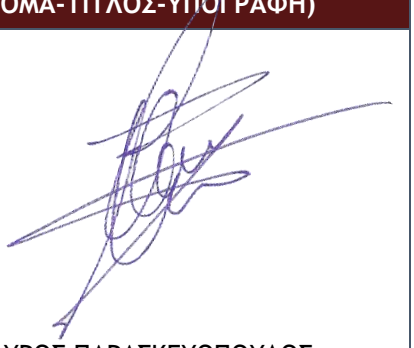
ΕΚΠ - ΕΙΔΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ ΠΙΣΤΟΠΟΙΗΣΗΣ ISO/IEC 27001:2022

ΦΟΡΕΑΣ ΠΙΣΤΟΠΟΙΗΣΗΣ MAGNUS CERT ΙΚΕ

ΣΥΝΤΑΞΗ (ΟΝΟΜΑ-ΤΙΤΛΟΣ-ΥΠΟΓΡΑΦΗ)	ΕΓΚΡΙΣΗ (ΟΝΟΜΑ-ΤΙΤΛΟΣ-ΥΠΟΓΡΑΦΗ)
 ΣΤΑΥΡΟΣ ΠΑΡΑΣΚΕΥΟΠΟΥΛΟΣ ΥΠΕΥΘΥΝΟΣ ΔΙΑΧΕΙΡΙΣΗΣ ΣΥΣΤΗΜΑΤΩΝ	 ΜΑΡΙΑ ΧΡΙΣΤΟΦΟΡΟΥ ΔΙΑΧΕΙΡΙΣΤΡΙΑ

ΠΙΝΑΚΑΣ ΑΝΑΘΕΩΡΗΣΕΩΝ			
Έκδοση	Ημερομηνία	Περιγραφή Αναθεώρησης	Έγκριση Από

Ο παρών Ειδικός Κανονισμός Πιστοποίησης τίθεται σε ισχύ και αναθεωρείται σύμφωνα με τις ισχύουσες σχετικές διαδικασίες για τα ελεγχόμενα έγγραφα & αρχεία του Φορέα Πιστοποίησης **MAGNUS CERT ΙΚΕ.**

Ο παρών Ειδικός Κανονισμός Πιστοποίησης είναι ιδιοκτησία του Φορέα Πιστοποίησης **MAGNUS CERT ΙΚΕ** και βρίσκεται αναρτημένος στον ιστότοπο του Φορέα για Δημόσια Πληροφόρηση.

ΠΕΡΙΕΧΟΜΕΝΑ

1. Σκοπός & Πεδίο Εφαρμογής

Σκοπός του παρόντος Ειδικού Κανονισμού είναι η παροχή υπηρεσιών πιστοποίησης, επακόλουθης επιτήρησης, επαναπιστοποίησης, έκτακτης επιθεώρησης, αύξησης πεδίου, μείωσης πεδίου, της εφαρμογής Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ) οργανισμών, που εδράζει και συμμορφώνεται με τις απαιτήσεις του διεθνούς προτύπου ISO/IEC 27001:2022.

1.1 Πεδίο εφαρμογής

Ο παρών Ειδικός Κανονισμός Πιστοποίησης χρησιμοποιείται σε συνδυασμό με τον Γενικό Κανονισμό Πιστοποίησης, το Εγχειρίδιο Συστημάτων Διαχείρισης, τις Διαδικασίες και τις Οδηγίες Εργασίας του Φορέα Πιστοποίησης, που περιγράφουν όλη την διεργασία της Πιστοποίησης. Ειδικότερα ο Φορέας Πιστοποίησης πληροί τα κριτήρια του Διεθνούς Προτύπου ISO/IEC 17021-1:2015 και του ISO/IEC 27006-1:2024.

Ο οργανισμός που επιλέγει να σχεδιάσει και εφαρμόσει ένα Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών – ΣΔΑΠ (Information Security Management System – ISMS) κατά ISO/IEC 27001:2022, οφείλει να συμμορφωθεί με τις απαιτήσεις που θέτει το πρότυπο και να επιζητήσει την σχετική πιστοποίηση από τρίτο ανεξάρτητο φορέα, οπότε σκοπεύει ή/και χρειάζεται:

- Να αποδείξει ότι το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών διατηρεί την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των πληροφοριών με εφαρμογή της διεργασίας διαχείρισης της διακινδύνευσης και να εμπνέει εμπιστοσύνη στα ενδιαφερόμενα μέρη για την επαρκή διαχείριση της.
- Να αποδείξει την ικανότητα του και τη στρατηγική του απόφαση για την εγκατάσταση, την εφαρμογή, τη διατήρηση και συνεχή βελτίωση ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών.
- Να αποδείξει ότι το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών εντάσσεται και ενσωματώνεται στις διεργασίες του Οργανισμού και στη συνολική δομή διαχείρισης και ότι η ασφάλεια πληροφοριών λαμβάνεται υπόψη κατά το σχεδιασμό των διεργασιών, των πληροφοριακών συστημάτων, καθώς και των ελέγχων.

2. Αναφορές

- Εγχειρίδιο Συστημάτων Διαχείρισης ΕΔΣ
- Διαδικασίες ΣΔ
- Γενικός Κανονισμός Πιστοποίησης ΓΚΠ

- ISO/IEC 17021-1:2015 Αξιολόγηση της συμμόρφωσης– Απαιτήσεις για φορείς επιθεώρησης και πιστοποίησης Συστημάτων Διαχείρισης - Μέρος 1: Απαιτήσεις
- ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection — Information security management systems — Requirements
- ISO/IEC 27000:2018, Information technology -- Security techniques -- Information security management systems — Overview and vocabulary
- ISO/IEC 27002:2022, Information security, cybersecurity and privacy protection — Information security controls
- ISO/IEC 27003:2017, Information technology -- Security techniques -- Information security management systems — Guidance
- ISO/IEC 27004:2016, Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation
- ISO/IEC 27005:2022, Information security, cybersecurity and privacy protection — Guidance on managing information security risks
- ISO/IEC 27006-1:2024 Information security, cybersecurity and privacy protection — Requirements for bodies providing audit and certification of information security management systems - Part 1: General
- ISO/IEC 27007:2020 Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing
- ISO/IEC TS 27008:2019 Information technology – Security techniques - Guidelines for the assessment of information security controls
- GDPR ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2016/679 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων)
- ISO 31000:2018, Risk management — Principles and guidelines
- ΕΣΔ-ΚΑΔ Κανονισμός Διαπίστευσης του Εθνικού Συστήματος Διαπίστευσης
- IAF MD Κατευθυντήριες Οδηγίες της Διεθνούς Διαπίστευσης και τις σχετικές τροποποιήσεις που εκδίδονται

3. Όροι και Ορισμοί - Συντομογραφίες

Επιθεώρηση πιστοποίησης	επιθεώρηση που διεξάγεται από έναν οργανισμό επιθεώρησης ανεξάρτητο από τον πελάτη και τα μέρη που βασίζονται πάνω του, με σκοπό την πιστοποίηση του Συστήματος Διαχείρισης του πελάτη

Πελάτης	οργανισμός του οποίου το Σύστημα Διαχείρισης επιθεωρείται για σκοπούς πιστοποίησης κατά το διεθνές πρότυπο
Τεχνική περιοχή	η τεχνική περιοχή χαρακτηρίζεται από ομοιότητες των διεργασιών που σχετίζονται με ένα συγκεκριμένο τύπο Συστήματος Διαχείρισης
Επιθεωρητής	πρόσωπο το οποίο διαθέτει την ικανότητα να διενεργεί επιθεώρηση βάσει του διεθνές πρότυπου
Τεχνικός εμπειρογνώμονας	Πρόσωπο που παρέχει εξειδικευμένη τεχνογνωσία ή εμπειρογνωμοσύνη στην ομάδα επιθεώρησης (εξειδικευμένη τεχνογνωσία ή εμπειρογνωμοσύνη είναι ότι αφορά τον οργανισμό, τις διεργασίες ή τις δραστηριότητες που επιθεωρούνται).
Οδηγός	πρόσωπο που ορίζεται από τον πελάτη για να βοηθήσει την ομάδα επιθεώρησης
Παρατηρητής	πρόσωπο που συνοδεύει την ομάδα επιθεώρησης αλλά δεν επιθεωρεί
Ενδιαφερόμενο μέρος	πρόσωπο ή ομάδα που ενδιαφέρεται ή επηρεάζεται από την επίδοση ενός οργανισμού
Πιστοποίηση	είναι η επιβεβαίωση τρίτου μέρους που αναφέρεται σε προϊόντα, διεργασίες, συστήματα και πρόσωπα. Με τον όρο επιβεβαίωση τρίτου μέρους νοείται η έκδοση δήλωσης (δηλ. πιστοποιητικού), από ανεξάρτητο φορέα ως προς το πρόσωπο ή τον οργανισμό, που παρέχει το προς αξιολόγηση συμμόρφωσης αντικείμενο, ότι η επαλήθευση των καθορισμένων απαιτήσεων, έχει τεκμηριωθεί επαρκώς
Χρόνος επιθεώρησης	χρόνος που απαιτείται για το σχεδιασμό και την ολοκλήρωση μιας πλήρους και αποτελεσματικής επιθεώρησης του Συστήματος Διαχείρισης του πελάτη
Διάρκεια της επιθεώρησης του Συστήματος Διαχείρισης	Μέρος του χρόνου επιθεώρησης, το οποίο δαπανείται στην διενέργεια ενεργειών επιθεώρησης με εκκίνηση την εναρκτήρια συνάντηση και λήξη την καταληκτική συνάντηση. Σημείωση: Τυπικές ενέργειες επιθεώρησης περιλαμβάνουν: - Διενέργεια εναρκτήριας συνάντησης - Διενέργεια ανασκόπησης τεκμηρίωσης κατά τη διάρκεια της επιθεώρησης - Επικοινωνία κατά τη διάρκεια της επιθεώρησης - Ανάθεση ρόλων και υπευθυνοτήτων για παρατηρητές και βοηθητικό προσωπικό - Συλλογή και επαλήθευση πληροφοριών - Δημιουργία ευρημάτων επιθεώρησης - Προετοιμασία για τα συμπεράσματα της επιθεώρησης - Διενέργεια καταληκτικής συνάντησης (MD5)
Διακινδύνευση	η επίδραση της αβεβαιότητας
Πλαίσιο λειτουργίας	επιχειρησιακό περιβάλλον. Συνδυασμός εσωτερικών και εξωτερικών παραμέτρων που μπορούν να επηρεάσουν την προσέγγιση του οργανισμού για τη καθιέρωση και επίτευξη των στόχων του.
Διαρκής βελτίωση	επαναλαμβανόμενη διεργασία του Συστήματος Διαχείρισης για την ενίσχυση της αποτελεσματικότητας του στην επίτευξη βελτιώσεων της συνολικής επίδοσης, σύμφωνα με την πολιτική του οργανισμού
Διαδικασία	καθορισμένος τρόπος εκτέλεσης μιας δραστηριότητας ή διεργασίας
Εσωτερική επιθεώρηση	συστηματική, ανεξάρτητη και τεκμηριωμένη διεργασία συλλογής τεκμηρίων επιθεώρησης και αντικειμενικής αξιολόγησης τους

