Κ.Δ.Π ……/2024

Ο ΠΕΡΙ ΑΣΦΑΛΕΙΑΣ ΔΙΚΤΥΩΝ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ ΝΟΜΟΣ 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 του Νόμου 89(Ι)/2020

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 και στα Παραρτήματα 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 είναι οχτώ (8) ώρες περιλαμβανομένων διαλειμμάτων (ενός 30 συνεχόμενων λεπτών και ενός 15 συνεχόμενων λεπτών ή με κάποιο άλλο 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 επιτήρηση 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) το 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 την δυνατότητα πρόσβασης την 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 στην Συμφωνία ο Φορέας·

«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 αρμόδιος 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·

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 υπεύθυνο 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 των απαιτήσεων του ΠΑΡΑΡΤΗΜΑΤΟΣ ΙΙΙ της Απόφασης Κ.Δ.Π. 389/2020 και μια αντιστοίχισή τους προς διακριτά επίπεδα ωριμότητας για το κάθε μέτρο ασφάλειας·

89(Ι)/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·

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

«συνολικός αριθμός εργαζομένων» σημαίνει το σύνολο των ατόμων του Φορέα που εμπλέκονται άμεσα στο πεδίο εφαρμογής του ελέγχου. Για τον υπολογισμό του συνολικού αριθμό των εργαζομένων δεν λαμβάνεται υπόψη ο τρόπος εργοδότησης και μετρώνται εργαζόμενοι που διενεργούν εργασία στα πλαίσια 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 καιρό 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 και στα Παραρτήματα 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 ασφαλείας 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 εκδηλώθηκαν 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 οποιοδήποτε Φορέα, ανεξάρτητα με το χρονικό διάστημα ολοκλήρωσης του προηγούμενου ελέγχου.

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 τους, που περιλαμβάνουν τουλάχιστον τα εξής:

(α) Το 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.

(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 το χρόνο ελέγχου, σύμφωνα με το οριζόμενα στο ΠΑΡΑΡΤΗΜΑ Α:

Νοείται ότι, ο Φορέας σε συνεννόηση με τον επικεφαλής ελεγκτή επαναϋπολογίζει και συμφωνεί το χρόνο διάρκειας 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.

(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 οποιαδήποτε πληροφορία και έγγραφα του ζητηθεί και είναι σχετική 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 έλεγχο τους και εξουσιοδοτημένο μέλος του προσωπικού της Αρχής για το χειρισμό διαβαθμισμένων πληροφοριών/εγγράφων.

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 ολοκλήρωση 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 οι οποίοι πρέπει να 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 περισσότερους ελεγκτές από έναν εάν είναι φυσικό πρόσωπο ή στην περίπτωση που η συμφωνία συναφθεί με νομικό πρόσωπο θα πρέπει να αναφέρονται σε αυτήν όλοι οι ελεγκτές και 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 στην 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.

Περιεχόμενο συμφωνίας.

15. Η Σύμβαση 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 ένα (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) το πλάνο ελέγχου, που 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 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· και

(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.

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.

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 το 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 προσκομίσει ο Φορέας.

(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 συνάντησης 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 εκπρόσωποι 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.

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/είσοδος στις ελεγχόμενες εγκαταστάσεις και η πρόσβαση/είσοδος στις εγκαταστάσεις που δραστηριοποιείται ο Φορέας πραγματοποιείται χωρίς περιττές καθυστερήσεις.

(2) Ο/οι ελεγκτής/ές κατά την άφιξη 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 δεν διαρκεί περισσότερο από 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 τη Κ.Δ.Π. 389/2020 συνοδευόμενες με 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 ελεγκτής

(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 ελεγκτής, 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 ελεγκτής, 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 συνάντησης, στην οποία θα ζητηθεί και υπογραφή της σχετικής Έκθεσης Ελέγχου Ωριμότητας Κυβερνοασφάλειας από εκπρόσωπο της ανώτατης της 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, ο ελεγκτής υποχρεούται να συνεννοηθεί με τον εκπρόσωπο του Φορέα για τη 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, την στρατηγική, το πελατολόγιο, την πολιτική μισθοδοσίας του προσωπικού του Φορέα:

