

ΠΡΟΣΘΕΤΕΣ ΠΛΗΡΟΦΟΡΙΕΣ / ΑΠΑΙΤΗΣΕΙΣ ΓΙΑ ΤΗΝ ΕΠΙΘΕΩΡΗΣΗ

1. Γενικά.

Κατά τη διαδικασία πιστοποίησης, η Q-CERT θα επαληθεύσει ότι το σύστημα βρίσκεται σε λειτουργία για επαρκές χρονικό διάστημα και ότι υπάρχουν επαρκή αποδεικτικά στοιχεία που τεκμηριώνουν ότι έχουν υλοποιηθεί, είναι αποτελεσματικές και θα διατηρηθούν οι ρυθμίσεις για τις ανασκοπήσεις της διοίκησης και τους εσωτερικούς ελέγχους του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ISMS), καλύπτοντας το πεδίο της πιστοποίησης

2. Πρόσβαση σε αρχεία του οργανισμού

Κατά την υποβολή αίτησης για την πιστοποίηση του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ISMS), ο αιτών οφείλει να ενημερώσει την Q-CERT (μέσω της αίτησης ή με οποιοδήποτε άλλο μέσο) σε περίπτωση που οποιαδήποτε πληροφορία σχετική με το ISMS (όπως αρχεία ISMS ή πληροφορίες σχετικά με τον σχεδιασμό και την αποτελεσματικότητα των ελέγχων) δεν μπορεί να διατεθεί προς εξέταση από την ομάδα επιθεώρησης λόγω του ότι περιέχει εμπιστευτικές ή ευαίσθητες πληροφορίες.

Σε μια τέτοια περίπτωση, η Q-CERT θα αξιολογήσει κατά πόσον είναι εφικτή η επαρκής επιθεώρηση του ISMS χωρίς την εν λόγω πληροφορία. Εάν, μέσω της διαδικασίας αξιολόγησης της αίτησης, ο εξουσιοδοτημένος εκπρόσωπος της Q-CERT κρίνει ότι δεν είναι δυνατή η επαρκής επιθεώρηση του ISMS χωρίς την εξέταση των εν λόγω εμπιστευτικών ή ευαίσθητων πληροφοριών, η Q-CERT θα ενημερώσει τον πελάτη ότι η επιθεώρηση για την πιστοποίηση δεν μπορεί να πραγματοποιηθεί έως ότου διασφαλιστεί η κατάλληλη πρόσβαση

3. Αριθμός Προσωπικού στο πεδίο πιστοποίησης

Προκειμένου να εκτιμηθεί ορθά η απαιτούμενη διάρκεια της επιθεώρησης κατά την υποβολή της αίτησης και/ή όταν αυτό κριθεί απαραίτητο, ο αιτών θα πρέπει να παρέχει πληροφορίες σχετικά με το προσωπικό που εμπλέκεται στο πεδίο εφαρμογής της πιστοποίησης, όπως:

- Συνολικός αριθμός προσωπικού που εμπίπτει στο πεδίο εφαρμογής της πιστοποίησης (για τις κύριες εγκαταστάσεις καθώς και για κάθε επιπλέον τοποθεσία, όπου αυτό ισχύει).
- Αριθμός ατόμων από το σύνολο που:
 - ✓ διαθέτουν πρόσβαση μόνο για ανάγνωση σε πληροφορίες για την εκτέλεση των καθηκόντων τους.

ANNEX F

ISO/IEC 27001:2022

- ✓ δεν έχουν πρόσβαση στις εγκαταστάσεις επεξεργασίας πληροφοριών του οργανισμού που εμπίπτουν στο πεδίο εφαρμογής του ISMS.
- ✓ έχουν συγκεκριμένη, αποδεδειγμένα περιορισμένη πρόσβαση στις εγκαταστάσεις επεξεργασίας πληροφοριών του οργανισμού που εμπίπτουν στο πεδίο εφαρμογής του ISMS.
- ✓ εκτελούν δραστηριότητες για τις οποίες έχουν εφαρμοστεί αυστηροί περιορισμοί για την αποτροπή αποκάλυψης πληροφοριών, π.χ. μέτρα που απαγορεύουν την είσοδο προσωπικών αντικειμένων και συσκευών στον χώρο εργασίας.

4. Εξ ολοκλήρου απομακρυσμένος έλεγχος λόγω απουσίας φυσικής τοποθεσίας

Σε περίπτωση που καμία δραστηριότητα του οργανισμού, η οποία εμπίπτει στο πεδίο εφαρμογής της πιστοποίησης, δεν πραγματοποιείται σε καθορισμένη φυσική τοποθεσία, το γεγονός αυτό θα πρέπει να γνωστοποιηθεί με σαφήνεια στην Q-CERT μέσω της αίτησης.