	προκειμένου να προσδιοριστεί ο βαθμός ικανοποίησης των καθορισμένων από τον οργανισμό, κριτηρίων επιθεώρησης του Συστήματος Διαχείρισης
Διορθωτική ενέργεια	ενέργεια για την εξάλειψη του αιτίου μιας εντοπισμένης μη συμμόρφωσης
Μη συμμόρφωση	η μη ικανοποίηση μιας απαίτησης

4. Υπευθυνότητες και Αρμοδιότητες

Αρμόδιος για τον έλεγχο της εφαρμογής και τον χειρισμό της παρούσας διαδικασίας είναι ο Τεχνικός Διευθυντής ή οι Αναπληρωτές του. Υπεύθυνος για την αναθεώρηση του Παρόντος Κανονισμού είναι ο ΥΔΣ. Οι Επικεφαλής Επιθεωρητές και οι Επιθεωρητές, καθώς επίσης και το προσωπικό που εμπλέκεται στη διαδικασία πιστοποίησης έχουν την ευθύνη εφαρμογής του παρόντος κανονισμού για το μέρος των εργασιών που πραγματοποιούν.

5. Ανάπτυξη Ειδικού Κανονισμού

5.1 Γενικά

Το προσωπικό του Φορέα Πιστοποίησης προετοιμάζει και διενεργεί την επιθεώρηση, εφαρμόζοντας όλες τις σχετικές Διαδικασίες και συμπληρώνοντας τα αντίστοιχα Έντυπα. Οι σχετικές διαδικασίες εδράζουν στις απαιτήσεις των τυποποιητικών εγγράφων περί διενέργειας επιθεωρήσεων Συστημάτων Διαχείρισης και του προτύπου ISO/IEC 27006-1:2024.

Η αξιολόγηση συμμόρφωσης κατά την αρχική επιθεώρηση συνίσταται σε δύο διακριτά Στάδια, την επιθεώρηση 1ου Σταδίου και την επιθεώρηση 2ου Σταδίου, τα οποία διενεργούνται με προσχεδιασμένο και προγραμματισμένο τρόπο στο πλαίσιο σχετικής επίσκεψης στις εγκαταστάσεις του υπό πιστοποίηση οργανισμού.

5.2 Επικεφαλής επιθεωρητές, επιθεωρητές και Τεχνικοί Εμπειρογνώμονες

Οι επιθεωρητές που χρησιμοποιεί ο Φορέας Πιστοποίησης και στελεχώνουν την αντίστοιχη Ομάδα Επιθεώρησης (η οποία ορίζεται ανά επιθεώρηση όπως περιγράφεται παρακάτω), είναι αναγνωρισμένα και εξουσιοδοτημένα πρόσωπα ως επιθεωρητές Συστημάτων Διαχείρισης Ασφάλειας Πληροφοριών σύμφωνα με τα πρότυπα ISO/IEC 27001:2022 και ISO/IEC 27006-1:2024 σε συμμόρφωση με τις απαιτήσεις της Διαδικασίας Δ05 Διαχείριση Προσωπικού του ΦΠ. Για την επάρκεια των επιθεωρητών σε ό,τι αφορά τη διενέργεια εξωτερικών επιθεωρήσεων σε Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών ισχύουν οπωσδήποτε τα προβλεπόμενα στο πρότυπο ISO/IEC 27006-1:2024.

Με ευθύνη του Τεχνικού Διευθυντή ή/ και του ΥΔΣ του Φορέα Πιστοποίησης συμπληρώνονται και τηρούνται διαρκώς ενήμερα τα σχετικά αρχεία βασικών προσόντων, αποτελεσμάτων αξιολόγησης, εκπαίδευσης/επιμόρφωσης και έγκρισης επιθεωρητών (Αρχείο Προσωπικού).

Οι βασικές γνώσεις/ ικανότητες/ δεξιότητες που πρέπει να έχει ένα άτομο προκειμένου να μπορεί να αναγνωριστεί ως επιθεωρητής Συστημάτων Διαχείρισης Ασφάλειας Πληροφοριών κατά ISO/IEC 27001:2022 προέρχονται σε γενικές γραμμές από τις ακόλουθες απαιτήσεις:

- ISO/IEC 27006-1:2024 παρ. 7 και Annex A.
- ISO/IEC 17021-1 παρ. 7 και Annex A.

και καλύπτουν τις ακόλουθες ενότητες:

1. Γνώσεις ασφάλειας πληροφοριών
2. Τεχνικές γνώσεις της επιθεωρούμενης δραστηριότητας*
3. Γνώσεις για τα Συστήματα Διαχείρισης
4. Γνώσεις για τις αρχές της επιθεώρησης
5. Γνώσεις σχετικά με την παρακολούθηση, μέτρηση, ανάλυση και αξιολόγηση στα πλαίσια ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών
6. Ικανότητα στην επιθεώρηση συστήματος ISO/IEC 27001:2022
7. Ικανότητα να αναγνωρίζει τις ενδείξεις περιστατικών ασφάλειας πληροφοριών στο επιθεωρούμενο σύστημα στις αντίστοιχες απαιτήσεις του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών σύμφωνα με το ISO/IEC 27001:2022.
8. Το πρότυπο ISO/IEC 27001:2022 καθώς και τις σχετικές τροποποιήσεις που εκδίδονται από τον ISO.
9. Γνώσεις σε σχέση με τους κινδύνους ανά δραστηριότητα λειτουργίας.
10. Ορισμούς, διεργασίες και τεχνολογίες που σχετίζονται με την εφαρμογή της ασφάλειας πληροφοριών σε έναν οργανισμό.

*Οι παραπάνω απαιτήσεις ισχύουν υποχρεωτικά για κάθε ένα από τα μέλη της ομάδας επιθεώρησης με εξαίρεση το (2) Τεχνικές γνώσεις της επιθεωρούμενης δραστηριότητας, το οποίο θα πρέπει να καλύπτεται από το σύνολο της ομάδας επιθεώρησης.

Ειδικότερα τα κριτήρια Επιθεωρητών, Επικεφαλής Επιθεωρητών και Τεχνικών Εμπειρογνωμόνων αναλύονται παρακάτω.

5.3 Κριτήρια επιλογής επιθεωρητών

Οι ελάχιστες απαιτήσεις που πρέπει να πληρούνται προκειμένου να αναγνωριστεί ένα άτομο ως Επιθεωρητής Συστημάτων Διαχείρισης Ασφάλειας Πληροφοριών βάσει του ISO/IEC 27001:2022 είναι:

1. Επαγγελματική εκπαίδευση ή επιμόρφωση επιπέδου (κατ' ελάχιστον) Ανώτατης Εκπαίδευσης.
2. Τέσσερα (4) χρόνια κατ' ελάχιστον πρακτική και πλήρους απασχόλησης επαγγελματική απασχόληση στο αντικείμενο της πληροφορικής (IT) εκ των οποίων τα δύο τουλάχιστον σε ρόλο ή λειτουργία που να σχετίζεται με την ασφάλεια πληροφοριών.
3. Εκπαίδευση διάρκειας πέντε (5) ημερών στο αντικείμενο των επιθεωρήσεων Συστημάτων Διαχείρισης Ασφάλειας Πληροφοριών και στην διαχείριση της επιθεώρησης.
4. Παρακολούθηση ως εκπαιδευόμενος επιθεωρητής τουλάχιστον 10 Ανθρωποημερών (Α/Η) επιθεώρησης (περιλαμβανομένων των διαδικασιών ανασκόπησης της τεκμηρίωσης, αξιολόγησης της διακινδύνευσης, υλοποίησης της επιθεώρησης και της αναφοράς της επιθεώρησης). Οι Α/Η αυτές θα πρέπει να προέρχονται από τουλάχιστον έναν αρχικό έλεγχο πιστοποίησης ISO/IEC 27001 (στάδιο 1 και στάδιο 2) ή επαναπιστοποίηση και τουλάχιστον έναν έλεγχο επιτήρησης. Αυτή η εμπειρία θα αποκτηθεί θα πρέπει να έχει αποκτηθεί τα τελευταία 5 χρόνια.
5. Εκπαίδευση στο ΣΔ της **MAGNUS CERT**.
6. Εμπειρία που είναι σχετική και πρόσφατη.
7. Διατήρηση της γνώσης και των ικανοτήτων στο αντικείμενο της ασφάλειας πληροφοριών και της επιθεώρησης μέσω συνεχούς επαγγελματικής ανάπτυξης.

Οι επιθεωρητές όπως αναφέρεται και στη σύμβαση συνεργασίας με το Φορέα Πιστοποίησης, την οποία υπογράφουν, φέρουν ακέραια την ευθύνη για την διαρκή ενημέρωσή τους σε σχέση με τις μεταβολές της νομοθεσίας που διέπει αφενός μεν τις υπηρεσίες αξιολόγησης συμμόρφωσης/ επιθεώρησης για τις οποίες έχουν εξουσιοδοτηθεί, αφετέρου τη λειτουργία και τα προϊόντα των υπό πιστοποίηση οργανισμών/επιχειρήσεων.

