από την ημερομηνία έκδοσης του, σύμφωνα με τα προβλεπόμενα για τη διαδικασία του εξεταστικού φορέα για την επιτήρηση των πιστοποιητικών, όπως αυτές έχουν κοινοποιηθεί, και
- τηρεί τις απαιτήσεις του παρόντος Πλαισίου.

8.12 Υποχρέωση Ελέγχου του πιστοποιητικού επιτυχίας στην εξέταση

Ο Κυπριακός Οργανισμός Τυποποίησης (CYS) υποχρεούται, συμπληρωματικά με την σχετική και έγκαιρη ενημέρωση του από τον εξεταστικό φορέα, να πραγματοποιεί τους παρακάτω ελέγχους:

- Να ελέγξει την πιθανότητα οριστικής ανάκλησης της ισχύος του, ανατρέχοντας στη σχετική λίστα ανακληθέντων πιστοποιητικών που δημοσιεύει ο αντίστοιχος εξεταστικός φορέας.
- Να ελέγξει το γνωστικό αντικείμενο για το οποίο έχει εκδοθεί το συγκεκριμένο πιστοποιητικό του εξεταστικού φορέα.
- Να ελέγξει την εγκυρότητα του πιστοποιητικού μέσω της καταχώρησης του κωδικού του στο σχετικό εργαλείο/υποδομή που διαθέτει ο εξεταστικός φορέας.
- Να ζητήσει όπως κάθε αντίγραφο του πιστοποιητικού φέρει σφραγίδα ελέγχου του εξεταστικού φορέα.

8.13 Παρεχόμενες Εγγυήσεις - Υποχρεώσεις από τον εξεταστικό φορέα

Με την έκδοση και χορήγηση ενός πιστοποιητικού επιτυχίας στην εξέταση, ο εξεταστικός φορέας εγγυάται:

- την ακρίβεια, κατά τη στιγμή της έκδοσης, όλων των πληροφοριών που περιέχονται σε αυτό, καθώς και την ύπαρξη/εγκυρότητα όλων των στοιχείων που απαιτούνται για την έκδοσή του,

- ότι το πρόσωπο, η ταυτότητα του οποίου βεβαιώνεται σε αυτό, κατά τη στιγμή της έκδοσης κατείχε γνώσεις/δεξιότητες ή/και ικανότητες που αντιστοιχούσαν στα αναγραφόμενα γνωστικά αντικείμενα,

- ότι θα καταβάλει κάθε λογική προσπάθεια ώστε να δημοσιεύονται οι ανακλήσεις (και οι αναστολές χρήσης) πιστοποιητικών του, σύμφωνα πάντα με τους όρους και τις αντίστοιχες εφαρμοζόμενες διαδικασίες του.

8.14 Αντικανονική Χρήση Πιστοποιητικών επιτυχίας στην εξέταση – Ανάκληση – Αναστολή πιστοποιητικού επιτυχίας στην εξέταση

Σε περίπτωση που γίνεται αντικανονική χρήση των πιστοποιητικών επιτυχίας στις εξετάσεις, προβλέπεται ανάκληση ή αναστολή των πιστοποιητικών ανάλογα με την περίπτωση.

Αναστολή πιστοποιητικού αφορά στην προσωρινή απαγόρευση χρήσης του πιστοποιητικού, ενώ η ανάκληση πιστοποιητικού αφορά στην δια παντός απόσυρσή του και τη διαγραφή του κατόχου του από τα μητρώα των κατόχων πιστοποιητικού του εξεταστικού φορέα.

Η ανάκληση πιστοποιητικού λαμβάνει χώρα στις παρακάτω περιπτώσεις:

1. Κατόπιν εξέτασης σχετικής ένστασης, παραπόνου ή καταγγελίας μη συμμόρφωσης με τη διαδικασία εξέτασης, διόρθωσης ή πιστοποίησης που οδηγεί στην απόφαση για την ανάλυση ενός ή περισσοτέρων πιστοποιητικών.
2. Καταγγελία για μη τήρηση των Κανόνων Χρήσης του πιστοποιητικού και όποιες άλλες δεσμεύσεις, εγγράφως, έχει αποδεχτεί το εγκεκριμένο πρόσωπο με την υπογραφή του.
3. Μη συμμόρφωση με όλες τις σχετικές ρυθμίσεις της νομοθεσίας και του συστήματος πιστοποίησης.
4. Ο κάτοχος χρησιμοποιεί το πιστοποιητικό κατά τρόπο που θίγει την υπόληψη του εξεταστικού φορέα.
5. Ο κάτοχος χρησιμοποιεί το πιστοποιητικό για γνωστικά αντικείμενα για τα οποία δεν έχει πιστοποιηθεί.
6. Ο κάτοχος κάνει χρήση του πιστοποιητικού ή μέρος αυτού με τρόπο που δημιουργεί λανθασμένα συμπεράσματα.
7. Ο κάτοχος, κατά την αίτηση συμμετοχής στην εξέταση, είχε υποβάλει στοιχεία που τελικά αποδείχθηκαν παραπλανητικά ή ψευδή.
8. Ο κάτοχος δεν συμμετέχει στη διαδικασία επιτήρησης του πιστοποιητικού.