Νοείται περαιτέρω ότι, εάν οι πληροφορίες που προνοούνται στην πρώτη επιφύλαξη της παρούσας παραγράφου, ο ελεγκτής δύναται να τις ζητά εάν υποστηρίζουν την κάλυψη κάποια 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 ι συνεντεύξεις, παρακολούθησης διεργασιών και δραστηριοτήτων, παρατήρησης 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, να εξασφαλίζει, στο μέγιστο βαθμό, ότι η πληροφορία που ελέγχει είναι:

(i) πλήρης, δηλαδή 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 να επιβεβαιώνει, στο 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 συγκρίνονται προς τις απαιτήσεις του κάθε επιπέδου, με σκοπό να εξεταστεί κατά πόσο υπάρχει πλήρη 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, τότε 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 πλήρης 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 του Φορέα, ακόμη και στις περιπτώσεις που είναι άριστα καταρτισμένος ή πιστοποιημένος ή/και κατάλληλα εκπαιδευμένος:

Νοείται ότι, σε εξαιρετικές περίπτωση που ο ελεγκτής ζητήσει παρέμβαση σε πληροφοριακό εξοπλισμό θα γίνεται μόνο στη παρουσία του εκπροσώπου του Φορέα.

Ολοκλήρωση του ελέγχου και ετοιμασία της Έκθεσης Ελέγχου Ωριμότητας Κυβερνοασφάλειας.

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 την 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 ο επικεφαλής ελεγκτής, υποχρεούται να επισημαίνει τις αποκλίσεις που υπάρχουν από την επίτευξη του επόμενου επιπέδου ωριμότητας.

(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 Έκθεση 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 υποχρεούνται να συμμετέχουν εκπρόσωποι της 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 διασφάλισης 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 διασφάλισης 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. Σε αντίθετη περίπτωση, 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 διοίκησης του Φορέα την Έκθεση Ελέγχου Ωριμότητας Κυβερνοασφάλειας και ο εκπρόσωπος της 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 εκ μέρους του ελεγκτή και ότι ο Φορέας δεν συμμορφώνεται με τις υποχρεώσεις του, ως αυτές προνοούνται στο Νόμο και στη δυνάμει αυτού εκδοθείσα νομοθεσία.

(2) Ο ελεγκτής ή ο επικεφαλής ελεγκτής, υποχρεούται να κοινοποιεί στην Αρχή αντίγραφο της υπογεγραμμένης, από τον Φορέα και τον ελεγκτή ή τον επικεφαλής ελεγκτή, Έκθεσης Ελέγχου Ωριμότητας Κυβερνοασφάλειας του Φορέα και να την ενημερώνει 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 Φορέας και να ζητήσει αναθεώρηση τους.

(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 κυβερνοασφάλειας.

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 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 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 να 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 την 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 άλλες 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 στα πλαίσια 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 στα πλαίσια διενέργειας των ελέγχων·

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

(θ) γνωρίζει και μπορεί να αναγνωρίσει και να ανακαλέσει τις σχετικές νομικές και κανονιστικές απαιτήσεις στα πλαίσια διενέργειας των ελέγχων.

(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 Διαχείριση τρίτων μερών και προμηθευτών

(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

Προσόντα και επαγγελματική εμπειρία ελεγκτή.

29. Ο ελεγκτής υποχρεούται να διαθέτει τα προσόντα και την επαγγελματική πείρα ως αυτά περιγράφονται στο 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) παραδίδει αντίγραφο της υπογεγραμμένης Έκθεσης Ελέγχου Ωριμότητας Κυβερνοασφάλειας στην Αρχή·

(θ) προστατεύει την ακεραιότητα, διαθεσιμότητα και εμπιστευτικότητα των σχετικών αρχείων ελέγχου κατά την 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) να 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

32. (1) Για να ενταχθεί κάποιος στο Μητρώο Ελεγκτών Κυβερνοασφάλειας προ απαιτείται να κατέχει όσα προνοούνται στο Κεφάλαιο V της παρούσας Απόφασης και να ακολουθήσει τα

Μητρώο στο Μητρώο Ελεγκτών Κυβερνοασφάλειας.

βήματα που προνοούνται στο ΠΑΡΑΡΤΗΜΑ ΣΤ «Πλαίσιο εγγραφής ελεγκτών κυβερνοασφάλειας».

Κεφάλαιο VII – Υποβολή και διαχείριση παραπόνων, καταγγελιών και ενστάσεων

Υποβολή Παραπόνων, Καταγγελιών και Ενστάσεων.