5.4 Κριτήρια επιλογής επικεφαλής επιθεωρητών

Οι Επικεφαλής Επιθεωρητές που ηγούνται της Ομάδας Επιθεώρησης πρέπει να πληρούν τα ελάχιστα κριτήρια των επιθεωρητών (παρ. 5.3) και ταυτόχρονα να έχουν συμμετάσχει ενεργά σε όλα τα στάδια τουλάχιστον τριών επιθεωρήσεων Συστημάτων Διαχείρισης Ασφάλειας Πληροφοριών σύμφωνα με το ISO/IEC 27001:2022. Η συμμετοχή περιλαμβάνει και τις αρχικές διαδικασίες για τον προσδιορισμό της έκτασης και των ορίων της επιθεώρησης, τον σχεδιασμό, την ανασκόπηση της τεκμηρίωσης και της αξιολόγησης διακινδύνευσης, την υλοποίηση της επιθεώρησης και την σύνταξη της σχετικής έκθεσης επιθεώρησης.

Επικεφαλής επιθεωρητές που έχουν αναγνωριστεί ως τέτοιοι τεκμηριωμένα από άλλο Διαπιστευμένο Φορέα Πιστοποίησης, γίνονται αποδεκτοί ως επικεφαλής επιθεωρητές χωρίς επιπλέον διαδικασίες.

5.5 Ομάδα επάρκειας επιθεώρησης

Η ομάδα επιθεώρησης καθορίζεται επίσημα κατά την ανασκόπηση της αίτησης. Η εντολή που δόθηκε στην ομάδα επιθεώρησης καθορίζεται σαφώς και γνωστοποιείται στο πελάτη. Μια ομάδα επιθεώρησης μπορεί να αποτελείται από ένα ή περισσότερα άτομα βάσει των απαιτήσεων που περιγράφονται στο παρόν κεφάλαιο.

Ο Φορέας Πιστοποίησης κατά τον καθορισμό της ομάδας επιθεώρησης φροντίζει ώστε να πληρούνται τα ακόλουθα:

- Όλοι οι επιθεωρητές (Auditor(s), Lead Auditor) θα πρέπει να έχουν αποδεδειγμένα και τεκμηριωμένα:
  - Γνώσεις ασφάλειας πληροφοριών
  - Γνώσεις για τα Συστήματα Διαχείρισης
  - Γνώσεις για τις αρχές διεξαγωγής της επιθεώρησης
  - Γνώσεις σχετικά με την παρακολούθηση, μέτρηση, ανάλυση και αξιολόγηση στα πλαίσια ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών
  - Ικανότητα να αναγνωρίζει τις ενδείξεις περιστατικών ασφάλειας πληροφοριών στο επιθεωρούμενο σύστημα στις αντίστοιχες απαιτήσεις του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών σύμφωνα με το πρότυπο ISO/IEC 27001:2022, καθώς και τις σχετικές τροποποιήσεις που εκδίδονται από τον ISO.
  - Γνώσεις σε σχέση με τους κινδύνους ανά δραστηριότητα λειτουργίας.
  - Ορισμούς, διεργασίες και τεχνολογίες που σχετίζονται με την εφαρμογή της ασφάλειας πληροφοριών σε έναν οργανισμό
  - Πρακτική κατάλληλη εμπειρία στα παραπάνω θέματα.

Παράλληλα, στο σύνολό της η ομάδα θα πρέπει να έχει τα ακόλουθα:

- Τεχνικές γνώσεις της επιθεωρούμενης δραστηριότητας
- Γνώσεις σχετικά με το νομοθετικό και κανονιστικό πλαίσιο του επιθεωρούμενου οργανισμού (το οποίο δύναται να είναι διαφορετικό ανά δραστηριότητα ή και τοποθεσία)

Για την απόδειξη των παραπάνω ο οργανισμός τηρεί τεκμηριωμένες αποδείξεις για το σύνολο των κριτηρίων που αναφέρονται στα κεφάλαια 5.3, 5.4 και 5.5.

Ο Φορέας Πιστοποίησης, με ευθύνη του Τεχνικού Διευθυντή και με την αρωγή των Τεχνικών Εμπειρογνωμόνων που διαθέτει, παρακολουθεί τουλάχιστον ανά τρίμηνο τις όποιες εξελίξεις των απαιτήσεων των σχετικών προτύπων και της κείμενης νομοθεσίας, ενημερώνοντας κατάλληλα το έντυπο ΕΔ02-2 Παρακολούθηση Εξωτερικών Εγγράφων και κοινοποιώντας τις σχετικές πληροφορίες στους Επιθεωρητές μέσω της κοινόχρηστης βάσης δεδομένων του Φορέα Πιστοποίησης όπου διαθέτουν πρόσβαση με συγκεκριμένους κωδικούς και σε συγκεκριμένο χώρο της (δεσμευμένο αποκλειστικά για δική τους χρήση) ή με άλλο ισοδύναμο τρόπο κοινοποίησης. Η συλλογή της πληροφορίας όσον αφορά τις αλλαγές στη νομοθεσία πραγματοποιείται από το Εθνικό Τυπογραφείο (et.gr), τη Διαύγεια (diavgeia.gov.gr) ή από την νομοθετική βάση δεδομένων που διαθέτει ο Φορέας Πιστοποίησης. Σε περίπτωση εφαρμόσιμων αλλαγών υλοποιούνται όλες οι σχετικές διαδικασίες όπως Δ02 Έλεγχος Εγγράφων και Αρχείων, Δ04 Εσωτερικές Επιθεωρήσεις κ.λπ., καθώς και οι προβλεπόμενες σχετικές ενέργειες που αναφέρονται στο Γενικό Κανονισμό Πιστοποίησης.

5.6 Επάρκεια Εμπλεκόμενου Προσωπικού Συστημάτων Διαχείρισης Ασφάλειας Πληροφοριών

Οι ρόλοι οι οποίοι εμπλέκονται στην διεργασία της πιστοποίησης είναι:

- Οι ανασκοπούντες τις αιτήσεις
- Οι αρμόδιοι χορήγησης της πιστοποίησης

Εκτός από τα βασικά προσόντα που έχει προσδιορίσει ο Φορέας Πιστοποίησης, όπως ορίζονται στη διαδικασία Δ05 Διαχείριση Προσωπικού, ειδικά για τα Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών βάσει του προτύπου ISO/IEC 27001:2022, απαιτούνται τα ακόλουθα σύμφωνα με το Annex A του προτύπου ISO/IEC 27006-1:2024:

Α. Οι ανασκοπούντες τις αιτήσεις είναι υπεύθυνοι για:

- Τον καθορισμό της σύνθεσης της ομάδας επιθεώρησης από τους κατάλληλους εγκεκριμένους επιθεωρητές ή/ και εμπειρογνώμονες.
- Την ανασκόπηση των υποβαλλόμενων αιτήσεων πιστοποίησης και την κατάρτιση, ενημέρωση και αναθεώρηση του Σχεδίου Προγράμματος Επιθεώρησης του τριετούς κύκλου έργου πιστοποίησης.
- Τον καθορισμό των ανθρωποημερών επιθεώρησης.

Απαιτείται να έχουν γνώσεις για τα ακόλουθα:

- Τα πρότυπα που είναι σχετικά με την ανάπτυξη και εφαρμογή ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών, αλλά και πρότυπα που είναι σχετικά και χρησιμοποιούνται στη διεργασία πιστοποίησης.
- Ορισμούς, διεργασίες και τεχνολογίες που σχετίζονται με την εφαρμογή της ασφάλειας πληροφοριών σε έναν οργανισμό.
- Το αντικείμενο, τις σχετικές διεργασίες, τα είδη των οργανισμών, το μέγεθος, τη διαχείριση, τη δομή, τις λειτουργίες και τις σχέσεις ανάμεσα στην ανάπτυξη και την υλοποίηση ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών και των δραστηριοτήτων της πιστοποίησης περιλαμβανομένων και των εργασιών που προέρχονται από εξωτερικά μέρη.

Β. Οι αρμόδιοι χορήγησης της πιστοποίησης είναι υπεύθυνοι (κατά κατηγορία πιστοποίησης και τομέα ευθύνης τους) για:

- Τη λήψη απόφασης χορήγησης ή μη, πιστοποίησης και την τελική εισήγηση προς τον Διαχειριστή του Φορέα Πιστοποίησης για την σχετική επικύρωση και έκδοση Πιστοποιητικού Συμμόρφωσης.
- Τον έλεγχο της επάρκειας των αναφορών επιθεώρησης/ αξιολόγησης που συντάσσει ο Επικεφαλής Επιθεωρητής και ιδιαίτερα σε ό,τι αφορά την επάρκεια των αποδεικτικών στοιχείων που συλλέγονται και καταγράφονται, ώστε να τεκμηριωθούν τα ευρήματα της επιθεώρησης και η άρση των μη συμμορφώσεων που εντοπίζονται μέσω καταλλήλων, αποτελεσματικών και επαρκών διορθώσεων και διορθωτικών ενεργειών.
- Την επισήμανση στον Τεχνικό Διευθυντή και στον Επικεφαλής Επιθεωρητή θεμάτων και σημείων που απαιτούν ιδιαίτερης προσοχής και χρήζουν εξέτασης ή αποσαφήνισης, είτε κατά το στάδιο πριν την απόφαση χορήγησης είτε κατά το στάδιο των μελλοντικών επισκέψεων επιθεώρησης επιτήρησης.

- Τη διαρκή τήρηση ενημέρωσης σχετικά με τις εξελίξεις της κείμενης νομοθεσίας που διέπει τη πιστοποίηση, αλλά και την λειτουργία των υπό πιστοποίηση οργανισμών και επιχειρήσεων του τομέα ευθύνης τους και ανά τεχνική περιοχή δραστηριοτήτων.
- Την συνεισφορά στην αξιολόγηση επίδοσης των επιθεωρητών και εμπειρογνωμόνων που χρησιμοποιεί ο Φορέας Πιστοποίησης με βάση τα στοιχεία που προκύπτουν από την ανασκόπηση των αναφορών επιθεώρησης που υποβάλλονται για έλεγχο.
- Την παρακολούθηση και αξιολόγηση του ιστορικού επίδοσης των πιστοποιημένων ΣΔ που εφαρμόζουν οι πελάτες του ΦΠ για την συνολική τριετία ισχύος της πιστοποίησης και την λήψη απόφασης για αλλαγές στον προγραμματισμό των απαιτούμενων επιθεωρήσεων (αλλαγή στη συχνότητα διενέργειας των επιτηρήσεων, στον αριθμό ανθρωποημερών κάθε επιθεώρησης, στη σύνθεση της Ομάδας Επιθεώρησης κ.λπ.).