Η ανάκληση ενός πιστοποιητικού πραγματοποιείται μετά από απόφαση του αρμόδιου οργάνου του εξεταστικού φορέα. Ο κάτοχος του πιστοποιητικού ενημερώνεται εγγράφως για την απόφαση ανάκλησης του πιστοποιητικού και οφείλει να επιστρέψει άμεσα το πιστοποιητικό του στον εξεταστικό φορέα (μαζί με οποιαδήποτε άλλο έγγραφο που πιθανώς τεκμηριώνει την εγκυρότητα της πιστοποίησης). Περαιτέρω, απαγορεύεται να κάνει χρήση και να επικαλείται την εν λόγω πιστοποίηση ή να διανέμει αντίγραφα του ανακληθέντος πιστοποιητικού του.

Η ανάκληση κάθε πιστοποιητικού ανακοινώνεται κατ' ελάχιστο στον ιστότοπο του εξεταστικού φορέα και, όπου απαιτείται, σε μέσα μαζικής ενημέρωσης, έντυπα ή μη.

Η αναστολή του πιστοποιητικού για συγκεκριμένο χρονικό διάστημα μπορεί να λειτουργήσει προειδοποιητικά ή διερευνητικά για τις περιπτώσεις που αναφέρονται στην ανάκληση. Στην περίπτωση αναστολής πιστοποιητικού ακολουθείται η παραπάνω διαδικασία ενημέρωσης του κατόχου του πιστοποιητικού, με την οποία ο κάτοχός του ενημερώνεται επιπλέον για τους λόγους αναστολής, καθώς και τους όρους συμμόρφωσης με τεθείσα προθεσμία ανταπόκρισης από τον κάτοχο του πιστοποιητικού. Στην περίπτωση που δεν υπάρχει ανταπόκριση εκ μέρους του, τότε εκκινεί η διαδικασία ανάκλησης του πιστοποιητικού.

Όταν ανασταλεί το πιστοποιητικό ενός προσώπου, τότε ο κάτοχος του πιστοποιητικού αυτού οφείλει να σταματήσει την περαιτέρω προώθηση της πιστοποίησής του και να συνεργαστεί με τον εξεταστικό φορέα, ώστε να επιλυθούν όλα τα θέματα που οδήγησαν στην αναστολή του πιστοποιητικού.

Οι εξεταστικοί φορείς υποχρεούνται να ενημερώνουν γραπτώς τον Κυπριακό Οργανισμό Τυποποίησης (CYS) για την αναστολή, ανάκληση ή περιορισμό του πεδίου εφαρμογής της πιστοποίησης και αυτός οφείλει αντίστοιχα να διαγράψει μόνιμα ή προσωρινά από το Μητρώο τον κάτοχο του.

9. Δήλωση Εμπιστευτικότητας και Αμεροληψίας

Όλο το προσωπικό, οι συνεργάτες και οι εμπειρογνώμονες του εξεταστικού φορέα που εμπλέκονται άμεσα ή έμμεσα με τον μηχανισμό αξιολόγησης του πλαισίου πιστοποίησης «Ελεγκτή Ωριμότητας Κυβερνοασφάλειας», όπως τα μέλη των Επιτροπών, οι Υπεύθυνοι των Εξεταστικών Κέντρων, οι επιτηρητές, κλπ. δεσμεύονται εγγράφως (με Δήλωση Εμπιστευτικότητας - Αμεροληψίας) ότι κατά την άσκηση των καθηκόντων τους θα παρέχουν εγγυήσεις για την τήρηση της εγκυρότητας, της αξιοπιστίας και της αντικειμενικότητας του εξεταστικού μηχανισμού.

10. Προστασία Προσωπικών Δεδομένων

Οι ενδιαφερόμενοι, κατά τη διαδικασία υποβολής της αίτησης για συμμετοχή στις εξετάσεις, συμπληρώνουν τα προσωπικά τους στοιχεία και ταυτόχρονα επιτρέπουν στον εξεταστικό φορέα να διαχειρίζεται τα δεδομένα αυτά με πλήρη εμπιστευτικότητα και χωρίς να επηρεάζεται η αξιολόγησή τους.

Επιπλέον, με την αίτηση στον Κυπριακό Οργανισμό Τυποποίησης (CYS) για εγγραφή στο Μητρώο Ελεγκτών Κυβερνοασφάλειας, τα προσωπικά στοιχεία του εγκεκριμένου ελεγκτή θα καταχωρηθούν στο Μητρώο Ελεγκτών Κυβερνοασφάλειας και θα είναι διαθέσιμα στον ιστότοπο του Κυπριακό Οργανισμό Τυποποίησης (CYS).

Η συλλογή και επεξεργασία των προσωπικών δεδομένων από τους εξεταστικούς φορείς και τον Κυπριακό Οργανισμό Τυποποίησης (CYS) θα γίνεται σύμφωνα με την εθνική και ενωσιακή νομοθεσία σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Σε κάθε περίπτωση, ο υποψήφιος έχει δικαίωμα να απευθυνθεί στον εξεταστικό φορέα για να κάνει χρήση των δικαιωμάτων «Ενημέρωσης» «Διόρθωσης», «Διαγραφής» και «Πρόσβασης» των άρθρων της εθνικής και ενωσιακής νομοθεσίας, σχετικά με τους όρους και περιορισμούς που περιέχονται στις αντίστοιχες ενημερώσεις τις οποίες έχει λάβει και ενεργητικά αποδεχθεί ο υποψήφιος κατά τη διάρκεια της υποβολής των σχετικών αιτήσεων.

