

Περιγραφή	Ελεγκτής Ωριμότητας Κυβερνοασφάλειας (Cybersecurity Maturity Auditor)
Σύνοψη	Διενεργεί ελέγχους κυβερνοασφάλειας με την χρήση του Μοντέλου Ωριμότητας Κυβερνοασφάλειας της Αρχής Ψηφιακής Ασφάλειας Κύπρου.
Αποστολή	<p>Διεξάγει ανεξάρτητους ελέγχους επί του Μοντέλου Ωριμότητας Κυβερνοασφάλειας (Cybersecurity Maturity Model) της Αρχής Ψηφιακής Ασφάλειας Κύπρου, το οποίο είναι δομημένο και καλύπτει τις απαιτήσεις του Παραρτήματος III: Πλαίσιο μέτρων ασφαλείας της περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών (Μέτρα Ασφάλειας Φορέων Εκμετάλλευσης Βασικών Υπηρεσιών και Φορέων Κρίσιμων Υποδομών Πληροφοριών) Απόφασης του 2020 (Κ.Δ.Π. 389/2020).</p> <p>Ο σκοπός των ελέγχων είναι η συστηματική, ανεξάρτητη και τεκμηριωμένη</p> <ul style="list-style-type: none"> - αναγνώριση του επιπέδου διαβάθμισης ωριμότητας των ελεγχόμενων οργανισμών έναντι των απαιτήσεων του παραρτήματος III της Κ.Δ.Π. 389/2020, - προσδιορισμός των περιπτώσεων (ανά μέτρο ασφαλείας) που η συμμόρφωση του οργανισμού είναι σε επίπεδο μικρότερο από τις σχετικές επιταγές της νομοθεσίας (μικρότερο του 3) - 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 Ψηφιακής Ασφάλειας.
Παραδοτέα	<ul style="list-style-type: none"> - Πλάνο (schedule) του εκάστοτε ανατεθειμένου ελέγχου (σύμφωνα με το χρονοδιάγραμμα που προβλέπει η Διαδικασία Διεξαγωγής Ελέγχων Ωριμότητας Κυβερνοασφάλειας) - Συμπληρωμένο το Ερωτηματολόγιο του Μοντέλου Ωριμότητας Κυβερνοασφάλειας για τον κάθε υλοποιημένο έλεγχο - Συμπληρωμένη Έκθεση Ελέγχου Ωριμότητας Κυβερνοασφάλειας για τον κάθε υλοποιημένο έλεγχο
Κύρια Καθήκοντα	<ul style="list-style-type: none"> - Διενεργεί επικοινωνία με τους Φορείς σχετικά με τις αναθέσεις ελέγχων ωριμότητας κυβερνοασφάλειας σύμφωνα με τις απαιτήσεις του Παραρτήματος III της Κ.Δ.Π. 389/2020 με σκοπό τον προγραμματισμό και προετοιμασία για τον εκάστοτε έλεγχο. - Επικουρεί την Αρχή Ψηφιακής Ασφάλειας στον καλύτερο προσδιορισμό της διάρκειας του ανατεθειμένου ελέγχου σε περίπτωση που χρειαστεί. - Δημιουργεί, επικοινωνεί στον ελεγχόμενο οργανισμό και ακολουθεί πλάνο ελέγχου (σύμφωνα με το χρονοδιάγραμμα που προβλέπει η Διαδικασία Διεξαγωγής Ελέγχων Ωριμότητας Κυβερνοασφάλειας) για κάθε περίπτωση ανατεθειμένου ελέγχου. - Ακολουθεί τις βέλτιστες πρακτικές ελέγχου, τις προδιαγραφές της Διαδικασία Διεξαγωγής Ελέγχων Ωριμότητας Κυβερνοασφάλειας, τις σχετικές νομικές, κανονιστικές και

Περιγραφή	Ελεγκτής Ωριμότητας Κυβερνοασφάλειας (Cybersecurity Maturity Auditor)