Απαιτείται να έχουν γνώσεις για τα ακόλουθα:

- Συστήματα Διαχείρισης γενικά
- Διεργασίες και διαδικασίες επιθεώρησης
- Αρχές, πρακτικές και τεχνικές της επιθεώρησης
- Απαιτήσεις τεκμηρίωσης σε σχέση με το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών, την ιεραρχία και τις συσχετίσεις μεταξύ τους
- Διεργασίες που σχετίζονται με το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών
- Γνώσεις σχετικά με το νομοθετικό και κανονιστικό πλαίσιο σχετικά με την ασφάλεια πληροφοριών

5.7 Σύγκρουση συμφερόντων

Τα μέλη της Ομάδας Επιθεώρησης που εκάστοτε καθορίζεται, δεν έχουν καμία σχέση με τις υπό επιθεώρηση επιχειρήσεις συμπεριλαμβανομένης οποιασδήποτε σχέσης παροχής συμβουλευτικών υπηρεσιών, καθώς και κάθε άλλης εργασιακής ή εμπορικής ή/ και συγγενικής σχέσης ή σχέσης δυνάμενης να θέσει υπό αμφισβήτηση την αξιοπιστία του έργου της επιθεώρησης και τις παρεχόμενες υπηρεσίες πιστοποίησης του Φορέα Πιστοποίησης, τουλάχιστον για τα τελευταία (2) χρόνια. Για τον επαρκή έλεγχο του θεμελιώδους ζητήματος της ανεξαρτησίας και της ακεραιότητας των παρεχόμενων υπηρεσιών πιστοποίησης, ο Φορέας Πιστοποίησης εφαρμόζει σχετική τεκμηριωμένη διαδικασία αμεροληψίας και ακεραιότητας βάσει της Δ09 Αμεροληψίας

& Διαχείριση Διακινδύνευσης, και ελέγχει διαρκώς και με κάθε πρόσφορο μέσο, την ύπαρξη τέτοιων φαινομένων σε κάθε έργο πιστοποίησης που αναλαμβάνεται. Επίσης, ο φορέας πιστοποίησης δεν μπορεί να αναλάβει εσωτερικές επιθεωρήσεις επί του πεδίου εφαρμογής του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών που πρόκειται να επιθεωρήσει και είναι ανεξάρτητος από τον οργανισμό (ή τους οργανισμούς) που παρέχουν εσωτερικές επιθεωρήσεις.

Βάσει του ISO/IEC 27006-1:2024, παρ. 5.2. οι ακόλουθες δραστηριότητες δεν δημιουργούν κάποια σύγκρουση συμφερόντων:

- Διοργάνωση και συμμετοχή ως εισηγητής σε εκπαιδευτικά προγράμματα με αντικείμενο την διαχείριση ασφάλειας πληροφοριών, σχετικά Συστήματα Διαχείρισης ή επιθεώρηση, με την προϋπόθεση ότι σε αυτά τα προγράμματα προσφέρονται για γενικές πληροφορίες και όχι ειδικές συμβουλές σχετικά με την υλοποίηση των αντικειμένων αυτών σε συγκεκριμένο οργανισμό
- Διάθεση ή δημοσιοποίηση (κατόπιν αίτησης) πληροφοριών σχετικά με το πώς ο φορέας πιστοποίησης ερμηνεύει τις απαιτήσεις των προτύπων επιθεωρήσεων πιστοποίησης
- Διενέργεια δραστηριοτήτων πριν από την επιθεώρηση οι οποίες έχουν ως στόχο τον προσδιορισμό της ετοιμότητας του οργανισμού για την επιθεώρηση πιστοποίησης (χωρίς όμως αυτές οι δραστηριότητες να καταλήγουν σε συμβουλή σχετικά με τον τρόπο υλοποίησης και δεν χρησιμοποιούνται για να μειώσουν τον χρόνο της επιθεώρησης)
- Διενέργεια επιθεωρήσεων δευτέρου και τρίτου μέρους προς πρότυπα ή κανονισμούς που δεν ανήκουν στο αντικείμενο της διαπίστευσης
- Αναγνώριση περιθωρίων βελτίωσης κατά τη διάρκεια της επιθεώρησης χωρίς όμως να προτείνουν συγκεκριμένες λύσεις

5.8 Διενέργεια Επιθεώρησης και Χορήγηση Πιστοποίησης

Οι όροι και διαδικασίες για τη υλοποίηση της αξιολόγησης/ επιθεώρησης και την επακόλουθη ή μη χορήγηση σχετικής πιστοποίησης, παρατίθενται και περιγράφονται στο Γενικό Κανονισμό Πιστοποίησης Συστημάτων Διαχείρισης του Φορέα Πιστοποίησης. Στα παρακάτω παρατίθενται εξειδικευμένες απαιτήσεις που σχετίζονται με την επιθεώρηση και αξιολόγηση συμμόρφωσης Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών κατά τα πρότυπα ISO/IEC 27001:2022 και του ISO/IEC 27006-1:2024.Το απαιτούμενα προσόντα για τον αρμόδιο χορήγησης πιστοποίησης παρουσιάζονται στον πίνακα Α1 του ISO/IEC 27006-1:2024 που ενσωματώνεται στην παράγραφο 5.8.1.

5.8.1 Αίτηση και Ανασκόπηση της Αίτησης

Ο φορέας πιστοποίησης απαιτεί από τον πελάτη να έχει ένα τεκμηριωμένο και εφαρμοζόμενο Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών που συμμορφώνεται με το πρότυπο ISO/IEC 27001:2022 και άλλα σχετικά έγγραφα που απαιτούνται για την πιστοποίηση. Κατά τα λοιπά ισχύουν όλα τα προβλεπόμενα στο Γενικό Κανονισμό Πιστοποίησης.

Ο υπεύθυνος ανασκόπησης πρέπει να έχει τα κατάλληλα προσόντα όπως αυτά περιγράφονται τον πίνακα Α1 σύμφωνα με το ISO/IEC 17021-1 και το ISO/IEC 27006-1:2024. Ο Φορέας Πιστοποίησης διαβεβαιώνεται σχετικά με τις γνώσεις του ρόλου αυτού, που πρέπει να κατέχει το τεχνολογικό, νομικό και κανονιστικό πλαίσιο σχετικά με το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών, ώστε να το αξιολογήσει. Ο κάτωθι πίνακας Α1 αποτυπώνει την συνολική γνώση και τις ικανότητες που απαιτούνται για την ανασκόπηση αίτησης, αλλά και τον Αρμόδιο Χορήγησης Πιστοποίησης.

Table A.1 — Knowledge for ISMS auditing and certification			
	Certification functions		
Knowledge	**Conducting the application review to determine audit team competence required, to select the audit team members,and to determine the audit time**	**Reviewing audit reports and making certification decisions**	**Auditing and leading the audit team**
Information security management terminology, principles, practices and techniques		7.1.2.4.2	7.1.2.1.2
Information security management system standards /normative documents	7.1.2.3.1	7.1.2.4.3	7.1.2.1.3
Business management practices			7.1.2.1.4
Client business sector	7.1.2.3.2	7.1.2.4.4	7.1.2.1.5
Client products, processes and organization	7.1.2.3.3	7.1.2.4.5	7.1.2.1.6

5.8.2 Πρόγραμμα Επιθεώρησης και Σχέδιο Επιθεώρησης

Το Πρόγραμμα Επιθεώρησης για τις επιθεωρήσεις Συστημάτων Διαχείρισης Ασφάλειας Πληροφοριών πρέπει να λαμβάνει υπόψιν του και τα control του Annex A που εφαρμόζει ο οργανισμός βάσει της Δήλωσης Εφαρμογής (Statement of Applicability). Κατά τα λοιπά ισχύουν ότι προβλέπεται στο Γενικό Κανονισμό Πιστοποίησης που περιγράφει λεπτομερώς τις απαιτήσεις των παραγράφων 9.1.3 και 9.2.3 του ISO/IEC 17021-1.

Το σχέδιο επιθεώρησης πρέπει να προσδιορίζει τη χρήση βοηθητικών τεχνικών επιθεώρησης που θα χρησιμοποιηθούν κατά τη διάρκεια της επιθεώρησης (σε περίπτωση που αυτές θα χρησιμοποιηθούν), ανάλογα με την περίπτωση. Το δίκτυο βοηθητικών τεχνικών επιθεώρησης μπορεί να περιλαμβάνει, για παράδειγμα, τηλεδιάσκεψη, διαδικτυακή σύσκεψη, διαδραστική επικοινωνία που βασίζεται στο διαδίκτυο και απομακρυσμένη ηλεκτρονική πρόσβαση στην τεκμηρίωση ή τις διεργασίες του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών. Η εστίαση των εν λόγω τεχνικών θα πρέπει να ενισχύει την αποτελεσματικότητα και αποδοτικότητα της επιθεώρησης και να διασφαλίζει την ακεραιότητα της διεργασίας επιθεώρησης.

5.8.3 Καθορισμός Χρόνου Επιθεώρησης

Για τις αρχικές επιθεωρήσεις ισχύει ο παρακάτω πίνακας με παραπομπές στις παραγράφους του ISO/IEC 27006-1:2024.

Number of persons doing work under the organization's control	ISMS audit time for initial audit (auditor days)		Number of persons doing work under the organization's control	ISMS audit time for initial audit (auditor days)
1~10	5		876~1175	18.5
11~15	6		1176~1550	19.5
16~25	7		1551~2025	21
26~45	8.5		2026~2675	22
46~65	10		2676~3450	23
66~85	11		3451~4350	24
86~125	12		4351~5450	25
126~175	13		5451~6800	26
176~275	14		6801~8500	27
276~425	15		8501~10700	28
426~625	16.5		> 10,700	Follow progression above

Table B.1 — Audit time chart

Για τις επιθεωρήσεις πιστοποίησης ισχύουν όλα όσα περιγράφονται στο Γενικό Κανονισμό Πιστοποίησης (1/3 του αρχικού χρόνου για την επιτήρηση και 2/3 για την επαναξιολόγηση).

Οι τιμές που εμφανίζονται στην στήλη «ISMS audit time for initial audit (auditor days)» του παραπάνω πίνακα, αποτελούν την τιμή βάσης της αρχικής επιθεώρησης και μπορεί να αυξηθούν ή μειωθούν βάση της πολυπλοκότητας του οργανισμού.

