Όνομα Οργανισμού

Διαδικασία Ελέγχου Αποτελεσματικότητας Μέτρων

|  |  |
| --- | --- |
| **Περιεχόμενο:** | Διαδικασία Ελέγχου Αποτελεσματικότητας Μέτρων |
| **Δημιουργός:** |  |
| **Έκδοση:** | 1.0 |
| **Ημερομηνία Έκδοσης:** | ηη/μμ/χχχχ |
| **Εμπιστευτικότητα:** |  |
| **Ιδιοκτήτης:** |  |

Διανομή

| Ρόλος | Όνομα | Οργανισμός | Τοποθεσία | Αριθμός Αντιτύπων |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Καταγραφή Τροποποιήσεων

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Κατάσταση Έκδοσης | Έκδοση | Ημερομηνία | Ενέργειες από | Περιγραφή |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Αναφορές

|  |  |  |
| --- | --- | --- |
| **Αρ.** |  | **Αναφορά Εγγράφου** |
| 1 |  |  |
| 2 |  |  |
| 3 |  |  |

Υποστηρικτικό Υλικό

|  |  |
| --- | --- |
| **Αρ.** | **Αναφορά** |
| 1 |  |
| 2 |  |
| 3 |  |

Ειδικό Λεξιλόγιο

Οι όροι και συντμήσεις ορίζονται πιο κάτω:

| Όροι και συντμήσεις | Περιγραφή |
| --- | --- |
|  |  |
|  |  |
|  |  |

Πίνακας Περιεχομένων

[1. Εισαγωγή 4](#_Toc190432412)

[1.1. Σκοπός 4](#_Toc190432413)

[1.2. Πεδίο Εφαρμογής 4](#_Toc190432414)

[2. Ρόλοι και Αρμοδιότητες 5](#_Toc190432415)

[3. Έλεγχοι με βάση την Απόφαση Κ.Δ.Π. 389/2020 6](#_Toc190432416)

[3.1. Σκοπός 6](#_Toc190432417)

[3.2. Πεδίο Εφαρμογής ελέγχου 6](#_Toc190432418)

[3.3. Πόροι 6](#_Toc190432419)

[3.4. Κριτήρια 7](#_Toc190432420)

[3.5. Πρόγραμμα 7](#_Toc190432421)

[3.6. Μέθοδοι 7](#_Toc190432422)

[3.7. Πρόγραμμα Προ-Ελέγχου 7](#_Toc190432423)

[3.8. Προετοιμασία Εκθέσεων & Ανακοίνωση Ευρημάτων 8](#_Toc190432424)

[4. Αναθεώρηση 9](#_Toc190432425)

[5. Αναφορές 9](#_Toc190432426)

# Εισαγωγή

# Σκοπός

Σκοπός της παρούσας διαδικασίας η καθιέρωση μιας συστηματικής προσέγγισης για την αξιολόγηση και την επαλήθευση της αποτελεσματικότητας(παρακολούθηση, μέτρηση, ανάλυση και αξιολόγηση) των ελέγχων και των μέτρων ασφαλείας που εφαρμόζονται στον [Όνομα Οργανισμού] βάσει του Πλαισίου Διαχείρισης Ασφάλειας Πληροφοριών της Απόφασης Κ.Δ.Π. 389/2020 και άλλων προτύπων ασφάλειας στον κυβερνοχώρο όπως το ISO 27001:2022.