	<p>συμβατικές απαιτήσεις κατά τη διάρκεια διεξαγωγής του ελέγχου.</p> <ul style="list-style-type: none"> - Ανασκοπεί αντικειμενικές αποδείξεις για κάθε επιτεύξιμο επίπεδο ωριμότητας των ελεγχόμενων οργανισμών και τις καταγράφει στον κατάλληλο χώρο εντός του ερωτηματολογίου ελέγχου. - Συγκρίνει τις αντικειμενικές αποδείξεις με τις απαιτήσεις ανά επίπεδο ανά μέτρο και εξάγει ανεξάρτητα και αντικειμενικά αποτελέσματα σχετικά με το μέγιστο επίπεδο που έχει επιτύχει ανά περίπτωση ο κάθε ελεγχόμενος οργανισμός. - Συντάσσει Έκθεση Ελέγχου Ωριμότητας Κυβερνοασφάλειας ακολουθώντας τη Διαδικασία Διεξαγωγής Ελέγχων Ωριμότητας Κυβερνοασφάλειας, την παραδίδει στον ελεγχόμενο οργανισμό και λαμβάνει την επιβεβαίωση από αυτόν. Παραδίδει αντίγραφο της τελικής έκδοσης Έκθεσης Ελέγχου Ωριμότητας Κυβερνοασφάλειας στην Αρχή Ψηφιακής Ασφάλειας. - Προστατεύει την ακεραιότητα, διαθεσιμότητα και εμπιστευτικότητα των σχετικών αρχείων ελέγχου κατά τη διάρκεια του ελέγχου. Καταστρέφει με ασφάλεια τα αρχεία, μετά την σχετική ενημέρωση από την Αρχή Ψηφιακής Ασφάλειας. - Βρίσκεται στη διάθεση της Αρχής Ψηφιακής Ασφάλειας και του ελεγχόμενου οργανισμού για πιθανές διευκρινήσεις επί των διενεργηθέντων ελέγχων. - Τηρεί τις συμβατικές υποχρεώσεις σε σχέση με την ηθική, την εχεμύθεια και την επαγγελματική συμπεριφορά κατά τη διάρκεια των ελέγχων και μετά το πέρας αυτών (όπως προκύπτει από τις σχετικές συμβάσεις). - Τηρεί ενεργή ασφάλεια Επαγγελματικής Ευθύνης (Professional Indemnity insurance) ή/και Ασφάλεια Σφαλμάτων και Παραλείψεων (Errors and Omissions insurance) (περιλαμβανομένων και των προβλεπόμενων μέτρων), αποζημίωση ύψους όπως προβλέπεται στη σχετική νομοθεσία.
Βασικές Δεξιότητες	<ul style="list-style-type: none"> - Ακολουθεί και να εφαρμόζει βέλτιστες πρακτικές για την διενέργεια ελέγχων και την Διαδικασία Διεξαγωγής Ελέγχων Ωριμότητας Κυβερνοασφάλειας. - Εφαρμόζει σχήμα δειγματοληψίας κατά την κατάρτιση του πλάνου δειγματοληψίας ανά μέτρο ασφαλείας. - Εξηγεί (στο εμπλεκόμενο προσωπικό του ελέγχου) τις απαιτήσεις και τον τρόπο λειτουργίας του Μοντέλου Ωριμότητας Κυβερνοασφάλειας - Οργανώνει και εργάζεται στα πλαίσια του ελέγχου με συστηματικό και ανεξάρτητο τρόπο - Αναγνωρίζει τις πηγές πληροφοριών που μπορεί να αποτελέσουν αντικειμενικές αποδείξεις του ελέγχου και τις ανασκοπεί με κατάλληλο τρόπο - Συγκρίνει τις αντικειμενικές αποδείξεις προς τις απαιτήσεις και εξάγει αντικειμενικά συμπεράσματα

Περιγραφή	Ελεγκτής Ωριμότητας Κυβερνοασφάλειας (Cybersecurity Maturity Auditor)		
	<ul style="list-style-type: none"> - Διενεργεί τους ελέγχους με ακεραιότητα, αμεροληψία και ανεξαρτησία - Εκφράζει αποτελεσματικά τα συμπεράσματα του ελέγχου προφορικά και γραπτά - Καταγράφει με απλό και κατανοητό τρόπο τις αντικειμενικές αποδείξεις και το επίπεδο διαβάθμισης ωριμότητας που έχει επιτευχθεί. - Ικανότητα χρήσης ηλεκτρονικών υπολογιστών και ιδιαίτερα προγραμμάτων όπως το Microsoft Office (Word, Excel, PowerPoint etc.). - Ακεραιότητα χαρακτήρα, εχεμύθεια, οργανωτική και διοικητική ικανότητα, πρωτοβουλία, υπευθυνότητα, ευθυκρισία και ικανότητα αποτελεσματικής συνεργασίας. 		
