**Ε1. Αντικείμενο**

Ο παρών ειδικός κανονισμός πιστοποίησης αφορά τις διαδικασίες που εφαρμόζει η BQC για την αξιολόγηση και πιστοποίηση συστημάτων διαχείρισης προσωπικών δεδομένων σύμφωνα με τα πρότυπα της σειράς **ISO/IEC 27701:2019** ή άλλα αντίστοιχα ευρωπαϊκά ή διεθνή πρότυπα ή τυποποιητικά έγγραφα. Η συνολική διαχείριση και η χορήγηση του πιστοποιητικού συμμόρφωσης ικανοποιεί τις απαιτήσεις του προτύπου **ISO/IEC 17021-1:2015**, και βασίζεται σε πρόσθετες απαιτήσεις πάνω στο **ISO/IEC 27001** (του προτύπου συστήματος διαχείρισης ασφάλειας πληροφοριών), **ISO/IEC 27002:2022** (του κώδικα πρακτικής για τους ελέγχους ασφάλειας πληροφοριών), **ISO/IEC 27006:2015 και ISO/IEC 27006-2:2021** (τις απαιτήσεις και οδηγίες στους φορείς που παρέχουν έλεγχο και πιστοποίηση συστήματος διαχείρισης της ασφάλειας των πληροφοριών), του Ε.ΣΥ.Δ. καθώς και του Γενικού Κανονισμού Πιστοποίησης της BQC.

Το **ISO/IEC 27701:2019** αποτελεί επέκταση των απαιτήσεων και των οδηγιών που ορίζονται στο πρότυπο **ISO/IEC 27001** για την ασφάλεια και διαχείριση απορρήτου. Είναι το πλαίσιο του συστήματος διαχείρισης για την προστασία των προσωπικά αναγνωρίσιμων πληροφοριών για να αποδειχθεί η συμμόρφωση με τους κανονισμούς προστασίας δεδομένων, όπως ο **Γενικός Κανονισμός για την Προστασία των Δεδομένων (GDPR)**.

**Προκειμένου μία επιχείρηση να πιστοποιηθεί κατά ISO/IEC 27701:2019, πρέπει να διαθέτει ήδη εφαρμογή συστήματος διαχείρισης σύμφωνα με το ISO/IEC 27001 (πιστοποιημένη ή όχι) ή να επιλέξει την παράλληλη πιστοποίησή της με βάση τα δύο πρότυπα** για την επεξεργασία προσωπικών δεδομένων εντός ενός συστήματος διαχείρισης ασφάλειας πληροφοριών.

**2. Όροι – Συντομογραφίες – Ορισμοί**

Οι όροι που χρησιμοποιούνται στο παρόν κείμενο είναι σύμφωνοι με τους όρους που αναφέρονται στην §2 του Γενικού Κανονισμού Πιστοποίησης της BQC και με τα πρότυπα **ISO/IEC 27000:2018** «Τεχνολογία Πληροφοριών – Τεχνικές Ασφάλειας – Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών – Επισκόπηση και λεξιλόγιο», **ISO/IEC 27701:2019** «εφαρμογή πολιτικών που εξασφαλίζουν την ακεραιότητα, εμπιστευτικότητα και διαθεσιμότητα των πληροφοριών και πλήρη συμμόρφωση με τις ισχύουσες νομοθετικές απαιτήσεις διαχείρισης προσωπικών δεδομένων» και **ISO/IEC 17000:2020**.

**Σύστημα Διαχείρισης Προσωπικών Δεδομένων (ΣΔΠΔ):** μέρος του συστήματος διαχείρισης που εστιάζεται στις απαιτήσεις διαχείρισης των προσωπικών δεδομένων (των εργαζομένων, των πελατών και των συνεργατών) και παρέχει κατευθυντήριες οδηγίες για τους υπευθύνους επεξεργασίας και τους εκτελούντες την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

**PII controller / υπεύθυνος επεξεργασίας:** φυσικό ή νομικό πρόσωπο, δημόσια αρχή, υπηρεσία ή άλλος φορέας που, μόνος ή από κοινού με άλλους, καθορίζει τους σκοπούς και τα μέσα επεξεργασίας δεδομένων προσωπικού χαρακτήρα, όταν οι σκοποί και τα μέσα αυτής της επεξεργασίας καθορίζονται από το δίκαιο της Ευρωπαϊκής Ένωσης ή του κράτους μέλους.