Οι στόχοι αυτής της διαδικασίας ελέγχου είναι:

* Να διασφαλιστεί ότι οι διαδικασίες ασφάλειας των πληροφοριών διεξάγονται αποτελεσματικά, αποδοτικά και οικονομικά προς όφελος του [Όνομα Οργανισμού].
* Αξιολόγηση του κατά πόσον τα εφαρμοζόμενα μέτρα ασφαλείας επιτυγχάνουν τους επιδιωκόμενους στόχους τους.
* Διασφάλιση συνεχούς βελτίωσης με τον προσδιορισμό της συμμόρφωσης ή τον εντοπισμό οποιωνδήποτε τομέων μη συμμόρφωσης και κενών ασφαλείας με την Απόφαση Κ.Δ.Π. 389/2020.
* Ενίσχυση της διαχείρισης κινδύνου - Εντοπισμός αδυναμιών και σύσταση διορθωτικών ενεργειών.
* Τον προσδιορισμό περαιτέρω ευκαιριών συνεχούς βελτίωσης, οι οποίες ενδέχεται να εκτείνονται πέραν των κριτηρίων της Απόφασης Κ.Δ.Π. 389/2020.
* Να παρέχει στον [Όνομα Οργανισμού] εσωτερική διαβεβαίωση ότι η διαχείριση της ασφάλειας των πληροφοριών γίνεται αποτελεσματικά και ότι ελαχιστοποιούνται οι κίνδυνοι για την επιχείρηση.

# Πεδίο Εφαρμογής

Η παρούσα διαδικασία ισχύει για:

* όλους τους ελέγχους ασφαλείας που εφαρμόζονται εντός του οργανισμού.
* Στοιχεία του Πλαισίου Διαχείρισης Ασφάλειας Πληροφοριών συμπεριλαμβανομένων των τεχνικών, διοικητικών και φυσικών ελέγχων.
* Όλους τους υπαλλήλους, τους συνεργάτες και τους τρίτους παρόχους υπηρεσιών που είναι υπεύθυνοι για την εφαρμογή και τη διαχείριση των ελέγχων ασφαλείας.
* Περιοδικές αξιολογήσεις (π.χ. ετήσιες) και αξιολογήσεις βάσει γεγονότων (π.χ. μετά από περιστατικά ασφαλείας ή σημαντικές αλλαγές στο σύστημα).

# Ρόλοι και Αρμοδιότητες

Ως ελάχιστοι ρόλοι στα πλαίσια ελέγχων καθορίζονται οι ακόλουθοι:

| Ρόλος | Αρμοδιότητα |
| --- | --- |
| Ελεγκτής (Εσωτερικού ή Εξωτερικού Ελέγχου)  Internal or Third Party Auditor | * Προετοιμασία και εκτέλεση του Προγράμματος Ελέγχου * Επιβολή των βέλτιστων αρχών και πρακτικών ελέγχου κατά τη συλλογή και ανταλλαγή ευρημάτων ως μέρος της ελεγκτικής δραστηριότητας * Σύνταξη έκθεσης εσωτερικού ελέγχου. |
| Υπεύθυνος για την Ασφάλεια Δικτύων και Συστημάτων Πληροφοριών (ΥΑΠ) | * Υπεύθυνος για τον σχεδιασμό, την υλοποίηση και τη διαχείριση των πολιτικών και των διαδικασιών ασφάλειας πληροφοριών * Παρακολούθηση απειλών και ευπαθειών * Ανάλυση των κινδύνων ασφάλειας πληροφοριών και ανάπτυξη στρατηγικών για τη μείωσή τους * Εφαρμογή ελέγχων ασφαλείας * Διαχείριση επιθέσεων και παραβιάσεων * Επικοινωνία με ενδιαφερόμενα μέρη * Διαχείριση αποκατάστασης και επαναφοράς * Παρακολούθηση υλοποίησης ευρημάτων ελέγχου |
| Προϊστάμενος Πληροφορικής | * Σχεδιασμός και εφαρμογή πολιτικών ασφαλείας (σε συνεργασία με ΥΑΠ) * Διαχείριση συστημάτων ασφαλείας * Ανάπτυξη και εφαρμογή ελέγχων ασφαλείας * Διαχείριση καταστάσεων επείγουσας ανάγκης * Διαχείριση επιθέσεων * Ενημέρωση για νέες απειλές |
| Διευθύνουσα Επιτροπή Ασφάλειας Πληροφοριών (Information Security Steering Committee) | * Υπεύθυνη για την καθοδήγηση, την εποπτεία και την υποστήριξη των προσπαθειών ασφαλείας πληροφοριών * Έγκριση προγράμματος ελέγχου ασφαλείας πληροφοριών, συμπεριλαμβανομένων των ελέγχων, διαδικασιών και πολιτικών * Ενημέρωση σχετικά με τη μη συμμόρφωση με τις πολιτικές ασφαλείας * Προώθηση τυχόν αλλαγών στις πολιτικές * Συμβουλευτικό όργανο της διοίκησης για θέματα ασφάλειας * Ανάπτυξη και υλοποίηση εκπαιδευτικών προγραμμάτων ασφαλείας για το προσωπικό * Παρακολούθηση της αποτελεσματικότητας των μέτρων ασφαλείας πληροφοριών |