ΠΡΟΣΑΡΤΗΜΑΤΑ

ΠΡΟΣΑΡΤΗΜΑ 1 – ΔΕΟΝΤΟΛΟΓΙΚΟΙ ΚΑΝΟΝΕΣ ΕΠΑΓΓΕΛΜΑΤΟΣ

Ο ελεγκτής που είναι εγγεγραμμένος στο Μητρώο Ελεγκτών Κυβερνοασφάλειας υποχρεούται να τηρεί τους δεοντολογικούς κανόνες του επαγγέλματος ως ακολούθως:

- να ενεργεί επαγγελματικά και ηθικά,
- να επιδιώκει και να αναζητά την αναγνώριση, την ανάπτυξη και το κύρος του επαγγέλματος,
- να ενημερώνει και να μην αποκρύπτει από ελεγχόμενους αλλά και από την Αρχή πιθανά φαινόμενα σύγκρουσης συμφερόντων ή άλλους περιορισμούς που μπορεί να επηρεάσουν την ορθή, αποτελεσματική, ανεξάρτητη και αντικειμενική εκτέλεση του ανατεθειμένου έργου ελέγχου,
- να μην αποκαλύπτει οποιαδήποτε πληροφορία είναι εμπιστευτική, εκτός αν άλλως ορίζεται από τον νόμο ή από συμφωνία με τον/τους εμπλεκόμενο/ους,
- να μην δέχεται οποιασδήποτε μορφής πίεση (χρήματα, δώρα κτλ.) από οποιονδήποτε που θα μπορούσε να επηρεάσει την επαγγελματική του κρίση,
- να είναι δίκαια και επαγγελματική η υπηρεσία του, βασισμένη σε αντικειμενικά κριτήρια,
- να μην δρα κατά τέτοιο τρόπο που θα μπορούσε να επηρεάσει ή να βλάψει τη φήμη της Αρχής, του εξεταστικού φορέα, του Κυπριακού Οργανισμού Τυποποίησης (CYS) ή τη διαδικασία πιστοποίησης και να συνεργάζεται σε κάθε προσπάθεια έρευνας όταν προκύπτει παραβίαση του κώδικα δεοντολογίας,
- να τηρεί πλήρες και αξιόπιστο αρχείο παραπόνων ή ενστάσεων σχετικά με την παροχή υπηρεσίας του,
- να μην έχει οποιαδήποτε επαγγελματική ή/και συμβουλευτική σχέση, σχετικά με τα θέματα που εμπίπτουν με την Απόφαση Κ.Δ.Π. 389/2020, με τον Φορέα τα τελευταία τουλάχιστον τρία (3) χρόνια.

- Κάθε υποψήφιος υπογράφει Υπεύθυνη Δήλωση ότι αποδέχεται και έχει κατανοήσει το παρόν Πλαίσιο και τις πρόνοιες της παρούσας Απόφασης.

ΠΡΟΣΑΡΤΗΜΑ 2 – ΠΡΟΓΡΑΜΜΑ ΕΚΠΑΙΔΕΥΣΗΣ

Εκπαίδευση για τον Ελεγκτή Ωριμότητας Κυβερνοασφάλειας			
Πρόγραμμα Εκπαίδευσης			
Α/Α	**ΑΝΑΛΥΣΗ ΠΕΡΙΕΧΟΜΕΝΟΥ ΕΝΟΤΗΤΩΝ**	**ΔΙΑΡΚΕΙΑ (Διδ. ώρες)**	**Ημέρα**
1.0	**Εισαγωγή** Παρουσίαση του αντικειμένου και του σκοπού της εκπαίδευσης. Γνωριμία των συμμετεχόντων Παρουσίαση των μεθόδων και του τρόπου διενέργειας της εκπαίδευσης.	1	1η
2.1	**LM0: Βασικό νομικό και κανονιστικό πλαίσιο** Η σχετική ευρωπαϊκή οδηγία Η εθνική νομοθεσία – Ιστορική αναδρομή Ισχύουσα εθνική νομοθεσία Πηγές – Σημεία αναζήτησης	1	
2.2	**LM0: Βασικό νομικό και κανονιστικό πλαίσιο** Σημαντικοί όροι και ορισμοί Ανάλυση των βασικών όρων με παραδείγματα	1	
2.3	**LM0: Βασικό νομικό και κανονιστικό πλαίσιο** Κατηγοριοποίηση οντοτήτων Άσκηση 1 Διαφοροποιήσεις ανάμεσα σε Οδηγία NIS1 και Οδηγία NIS2 Υποχρεώσεις Φορέων Άσκηση 2	2	
3.1	**LM1: Η Απόφαση Κ.Δ.Π. 389/2020** Η δομή της Απόφασης Κ.Δ.Π. 389/2020	0,2	
3.2 (a)	**LM1: Η Απόφαση Κ.Δ.Π. 389/2020** Αξιολόγηση κινδύνων Βασικοί όροι και ορισμοί στο αντικείμενο της αξιολόγησης κινδύνων Άσκηση 3 Βασικές απειλές Κριτήρια αξιολόγησης κινδύνων Άσκηση 4 Άσκηση 5	2,6	
Τέλος 1ης ημέρας **Απορίες – διευκρινήσεις**		0,2	
Έναρξη 2ης ημέρας **Απορίες – διευκρινήσεις – σύντομη ανασκόπηση της προηγούμενης μέρας**		0,2	2η
3.2 (b)	**LM1: Η Απόφασης Κ.Δ.Π. 389/2020** Διεργασία για την διαχείριση κινδύνων Ανάλυση των μέτρων RM1, RM2, RM3, RM4, RM5, RM6 Άσκηση 6 Άσκηση 7	2,6	
3.3	**LM1: Η Απόφαση Κ.Δ.Π. 389/2020** Επιχειρησιακή συνέχεια και αντιμετώπιση εκτάκτων συνθηκών Βασικοί όροι και ορισμοί στο αντικείμενο της επιχειρησιακής συνέχειας Ανάλυση των μέτρων BCR1 (Business Impact analysis) Άσκηση 8 Ανάλυση των μέτρων BCR2 Ανάλυση των μέτρων BCR3 Άσκηση 9 Ανάλυση των μέτρων BCR4	4	
3.4	**LM1: Η Απόφαση Κ.Δ.Π. 389/2020** Εφαρμογή πλαισίου Παρουσίαση των 70 μέτρων ασφάλειας Διακυβέρνηση και ρόλοι	1	