Παράδειγμα: Εταιρία η οποία συλλέγει οικονομικά στοιχεία πελατών της (π.χ. τιμολόγια πληρωμών, οικονομικές συναλλαγές) με σκοπό να τα διαθέσει σε εξωτερικό συνεργάτη για την διαχείριση των πληρωμών της.

**PII processor / εκτελών την επεξεργασία:** φυσικό ή νομικό πρόσωπο, δημόσια αρχή, υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπεύθυνου επεξεργασίας.

Παράδειγμα: Εταιρία η οποία πραγματοποιεί διαχείριση πληρωμών (λογιστικές υπηρεσίες) για λογαριασμό εντολέα της, με επεξεργασία των δεδομένων που λαμβάνει από τον εντολέα της.

**PII processor & controller / υπεύθυνος επεξεργασίας: και εκτελών την επεξεργασία:** φυσικό ή νομικό πρόσωπο, δημόσια αρχή, υπηρεσία ή άλλος φορέας που, μόνος ή από κοινού με άλλους, καθορίζει τους σκοπούς και τα μέσα επεξεργασίας δεδομένων προσωπικού χαρακτήρα, όταν οι σκοποί και τα μέσα αυτής της επεξεργασίας καθορίζονται από το δίκαιο της Ευρωπαϊκής Ένωσης ή του κράτους μέλους, και επεξεργάζεται τα προσωπικά δεδομένα αυτά.

Παράδειγμα: Εταιρία η οποία συλλέγει οικονομικά στοιχεία πελατών της (πχ, τιμολόγια πληρωμών, οικονομικές συναλλαγές), και τα επεξεργάζεται η ίδια με σκοπό την πληρωμή τους.

### 3. Διαδικασία Πιστοποίησης

#### 3.1 Αίτηση Πιστοποίησης

Οι οργανισμοί που επιθυμούν να πιστοποιήσουν το ΣΔΠΔ που εφαρμόζουν, απευθύνονται στην BQC και ενημερώνονται πως απαιτείται η πλήρης εφαρμογή του προς πιστοποίηση ΣΔΠΔ και η ύπαρξη αντίστοιχων αρχείων για διάστημα τουλάχιστον δύο (2) μηνών. Στη συνέχεια, συμπληρώνουν το πληροφοριακό ερωτηματολόγιο **E050-1** το οποίο αποστέλλεται ατελώς και επέχει θέση αίτησης πιστοποίησης.

#### 3.2 Ανασκόπηση αίτησης

Αφού η αίτηση πιστοποίησης επιστραφεί συμπληρωμένη από τον οργανισμό, παραδίδεται στη Διεύθυνση Πιστοποίησης, η οποία διεξάγει μια ανασκόπηση της αίτησης (**E050-69**) και των συμπληρωματικών πληροφοριών, ώστε να υπολογιστούν οι απαιτούμενες ανθρωποημέρες για τη διεξαγωγή της επιθεώρησης, αλλά και να διασφαλιστεί ότι:

α) οι πληροφορίες αναφορικά με τον υποψήφιο οργανισμό και το σύστημα διαχείρισής του επαρκούν για τη διεξαγωγή της επιθεώρησης,

β) οι απαιτήσεις για πιστοποίηση καθορίζονται και τεκμηριώνονται σαφώς,

γ) τυχόν γνωστές διαφορές στην κατανόηση μεταξύ υποψήφιου οργανισμού και BQC επιλύονται,

δ) η BQC διαθέτει την ικανότητα και τη δυνατότητα να εκτελέσει τις δραστηριότητες πιστοποίησης,

ε) το αιτούμενο πεδίο της πιστοποίησης, οι εγκαταστάσεις του οργανισμού, ο απαιτούμενος χρόνος για την ολοκλήρωση των επιθεωρήσεων και άλλα στοιχεία που επηρεάζουν τις δραστηριότητες της πιστοποίησης λαμβάνονται υπόψη (γλώσσα, ζητήματα ασφάλειας, κίνδυνοι για την αμεροληψία κ.λπ.),

στ) το προς πιστοποίηση ΣΔΠΔ εφαρμόζεται για διάστημα τουλάχιστον δυο (2) μηνών.