# Έλεγχοι με βάση την Απόφαση Κ.Δ.Π. 389/2020

# Σκοπός

Κατά την διεκπεραίωση ενός ελέγχου, θα πρέπει να καθοριστεί ο λόγος για τον οποίο πρέπει να διενεργηθεί ο έλεγχος. Σκοπός ενός συγκεκριμένου ελέγχου θα μπορούσε να είναι ο προσδιορισμός του επιπέδου συμμόρφωσης με έναν συγκεκριμένο νόμο, κανονισμό, πρότυπο ή Απόφαση (π.χ. Κ.Δ.Π. 389/2020). Επιπρόσθετα, ο σκοπός ενός ελέγχου θα μπορούσε να είναι να καθορίσει εάν έχουν αποκατασταθεί συγκεκριμένες ελλείψεις ελέγχου που εντοπίστηκαν σε προηγούμενους ελέγχους ή να καθοριστεί το επίπεδο συμμόρφωσης με έναν νέο νόμο ή πρότυπο στο οποίο μπορεί να υπόκειται ο οργανισμός στο μέλλον.

# Πεδίο Εφαρμογής ελέγχου

Οι έλεγχοι καλύπτουν όλα τα πληροφοριακά στοιχεία ενεργητικού του [Όνομα Οργανισμού]. Κατά περίπτωση, θα πραγματοποιούνται επίσης συναντήσεις με πρόσθετα εμπλεκόμενα μέρη. Οι πτυχές των υπηρεσιών που παρέχονται από εξωτερικούς συνεργάτες δεν θα ελέγχονται άμεσα, αλλά η διαχείριση των εν λόγω προμηθευτών θα πρέπει να ελέγχεται με τη δέουσα επιμέλεια.

Ενδέχεται επίσης να διενεργηθούν πιο συγκεκριμένοι έλεγχοι. Το πεδίο εφαρμογής των ελέγχων αυτών μπορεί να είναι πολυδιάστατο:

* Μια καθορισμένη περίοδος – δηλαδή αρχεία που καλύπτουν ημερομηνία έναρξης και ημερομηνία λήξης μπορεί να περιλαμβάνουν το σώμα των αποδεικτικών στοιχείων
* Γεωγραφία – Έλεγχος πληροφοριακών στοιχείων ενεργητικού π.χ. έλεγχος συστημάτων φυσικής ασφάλειας σε μία συγκεκριμένη τοποθεσία
* Τεχνολογία – Έλεγχος πληροφοριακών στοιχείων ενεργητικού που χρησιμοποιούν συγκεκριμένο λειτουργικό σύστημα, βάση δεδομένων, εφαρμογή ή άλλη πτυχή.
* Επιχειρησιακή διαδικασία – συστήματα που υποστηρίζουν συγκεκριμένες διαδικασίες/διεργασίες, όπως Λογιστήριο, καταχώρηση παραγγελιών ή υποστήριξη πελατών
* Τμήμα του οργανισμού – Έλεγχος ενός ολόκληρου Τμήματος του Οργανισμού

# Πόροι

Ο Υπεύθυνος Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών εκτελεί το πρόγραμμα ελέγχου με τη συμβολή την Ανώτατη Διοίκηση του [Όνομα Οργανισμού] και του προσωπικού.