Εκπαίδευση για τον Ελεγκτή Ωριμότητας Κυβερνοασφάλειας			
Πρόγραμμα Εκπαίδευσης			
Α/Α	**ΑΝΑΛΥΣΗ ΠΕΡΙΕΧΟΜΕΝΟΥ ΕΝΟΤΗΤΩΝ**	**ΔΙΑΡΚΕΙΑ (Διδ. ώρες)**	**Ημέρα**
	Ο Υπεύθυνος για την ασφάλεια δικτύων και συστημάτων πληροφοριών		
Τέλος 2ης ημέρας **Απορίες – διευκρινήσεις**		0,2	
Έναρξη 3ης ημέρας **Απορίες – διευκρινήσεις – σύντομη ανασκόπηση της προηγούμενης μέρας**		0,2	
3.4	**LM1: Η Απόφαση Κ.Δ.Π. 389/2020** Ανάλυση των μέτρων GOV1 Το European Cybersecurity Skills Framework (ecsf) Άσκηση 10 Ανάλυση των μέτρων EIM1, EIM2, EIM3, EIM4, EIM5, EIM6 Βασικοί όροι και ορισμοί σχετικά με τα περιστατικά ασφαλείας Άσκηση 11	2	
4.1	**LM2: Βασικές αρχές και πρότυπα ελέγχου** Η έννοια του conformity assessment Βασικοί όροι Αρχές τις επιθεώρησης σύμφωνα με το EN ISO 19011:2018 Πρότυπα conformity assessment Άσκηση 12 (a) Άσκηση 12 (b) Άσκηση 12 (c) Άσκηση 12 (d) Άσκηση 12 (e) Εφαρμογή των βασικών αρχών στα πλαίσια του μοντέλου ωριμότητας κυβερνοασφάλειας (cybersecurity maturity model) Περιγραφή ρόλου ελεγκτή και επαγγελματική επάρκεια Δειγματοληψία στα πλαίσια του ελέγχου Άσκηση 13 Άσκηση 14	3,6	3η
5.1	**LM3: Βασικά πρότυπα και άλλες πηγές πληροφοριών ελέγχου** Εισαγωγή στην έννοια του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών Η οικογένεια των προτύπων της διαχείρισης ασφάλειας πληροφοριών Η οικογένεια των προτύπων της διαχείρισης επιχειρησιακής συνέχειας Άλλα πρότυπα και στοιχεία πληροφόρησης Άσκηση 15	2	
Τέλος 3ης ημέρας **Απορίες – διευκρινήσεις**		0,2	
Έναρξη 4ης ημέρας **Απορίες – διευκρινήσεις – σύντομη ανασκόπηση της προηγούμενης μέρας**		0,2	4η
6.1	**LM4: Το Μοντέλο ωριμότητας της Αρχής Ψηφιακής Ασφάλειας** Εισαγωγή στο μοντέλο ωριμότητας κυβερνοασφάλειας (cybersecurity maturity model) Η κλίμακα του μοντέλου ωριμότητας κυβερνοασφάλειας (cybersecurity maturity model) Η δομή του μοντέλου ωριμότητας κυβερνοασφάλειας (cybersecurity maturity model) Άσκηση 16 Άσκηση 17 Άσκηση 18	3	
7.1	**LM5: Διενέργεια και τεκμηρίωση του ελέγχου** Εισαγωγή στην διεργασία της επιθεώρησης σύμφωνα με το ISO 19011 Η διαδικασία διενέργειας των ελέγχων συμμόρφωσης Διαδικασία πιστοποίησης ελεγκτών και εγγραφής στο μητρώο Βοηθητικά έγγραφα για τον έλεγχο: Πλάνο ελέγχου	3,6	

Εκπαίδευση για τον Ελεγκτή Ωριμότητας Κυβερνοασφάλειας			
Πρόγραμμα Εκπαίδευσης			
Α/Α	**ΑΝΑΛΥΣΗ ΠΕΡΙΕΧΟΜΕΝΟΥ ΕΝΟΤΗΤΩΝ**	**ΔΙΑΡΚΕΙΑ (Διδ. ώρες)**	**Ημέρα**
	Διάρκεια ελέγχου Άσκηση 19 Δομή του ελέγχου Οδηγίες για την διενέργεια των ελέγχων Τρόποι συλλογής πληροφοριών		
Τέλος 4ης ημέρας **Απορίες – διευκρινήσεις**		0,2	
Έναρξη 5ης ημέρας **Απορίες – διευκρινήσεις – σύντομη ανασκόπηση της προηγούμενης μέρας**		0,2	5η
7.1	**LM5: Διενέργεια και τεκμηρίωση του ελέγχου** Άσκηση 20 Άσκηση 21 Άσκηση 22 Άσκηση 23 Άσκηση 24 Βοηθητικά έγγραφα για τον έλεγχο: Ερωτηματολόγιο ελέγχου Άσκηση 25 Βοηθητικά έγγραφα για τον έλεγχο: Έκθεση Ελέγχου Άσκηση 26 Βασικές οδηγίες για την συμπεριφορά των ελεγκτών Άσκηση 27	7,6	
Τέλος 5ης ημέρας (τέλος εκπαιδευτικού προγράμματος) **Απορίες – διευκρινήσεις**		0,2	