Οι τιμές αυτές περιλαμβάνουν τον χρόνο που απαιτείται για την διενέργεια του 1ου Σταδίου, του 2ου Σταδίου, της προετοιμασίας, της δημιουργίας της έκθεσης επιθεώρησης και της συνολικής τεκμηρίωσης της επιθεώρησης.

Για τον προσδιορισμό της πολυπλοκότητας του συστήματος, και χρησιμοποιώντας τα στοιχεία που δίδονται από τον οργανισμό στην αίτηση, χρησιμοποιούνται οι ακόλουθοι πίνακες του παραρτήματος C του ISO/IEC 27006-1:2024.

Factors (see B.3.4)	Table C.1 — Classification of factors for calculating audit time		
	Impact on effort		
	Reduced effort	Normal effort	Increased effort
a) complexity of the ISMS: • information security requirements [confidentiality, integrity and availability, (CIA)] • number of critical assets • number of processes and services	• Only little sensitive or confidential information, low availability requirements • Few critical assets (in terms of CIA) • Only one key business process with few interfaces and few business units involved	• Higher availability requirements or some sensitive / confidential information • Some critical assets • 2–3 simple business processes with few interfaces and few business units involved	• Higher amount of sensitive or confidential information (e.g. health, personally identifiable information, insurance, banking) or high availability requirements • Many critical assets • More than 2 complex processes with many interfaces and business units involved
b) the type(s) of business performed within scope of the ISMS	• Low risk business without regulatory requirements	• High regulatory requirements	• High risk business with (only) limited regulatory requirements
c) previously demonstrated performance of the ISMS	• Recently certified • Not certified but ISMS fully implemented over several audit and improvement cycles, including documented internal audits, management reviews and effective continual improvement system	• Recent surveillance audit • Not certified but partially implemented ISMS: Some management system tools are available and implemented; some continual improvement processes are in place but partially documented	• No certification and no recent audits • ISMS is new and not fully established • (e.g. lack of management system specific control mechanisms immature • continual improvement processes, • ad hoc process execution)
d) extent and diversity of technology utilized in the implementation	• Highly standardized environment with low diversity (few IT-platforms, servers,	• Standardized but diverse IT platforms, servers, operating systems, databases, networks	• High diversity or complexity of IT • (e.g. many different segments of networks, types of servers or databases,

of the various components of the ISMS (e.g. number of different IT plat- forms, number of segregated networks)	operating systems, data- bases, networks, etc.)		• number of key applications)
e) extent of outsourcing and third-party arrangements used within the scope of the ISMS	• No outsourcing and little dependency on suppliers, or • Well-defined, managed and monitored outsourcing arrangements • Outsourcer has a certified ISMS • Relevant independent assurance reports are available	• Several partly managed outsourcing • arrangements	• High dependency on outsourcing or suppliers with large impact on important business activities, or • Unknown amount or extent of outsourcing, or • Several unmanaged outsourcing arrangements
f) extent of information system development	• No in-house system development • Use of standardized software plat- forms	• Use of standardized software plat- forms with complex configuration/ parameterization • (Highly) customized software • Some development activities (in-house or outsourced)	• Extensive internal software development activities with several ongoing projects for important business purpose
g) number of sites and number of Disaster Recovery (DR) sites	• Low availability requirements and • no or one alternative DR site	• Medium or High availability requirements and no or one alternative DR site	• High availability requirements e.g.24/7 services • Several alternative DR sites • Several Data Centers
h) for surveillance or re-certification audit: The amount and extent of change relevant to the ISMS in accordance with ISO/IEC 17021-1, 8.5.3	• No changes since last recertification audit	• Minor changes in scope or SoA of ISMS, e.g. some policies, documents, etc. • Minor changes in the factors above	• Major changes in scope or SoA of ISMS, e.g. new processes, new business units, areas, risk assessment management methodology, policies, documentation, risk treatment • Major changes in the factors above

C.2 - Factors related to business and organization (other than IT)		
Type(s) of business and regulatory requirements		1. Organization works in non-critical business sectors and non-regulated sectors *
		2. Organization has customers in critical business sectors *
		3. Organization works in critical business sectors *
Process and tasks		1. Standard processes with standard and repetitive tasks; lots of persons doing work under the organization's control carrying out the same tasks; few products or services
		2. Standard but non-repetitive processes, with high number of products or services
		3. Complex processes, high number of products and services, many business units included in the scope of certification (ISMS covers highly complex processes or relatively high number or unique activities)

Level of establishment of the MS		1. ISMS is already well established and/or other management systems are in place
		2. Some elements of other management systems are implemented, others not
		3. No other management system implemented at all, the ISMS is new and not established
* Critical business sectors are sectors that may affect critical public services that will cause risk to health, security, economy, image and government ability to function that may have a very large negative impact to the country.		

C.3 — Factors related to IT environment		
IT infrastructure complexity		1. Few or highly standardized IT platforms, servers, operating systems, databases, networks, etc.
		2. Several different IT platforms, servers, operating systems, databases, networks
		3. Many different IT platforms, servers, operating systems, databases, networks
Dependency on outsourcing and suppliers, including cloud services		1. Little or no dependency on outsourcing or suppliers
		2. Some dependency on outsourcing or suppliers, related to some but not all important business activities
		3. High dependency on outsourcing or suppliers, large impact on important business activities
Information System development		1. None or a very limited in-house system/application development
		2. Some in-house or outsourced system/application development for some important business purposes
		3. Extensive in-house or outsourced system/application development for important business purposes

C.4 — Impact of factors on audit time				
	IT complexity			
		Low (from 3 to 4)	**Medium (from 5 to 6)**	**High (from 7 to 9)**
Business complexity	**High (from 7 to 9)**	+5 % to +20 %	+10 % to +50 %	+20 % to +100 %
	Medium (from 5 to 6)	-5 % to -10 %	0 %	+10 % to +50 %
	Low (from 3 to 4)	-10 % to -30 %	-5 % to -10 %	+5 % to 20 %

5.8.4 Δειγματοληψία Πολλαπλών Εγκαταστάσεων

Όπου ένας πελάτης έχει μια σειρά από τοποθεσίες (sites) που πληρούν τα κριτήρια από το a) ως το c) παρακάτω, ο Φορέας Πιστοποίησης εξετάζει χρησιμοποιώντας μια προσέγγιση βασισμένη σε δείγμα προς επιθεώρηση πιστοποίησης πολλαπλών τοποθεσιών:

a) Όλα τα sites λειτουργούν κάτω από το ίδιο ΣΔΑΠ, που διαχειρίζεται κεντρικά, και υπόκεινται σε κεντρική ανασκόπηση από τη Διοίκηση.

b) Όλες οι τοποθεσίες περιλαμβάνονται στο πρόγραμμα επιθεώρησης του ΣΔΑΠ του πελάτη.

c) Όλες οι τοποθεσίες περιλαμβάνονται στο πρόγραμμα ανασκόπησης του ΣΔΑΠ του πελάτη.

Ο Φορέας Πιστοποίησης σύμφωνα και με τα προβλεπόμενα στο Γενικό Κανονισμό Πιστοποίησης διαθέτει μια προσέγγιση βασισμένη σε δειγματοληψία πολλαπλών εγκαταστάσεων, που για το ΣΔΑΠ εξασφαλίζει επιπλέον τα ακόλουθα:

a) Η ανασκόπηση της αρχικής σύμβασης προσδιορίζει, για το μεγαλύτερο δυνατό βαθμό, τη διαφορά μεταξύ των sites, ώστε να μπορεί να καθοριστεί ένα επαρκές επίπεδο της δειγματοληψίας.
b) Έχουν ληφθεί για δειγματοληψία αντιπροσωπευτικού αριθμού των τοποθεσιών από τον Φορέα Πιστοποίησης, λαμβάνοντας υπόψη:
    1) τα αποτελέσματα των εσωτερικών επιθεωρήσεων από τα κεντρικά γραφεία και τις τοποθεσίες,
    2) τα αποτελέσματα της ανασκόπησης από τη Διοίκηση,
    3) παραλλαγές στο μέγεθος των sites,
    4) παραλλαγές στον επιχειρησιακό/ επιχειρηματικό σκοπό των sites,
    5) πολυπλοκότητα των πληροφοριακών συστημάτων ή συστημάτων πληροφοριών των διαφορετικών sites,
    6) διαφοροποιήσεις στις εργασιακές πρακτικές.
    7) παραλλαγές σε δραστηριότητες που αναλαμβάνονται,
    8) παραλλαγές του σχεδιασμού και της λειτουργίας των ελέγχων,
    9) πιθανή αλληλεπίδραση με κρίσιμα πληροφοριακά συστήματα ή συστήματα πληροφοριών για επεξεργασία ευαίσθητων πληροφοριών,
    10) τυχόν διαφορετικές νομικές απαιτήσεις,
    11) γεωγραφικές και πολιτιστικές πτυχές,
    12) κατάσταση επιπέδου επικινδυνότητας των sites,
    13) περιστατικά ασφάλειας πληροφοριών στις συγκεκριμένες τοποθεσίες.
c) Ένα αντιπροσωπευτικό δείγμα επιλέγεται από όλα τα sites εντός του πεδίου εφαρμογής του ΣΔΑΠ του πελάτη. Αυτή η επιλογή βασίζεται σε ρυθμιστική επιλογή που αντανακλά τους παράγοντες που παρουσιάζονται στο στοιχείο b).
d) Κάθε τοποθεσία που περιλαμβάνεται στο ΣΔΑΠ και υπόκειται σε σημαντικούς κινδύνους επιθεωρείται από τον φορέα πιστοποίησης πριν από την πιστοποίηση.
e) Το πρόγραμμα επιθεώρησης έχει σχεδιαστεί λαμβάνοντας υπόψη τις ανωτέρω απαιτήσεις και καλύπτει αντιπροσωπευτικά δείγματα από το πεδίο εφαρμογής της πιστοποίησης του ΣΔΑΠ εντός περιόδου τριών ετών.

f) Στην περίπτωση εντοπισμού μιας μη συμμόρφωσης, είτε στα κεντρικά γραφεία είτε σε ένα μόνο site, η διορθωτική ενέργεια ισχύει για τα κεντρικά γραφεία και όλες τις τοποθεσίες που καλύπτονται από το πιστοποιητικό.