33. (1) Ο Φορέας και ο ελεγκτής ή ο επικεφαλής ελεγκτής δύναται να υποβάλλουν παράπονο, καταγγελία και ένσταση στην Αρχή ηλεκτρονικά σε συγκεκριμένη πλατφόρμα που θα θέσει σε λειτουργία προς το σκοπό αυτό 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.

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 το παράπονο, η καταγγελία και η ένσταση, 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.

(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 το 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 Απόφαση 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 αποτελέσουν 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/ η καταγγελίας/ η ένστασης.

(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 από οποιοδήποτε 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 αντικτύπου 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 απόδειξης 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 ενώπιον της, μετά από την διενέργεια του ελέγχου, να εκδίδει 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 Απόφασης, 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 ζημία που προκλήθηκε στην Αρχή και θα την επωμιστεί.

ΜΕΡΟΣ III
Τελικές Διατάξεις

Τροποποιήσεις.

38. Η Αρχή δύναται με Απόφαση της να καταργεί/αντικαθιστά, τροποποιεί ή/και να συμπληρώνει την παρούσα Απόφαση, τα Παραρτήματα και τα Προσαρτήματα 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 τις ακριβείς απαιτήσεις 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 κρισιμότητα του Φορέα

4. Προσδιορισμός των σημείων στα οποία θα διενεργηθεί ο έλεγχος. Ο έλεγχος δύναται να διενεργηθεί σε μια ή σε περισσότερες φυσικές τοποθεσίες.

5. Προσδιορισμός της τεχνικής πολυπλοκότητας του πεδίου εφαρμογής του ελέγχου.

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 Φορές 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>ΠΡΟΔΙΑΓΕΓΡΑΜΜΕΝΗ ΕΛΑΧΙΣΤΗ ΔΙΑΡΚΕΙΑ ΕΛΕΓΧΟΥ</td><td colspan="2"></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 ελεγκτής) 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.	

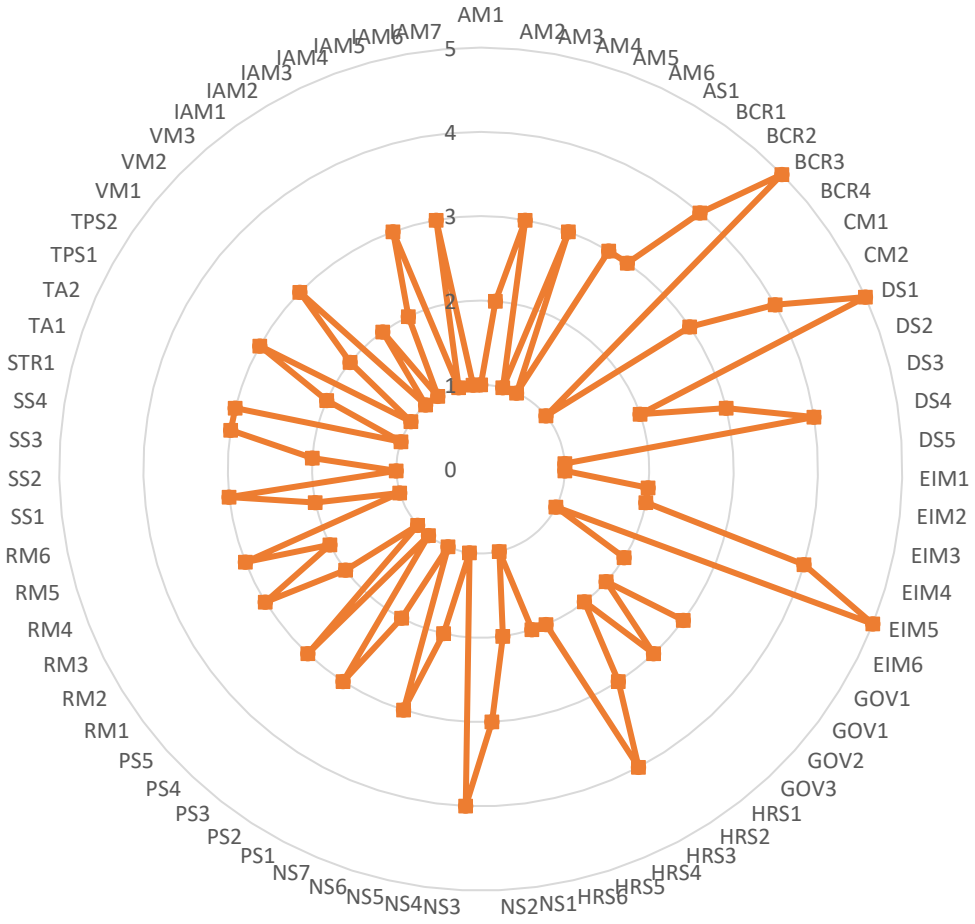
ΕΚΘΕΣΗ ΕΛΕΓΧΟΥ ΩΡΙΜΟΤΗΤΑΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ[1]		
	Σχόλια σχετικά με την απόκλιση από την προγραμματισμένη διάρκεια ελέγχου	[Παραδείγματα] - *Ο Φορέας έχει εντάξει εντός του πεδίου εφαρμογής ένα σύνολο νέων συστημάτων που δεν είχαν ελεγχθεί σε προηγούμενους ελέγχους με αποτέλεσμα να απαιτηθεί 0,5 ημέρες 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 την διενέργεια του ελέγχου.
	☐	Κατά τη διάρκεια του ελέγχου προέκυψαν τα ακόλουθα, τα οποία είχαν δυσμενή επίδραση στην 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 οργανισμού 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	