Σε τέτοιες περιπτώσεις, τα έγγραφα της πιστοποίησης θα αναφέρουν ρητά ότι όλες οι δραστηριότητες του οργανισμού διεξάγονται απομακρυσμένα

5. Πεδίο Πιστοποίησης

- Κατά τη διάρκεια της επιθεώρησης, η Q-CERT θα διασφαλίζει ότι οι διασυνδέσεις με υπηρεσίες ή δραστηριότητες που δεν εμπίπτουν πλήρως στο πεδίο εφαρμογής του ISMS αντιμετωπίζονται εντός του ISMS που υπόκειται σε πιστοποίηση και περιλαμβάνονται στην εκτίμηση κινδύνου για την ασφάλεια πληροφοριών του πελάτη. Παράδειγμα τέτοιας περίπτωσης αποτελεί η κοινή χρήση εγκαταστάσεων (π.χ. συστημάτων πληροφορικής, βάσεων δεδομένων και τηλεπικοινωνιακών συστημάτων ή η ανάθεση επιχειρηματικής λειτουργίας σε εξωτερικό φορέα) με άλλους οργανισμούς.
- Η έκδοση της Δήλωσης Εφαρμοσιμότητας (Statement of Applicability) θα περιλαμβάνεται στα έγγραφα της πιστοποίησης.

ΣΗΜΕΙΩΣΗ: Τυχόν τροποποίηση της Δήλωσης Εφαρμοσιμότητας που δεν μεταβάλλει την κάλυψη των ελέγχων στο πεδίο εφαρμογής της πιστοποίησης δεν απαιτεί ενημέρωση των εγγράφων της πιστοποίησης

6. Διάρκεια Επιθεώρησης και Ομάδα Επιθεώρησης για την Αρχική Επιθεώρηση Πιστοποίησης

Τόσο η διάρκεια όσο και η ομάδα επιθεώρησης μπορεί να τροποποιηθούν ανάλογα με τα αποτελέσματα της Φάσης Ι της επιθεώρησης.

Σημείωση: Το παρόν, σε συνδυασμό με τον κανονισμό πιστοποίησης αποτελούν μέρος των δεσμεύσεων που υπογράφει ότι αποδέχεται ο πελάτης μέσω της σύμβασης (F-2002) με το Φορέα.

ANNEX F

ISO/IEC 27001:2022

Η διαδικασία αρχικής πιστοποίησης απαιτεί την παρουσίαση της έκθεσης επιθεώρησης Σταδίου Ι στον πελάτη και την αποστολή της στα κεντρικά γραφεία της Q-CERT. Η Q-CERT (ένα άτομο που δεν έχει συμμετάσχει στη διαδικασία επιθεώρησης) θα αξιολογήσει τα ευρήματα και θα αποφασίσει εάν η ομάδα επιθεώρησης που ορίστηκε εξ αρχής πληροί τις απαιτήσεις της δραστηριότητας του Οργανισμού (καλύπτοντας τα ισχύοντα σημεία στο Παράρτημα Α του προτύπου) ή εάν θα πρέπει να επαναπροσδιοριστεί και εάν η υπολογιζόμενη διάρκεια της επιθεώρησης εξακολουθεί να είναι επαρκής για τους σκοπούς των δραστηριοτήτων πιστοποίησης..

7. Τροποποίηση του πεδίου πιστοποίησης

Όταν ένας πιστοποιημένος πελάτης ζητά επέκταση ή αλλαγή του πεδίου για το οποίο είναι πιστοποιημένος, οφείλει να παρέχει στην Q-CERT τις ακόλουθες πληροφορίες:

- a) το είδος της επέκτασης,
- b) τη δραστηριότητα/τις δραστηριότητες της υφιστάμενης πιστοποίησης,
- c) τον αριθμό των εγκαταστάσεων όπου λαμβάνει χώρα η δραστηριότητα/οι δραστηριότητες,
- d) τους σχετικούς κινδύνους για την ασφάλεια των πληροφοριών που συνδέονται με τη δραστηριότητα/τις δραστηριότητες,
- e) τον αριθμό των ελέγχων που σχετίζονται με την επέκταση,
- f) τον αριθμό των ατόμων που εκτελούν εργασία υπό τον έλεγχο του οργανισμού στο πλαίσιο του νέου πεδίου, και
- g) τον χρόνο που απαιτείται για την αξιολόγηση της ενσωμάτωσης του διευρυμένου πεδίου στο ΣΔΑΠ (ISMS).

Χρόνος επιθεώρησης θα προστεθεί στη συνολική διάρκεια για την ανασκόπηση του ΣΔΑΠ του πελάτη. Ο επιπρόσθετος αυτός χρόνος θα είναι τουλάχιστον:

- 1) 0,5 ημέρες επιθεωρητή, εάν η επιθεώρηση για την επέκταση του πεδίου διεξάγεται ταυτόχρονα με επιθεώρηση επιτήρησης ή επαναπιστοποίησης.
- 2) 1,0 ημέρα επιθεωρητή, όταν η επιθεώρηση για την επέκταση του πεδίου διεξάγεται ως ξεχωριστή επιθεώρηση.