Η επιθεώρηση πρέπει να καλύπτει δραστηριότητες στην έδρα του πελάτη, ώστε να διασφαλίσει ότι το ΣΔΑΠ ισχύει για όλες τις τοποθεσίες και αντικατοπτρίζει την κεντρική διαχείριση σε επιχειρησιακό επίπεδο. Η επιθεώρηση πρέπει να καλύπτει όλα τα θέματα που περιγράφονται παραπάνω.

Ο αριθμός των ανθρωποημερών ανά τοποθεσία, συμπεριλαμβανομένου της έδρας/ του κεντρικού γραφείου, υπολογίζεται για κάθε τοποθεσία. Μειώσεις μπορεί να εφαρμοστούν για να ληφθούν υπόψη τα τμήματα της επιθεώρησης που δεν είναι σχετικές σε ό,τι αφορά την έδρα/ το κεντρικό γραφείο ή τις ανά τοποθεσία διευθύνσεις. Οι λόγοι πρέπει να καταγράφονται κατά την ανασκόπηση αίτησης εντός του εντύπου ΕΔ10-4 Ανασκόπηση Αίτησης ISO 27001.

5.8.5 Ενέργειες πριν τη διεξαγωγή της επιθεώρησης

Ο Φορέας Πιστοποίησης απαιτεί σε κάθε περίπτωση ο πελάτης να διενεργεί όλες τις απαραίτητες διευθετήσεις για την πρόσβαση σε εκθέσεις εσωτερικών επιθεωρήσεων και εκθέσεις από ανεξάρτητες αξιολογήσεις της ασφάλειας των πληροφοριών. Τουλάχιστον οι ακόλουθες πληροφορίες πρέπει να παρέχονται από τον πελάτη κατά το στάδιο 1 της επιθεώρησης αρχικής πιστοποίησης:

a) Γενικές πληροφορίες σχετικά με το ΣΔΑΠ και τις δραστηριότητες που καλύπτονται,
b) Ένα αντίγραφο της απαιτούμενης τεκμηρίωσης του ΣΔΑΠ

Ενδεικτικά:

- Πολιτική Ασφαλείας
- Πεδίο Εφαρμογής
- Πολιτική Ασφάλειας Πληροφοριών
- Διαδικασία Αξιολόγησης Κινδύνου
- Δήλωση Εφαρμογής
- Στόχοι Ασφάλειας
- Πρόγραμμα Εσωτερικών Επιθεωρήσεων
- Αποτελέσματα της τελευταίας εσωτερικής επιθεώρησης
- Πρακτικά της τελευταίας ανασκόπησης από τη διοίκηση

Ο Φορέας Πιστοποίησης δεν πιστοποιεί ένα ΣΔΑΠ εκτός και αν έχει εφαρμοστεί τουλάχιστον μία φορά με την ολοκλήρωση μίας ανασκόπησης από τη διοίκηση και μίας εσωτερικής επιθεώρησης που καλύπτει το πεδίο της πιστοποίησης.

Πεδίο Εφαρμογής

Η ομάδα επιθεώρησης θα επιθεωρήσει τον αιτούμενο οργανισμό στο πεδίο εφαρμογής που έχει αιτηθεί σύμφωνα με όλες τις εφαρμόσιμες απαιτήσεις πιστοποίησης. Σε κάθε περίπτωση κανένας οργανισμός δεν μπορεί να αιτηθεί πιστοποίηση έναντι των απαιτήσεων του ISO/IEC 27001:2022 εξαιρώντας οποιαδήποτε από τις απαιτήσεις που περιέχονται στις παραγράφους 4 έως 10 του προτύπου. Οι απαιτήσεις αυτές εμπλουτίζονται ανά περίπτωση με τις αντίστοιχες απαιτήσεις των Controls του Annex A του προτύπου, που εφαρμόζονται από τον οργανισμό βάσει των επιθυμιών του, της διεργασίας διαχείρισης κινδύνου και αποτυπώνονται στην Δήλωση Εφαρμογής του (Statement of Applicability).

Η ομάδα επιθεώρησης θα επιβεβαιώσει ότι οι απαιτήσεις του προτύπου ISO/IEC 27001:2022 παρ. 4.3. πληρούνται όσον αφορά το πεδίο εφαρμογής.

Η έκφραση του πεδίου εφαρμογής δεν είναι παραπλανητική, δεν περιέχει αναγραφές σε προϊόντα, ενώ λέξεις όπως «Ασφαλές», «Ασφάλεια», «Εξασφάλιση» κ.λπ. δεν αναφέρονται στο επίπεδο ασφάλειας του οργανισμού και δεν υπονοείται ότι η συγκεκριμένη υπηρεσία ή διεργασία είναι πιο διασφαλισμένη από κάποια άλλη.

Ο Φορέας Πιστοποίησης οφείλει να εξασφαλίσει ότι η διαδικασία και τα αποτελέσματα της αξιολόγησης και αντιμετώπισης κινδύνων αντικατοπτρίζουν τις δραστηριότητες και τα όριά τους όπως αυτό φαίνεται στο πεδίο εφαρμογής. Το ίδιο πρέπει να ισχύει και για την Δήλωση Εφαρμογής. Ο Φορέας Πιστοποίησης απαιτείται να επαληθεύσει ότι υπάρχει μια Δήλωση Εφαρμογής ανά πεδίο εφαρμογής.

Ο Φορέας Πιστοποίησης θα πρέπει να διασφαλίζει ότι οι διεπαφές με υπηρεσίες και δραστηριότητες που δεν είναι (πλήρως ή μερικώς) εντός πεδίου εφαρμογής του ΣΔΑΠ έχουν αναγνωριστεί και αποτυπώνονται και μέσα από την διεργασία της διαχείρισης κινδύνου.

5.8.6 Διενέργεια της επιθεώρησης

Οι επιθεωρήσεις διενεργούνται από την κατάλληλα ορισμένη Ομάδα Επιθεώρησης που δύναται να αποτελείται από Επιθεωρητές και Τεχνικούς Εμπειρογνώμονες υπό την καθοδήγηση και το συντονισμό ενός Επικεφαλής Επιθεωρητή, σύμφωνα με τις

Διαδικασίες, Οδηγίες Εργασίας και τα Έντυπα που έχει συντάξει ο Φορέας Πιστοποίησης και αποτελούν πνευματική ιδιοκτησία του. Αυτές είναι οι ακόλουθες:

- Διαδικασία Πιστοποίησης και τα σχετικά Έντυπα,
- Διαδικασία Ελέγχου Χρήσης Λογότυπου και Σημάτων,
- Διαδικασίες που αφορούν το Προσωπικό και τα σχετικά Έντυπα,
- Διαδικασία Αμεροληψίας,
- Διαδικασία Προστασίας της Εμπιστευτικότητας,
- Γενικός Κανονισμός Πιστοποίησης,
- Ειδικός Κανονισμός Πιστοποίησης ISO/IEC 27001:2022,

Οι αντικειμενικοί σκοποί της επιθεώρησης πρέπει να περιλαμβάνουν τον καθορισμό της αποτελεσματικότητας του συστήματος διαχείρισης, ώστε να επιβεβαιωθεί ότι ο πελάτης, βάσει της αξιολόγησης των κινδύνων έχει υλοποιήσει εφαρμόσιμους ελέγχους και έχει επιτύχει τους στόχους της ασφάλειας επικοινωνίας.

Η ομάδα επιθεώρησης καθορίζεται επίσημα κατά την ανασκόπηση της αίτησης και εφοδιάζεται με τα κατάλληλα έγγραφα εργασίας. Η εντολή που δίνεται στην ομάδα επιθεώρησης καθορίζεται σαφώς και γνωστοποιείται στο πελάτη. Μια ομάδα επιθεώρησης μπορεί να αποτελείται από ένα άτομο, υπό την προϋπόθεση ότι το πρόσωπο αυτό πληροί όλα τα κριτήρια που ορίζονται ανωτέρω.

Οι ενέργειες που συνθέτουν την επιθεώρηση στο πλαίσιο της επιζητούμενης πιστοποίησης, καθώς και οι μέθοδοι και τεχνικές που εφαρμόζονται, περιγράφονται στο Γενικό Κανονισμό Πιστοποίησης του Φορέα Πιστοποίησης. Στα ακόλουθα σημεία εξειδικεύεται το περιεχόμενο της επιθεώρησης και αναφέρονται συνοπτικά οι πτυχές του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών κατά ISO/IEC 27001:2022, που ελέγχονται και των οποίων αξιολογείται ο βαθμός συμμόρφωσης με τις αντίστοιχες απαιτήσεις που θέτει το διεθνές πρότυπο.

Το χρονικό διάστημα μεταξύ 1ου και 2ου Σταδίου δεν μπορεί να υπερβεί τους έξι (6) μήνες και σε αντίθετη περίπτωση επαναλαμβάνεται πλήρως το Στάδιο 1. Επισημαίνεται ρητά ότι εάν προκύψει ότι ο βαθμός συμμόρφωσης του επιθεωρούμενου οργανισμού, ο οποίος διερευνάται κατά το Στάδιο 1, δεν συμμορφώνεται με βασικές απαιτήσεις του προτύπου, μπορεί να σηματοδοτήσει αδυναμία εκτέλεσης του Σταδίου 2. Τούτο καθίσταται σαφές και γραπτώς στον επιθεωρούμενο οργανισμό, ο οποίος διά του εκπροσώπου του λαμβάνει ενυπόγραφα γνώση περί των αποτελεσμάτων της επιθεώρησης του Σταδίου 1.

Το Στάδιο 1 ενέχει τους ακόλουθους στόχους:

- να διαπιστωθεί ο βαθμός ετοιμότητας που επιδεικνύει ο επιθεωρούμενος οργανισμός για την επιθεώρηση του Σταδίου 2,
- να συλλεγούν όλα εκείνα τα αναγκαία δεδομένα και στοιχεία ώστε να σχεδιαστεί κατάλληλα και επαρκώς το πρόγραμμα της επιθεώρησης του Σταδίου 2,
- να ανασκοπηθεί
- και να επιβεβαιωθεί ότι ο επιθεωρούμενος οργανισμός έχει σχεδιάσει, υλοποιήσει και εφαρμόσει την βασική και απαιτητή από το πρότυπο ISO/IEC 27001:2022 τεκμηρίωση.