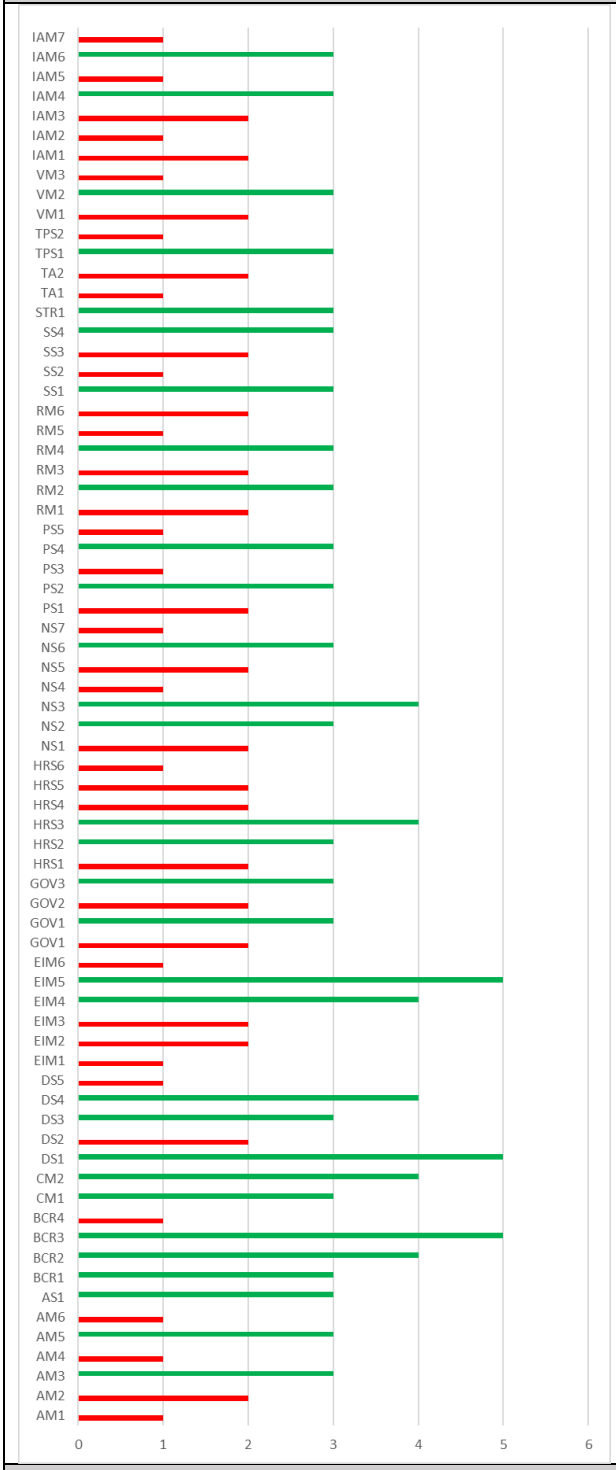
Επιτευχθέν Επίπεδο ωριμότητας κυβερνοασφάλειας ανά απαίτηση (σε γραφική παράσταση Radar)