Βασική Γνώση	<ul style="list-style-type: none"> - Γνωρίζει και μπορεί να ανακαλέσει γνώσεις σχετικά με τα μέτρα και τις λύσεις κυβερνοασφάλειας που συνδέονται με τα μέτρα του Παραρτήματος III της Κ.Δ.Π. 389/2020. - Καταλαβαίνει και μπορεί να ερμηνεύσει πως συγκεκριμένη πληροφορία συνδέεται με τις απαιτήσεις των μέτρων του Παραρτήματος III της Κ.Δ.Π. 389/2020. - Καταλαβαίνει και μπορεί να εξηγήσει την σύνδεση συγκεκριμένων λειτουργιών πληροφορικής και ασφάλειας με τις απαιτήσεις των μέτρων του Παραρτήματος III της Κ.Δ.Π. 389/2020. - Γνωρίζει και μπορεί να ανακαλέσει γνώσεις σχετικά με την σχετική αποτελεσματικότητα των μέτρων ασφαλείας και ειδικά αυτών του Παραρτήματος III της Κ.Δ.Π. 389/2020. - Καταλαβαίνει, μπορεί να συγκρίνει και να εξηγήσει τεχνικές και μεθόδους για την ανασκόπηση αντικειμενικών αποδείξεων στα πλαίσια των ελέγχων. - Καταλαβαίνει, μπορεί να συγκρίνει και να εξηγήσει την αξία, τα μειονεκτήματα, τις επιλογές και τον τρόπο επιλογής σχήματος δειγματοληψίας στα μέτρα ασφαλείας για την ανασκόπηση αντικειμενικών αποδείξεων στα πλαίσια των ελέγχων. - Καταλαβαίνει τις έννοιες της συστηματικότητας, ανεξαρτησίας, αμεροληψίας, αντικειμενικότητας και τεκμηρίωσης στα πλαίσια των ελέγχων. - Γνωρίζει, μπορεί να αναγνωρίσει και να ανακαλέσει τις σχετικές νομικές και κανονιστικές απαιτήσεις. <p>Ενδεικτικές ενότητες μέτρων, στις οποίες ο ελεγκτής απαιτείται να έχει γνώσεις:</p> <table style="width: 100%; border: none;"> <tr> <td style="width: 50%; vertical-align: top;"> <ul style="list-style-type: none"> - Αξιολόγηση Κινδύνων - Ασφάλεια ανθρώπινων πόρων - Ασφάλεια δεδομένων - Ασφάλεια δικτύου - Ασφάλεια εφαρμογών - Ασφάλεια συστημάτων - Διακυβέρνηση - Διαχείριση αλλαγών </td> <td style="width: 50%; vertical-align: top;"> <ul style="list-style-type: none"> - Διαχείριση ταυτότητας και πρόσβασης - Διαχείριση τρίτων μερών και προμηθευτών - Επιχειρησιακή συνέχεια και ανθεκτικότητα - Επιχειρησιακή Συνέχεια και Αντιμετώπιση Εκτάκτων Συνθηκών - Ευαισθητοποίηση και εκπαίδευση </td> </tr> </table>	<ul style="list-style-type: none"> - Αξιολόγηση Κινδύνων - Ασφάλεια ανθρώπινων πόρων - Ασφάλεια δεδομένων - Ασφάλεια δικτύου - Ασφάλεια εφαρμογών - Ασφάλεια συστημάτων - Διακυβέρνηση - Διαχείριση αλλαγών 	<ul style="list-style-type: none"> - Διαχείριση ταυτότητας και πρόσβασης - Διαχείριση τρίτων μερών και προμηθευτών - Επιχειρησιακή συνέχεια και ανθεκτικότητα - Επιχειρησιακή Συνέχεια και Αντιμετώπιση Εκτάκτων Συνθηκών - Ευαισθητοποίηση και εκπαίδευση