Σε περίπτωση που η BQC δεν δύναται να αναλάβει την πιστοποίηση, καταγράφεται ο λόγος στο έντυπο ανασκόπησης της αίτησης **E050-69**, ο οργανισμός ενημερώνεται εγγράφως και η διαδικασία διακόπτεται.

Εφόσον η BQC δύναται να αναλάβει την επιθεώρηση, συντάσσεται οικονομική προσφορά, η οποία αποστέλλεται στον οργανισμό προς υπογραφή μαζί με το γενικό κανονισμό πιστοποίησης της BQC.

Για τον καθορισμό του προγράμματος επιθεώρησης και τυχόν μεταγενέστερων τροποποιήσεών του, λαμβάνονται υπόψη οι απαιτήσεις όπως περιγράφονται στο **E050-69**.

- Στην περίπτωση που γίνεται **συνδυασμένη** πιστοποίηση των **ISO/IEC 27001και ISO/IEC 27701:2019:**

Η διάρκεια της αρχικής επιθεώρησης είναι η διάρκεια που προκύπτει από το **ISO/IEC 27006:2015** προσαυξημένη κατά:

20% αν ο οργανισμός είναι PII processor

30% αν ο οργανισμός είναι PII controller

50% αν ο οργανισμός είναι PII controller & processor.

Με βάση το ISO/IEC 27006-2:2021, ο πρόσθετος χρόνος ελέγχου για έναν αρχικό έλεγχο PIMS (στάδιο 1 και στάδιο 2) θα πρέπει να είναι κατ' ελάχιστον:

2,5 ημέρες για οργανισμό "PII processor"
3 ημέρες για οργανισμό "PII controller" ή
3,5 ημέρες για οργανισμό "PII processor & controller"
Η διάρκεια των επιθεωρήσεων επιτήρησης είναι το 1/3 της χρονικής διάρκειας της αρχικής επιθεώρησης
Η διάρκεια της επιθεώρησης επαναπιστοποίησης είναι τα 2/3 της χρονικής διάρκειας της αρχικής επιθεώρησης

- Στην περίπτωση που γίνεται **ξεχωριστά** πιστοποίηση του **ISO/IEC 27701:2019** – με την προϋπόθεση της ύπαρξης ήδη πιστοποίησης του συστήματος ΣΔΑΠ:

Ως διάρκεια της αρχικής επιθεώρησης υπολογίζεται η διάρκεια αρχικής αξιολόγησης κατά ISO/IEC 27001 προσαυξημένη κατά:
20% αν ο οργανισμός είναι PII processor
30% αν ο οργανισμός είναι PII controller
50% αν ο οργανισμός είναι PII controller & processor.
Με βάση το ISO/IEC 27006-2:2021, ο πρόσθετος χρόνος ελέγχου για έναν αρχικό έλεγχο PIMS (στάδιο 1 και στάδιο 2) θα πρέπει να είναι κατ' ελάχιστον:
2,5 ημέρες για οργανισμό "PII processor"
3 ημέρες για οργανισμό "PII controller" ή
3,5 ημέρες για οργανισμό "PII processor & controller"
Η διάρκεια των επιθεωρήσεων επιτήρησης είναι το 1/3 της χρονικής διάρκειας της αρχικής επιθεώρησης
Η διάρκεια της επιθεώρησης επαναπιστοποίησης είναι τα 2/3 της χρονικής διάρκειας της αρχικής επιθεώρησης

<u>Παράγοντες που μπορεί να επηρεάσουν τη διάρκεια μιας επιθεώρησης:</u>
Σύμφωνα με τους πίνακες C2, C3 & C4 του ISO/IEC 27006:2015

<u>Μείωση της διάρκειας επιθεώρησης λόγω ύπαρξης πολλαπλών συστημάτων διαχείρισης:</u>
Στην περίπτωση που το σύστημα διαχείρισης του οργανισμού είναι ενοποιημένο (integrated) και δομημένο έτσι ώστε να περιλαμβάνει κοινές αρμοδιότητες και διεργασίες για παραπάνω από ένα πρότυπα, τότε ο αριθμός των ανθρωποημερών καθορίζεται σύμφωνα με το έγγραφο **IAF MD11:2023**.