Κατά περίπτωση, καθορίζονται και άλλοι τύποι πόρων, όπως ο αριθμός των ανθρωποωρών που θα απαιτηθούν, οι δεξιότητες που απαιτούνται από τον ελεγχόμενο, τα εξειδικευμένα εργαλεία κ.λπ.

# Κριτήρια

Η Απόφαση Κ.Δ.Π. 389/2020 χρησιμοποιείται ως βάση των κριτηρίων ελέγχου. Μπορούν να προστεθούν πρόσθετα κριτήρια, εάν χρειαστεί.

# Πρόγραμμα

Ένας αρχικός έλεγχος θα πραγματοποιηθεί στις [Ορίστε χρονικό διάστημα], ο οποίος θα καλύπτει όλα τα εφαρμοζόμενα μέτρα σχετικά με την ασφάλεια πληροφοριών. Στη συνέχεια, οι έλεγχοι θα πραγματοποιούνται τουλάχιστο σε ετήσια βάση. Οι επιλεγμένες διαδικασίες επανεξετάζονται με την πρόθεση ότι όλες οι διαδικασίες θα καλύπτονται σε χρονικό πλαίσιο ενός έτους. Το λεπτομερές πρόγραμμα ελέγχων θα τηρείται από τον Υπεύθυνο Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών και θα διατίθεται κατόπιν αιτήματος.

# Μέθοδοι

Οι έλεγχοι θα συνίστανται σε συνδυασμό εργαστηρίων ανασκόπησης εγγράφων και ελέγχου και συνεντεύξεων με τη διοίκηση και το προσωπικό του οργανισμού. Τα κατάλληλα αρχεία θα εξεταστούν ως αποδεικτικά στοιχεία ότι ακολουθούνται οι τεκμηριωμένες διαδικασίες.

Επιπρόσθετα, αξιολογούνται δράσεις και αποτελέσματα που προέκυψαν από προηγούμενους ελέγχους.

# Πρόγραμμα Προ-Ελέγχου

Ο/Η Υπεύθυνος Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών λαμβάνει πληροφορίες σχετικά με τον έλεγχο που θα του επιτρέψουν να καταρτίσει το Πλάνο επιθεώρησης με ή χωρίς της συμβολή του ελεγκτή:

* Τοποθεσία ή τοποθεσίες που πρέπει να επισκεφθεί
* Κατάλογος των εφαρμογών που θα εξεταστούν
* Οι τεχνολογίες που υποστηρίζουν κάθε εφαρμογή
* Πολιτικές, πρότυπα και διαγράμματα που περιγράφουν το περιβάλλον

Χρησιμοποιώντας τις πληροφορίες που λαμβάνονται σχετικά με τους στόχους και το πεδίο εφαρμογής του ελέγχου, ο/η Υπεύθυνος Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών μπορεί πλέον να αναπτύξει διαδικασίες για τον έλεγχο. Για κάθε στόχο και έλεγχο που πρέπει να εξεταστεί, ο ελεγκτής μπορεί να καθορίσει:

* Μια λίστα με τα άτομα προς συνέντευξη
* Ερωτήσεις που πρέπει να γίνουν κατά τη διάρκεια κάθε συνέντευξης
* Τεκμηρίωση που πρέπει να ζητηθεί κατά τη διάρκεια κάθε συνέντευξης
* Εργαλεία ελέγχου που θα χρησιμοποιηθούν
* Ποσοστά και μεθοδολογίες δειγματοληψίας
* Πώς και πού θα αρχειοθετηθούν τα αποδεικτικά στοιχεία
* Πώς θα αξιολογηθούν τα αποδεικτικά στοιχεία

Σε σχέση με τον έλεγχο συμμόρφωσης της Απόφασης Κ.Δ.Π 389/2020 μέσω της διαδικασία διενέργειας ελέγχων ωριμότητας κυβερνοασφάλειας των Φορέων, που διενεργείται με τη χρήση μοντέλου ωριμότητας κυβερνοασφάλειας (cybersecurity maturity model) απαιτείται η αναδρομή στην Απόφαση Κ.Δ.Π 245/2024 για τις ελάχιστες απαιτήσεις κατάρτισης του Πλάνου Επιθεώρησης.