<ul style="list-style-type: none"> - Αξιολόγηση Κινδύνων - Ασφάλεια ανθρώπινων πόρων - Ασφάλεια δεδομένων - Ασφάλεια δικτύου - Ασφάλεια εφαρμογών - Ασφάλεια συστημάτων - Διακυβέρνηση - Διαχείριση αλλαγών 	<ul style="list-style-type: none"> - Διαχείριση ταυτότητας και πρόσβασης - Διαχείριση τρίτων μερών και προμηθευτών - Επιχειρησιακή συνέχεια και ανθεκτικότητα - Επιχειρησιακή Συνέχεια και Αντιμετώπιση Εκτάκτων Συνθηκών - Ευαισθητοποίηση και εκπαίδευση 		

Περιγραφή	Ελεγκτής Ωριμότητας Κυβερνοασφάλειας (Cybersecurity Maturity Auditor)
	<ul style="list-style-type: none"> - Διαχείριση ευπαθειών και ενημερώσεων ασφάλειας - Διαχείριση κινδύνων - Διαχείριση στοιχείων ενεργητικού - Διαχείριση συμβάντων και περιστατικών - Εφαρμογή Συστήματος/Πλαισίου Διαχείρισης Ασφάλειας- Εφαρμογή Τεχνικών και Οργανωτικών Μέτρων - Καταγραφή και παροχή Πληροφοριών - Στρατηγική - Φυσική ασφάλεια
Εκπαιδευτικά Προσόντα	<p>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 όπως:</p> <p>Επιστήμη 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), Πληροφορικής, Πληροφορικής και Τηλεπικοινωνιών, Ηλεκτρολόγου Μηχανικού & Μηχανικού Υπολογιστών, Εφαρμοσμένης Πληροφορικής, Ηλεκτρολόγου Μηχανικού & Τεχνολογίας Υπολογιστών, Μηχανικού Η/Υ και Πληροφορικής, Επιστήμης Υπολογιστών, Ηλεκτρονικού και Μηχανικού Υπολογιστών, Μηχανικών Πληροφοριακών & Επικοινωνιακών Συστημάτων, Μηχανικών Η/Υ Τηλεπικοινωνιών και Δικτύων, Επιστήμης και Τεχνολογίας Υπολογιστών, Επιστήμης και Τεχνολογίας Τηλεπικοινωνιών, Διδακτικής της Τεχνολογίας και Ψηφιακών Συστημάτων, Επιστημών και Πολιτισμού – Κατεύθυνση Η/Υ (Π.Σ.Ε.), Πληροφορική στην Εκπαίδευση, Electronic Systems Engineering, Telematics (Communications with software), Τεχνολογίες διαδικτύου και ασφάλεια, Ψηφιακών Συστημάτων, Διοίκησης επιχειρήσεων και πληροφοριακών συστημάτων, Θεμελιώσεις Πληροφορικής και Εφαρμογές, Πληροφοριακά συστήματα, Εξειδίκευση στα πληροφοριακά συστήματα, Μηχανική Λογισμικού για διαδικτυακές & φορητές εφαρμογές, πληροφορικής και τηλεματική, Μικροηλεκτρονική, Επιστήμης και Τεχνολογίας Υπολογιστών, Ολοκληρωμένα συστήματα υλικού και λογισμικού, Συστήματα Επεξεργασίας Σημάτων και επικοινωνιών, Επιστήμης Υπολογιστών, Ηλεκτρονικού Μηχανικού και Μηχανικού Υπολογιστών, Πληροφοριακά συστήματα και ψηφιακή καινοτομία, Κυβερνοασφάλεια και Επιστήμη Δεδομένων, Ανάπτυξη και ασφάλεια πληροφοριακών συστημάτων, Προηγμένες Τεχνολογίες Πληροφορικής, Επιστήμη και Μηχανική Δεδομένων, Ηλεκτρολογική Μηχανική, Εφαρμοσμένη Πληροφορική.</p> <p>Ο όρος Πανεπιστημιακός τίτλος καλύπτει και μεταπτυχιακό τίτλο.</p> <p>Σε περίπτωση απουσίας σχετικού τίτλου σπουδών όπως αναφέρονται πιο πάνω, γίνονται δεκτοί και άλλοι απόφοιτοι Πανεπιστημίου με άλλους τίτλους σπουδών με την προϋπόθεση ότι η επαγγελματική εμπειρία, που καταγράφεται στην ενότητα Επαγγελματική Εμπειρία, αντίστοιχα μετατρέπεται ως εξής:</p>