Η BQC μπορεί να δεχτεί συνδυασμένη τεκμηρίωση (π.χ. για ασφάλεια πληροφοριών, ποιότητα, υγεία & ασφάλεια και περιβάλλον) με την προϋπόθεση ότι το ΣΔΠΔ μπορεί να προσδιοριστεί με σαφήνεια όπως και οι αλληλεπιδράσεις του με τα άλλα συστήματα διαχείρισης.

<u>Εφαρμογή δειγματοληψίας λόγω ύπαρξης πολλαπλών εγκαταστάσεων</u>:
Όταν χρησιμοποιείται η δειγματοληψία πολλαπλών εγκαταστάσεων για την επιθεώρηση του συστήματος διαχείρισης ενός οργανισμού που καλύπτει την ίδια δραστηριότητα σε διάφορα σημεία, ακολουθώντας το έγγραφο **IAF MD1:2018**, η BQC αναπτύσσει ένα πρόγραμμα δειγματοληψίας ώστε να καλύπτει όλο το πλήθος των αρχείων ή όλα τα πεδία, τα προϊόντα και τα τμήματα του οργανισμού καθώς και όλες τις απαιτήσεις του προτύπου. Το πρόγραμμα δειγματοληψίας καθώς και ο αριθμός των εγκαταστάσεων που θα επιθεωρηθούν, ακολουθεί την παρακάτω μεθοδολογία:

- Σε κάθε επιθεώρηση θα επιθεωρείται η έδρα του οργανισμού.
- Για τις περαιτέρω εγκαταστάσεις ισχύουν τα εξής:
  - Αρχική Επιθεώρηση: Το μέγεθος του δείγματος θα είναι το αποτέλεσμα της τετραγωνικής ρίζας του αριθμού των περαιτέρω εγκαταστάσεων (π.χ. Συνολικός αριθμός εγκαταστάσεων: 4 – 1 έδρα και 3 επιπλέον εγκαταστάσεις, Αριθμός εγκαταστάσεων που θα επιθεωρηθούν: 1 +√3 = 1 + 2 = 3).
  - Επιθεώρηση Επιτήρησης: Το μέγεθος του δείγματος θα είναι το αποτέλεσμα της τετραγωνικής ρίζας του αριθμού των περαιτέρω εγκαταστάσεων πολλαπλασιασμένο με τον

συντελεστή 0,6. (π.χ. Συνολικός αριθμός εγκαταστάσεων: 4 – 1 έδρα και 3 επιπλέον εγκαταστάσεις, Αριθμός εγκαταστάσεων που θα επιθεωρηθούν: 1 + √3 × 0.6 = 1 + 1 = 2).

- Επιθεώρηση Επαναπιστοποίησης: Το μέγεθος του δείγματος θα πρέπει να είναι το ίδιο με αυτό της αρχικής επιθεώρησης. Παρόλα αυτά, όπου το ΣΔ είναι αποδεδειγμένα αποτελεσματικό για διάστημα τουλάχιστον 3 ετών, το μέγεθος του δείγματος μπορεί να είναι το αποτέλεσμα της τετραγωνικής ρίζας του αριθμού των περαιτέρω εγκαταστάσεων πολλαπλασιασμένο με τον συντελεστή 0,8. (π.χ. Συνολικός αριθμός εγκαταστάσεων: 4 – 1 έδρα και 3 επιπλέον εγκαταστάσεις, Αριθμός εγκαταστάσεων που θα επιθεωρηθούν: 1 + √3 × 0.8 = 1 + 2 = 3).

- Κατά την επιλογή των εγκαταστάσεων, τουλάχιστον 25% αυτών θα πρέπει να επιλέγεται τυχαία.