Ελεγκτής Ωριμότητας Κυβερνοασφάλειας- Πρόγραμμα Εκπαίδευσης	
Σκοπός του εκπαιδευτικού προγράμματος είναι να παρέχει τις γνώσεις και τις δεξιότητες σε επαγγελματίες πληροφορικής και κυβερνοασφάλειας, ώστε να μπορούν να διενεργούν με ελέγχους κυβερνοασφάλειας με τη χρήση του μοντέλου ωριμότητας κυβερνοασφάλειας (cybersecurity maturity model) της Αρχής Ψηφιακής Ασφάλειας.	
Στόχοι του προγράμματος	
Σκοπός 1: Η παροχή γνώσεων σχετικά με το νομικό και κανονιστικό πλαίσιο που διέπει τους ελέγχους ωριμότητας της Αρχής Ψηφιακής Ασφάλειας. Σκοπός 2: Η παρουσίαση της Απόφασης Κ.Δ.Π. 389/2020 και ενημέρωση σχετικά με την Αξιολόγηση Κινδύνων (ΜΕΡΟΣ ΙΙΙ + ΠΑΡΑΡΤΗΜΑ Ι + RM 1-6), την Επιχειρησιακή Συνέχεια και Αντιμετώπιση Έκτακτων Συνθηκών (ΜΕΡΟΣ ΙΙΙ + ΠΑΡΑΡΤΗΜΑ ΙΙ + BCR 1-4) και την Εφαρμογή πλαισίου (ΜΕΡΟΣ IV + ΠΑΡΑΡΤΗΜΑ ΙΙΙ). Σκοπός 3: Η παροχή γνώσεων σχετικά με τις βασικές έννοιες που διέπουν τους ελέγχους, περιλαμβανομένων των αρχών της εμπιστευτικότητας, ηθικής συμπεριφοράς, αντικειμενικότητας και αμεροληψίας / ανεξαρτησίας. Σκοπός 4: Η παρουσίαση των βασικών υποστηρικτικών εγγράφων, όπως είναι διάφορα διεθνή και ευρωπαϊκά πρότυπα, τα οποία θα μπορούσε ένας ελεγκτής κυβερνοασφάλειας με τη χρήση του μοντέλου ωριμότητας κυβερνοασφάλειας (cybersecurity maturity model) της Αρχής Ψηφιακής Ασφάλειας, να συμβουλευτεί για να διευκολύνει τη διενέργεια του ελέγχου. Σκοπός 5: Η παροχή γνώσεων και η εμβάθυνση επί της δομής και του τρόπου λειτουργίας του μοντέλου ωριμότητας κυβερνοασφάλειας (cybersecurity maturity model) της Αρχής Ψηφιακής Ασφάλειας. Η εξάσκηση της κριτικής και συνδυαστικής σκέψης που απαιτείται από έναν ελεγκτή κυβερνοασφάλειας, με την χρήση του μοντέλου ωριμότητας κυβερνοασφάλειας (cybersecurity maturity model) της Αρχής Ψηφιακής Ασφάλειας, κατά τη διενέργεια του ελέγχου. Σκοπός 6: Η παροχή γνώσεων, σε σχέση με την διαδικασία ελέγχου κυβερνοασφάλειας, με τη χρήση του μοντέλου ωριμότητας κυβερνοασφάλειας (cybersecurity maturity model) της Αρχής Ψηφιακής Ασφάλειας και η εμβάθυνση στον τρόπο με τον οποίο τα επιμέρους έγγραφα χρησιμοποιούνται κατά τη διάρκεια του ελέγχου.	
Δομή του προγράμματος σε Ενότητες Μάθησης - Learning Modules (LM)	
Τίτλος προγράμματος:	LM0: Βασικό νομικό και κανονιστικό πλαίσιο
	LM1: Η Απόφαση Κ.Δ.Π. 389/2020
	LM2: Βασικές αρχές και πρότυπα ελέγχου
	LM3: Βασικά πρότυπα και άλλες πηγές πληροφοριών ελέγχου
	LM4: Το μοντέλο ωριμότητας κυβερνοασφάλειας (cybersecurity maturity model) της Αρχής Ψηφιακής Ασφάλειας
	LM5: Διενέργεια και τεκμηρίωση του ελέγχου

ΠΡΟΣΑΡΤΗΜΑ 3 - ΠΕΡΙΕΧΟΜΕΝΟ ΕΞΕΤΑΣΗΣ ΠΙΣΤΟΠΟΙΗΣΗΣ

Το περιεχόμενο εξέτασης πιστοποίησης βασίζεται στο επαγγελματικό περίγραμμα του ελεγκτή κυβερνοασφάλειας.