# Προετοιμασία Εκθέσεων & Ανακοίνωση Ευρημάτων

Με την ολοκλήρωση ενός ελέγχου, θα συνταχθεί ένα προσχέδιο έκθεσης ελέγχου με τα πορίσματα και τις συστάσεις, και το περιεχόμενο θα κοινοποιηθεί αρχικά στους υπεύθυνους των εμπλεκόμενων τμημάτων, οι οποίοι θα έχουν την ευκαιρία να σχολιάσουν.

Θα συμφωνηθεί σχέδιο δράσης για την αντιμετώπιση τυχόν ελλείψεων και λήψη διορθωτικών μέτρων.

Η τελική έκθεση θα συνταχθεί και θα κοινοποιηθεί στους υπεύθυνους των εμπλεκόμενων τμημάτων και θα διατεθεί στην εκτελεστική ομάδα διαχείρισης, ανάλογα με την περίπτωση.

Οι έλεγχοι παρακολούθησης πραγματοποιούνται σύμφωνα με το σχέδιο δράσης για να διασφαλιστεί ότι έχουν αντιμετωπιστεί/εφαρμοστεί τυχόν ελλείψεις και διορθωτικά μέτρα.

Σε σχέση με τον έλεγχο συμμόρφωσης της Απόφασης Κ.Δ.Π 389/2020 μέσω της διαδικασία διενέργειας ελέγχων ωριμότητας κυβερνοασφάλειας των Φορέων, που διενεργείται με τη χρήση μοντέλου ωριμότητας κυβερνοασφάλειας (cybersecurity maturity model) θα πρέπει να ανατρέξετε στην Απόφαση Κ.Δ.Π 245/2024 για τις ελάχιστες απαιτήσεις για αποστολή της Έκθεσης στην Αρχή Ψηφιακής Ασφάλειας καθώς και ετοιμασίας και παρακολούθησης του σχεδίου δράσης.

# Αναθεώρηση

Τα έγγραφα σχετικά με τη Διαδικασία Ελέγχου Αποτελεσματικότητας Μέτρων επανεξετάζονται και να αναθεωρούνται τουλάχιστον ετησίως ή σε περίπτωση σημαντικών αλλαγών στο περιβάλλον του [Όνομα Οργανισμού] με στόχο να διασφαλίζεται ότι παραμένει επικαιροποιημένη, αποτελεσματική και ευθυγραμμισμένη με τις ανάγκες του οργανισμού, τυχόν νομικές/κανονιστικές απαιτήσεις και άλλες τεχνολογικές εξελίξεις όπως νέες αναδυόμενες απειλές κτλ.) Επιπρόσθετα, η διαδικασία δύναται να τροποποιείτε πριν και μετά από εσωτερικούς και εξωτερικούς ελέγχους ή μετά από αξιολογήσεις κινδύνου. Τέλος, η διαδικασία δύναται να αξιολογείται σε περίπτωση ενσωμάτωσης νέων ελέγχων ή εργαλείων ασφάλειας πληροφοριών έτσι ώστε η εισαγωγή αυτών να αντικατοπτρίζει τον αντίκτυπο τους στις μεθόδους επαλήθευσης.

# Αναφορές

|  |  |  |  |
| --- | --- | --- | --- |
| **Κατηγορία** | **ID** | **Μέτρο** | **Στόχος Μέτρου** |
| Διακυβέρνηση | GOV2 | Συμμόρφωση με νομικές και κανονιστικές υποχρεώσεις | Να εξασφαλιστεί η συμμόρφωση με όλες τις εφαρμοστέες νομικές και κανονιστικές υποχρεώσεις όσον αφορά την ασφάλεια δικτύων και πληροφοριών. |