Η δειγματοληψία πολλαπλών εγκαταστάσεων για την επιθεώρηση του ΣΔΠΔ μπορεί να εφαρμοστεί όταν οι εγκαταστάσεις του οργανισμού:

α) λειτουργούν κάτω από κοινό ΣΔΠΔ, το οποίο διαχειρίζεται, επιθεωρείται και ανασκοπείται κεντρικά,

β) περιλαμβάνονται στο πρόγραμμα εσωτερικών επιθεωρήσεων του οργανισμού και

γ) περιλαμβάνονται στο πρόγραμμα της ετήσιας ανασκόπησης του οργανισμού.

Η BQC πριν την εφαρμογή δειγματοληψίας στην επιθεώρηση ενός ΣΔΠΔ διασφαλίζει ότι:

α) κατά την αρχική ανασκόπηση της αίτησης αναγνωρίζονται, στο μέγιστο δυνατό βαθμό, οι διαφορές μεταξύ των εγκαταστάσεων ώστε να προσδιοριστεί ένα επαρκές επίπεδο δειγματοληψίας,

β) το δείγμα που επιλέγεται είναι αντιπροσωπευτικό λαμβάνοντας υπόψη:

i. τα αποτελέσματα των εσωτερικών επιθεωρήσεων,
ii. τα αποτελέσματα της ανασκόπησης της διοίκησης,
iii. διαφοροποιήσεις στο μέγεθος μεταξύ των εγκαταστάσεων,
iv. διαφοροποιήσεις στο πεδίο δραστηριότητας μεταξύ των εγκαταστάσεων,
v. την πολυπλοκότητα των συστημάτων πληροφοριών στις διάφορες εγκαταστάσεις,
vi. διαφοροποιήσεις στις εργασιακές πρακτικές,
vii. διαφοροποιήσεις στις δραστηριότητες που αναλαμβάνει η κάθε εγκατάσταση,
viii. διαφοροποιήσεις στο σχεδιασμό και τη λειτουργία των σημείων ελέγχου (controls),
ix. πιθανή αλληλεπίδραση με κρίσιμα συστήματα πληροφοριών ή συστήματα πληροφοριών που επεξεργάζονται ευαίσθητα δεδομένα,
x. διαφοροποιήσεις στις νομικές απαιτήσεις,
xi. γεωγραφικές και πολιτιστικές πτυχές,
xii. κατάσταση επικινδυνότητας των εγκαταστάσεων και
xiii. περιστατικά ασφάλειας πληροφοριών στις συγκεκριμένες εγκαταστάσεις.

γ) αντιπροσωπευτικό δείγμα επιλέγεται μεταξύ όλων των εγκαταστάσεων εντός του πεδίου εφαρμογής του ΣΔΠΔ. Η επιλογή βασίζεται στους παράγοντες ανωτέρω, καθώς και σε τυχαία επιλογή.

δ) στην επιθεώρηση πιστοποίησης περιλαμβάνονται όλες οι εγκαταστάσεις που υπόκεινται σε σημαντικούς κινδύνους,

ε) το πρόγραμμα επιθεώρησης σχεδιάζεται λαμβάνοντας υπόψη τα ανωτέρω και περιλαμβάνει αντιπροσωπευτικό δείγμα του πεδίου εφαρμογής του ΣΔΠΔ εντός του τριετούς κύκλου πιστοποίησης και

στ) στην περίπτωση που κατά την επιθεώρηση σε κάποια εγκατάσταση (είτε στα κεντρικά είτε σε κάποια από τις υπόλοιπες εγκαταστάσεις του οργανισμού) υπάρξουν ευρήματα που συνιστούν μη συμμόρφωση, τότε οι διορθωτικές ενέργειες εφαρμόζονται στο σύνολο των εγκαταστάσεων που καλύπτονται από το πιστοποιητικό.