Περιγραφή	Ελεγκτής Ωριμότητας Κυβερνοασφάλειας (Cybersecurity Maturity Auditor)
	<ul style="list-style-type: none"> - Δεκαετής 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.) <p>Πολύ καλή γνώση της Ελληνικής γλώσσας (σημείωση η Έκθεση Ελέγχου Ωριμότητας Κυβερνοασφάλειας θα είναι στην Ελληνική Γλώσσα). Πολύ καλή γνώση της Αγγλικής γλώσσας Εκπαίδευση 40 ωρών στο αντικείμενο «Ελεγκτές Ωριμότητας Κυβερνοασφάλειας σύμφωνα με το παράρτημα ΙΙΙ της Κ.Δ.Π. 389/2020». Πιστοποίηση/Επαναπιστοποίηση ως Ελεγκτής Ωριμότητας Κυβερνοασφάλειας σύμφωνα με το παράρτημα ΙΙΙ της Κ.Δ.Π. 389/2020 Ενεργή περίληψη του στο Μητρώο Ελεγκτών Κυβερνοασφάλειας.</p>
Επαγγελματική Πείρα	<ul style="list-style-type: none"> - Απαιτείται τουλάχιστον 4 χρόνια πλήρους απασχόλησης εργασιακή εμπειρία στον τομέα της Τεχνολογίας Πληροφοριών, εκ των οποίων τουλάχιστον 2 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.) - Απαιτείται ενεργό πιστοποιητικό ISO27001-Lead Auditor και τουλάχιστον τρεις (3) έλεγχοι τρίτου μέρους (third party audits) συνολικής διάρκειας 20 ημερών, που διενεργήθηκαν τα τελευταία πέντε (5) χρόνια. Η διάρκεια θα ελέγχεται από log book ή βεβαίωση που θα προσκομεί ο υποψήφιος, υπογεγραμμένη από φορέα πιστοποίησης. - Σε περίπτωση απουσίας του πιστοποιητικού ή/και της διάρκειας ελέγχων αν ο υποψήφιος επιτύχει στις εξετάσεις θα καταχωρείται στο Μητρώο ως εκπαιδευόμενος Ελεγκτής Ωριμότητας Κυβερνοασφάλειας και οφείλει να συνοδεύσει και να παρακολουθήσει δύο (2) ολοκληρωμένους ελέγχους με ελάχιστη συνολική διάρκεια δέκα (10) ημερών, από πιστοποιημένο Ελεγκτή Ωριμότητας Κυβερνοασφάλειας (βλ. Υποχρεώσεις πιο κάτω). Ακολούθως θα αλλάζει η κατάστασή του στο Μητρώο από εκπαιδευόμενος σε δόκιμο (junior) Ελεγκτή Ωριμότητας

Περιγραφή	Ελεγκτής Ωριμότητας Κυβερνοασφάλειας (Cybersecurity Maturity Auditor)
	Κυβερνοασφάλειας. Ο δόκιμος(junior) Ελεγκτής Ωριμότητας Κυβερνοασφάλειας θα μπορεί να επιλεγθεί για έλεγχο ωριμότητας ΜΟΝΟ από Μέτριας ή Χαμηλής Κρισιμότητας Φορείς και θα συνοδεύεται για επιτήρηση από την Αρχή Ψηφιακής Ασφάλειας. Αν η επιτήρηση του είναι επιτυχής τότε θα αλλάζει κατάσταση από δόκιμο(junior) σε εγκριμένο Ελεγκτή Ωριμότητας Κυβερνοασφάλειας.
Υποχρεώσεις	<ul style="list-style-type: none">- Αποδοχή τουλάχιστον δύο (2) αιτημάτων για συνοδεία από εκπαιδευόμενο Ελεγκτή Ωριμότητας Κυβερνοασφάλειας σε διεξαγωγή ελέγχων. Ο μέγιστος αριθμός συνοδευόμενων εκπαιδευόμενων ελεγκτών ανά έλεγχο σε Φορέα είναι δύο (2).