Ειδικότερα, κατά το Στάδιο 1, αξιολογούνται και ελέγχονται:

- Η καταλληλότητα του σχεδιασμού του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών σε ό,τι αφορά τη δυνατότητα κάλυψης των σκοπών, στόχων και της καθιερωμένης πολιτικής του οργανισμού (Ελέγχεται η τεκμηρίωση του πελάτη που απαιτείται στο πρότυπο ISO/IEC 27001:2022, η επαρκής κατανόηση του σχεδιασμού του ΣΔΑΠ στο πλαίσιο της οργάνωσης του πελάτη, η εκτίμηση κινδύνων και ο μετριασμός τους συμπεριλαμβανομένων των ελέγχων που καθορίζονται, η πολιτική ασφάλειας πληροφοριών και οι στόχοι).
- Κατά πόσον η διαπιστωμένη έκταση εφαρμογής των προβλέψεων του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών δικαιολογεί τη διενέργεια του επόμενου σταδίου της επιθεώρησης (Στάδιο 2).
- Ο βαθμός συμμόρφωσης των προγραμμάτων επαλήθευσης, επικύρωσης και βελτίωσης της αποτελεσματικότητας του εφαρμοζόμενου Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών με τις απαιτήσεις του εφαρμόσιμου προτύπου.
- Η διενέργεια Εσωτερικής Επιθεώρησης και Ανασκόπησης από τη Διοίκηση.
- Ο εντοπισμός περιπτώσεων και αδυναμιών στην εφαρμογή του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών που μπορεί να προκαλέσουν εμφάνιση δυνητικών μη συμμορφώσεων και χρήζουν ιδιαίτερης προσοχής κατά τη διεξαγωγή της τελικής αξιολόγησης συμμόρφωσης.

Με βάση τα ευρήματα που τεκμηριώνονται στο Στάδιο 1 στην έκθεση επιθεώρησης, αναπτύσσεται ένα σχέδιο επιθεώρησης για τη διεξαγωγή του Σταδίου 2. Εκτός από την αξιολόγηση της αποτελεσματικής εφαρμογής του ΣΔΑΠ σύμφωνα με το ISO/IEC 27001:2022, οι στόχοι του Σταδίου 2 αφορούν την επιβεβαίωση ότι ο πελάτης τηρεί τις δικές του πολιτικές, στόχους και διαδικασίες.

Για να γίνει αυτό, η επιθεώρηση θα επικεντρωθεί στα παρακάτω θέματα του πελάτη:

a) δέσμευση της Ανώτατης Διοίκησης για την πολιτική ασφάλειας πληροφοριών και τους στόχους της ασφάλειας πληροφοριών,
b) απαιτήσεις τεκμηρίωσης που περιλαμβάνονται στο πρότυπο ISO/IEC 27001:2022,
c) αξιολόγηση της ασφάλειας των πληροφοριών που σχετίζονται με τους κινδύνους και ότι οι εκτιμήσεις επικινδυνότητας παράγουν συνεπή, έγκυρα και συγκρίσιμα αποτελέσματα εάν η εκδήλωση των κινδύνων επαναληφθεί,
d) Προσδιορισμός των Control Objectives και Controls βάσει της αξιολόγησης κινδύνων για την ασφάλεια πληροφοριών και των διεργασιών αντιμετώπισής τους,
e) πληροφορίες επιδόσεων ασφαλείας και αποτελεσματικότητα του ΣΔΑΠ, αξιολόγηση σε σχέση με τους στόχους ασφάλειας πληροφοριών,
f) αντιστοιχία μεταξύ των καθορισμένων controls, τη Δήλωση Εφαρμογής και τα αποτελέσματα της αξιολόγησης των κινδύνων ασφάλειας πληροφοριών και τη διεργασία αντιμετώπισης και την πολιτική ασφάλειας πληροφοριών και τους στόχους.
g) εφαρμογή των controls, λαμβάνοντας υπόψη το εσωτερικό και εξωτερικό πλαίσιο λειτουργίας και τους συναφείς κινδύνους, την παρακολούθηση, μέτρηση και ανάλυση των διεργασιών ασφάλειας πληροφοριών του οργανισμού και τους ελέγχους, για να προσδιορισθεί αν τα στοιχεία ελέγχου είναι εφαρμοστέα και ανταποκρίνονται στους δεδηλωμένους στόχους ασφάλειας πληροφοριών,
h) τα προγράμματα, διεργασίες, διαδικασίες, αρχεία, εσωτερικές επιθεωρήσεις και ανασκοπήσεις της αποτελεσματικότητας του ΣΔΑΠ για να εξασφαλιστεί ότι αυτά είναι ανιχνεύσιμα στις αποφάσεις της Ανώτατης Διοίκησης και την πολιτική ασφάλειας πληροφοριών και τους στόχους.

Η Ομάδα Επιθεώρησης πρέπει να:

a) απαιτεί από τον πελάτη να αποδείξει ότι η αξιολόγηση της ασφάλειας πληροφοριών που σχετίζονται με τους κινδύνους είναι συναφείς και επαρκείς για τη λειτουργία του ΣΔΑΠ και εντός του πεδίου του ΣΔΑΠ.
b) διαπιστώσει κατά πόσον οι διαδικασίες του πελάτη για την ταυτοποίηση, την εξέταση και την αξιολόγηση της ασφάλειας των πληροφοριών που σχετίζονται με τους κινδύνους και τα αποτελέσματα της εφαρμογής τους είναι συνεπείς με την πολιτική, των σκοπών και των στόχων του πελάτη. Ο φορέας πιστοποίησης αποφασίζει, επίσης, εάν οι διαδικασίες που χρησιμοποιούνται στην αξιολόγηση των κινδύνων είναι κατάλληλες και εφαρμόζονται σωστά.

Σε ό,τι αφορά την έκθεση επιθεώρησης, εκτός από τις απαιτήσεις οι οποίες προβλέπονται στο πρότυπο ISO/IEC 17021-1, αυτή πρέπει να παρέχει και τις ακόλουθες πληροφορίες ή μια αναφορά σε αυτές:

a) μία σύνοψη της ανασκόπησης των εγγράφων,
b) την ανάλυση κινδύνου για την ασφάλεια πληροφοριών του πελάτη,
c) τυχόν αποκλίσεις από το πρόγραμμα επιθεώρησης (π.χ. περισσότερο ή λιγότερο χρόνο που δαπανάται σε ορισμένες τακτικές δραστηριότητες),
d) το πεδίο πιστοποίησης ΣΔΑΠ.

Η έκθεση επιθεώρησης είναι επαρκώς λεπτομερής, ώστε να διευκολύνει και να υποστηρίζει την απόφαση πιστοποίησης. Περιλαμβάνει τα ακόλουθα:

a) σημαντικές τεχνικές και τη μεθοδολογία επιθεώρησης που χρησιμοποιήθηκαν,
b) παρατηρήσεις που έγιναν, τόσο θετικές (π.χ. αξιοσημείωτα χαρακτηριστικά) όσο και αρνητικές (π.χ. πιθανές μη συμμορφώσεις)
c) σχόλια σχετικά με τη συμμόρφωση του ΣΔΑΠ του πελάτη με τις απαιτήσεις πιστοποίησης με μια σαφή δήλωση της μη συμμόρφωσης, μια αναφορά στην έκδοση της Δήλωσης Εφαρμογής και, ενδεχομένως, οποιαδήποτε χρήσιμη σύγκριση με τα αποτελέσματα της προηγούμενης επιθεώρησης πιστοποίησης του πελάτη. Συμπλήρωση ερωτηματολογίων, λιστών ελέγχου, παρατηρήσεις, σημειώσεις επιθεωρητών μπορεί να αποτελούν αναπόσπαστο μέρος της έκθεσης επιθεώρησης. Τα έγγραφα αυτά υποβάλλονται στον Φορέα Πιστοποίησης ως αποδεικτικά στοιχεία προς υποστήριξη της απόφασης χορήγησης πιστοποίησης. Πληροφορίες σχετικά με τα δείγματα που αξιολογούνται κατά τη διάρκεια της επιθεώρησης περιλαμβάνονται στην έκθεση επιθεώρησης. Η έκθεση εξετάζει την επάρκεια του πελάτη, την εσωτερική οργάνωση και τις διαδικασίες που εγκρίθηκαν από τον πελάτη για να εφαρμόσει το επιθεωρούμενο ΣΔΑΠ. Εκτός από τις απαιτήσεις που αναφέρονται στο ISO/IEC 17021-1, η έκθεση επιθεώρησης καλύπτει:
    - μια περίληψη από τις πιο σημαντικές παρατηρήσεις, θετικές καθώς και αρνητικές, όσον αφορά την εφαρμογή και την αποτελεσματικότητα απαιτήσεων και των ελέγχων του ΣΔΑΠ.
    - συστάσεις της ομάδας επιθεώρησης ως προς το κατά πόσον θα πρέπει να πιστοποιείται το ΣΔΑΠ του πελάτη ή όχι με αντίστοιχο πληροφοριακό υλικό ή επεξηγήσεις για να τεκμηριωθεί αυτή η σύσταση.

5.8.7 Επιτήρηση

Σκοπός της επιτήρησης είναι να επιβεβαιώσει ότι το εγκεκριμένο ΣΔΑΠ εξακολουθεί να εφαρμόζεται, να διατηρείται, να ανασκοπείται με τις επιπτώσεις των αλλαγών. Η επιθεώρηση επιτήρησης για να επιβεβαιώσει τη συνεχή συμμόρφωση με τις απαιτήσεις πιστοποίησης πρέπει να καλύπτει κατ' ελάχιστον:

a) τα στοιχεία συντήρησης του συστήματος όπως η αξιολόγηση των διακινδυνεύσεων και ο έλεγχος των απειλών για την ασφάλεια πληροφοριών, η Εσωτερική Επιθεώρηση του ΣΔΑΠ, η Ανασκόπηση από τη Διοίκηση και οι Διορθωτικές Ενέργειες,
b) επικοινωνία με τα εξωτερικά μέρη όπως απαιτείται από το πρότυπο ISO/IEC 27001:2022 και άλλα έγγραφα που απαιτούνται για την πιστοποίηση,
c) αλλαγές στη τεκμηρίωση του συστήματος,
d) περιοχές που υπόκεινται σε αλλαγές,
e) επιλεγμένες απαιτήσεις του ISO/IEC 27001:2022,
f) άλλες επιλεγμένες περιοχές ανάλογα με την περίπτωση.