### 3.3 Συγκρότηση ομάδας επιθεώρησης

Μετά την υπογραφή της σύμβασης από τον οργανισμό, η Διεύθυνση Πιστοποίησης της BQC, αφού λάβει υπόψη τις ανθρωποημέρες και τις

συνολικές ικανότητες της ομάδας επιθεώρησης που απαιτούνται για τη διεξαγωγή της επιθεώρησης, επιλέγει την ομάδα επιθεώρησης ή τον επιθεωρητή (και εμπειρογνώμονες, όπου αυτό απαιτείται) που θα επιτελέσει την επιθεώρηση έτσι ώστε:

- να είναι εξοικειωμένη με τους ισχύοντες νομικούς κανονισμούς και τις διαδικασίες πιστοποίησης της BQC.
- να έχει πλήρη γνώση της σχετικής μεθόδου αξιολόγησης και των εγγράφων αξιολόγησης.
- να έχει την κατάλληλη τεχνική γνώση των ειδικών δραστηριοτήτων για τις οποίες επιδιώκεται η πιστοποίηση και κατά περίπτωση των σχετικών διαδικασιών του οργανισμού.
- να διαθέτει έναν επαρκή βαθμό κατανόησης, ώστε να διενεργήσει μία αξιόπιστη αξιολόγηση της ικανότητας του προμηθευτή να παρέχει προϊόντα, διεργασίες και υπηρεσίες στο αντικείμενο της πιστοποίησης του οργανισμού.
- να είναι ικανή και να επικοινωνεί αποτελεσματικά, τόσο σε γραπτό όσο και σε προφορικό λόγο στην απαιτούμενη γλώσσα.
- να είναι απαλλαγμένη από οποιοδήποτε συμφέρον που μπορεί να την αναγκάσει να ενεργήσει διαφορετικά από έναν αμερόληπτο ή χωρίς διακρίσεις τρόπο, για παράδειγμα:
  - ➢ τα μέλη της ομάδας επιθεώρησης ή ο οργανισμός τους δεν πρέπει να έχουν προσφέρει συμβουλευτικές υπηρεσίες στον επιθεωρούμενο.
  - ➢ τα μέλη της ομάδας επιθεώρησης ή ο οργανισμός τους δεν πρέπει να έχει κανένα προηγούμενο ή προβλεπόμενο δεσμό με τον επιθεωρούμενο.
  - ➢ τα μέλη της ομάδας επιθεώρησης δεν πρέπει να έχουν οποιαδήποτε σχέση με οργανισμό ανταγωνιστικό ως προς τον επιθεωρούμενο.

### 3.4 Αρχική επαφή με τον επιθεωρούμενο

Ο Επικεφαλής Επιθεωρητής της ομάδας επιθεώρησης επικοινωνεί με τον εκπρόσωπο του επιθεωρούμενου. Σκοπός:

- ο Δημιουργία Διαύλων Επικοινωνίας με τον Επιθεωρούμενο.
- ο Επιβεβαίωση της εξουσιοδότησης διενέργειας της επιθεώρησης.
- ο Αίτηση για παροχή των απαραίτητων εγγράφων τεκμηρίωσης του Επιθεωρούμενου (όπως αυτή αναφέρεται στην §3.5.1 του παρόντος κανονισμού).
- ο Καθορισμός Κανόνων Υγείας και Ασφάλειας κατά την επιτόπια επιθεώρηση.
- ο Καθορισμός οποιωνδήποτε διευθετήσεων για την επιτόπια επιθεώρηση.
- ο Συμφωνία για την παρουσία παρατηρητών και συνοδών για την ομάδα επιθεώρησης.

Ο Επικεφαλής Επιθεωρητής για κάθε επιθεώρηση αναπτύσσει ένα πλάνο επιθεώρησης **E050-5**, το οποίο αποτελεί τη βάση της συμφωνίας για τη διεξαγωγή και τον προγραμματισμό των δραστηριοτήτων επιθεώρησης.

Όταν ενημερωθεί για τη σύνθεση της ομάδας επιθεώρησης και τον χρονικό προγραμματισμό, ο επιθεωρούμενος έχει το δικαίωμα να ζητήσει γραπτώς εντός τριών (3) ημερών από τη λήψη του πλάνου επιθεώρησης και με την κατάλληλη αιτιολόγηση, την αντικατάσταση μέλους ή μελών της ομάδας επιθεώρησης ή αλλαγή των ημερομηνιών επιθεώρησης. Σε τέτοιες περιπτώσεις η Διεύθυνση Πιστοποίησης επανακαθορίζει την ομάδα επιθεώρησης ή τον χρονικό προγραμματισμό της επιθεώρησης και ενημερώνει εκ νέου τον επιθεωρούμενο οργανισμό.