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 την 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, 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 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 Φορέα. Ο ρόλος του ιδιοκτήτη κινδύνων ορίζεται και περιγράφονται οι ρόλοι και οι αρμοδιότητές τους σε σχέση με την διαχείρισης 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 την 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) Ονοματεπώνυμο: Υπογραφή:	Ελεγκτής 2 Ονοματεπώνυμο: Υπογραφή:	Ελεγκτής 3 Ονοματεπώνυμο: Υπογραφή:	Ελεγκτής 4 Ονοματεπώνυμο: Υπογραφή:
Εκπρόσωπος Διοίκησης του Φορέα Ονοματεπώνυμο: Υπογραφή:			

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 την 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 αυτή 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 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 την 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 να γίνει ο σχετικός υπολογισμός, ο ελεγκτής μπορεί να έχει εξάγει από πριν ένα 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,
- προηγουμένως 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

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 την 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 οι 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 ζημίες, να υπονομεύσουν την εμπιστοσύνη των χρηστών και να προκαλέσουν σημαντική ζημία στην οικονομία της χώρας ή και της Ευρωπαϊκής Ένωσης (ανάλογα με το περιστατικό, την έκταση και την 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.

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

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

την Ένωση, στο 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 στην 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 3(γ) του άρθρου 16 της Απόφασης Κ.Δ.Π. 389/2020 προχώρησε στην δημιουργία ενός μοντέλου ωριμότητας κυβερνοασφάλειας (cybersecurity maturity model), με σκοπό την εξειδίκευση των απαιτήσεων της Απόφασης Κ.Δ.Π. 389/2020 και μια αντιστοίχιση 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 στον πυλώνα 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 αυτό-αξιολόγησης 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 συμμόρφωση 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·
παρέχει ένα 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 το Νόμο 89(I)/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(I)/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 αρμοδιότητα 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(I)/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 ωριμότητα 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 μια 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 το 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 καθώς και για την αποτελεσματική αξιολόγηση της κυβερνοασφάλειας στους Φορείς απαιτείται να έχουν συγκεκριμένες γνώσεις και δεξιότητες.

Για το σκοπό αυτό, 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 και δεξιότητες 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 το ρόλο του Διαχειριστή Τράπεζας Θεμάτων Εξέτασης, σε Οργανισμό, ο οποίος θα φέρει την ευθύνη για τα ακόλουθα:

- Την Διαχείριση: Οργάνωση, αποθήκευση και ασφαλής 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 την 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 την σχετική εντολή της Αρχής.

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

- Κρυπτογράφηση: Εφαρμογή ισχυρών αλγορίθμων 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 οποιαδήποτε 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 στοιχείαστον Κυπριακό Οργανισμό Τυποποίησης (CYS).
- Το Πιστοποιητικό επιτυχίας στην εξέταση θα πρέπει να έχει ληφθεί εντός 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 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 σε 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 τηλεματική 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 Ασφαλείας 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) 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. γ) Σε περίπτωση απουσίας του πιστοποιητικού 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 άλλο 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 επιτήρηση του είναι επιτυχής τότε η κατάσταση του στο Μητρώο Ελεγκτών Κυβερνοασφάλειας θα αλλάζει από δόκιμο (junior) σε εγκριμένο 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 αίτηση του, μαζί με τα απαραίτητα έγκυρα (και όπου χρειάζεται πστοποιημένα) έγγραφα/δικαιολογητικά, στα γραφεία του Κυπριακού Οργανισμού Τυποποίησης (CYS) είτε ταχυδρομικώς, είτε μέσω ηλεκτρονικού ταχυδρομείου και με τρόπο που διασφαλίζει την επιτυχή παράδοση του, 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 συμμόρφωση 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 αυτή, 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 συνεννόησής 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 έκδοσης 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 στους 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: Κατέχουν αποδεδειγμένη διδακτική εμπειρία άνω των 100 ωρών στο αντικείμενο της κυβερνοασφάλειας.

Γνώσεις:

- 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 θέματα 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.
- Διαθέτουν πενταετή τουλάχιστον πρακτική εμπειρία στον χώρο της πληροφορικής και της κυβερνοασφάλειας.