1. Θεματολογία - Περιεχόμενο Εξέτασης

Στη θεματολογία του Ελεγκτή Κυβερνοασφάλειας περιλαμβάνονται οι ακόλουθες ενότητες:
0: Το βασικό νομικό και κανονιστικό πλαίσιο
1: Η Απόφαση Κ.Δ.Π. 389/2020
2: Οι βασικές αρχές και τα πρότυπα ελέγχου
3: Τα βασικά πρότυπα και άλλες πηγές πληροφοριών ελέγχου
4: Το μοντέλο ωριμότητας κυβερνοασφάλειας
5: Η διενέργεια και τεκμηρίωση του ελέγχου

Η συνολική διάρκεια της εξέτασης διαφαίνεται στον ακόλουθο Πίνακα:

	Διάρκεια Θεωρητικής εξέτασης	Αριθμός ερωτήσεων Θεωρητικής εξέτασης
Ελεγκτής Κυβερνοασφάλειας	120 λεπτά (2 ώρες)	65

Πίνακας 1. Ελεγκτής Κυβερνοασφάλειας

Η εξέταση καλύπτει θεματικές ενότητες σύμφωνα με το σχήμα εξέτασης (Πίνακας 1) και αποτελείται αντίστοιχα από 65 ερωτήσεις πολλαπλής επιλογής, στις οποίες αντιστοιχεί μία μόνο σωστή απάντηση. Ο υποψήφιος έχει στη διάθεσή του 120 λεπτά για να ολοκληρώσει την εξέταση.

Παρών στη διαδικασία αυτή είναι ένας επιτηρητής. Οι ενότητες της εξεταστέας ύλης της θεωρητικής εξέτασης κοινοποιούνται στους υποψηφίους μετά την υποβολή αίτησης για συμμετοχή στις εξετάσεις, τον σχετικό έλεγχο και έγκριση της αίτησης και μόνον εφόσον ο υποψήφιος έχει εξοφλήσει το κόστος της εξέτασης. Προτείνεται οι υποψήφιοι να έχουν στα χέρια τους τις ενότητες της εξεταστέας ύλης τουλάχιστον τρεις (3) εβδομάδες πριν τη θεωρητική εξέταση, προκειμένου να προετοιμαστούν.

Προκειμένου να αποφεύγεται η επανάληψη των ίδιων θεμάτων στις εξετάσεις, κάθε Ομάδα – Δεξαμενή ερωτήσεων επιδιώκεται να περιέχει τουλάχιστον τέσσερις φορές περισσότερα ερωτήματα από αυτά που συνολικά απαιτούνται στην εξέταση. Επιπλέον, ο αριθμός ερωτήσεων διαρκώς εμπλουτίζεται. Η επιλογή των ερωτημάτων γίνεται με τυχαίο τρόπο, με το εργαλείο δειγματοληψίας/ επιλογής, σύμφωνα με συγκεκριμένη διαδικασία.

ΠΡΟΣΑΡΤΗΜΑ 4 - ΥΠΟΔΕΙΓΜΑ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ ΕΠΙΤΥΧΙΑΣ ΣΤΗΝ ΕΞΕΤΑΣΗ

ΠΙΣΤΟΠΟΙΗΤΙΚΟ ΕΠΙΤΥΧΙΑΣ ΣΤΗΝ ΕΞΕΤΑΣΗ

Στο πλαίσιο του συστήματος του/της _____ (Εξεταστικός Φορέας) κατά το διεθνές πρότυπο ISO/IEC 17024 και της Κατευθυντήριας Οδηγίας για την Ανάπτυξη και Αναγνώριση Σχημάτων Πιστοποίησης Προσώπων-Συμμόρφωση με τις απαιτήσεις του ISO/IEC 17024,

Ο/η _____- (Εξεταστικός Φορέας) πιστοποιεί ότι ο/η

_____ (Ονοματεπώνυμο)

Έχει επιτύχει στις εξετάσεις του
Ελεγκτή Κυβερνοασφάλειας

Το παρόν πιστοποιητικό χορηγείται μετά από επιτυχή διαδικασία εξέτασης, σύμφωνα με το Πλαίσιο εγγραφής ελεγκτών κυβερνοασφάλειας.

Το παρόν πιστοποιητικό δεν είναι αρκετό για τη διενέργεια ελέγχων ωριμότητας κυβερνοασφάλειας που διενεργούνται σύμφωνα με τη νομοθεσία της Αρχής Ψηφιακής Ασφάλειας.

Η τρέχουσα κατάσταση εγκεκριμένων ελεγκτών μπορεί να αναζητηθεί στο σχετικό μητρώο που διατηρεί ο Κυπριακός Οργανισμός Τυποποίησης (CYS).

Το πιστοποιητικό είναι αυστηρά προσωπικό και δεν αποδεικνύει ότι ο κάτοχός του διαθέτει όλα τα προαπαιτούμενα για την αναγνώρισή του ως Ελεγκτή Κυβερνοασφάλειας.