Κατ' ελάχιστον σε κάθε επιτήρηση η ομάδα επιθεώρησης ανασκοπεί τα εξής:

a) την αποτελεσματικότητα του ΣΔΑΠ όσον αφορά την επίτευξη των στόχων της πολιτικής ασφάλειας πληροφοριών του πελάτη,
b) τη λειτουργία των διαδικασιών για την περιοδική αξιολόγηση και επανεξέταση της συμμόρφωσης με τις σχετικές πληροφορίες ασφαλείας, την κείμενη νομοθεσία και τους εφαρμοστέους κανονισμούς,
c) αλλαγές στους ελέγχους που καθορίζονται και τα αποτελέσματα των αλλαγών,
d) εφαρμογή και αποτελεσματικότητα των ελέγχων σύμφωνα με το πρόγραμμα επιθεώρησης.
e) προσφυγές και καταγγελίες
f) τυχόν μη συμμορφώσεις και παρατηρήσεις από προηγούμενη επιθεώρηση του ΣΔΑΠ

Οι επιθεωρήσεις επιτήρησης μπορεί να συνδυαστούν με επιτηρήσεις άλλων συστημάτων διαχείρισης, σύμφωνα με τα προβλεπόμενα στο Γενικό Κανονισμό Πιστοποίησης. Η αναφορά πρέπει να αναφέρει σαφώς τις πτυχές που σχετίζονται με κάθε σύστημα διαχείρισης.

5.8.8 Επαναπιστοποίηση

Αν κριθεί σκόπιμη η υλοποίηση πλήρους επαναξιολόγησης είτε λόγω χαμηλού βαθμού συμμόρφωσης του ΣΔΑΠ του οργανισμού με τις απαιτήσεις του προτύπου, είτε λόγω λήξης της τριετούς διάρκειας ισχύος της αρχικής πιστοποίησης (επίσκεψη επαναπιστοποίησης του τρίτου έτους) τότε αυτή εκτελείται με τους όρους και τις προϋποθέσεις που ισχύουν για την αρχική επιθεώρηση χωρίς να πραγματοποιείται η επιθεώρηση σε δύο στάδια υποχρεωτικά. Αίτηση δεν είναι απαραίτητο να υποβληθεί εκ νέου, εκτός εάν έχουν υπάρξει σημαντικές μεταβολές στο εφαρμοζόμενο ΣΔΑΠ ή επιζητείται επέκταση του πεδίου πιστοποίησης.

Για τις ανάγκες επαναπιστοποίησης δύναται η Ομάδα Επιθεώρησης που ορίζεται, να είναι διαφορετικής σύνθεσης ως προς τα πρόσωπα, από την Ομάδα που επιτέλεσε την αρχική επιθεώρηση ή/και τις ενδιάμεσες υποχρεωτικές επιτηρήσεις του πρώτου και του δεύτερου έτους ισχύος της αρχικής πιστοποίησης.

5.8.9 Χορήγηση Πιστοποίησης

Η απόφαση πιστοποίησης πρέπει να βασίζεται, επιπλέον των απαιτήσεων του ISO/IEC 17021-1, στη σύσταση της ομάδας επιθεώρησης για την χορήγηση πιστοποίησης όπως προβλέπεται στην έκθεση πιστοποίησής τους. Τα πρόσωπα που λαμβάνουν την απόφαση για τη χορήγηση πιστοποίησης δεν πρέπει κανονικά να ανατρέψουν μια αρνητική σύσταση της ομάδας επιθεώρησης. Εάν προκύψει μια τέτοια κατάσταση, ο οργανισμός πρέπει να το αποδείξει εγγράφως, ώστε να δικαιολογείται η απόφαση για την ανατροπή της σύστασης. Πιστοποίηση δεν χορηγείται στον πελάτη έως ότου υπάρξουν επαρκή αποδεικτικά στοιχεία για να αποδείξουν ότι οι ρυθμίσεις και οι σχετικές ενέργειες για τη διαχείριση των σχολίων και των εσωτερικών επιθεωρήσεων του ΣΔΑΠ έχουν υλοποιηθεί, είναι αποτελεσματικές και διατηρούνται.

5.8.10 Ισχύς, Ανανέωση, Επαναπιστοποίηση και Παύση

5.8.10.1 Ισχύς πιστοποίησης

Η περίοδος ισχύος της πιστοποίησης είναι τρία (3) έτη από την ημερομηνία πιστοποίησης που αναγράφεται στο Πιστοποιητικό Συμμόρφωσης, υπό την ελάχιστη προϋπόθεση της ετήσιας επιτήρησης. Συγκεκριμένα η 1η επιτήρηση διενεργείται εντός 12 μηνών από της ημερομηνίας ολοκλήρωσης του 2ου Σταδίου της επιθεώρησης αρχικής πιστοποίησης. Ο Φορέας Πιστοποίησης διατηρεί το δικαίωμα και εφόσον κριθεί σκόπιμο σχετικά, να προβεί και σε περισσότερες της μίας επίσκεψης επιτήρησης εντός του ιδίου έτους.

Η πιστοποίηση χάνει την ισχύ της όταν συντρέχουν οι λόγοι που περιγράφονται στο Γενικό Κανονισμό Πιστοποίησης.

5.8.10.2 Ανανέωση Πιστοποίησης

Οι σχετικοί όροι και προϋποθέσεις αναφέρονται εκτενώς στη προηγούμενη παράγραφο και στο Γενικό Κανονισμό Πιστοποίησης.

5.8.10.3 Επαναπιστοποίηση

Οι σχετικοί όροι και προϋποθέσεις αναφέρονται εκτενώς στη προηγούμενη παράγραφο και στο Γενικό Κανονισμό Πιστοποίησης.

5.8.10.4 Παύση Πιστοποίησης

Ένα Πιστοποιητικό Συμμόρφωσης παύει να ισχύει όταν αλλάξει η Δήλωση Εφαρμογής (Statement of Applicability) ή αλλάξει έδρα ο επιθεωρούμενος.

5.8.11 Αρχεία και Αρχειοθέτηση

5.8.11.1 Παύση Τήρησης Αρχείων

Ο Φορέας Πιστοποίησης διατηρεί Αρχείο Πιστοποίησης και Επιτήρησης, σε συνθήκες ασφαλείας και εμπιστευτικά, για όλη τη χρονική περίοδο λειτουργίας και δραστηριοποίησής του και τουλάχιστον για δύο πλήρεις τριετείς κύκλους πιστοποίησης για κάθε επιχείρηση/οργανισμό (πελάτη). Σε αυτό έχουν απεριόριστη πρόσβαση τα εντεταλμένα στελέχη του Φορέα Διαπίστευσης και οι πελάτες μόνο στους υποφακέλους έργων πιστοποίησης που τους αφορούν.

5.8.11.2 Περιεχόμενα Αρχείου Πιστοποίησης και Επιτήρησης

a) Ένας ενημερωμένος κατάλογος όλων των πιστοποιημένων οργανισμών με παρεχόμενη πληροφόρηση για το πεδίο πιστοποίησης και τις εγκαταστάσεις που αυτό αφορά, καθώς και τον σχετικό τεχνικό τομέα.
b) Το πρόγραμμα επιτήρησης των έργων πιστοποίησης.
c) Ένας διακριτός υποφάκελος για κάθε έργο πιστοποίησης που ανελήφθη συμπεριλαμβανομένων έργων που αφορούν οργανισμούς των οποίων έχει λήξει ή ανακληθεί η πιστοποίηση ή δεν χορηγήθηκε αυτή για οποιονδήποτε λόγο κατά την επιθεώρηση και ο οποίος περιέχει:
    - Έντυπα Αιτήσεων και Ανασκόπησης Αιτήσεων και Συμβάσεων,
    - Έκθεση Επιθεώρησης και όλα τα σχετικά Έντυπα που την απαρτίζουν,

- Αντίγραφο του Πιστοποιητικού Συμμόρφωσης που εκδόθηκε,
- Αναφορά στη Δήλωση Εφαρμογής (Statement of Applicability – SOA) βάσει του οποίου έγινε η επιθεώρηση.
- Οιαδήποτε αποδεικτικά στοιχεία ελήφθησαν ως τεκμήρια άρσης μη συμμορφώσεων και προβλημάτων.

6. Έντυπα

Για τις ανάγκες της τεκμηρίωσης του ΦΠ χρησιμοποιούνται τα παρακάτω έντυπα σε ηλεκτρονική ή φυσική μορφή:

Α/Α	ΚΩΔΙΚΟΣ	ΠΕΡΙΓΡΑΦΗ	ΧΡΟΝΟΣ ΤΗΡΗΣΗΣ	ΥΠΕΥΘΥΝΟΣ
1	ΕΔ10-1	Αίτηση Πιστοποίησης	≥ 6 έτη	Υ.Δ.Σ.
2	ΕΔ10-1 Παράρτημα Α ISO 27001:2022	Παράρτημα Αίτησης Α ISO 27001:2022	≥ 6 έτη	Υ.Δ.Σ.
3	ΕΔ10-4	Ανασκόπησης Αίτησης ISO 27001:2022	≥ 6 έτη	Υ.Δ.Σ.
4	ΕΔ11-1	Σχέδιο Επιθεώρησης 27001	≥ 6 έτη	Υ.Δ.Σ.
5	ΕΔ11-2Β	Αναφορά – Κατάλογος Σημείων Ελέγχου Σταδίου 1 ISO 27001:2022	≥ 6 έτη	Υ.Δ.Σ.
6	ΕΔ11-3Β	Αναφορά – Κατάλογος Σημείων Ελέγχου Σταδίου 2 ISO 27001:2022	≥ 6 έτη	Υ.Δ.Σ.
7	ΕΔ11-4Β	Σημειώσεις Επιθεωρητή ISO 27001:2022	≥ 6 έτη	Υ.Δ.Σ.
8	ΕΔ11-5	Αναφορά Μη Συμμορφώσεων/ Παρατηρήσεις/ Προτάσεις Βελτίωσης	≥ 6 έτη	Υ.Δ.Σ.
9	ΕΔ11-6	Παρουσιολόγιο Επιθεώρησης	≥ 6 έτη	Υ.Δ.Σ.
10	ΕΔ11-7	Απόφαση Χορήγησης	≥ 6 έτη	Υ.Δ.Σ.
11	ΕΔ11-8	Αίτηση Μεταβολών	≥ 6 έτη	Υ.Δ.Σ.
12		Πιστοποιητικό	≥ 6 έτη	Υ.Δ.Σ.