Εκπαίδευση:

- 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 αντιπρόσωπο 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, πατρώνυμο, 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, δύναται σε συγκεκριμένο σημείο της αίτησης, ο εξεταστικός φορέας να δίνει τη δυνατότητα στον υποψήφιο να επιλέγει τη χρονική περίοδο και το εξεταστικό κέντρο στο οποίο επιθυμεί να συμμετέχει για τη διαδικασία των εξετάσεων.
- Ειδικές συνθήκες που πρέπει να ληφθούν υπόψη για την ασφαλή και ισότιμη συμμετοχή του υποψηφίου στις εξετάσεις, όπως για παράδειγμα 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 και υπογραφή υποψηφίου.
- 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 τα ακόλουθα:

1. Έλεγχος των πεδίων υποχρεωτικής συμπλήρωσης
2. Ταυτοποίηση στοιχείων αίτησης και προσκομισθέντων εγγράφων/δικαιολογητικών

3. Ύπαρξη ιδιόχειρης υπογραφής
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 την διεξαγωγή των εξετάσεων

Η αίτηση που δεν ικανοποιεί, στο σύνολο της, τα προ απαιτούμενά απορρίπτεται. Στην περίπτωση που διαπιστωθεί οποιοδήποτε πρόβλημα, και πριν τη διεξαγωγή των εξετάσεων, ο υποψήφιος ενημερώνεται για την απόρριψη της αίτησης 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 προ απαιτήσεων 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 την διαδικασία κατάρτισης του προγράμματος εξετάσεων λαμβάνει υπόψη το πλήθος, τη γεωγραφική κατανομή και τις ειδικές συνθήκες των αιτήσεων.

Ειδικότερα, ο εξεταστικός φορέας συντάσσεται 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 του κοινού 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.

8.3 Πληροφορίες για την 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 τις εξετάσεις και την έκδοση και χορήγησης πιστοποιητικού επιτυχίας στην εξέταση.

Κατά κανόνα οι εξετάσεις υλοποιούνται σε ηλεκτρονική μορφή, μέσω ηλεκτρονικών υπολογιστών που βρίσκονται στο 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 αυτή την περίπτωση ο Διαχειριστής Τράπεζας Θεμάτων Εξέτασης αποστέλνει, με ασφαλή τρόπο, τα θέματα των εξετάσεων στον εξεταστικό φορέα, τα οποία διατηρούνται με ασφάλεια από τον εξεταστικό φορέα και λίγη ώρα πριν την έναρξη των εξετάσεων, ο εξεταστικός φορέας οφείλει να τα εκτυπώσει για να τα δώσει 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 ύπαρξη 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 την 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 το συσχετισμό του κάθε εξεταζόμενου υποψηφίου με το

αποτέλεσμα της εξέτασης / αξιολόγησης 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 κόλλημα (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, πιστοποιούν 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 αρμοδίου 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 υποψήφιου 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: Μοναδικός αριθμός 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 έκδοση του που ίσχυε κατά την περίοδο χορήγησης του πιστοποιητικού.
4. Πεδίο Εφαρμογής: Η εξής ονομασία της πιστοποίησης «Ελεγκτής Ωριμότητας Κυβερνοασφάλειας»
5. Ημερομηνία Έκδοσης: Η 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: Η υπογραφή του αρμόδιου εκπροσώπου του εξεταστικού φορέα.
- Σφραγίδα: Η 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: Κωδικοί 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 3**.**

8.8 Διαδικασία Επιτήρησης Πιστοποιητικών

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[3], εντός 3 ετών από την αρχική έγκριση. Υπεύθυνη για την υλοποίηση τους είναι η Αρχή. Επιπρόσθετα, θα πρέπει να έχει διενεργήσει τουλάχιστον δύο (2) ολοκληρωμένους ελέγχους με ελάχιστη συνολική διάρκεια δέκα (10) ημερών.

8.9 Διαδικασία Ανανέωσης της έγκρισης

Η Διαδικασία Ανανέωσης της έγκρισης θα πρέπει να γίνει εντός 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 ανάκληση τους (εφόσον υπάρχουν λόγοι που το επιβάλλουν), σύμφωνα με την Αντικανονική Χρήση Πιστοποιητικών χάνοντας σ' αυτήν την περίπτωση οριστικά την εγκυρότητά τους. Στην περίπτωση αυτή 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.

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 την 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 οποιοδήποτε 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 φορέα
- 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 φορέα.
- Να ζητήσει όπως κάθε αντίγραφο του πιστοποιητικού να 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.

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

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 απόσυρση 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 για 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 να 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.
9. Την αναφορά του πιστοποιητικού για απόδειξη γνώσεων/δεξιοτήτων ή/και ικανοτήτων εκτός του πεδίου του παρόντος Πλαισίου.