Αρ. Πιστοποιητικού : _____
Ημερομηνία έκδοσης: _____
Ημερομηνία λήξης: _____

_____ (Ονοματεπώνυμο)
Γενικός Διευθυντής / Διευθυντής Εξεταστικού Φορέα

Το Πλαίσιο εγγραφής ελεγκτών κυβερνοασφάλειας έχει αναπτυχθεί και διατηρείται από το_____
Το παρόν πιστοποιητικό εκδίδεται από τον / την _____ (Εξεταστικός Φορέας) και αποτελεί ιδιοκτησία του/της.
Έδρα: _____
Υπεύθυνος επικοινωνίας: _____ Τηλέφωνο επικοινωνίας.: _____ Διεύθυνση ηλεκτρονικού ταχυδρομείου (email):_____

Πιστοποιητικό που κυκλοφορεί και διακινείται στην αγορά και δεν είναι σύμφωνο με το παραπάνω πρότυπο πρέπει να κοινοποιείται στον εξεταστικό φορέα, προκειμένου να ληφθούν τα απαραίτητα μέτρα. Σε περίπτωση που υφίσταται λόγος, συστήνεται η εγκυρότητα και η ισχύς των πιστοποιητικών να ελέγχεται μέσω επικοινωνίας με τον εξεταστικό φορέα.

ΠΑΡΑΡΤΗΜΑ Ζ: ΕΝΤΥΠΟ ΥΠΟΒΟΛΗΣ ΠΑΡΑΠΟΝΩΝ / ΚΑΤΑΓΓΕΛΙΩΝ / ΕΝΣΤΑΣΕΩΝ

1. Προϋποθέσεις Υποβολής Παραπόνου/Καταγγελίας/Ένστασης:
α) Πριν από την υποβολή παραπόνου/καταγγελίας/ένστασης προς την Αρχή, ο παραπονούμενος οφείλει να απευθυνθεί εγγράφως στο πρόσωπο εναντίον του οποίου στρέφεται το παράπονο/ καταγγελία/ ένσταση, για επίλυση της διαφοράς που έχει προκύψει. Ο παραπονούμενος υποβάλλει παράπονο προς την Αρχή, μόνο σε περίπτωση που το πρόσωπο εναντίον του οποίου στρέφεται το παράπονο/ καταγγελία/ ένσταση δεν απαντήσει εντός προθεσμίας δεκαπέντε (15) ημερών από την ημερομηνία υποβολής παραπόνου ή δεν είναι ικανοποιημένος από την απάντηή του.

β) Παράπονα/καταγγελίες/ενστάσεις υποβάλλονται επώνυμα και περιλαμβάνουν όλα τα απαραίτητα στοιχεία που στοιχειοθετούν το παράπονο/καταγγελία/ένσταση, συμπεριλαμβανομένης και της σχετικής αλληλογραφίας που έχει προηγηθεί με το πρόσωπο εναντίον του οποίου στρέφεται το παράπονο/ καταγγελία/ ένσταση.

γ) Η Αρχή υποχρεούται να αποστέλλει αντίγραφο του παραπόνου/καταγγελίας/ένστασης προς το πρόσωπο εναντίον του οποίου στρέφεται το παράπονο/ καταγγελία/ ένσταση.

δ) Η συμπλήρωση όλων των πεδίων του εντύπου είναι υποχρεωτική.

2. Όροι υποβολής Παραπόνου/Καταγγελίας/Ένστασης:
α) Η Αρχή χειρίζεται καθηκόντως παράπονα/καταγγελίες/ενστάσεις που εμπίπτουν στο πεδίο των αρμοδιοτήτων που της παρέχει η ισχύουσα νομοθεσία στον τομέα της ασφάλειας δικτύων και συστημάτων πληροφοριών.

β) Ως εκ τούτου, η Αρχή, ως νομικό πρόσωπο, καθώς και τα στελέχη της Αρχής, δεν φέρουν οποιαδήποτε αστική ή ποινική ευθύνη για οποιαδήποτε υλική ή ηθική απώλεια είναι δυνατό να προκύψει κατά ή μετά τη διαχείριση παραπόνου/καταγγελίας/ένστασης.

γ) Η υποβολή παραπόνου/καταγγελίας/ένστασης δεν αίρει την δυνατότητα δικαστικής επίλυσης των διαφορών, για την απαίτηση αποκατάστασης οποιασδήποτε απώλειας ή βλάβης (υλικής ή ηθικής) από τους ελεγκτές και οι παραπονούμενοι Φορείς οφείλουν να απευθύνονται στα αρμόδια δικαστήρια.

δ) Κάθε παράπονο / καταγγελία / ένσταση λαμβάνει μοναδικό αριθμό.

1. ΣΤΟΙΧΕΙΑ ΠΑΡΑΠΟΝΟΥΜΕΝΟΥ
ΟΝΟΜΑ:
ΑΡ. ΜΗΤΡΩΟΥ ΕΛΕΓΚΤΗ[5]:
ΔΙΕΥΘΥΝΣΗ ΗΛΕΚΤΡΟΝΙΚΟΥ ΤΑΧΥΔΡΟΜΕΙΟΥ:
ΤΗΛΕΦΩΝΟ ΕΠΙΚΟΙΝΩΝΙΑΣ:
ΗΜΕΡΟΜΗΝΙΑ ΔΙΕΝΕΡΓΕΙΑΣ ΕΛΕΓΧΟΥ[6]:
ΗΜΕΡΟΜΗΝΙΑ ΛΗΞΗΣ ΕΛΕΓΧΟΥ[7]:

2. ΣΤΟΙΧΕΙΑ ΦΟΡΕΑ Ή ΕΛΕΓΚΤΗ ΩΡΙΜΟΤΗΤΑΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ, ΚΑΤΑ ΤΟΥ ΟΠΟΙΟΥ ΣΤΡΕΦΕΤΑΙ ΤΟ ΠΑΡΑΠΟΝΟ
ΟΝΟΜΑ:
ΑΡ. ΜΗΤΡΩΟΥ ΕΛΕΓΚΤΗ:

[5] Συμπληρώνεται μόνο στην περίπτωση που το παράπονο το υποβάλλει ελεγκτής.

[6] Συμπληρώνεται μόνο στην περίπτωση που το παράπονο το υποβάλλει ελεγκτής.

[7] Συμπληρώνεται μόνο στην περίπτωση που το παράπονο το υποβάλλει ελεγκτής.

ΗΜΕΡΟΜΗΝΙΑ ΔΙΕΝΕΡΓΕΙΑΣ ΕΛΕΓΧΟΥ:
ΗΜΕΡΟΜΗΝΙΑ ΛΗΞΗΣ ΕΛΕΓΧΟΥ:

3. ΣΥΝΟΠΤΙΚΗ ΠΕΡΙΓΡΑΦΗ ΠΑΡΑΠΟΝΟΥ
*Εάν υπάρχουν σχετικά αποδεικτικά έγγραφα είναι απαραίτητο να επισυναφθούν

4. ΕΠΙΚΟΙΝΩΝΙΑ ΤΟΥ ΠΑΡΑΠΟΝΟΥΜΕΝΟΥ ΜΕ ΤΟ ΠΡΟΣΩΠΟ ΕΝΑΝΤΙΟΝ ΤΟΥ ΟΠΟΙΟΥ ΣΤΡΕΦΕΤΑΙ ΤΟ ΠΑΡΑΠΟΝΟ/ ΚΑΤΑΓΓΕΛΙΑ/ ΕΝΣΤΑΣΗ ΚΑΙ ΑΛΛΕΣ ΕΝΕΡΓΕΙΕΣ ΠΟΥ ΕΓΙΝΑΝ
* Απαραίτητη η επισύναψη του εγγράφου/αλληλογραφίας με τον ελεγκτή.

5. ΣΧΕΤΙΚΑ ΕΓΓΡΑΦΑ ΚΑΙ ΣΤΟΙΧΕΙΑ ΠΟΥ ΣΤΟΙΧΕΙΟΘΕΤΟΥΝ ΤΟ ΠΑΡΑΠΟΝΟ
* Απαραίτητη η επισύναψη όλων των σχετικών εγγράφων που στοιχειοθετούν το παράπονο

6. ΘΕΡΑΠΕΙΑ ΠΟΥ ΑΙΤΕΙΤΑΙ Ο ΠΑΡΑΠΟΝΟΥΜΕΝΟΣ
* Συμπληρώστε εδώ.

ΑΙΤΙΟΛΟΓΙΚΗ ΕΚΘΕΣΗ

Σύμφωνα με τα άρθρα 17(ιζ), 17(ιη), 17(ιθ), 17(κβ), 17(κγ), 17(κστ), 19, 20(1)(α), 20(1)(β), 20(1)(γ), 20(1)(δ), 20(1)(ε), 21, 35(1), 35(2), 36, 37(1), 37(2), 37(3), 37(4), 38, 39, 40(1), 40(9), 43, 46 και 54 του Νόμου, η Αρχή Ψηφιακής Ασφάλειας εκδίδει την Απόφαση σχετικά με τη Διαδικασία Διενέργειας Ελέγχων Ωριμότητας Κυβερνοασφάλειας.

Η Απόφαση θεσμοθετεί και πραγματεύεται τις επιμέρους ενέργειες που διενεργούνται από τους Φορείς στο πλαίσιο του σχεδιασμού, της υλοποίησης και της ολοκλήρωσης των ελέγχων επί του συστήματος διαβάθμισης ωριμότητας. Σκοπός της παρούσας Απόφασης είναι η αναγνώριση του επιπέδου ωριμότητας των Φορέων έναντι των απαιτήσεων της Απόφασης Κ.Δ.Π. 389/2020, η ενημέρωση της Αρχής σχετικά με το επίπεδο ωριμότητας των Φορέων και ο καθορισμός πλάνου ενεργειών από τους Φορείς για την συμμόρφωσή τους σύμφωνα με τις πρόνοιες της Απόφασης Κ.Δ.Π. 389/2020 για τη βελτίωση του επιπέδου ασφαλείας των δικτύων και συστημάτων πληροφοριών τους.

Περαιτέρω, σκοπός των ελέγχων είναι η συστηματική, ανεξάρτητη και τεκμηριωμένη αναγνώριση του επιπέδου διαβάθμισης ωριμότητας των Φορέων έναντι των απαιτήσεων του ΠΑΡΑΡΤΗΜΑΤΟΣ ΙΙΙ της Απόφασης Κ.Δ.Π. 389/2020, ο προσδιορισμός των περιπτώσεων (ανά μέτρο ασφαλείας) που η συμμόρφωση του Φορέα είναι σε επίπεδο μικρότερο από τις σχετικές επιταγές της νομοθεσίας (μικρότερο του 3), ο προσδιορισμός των περιπτώσεων (ανά μέτρο ασφαλείας) που η συμμόρφωση του Φορέα είναι σε επίπεδο υψηλότερο από τις σχετικές επιταγές της νομοθεσίας (τουλάχιστον 3) και η ενημέρωση των Φορέων μέσω της παράδοσης της σχετικής Έκθεσης Ελέγχου Ωριμότητας Κυβερνοασφάλειας η οποία θα κοινοποιείται και στην Αρχή από τον ελεγκτή.