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 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 κάτοχος του πιστοποιητικού 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 της ανάκλησης του πιστοποιητικού.

Όταν ανασταλεί το πιστοποιητικό ενός προσώπου, τότε ο κάτοχος του πιστοποιητικού αυτού οφείλει να σταματήσει την περαιτέρω προώθηση της πιστοποίησης 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 το μηχανισμό αξιολόγησης του πλαίσιο 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 στο 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 το 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 Ο Υπεύθυνος για την ασφάλεια δικτύων και συστημάτων πληροφοριών	1	

Εκπαίδευση για τον Ελεγκτή Ωριμότητας Κυβερνοασφάλειας			
Πρόγραμμα Εκπαίδευσης			
Α/Α	**ΑΝΑΛΥΣΗ ΠΕΡΙΕΧΟΜΕΝΟΥ ΕΝΟΤΗΤΩΝ**	**ΔΙΑΡΚΕΙΑ (Διδ. ώρες)**	**Ημέρα**
Τέλος 2ης ημέρας **Απορίες – διευκρινήσεις**		0,2	
Έναρξη 3ης ημέρας **Απορίες – διευκρινήσεις – σύντομη ανασκόπηση της προηγούμενης μέρας**		0,2	3η
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	
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 πληροφόρηση 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 Διάρκεια ελέγχου Άσκηση 19 Δομή του ελέγχου Οδηγίες για την διενέργεια των ελέγχων Τρόποι συλλογής πληροφοριών	3,6	

Εκπαίδευση για τον Ελεγκτή Ωριμότητας Κυβερνοασφάλειας			
Πρόγραμμα Εκπαίδευσης			
Α/Α	**ΑΝΑΛΥΣΗ ΠΕΡΙΕΧΟΜΕΝΟΥ ΕΝΟΤΗΤΩΝ**	**ΔΙΑΡΚΕΙΑ (Διδ. ώρες)**	**Ημέρα**
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 την 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 Εκτάκτων Συνθηκών (ΜΕΡΟΣ ΙΙΙ + ΠΑΡΑΡΤΗΜΑ ΙΙ + BCR 1-4) και την Εφαρμογή πλαισίου (ΜΕΡΟΣ ΙV + 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 λειτουργία 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 την 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 - 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)

του

._____(Πατρώνυμο)

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 την 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 αναγνώριση 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.

ΠΡΟΣΑΡΤΗΜΑ 4 - 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 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:

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

Πίνακας 1. Ελεγκτή 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, κοινοποιείται 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 εξεταστές 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.

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 απάντηση 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, οι παραπονούμενοι Φορείς οφείλουν να απευθύνονται στα αρμόδια δικαστήρια.

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

1. ΣΤΟΙΧΕΙΑ ΠΑΡΑΠΟΝΟΥΜΕΝΟΥ
ΟΝΟΜΑ:
ΑΡ. ΜΗΤΡΩΟΥ ΕΛΕΓΚΤΗ[4]:
ΔΙΕΥΘΥΝΣΗ ΗΛΕΚΤΡΟΝΙΚΟΥ ΤΑΧΥΔΡΟΜΕΙΟΥ:
ΤΗΛΕΦΩΝΟ ΕΠΙΚΟΙΝΩΝΙΑΣ:
ΗΜΕΡΟΜΗΝΙΑ ΔΙΕΝΕΡΓΕΙΑΣ ΕΛΕΓΧΟΥ[5]:
ΗΜΕΡΟΜΗΝΙΑ ΛΗΞΗΣ ΕΛΕΓΧΟΥ[6]:

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

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

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.

Αιτιολογική Έκθεση

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 στα πλαίσια 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 συμμόρφωση 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 οργανισμού είναι σε επίπεδο μικρότερο από τις σχετικές επιταγές της νομοθεσίας (μικρότερο του 3), ο προσδιορισμός των περιπτώσεων (ανά μέτρο ασφαλείας) που η συμμόρφωση του οργανισμού είναι σε επίπεδο υψηλότερο από τις σχετικές επιταγές της νομοθεσίας (τουλάχιστον 3) και η ενημέρωση των ελεγχόμενων οργανισμών μέσω της παράδοσης της σχετικής Έκθεσης Ελέγχου Ωριμότητας Κυβερνοασφάλειας, η οποία θα κοινοποιείται και στην Αρχή από τον ελεγκτή.