Σημειώνεται ότι σε περίπτωση που στην ομάδα επιθεώρησης υπάρχει παρουσία τεχνικού εμπειρογνώμονα, μεταφραστή ή εκπαιδευόμενου επιθεωρητή, τότε αυτοί δεν προσμετρούνται ως επιθεωρητές στον υπολογισμό των ανθρωποημερών.

Εάν για οποιαδήποτε λόγο ο οργανισμός δεν μπορεί να ανταποκριθεί στο πλάνο επιθεώρησης, υποχρεούται να ενημερώσει τον ΦΠ. Σε περίπτωση που κατά την εναρκτήρια σύσκεψη ο επιθεωρητής αντιλαμβάνεται ότι δεν μπορεί να τηρηθεί το πλάνο

με ευθύνη του οργανισμού, αναβάλει την επιθεώρηση.

### 3.5 Επιθεώρηση αρχικής πιστοποίησης

Η επιθεώρηση αρχικής πιστοποίησης ενός συστήματος διαχείρισης διεξάγεται σε δύο στάδια: το πρώτο στάδιο και το δεύτερο στάδιο.

#### 3.5.1 Πρώτο στάδιο επιθεώρησης

Το πρώτο στάδιο της επιθεώρησης εκτελείται για να:
α) ανασκοπείται η τεκμηρίωση του συστήματος διαχείρισης του επιθεωρούμενου οργανισμού. Η BQC πρέπει να έχει σαφή κατανόηση του σχεδιασμού του ΣΔΠΔ που εφαρμόζει ο επιθεωρούμενος οργανισμός στο πλαίσιο της οργάνωσης του πελάτη, της αξιολόγησης και αντιμετώπισης κινδύνων (συμπεριλαμβανομένων των καθορισμένων σημείων ελέγχου - controls), της πολιτικής και των στόχων ασφάλειας πληροφοριών και, ιδίως, της ετοιμότητας του πελάτη για την επιθεώρηση. Για τον σκοπό αυτό, ο επιθεωρούμενος οργανισμός αποστέλλει στην BQC την τεκμηρίωση του συστήματος και ιδιαίτερα τεκμηρίωση όπως πολιτική ασφάλειας και πληροφοριών απορρήτου (information security and privacy policy), διαδικασία αξιολόγησης κινδύνου, στόχους, πολιτική διαχείρισης αλλαγών, τελευταία εσωτερική επιθεώρηση και ανασκόπηση διοίκησης, διορθωτικές ενέργειες, κατάλογο εγγράφων, δήλωση εφαρμοσιμότητας και πληροφοριών απορρήτου.
β) αξιολογείται η κατάσταση των εγκαταστάσεων και της τοποθεσίας του οργανισμού και διεξάγονται συζητήσεις με το προσωπικό, ώστε να καθοριστεί η ετοιμότητά του για το δεύτερο στάδιο της επιθεώρησης.
γ) ανασκοπείται η κατάσταση και η κατανόηση του πελάτη αναφορικά με τις απαιτήσεις του προτύπου, ειδικότερα για ό,τι αφορά τον εντοπισμό των κύριων ζητημάτων επίδοσης, των διεργασιών, των αντικειμενικών σκοπών και της λειτουργίας του συστήματος διαχείρισης.
δ) συλλέγονται οι απαραίτητες πληροφορίες αναφορικά με το πεδίο του συστήματος διαχείρισης, τις διεργασίες και τις εγκαταστάσεις του οργανισμού και τις σχετικές κανονιστικές και νομοθετικές απαιτήσεις συμμόρφωσης.
ε) παρέχεται ένα σημείο εστίασης για τον σχεδιασμό του 2ου σταδίου της επιθεώρησης, αντλώντας επαρκή κατανόηση του συστήματος διαχείρισης και των λειτουργιών του οργανισμού.
στ) αξιολογείται κατά πόσον προγραμματίζονται και εκτελούνται εσωτερικές επιθεωρήσεις και ανασκοπήσεις διοίκησης και πώς το επίπεδο της υλοποίησης του συστήματος διαχείρισης αιτιολογεί πως ο οργανισμός είναι έτοιμος για το 2ο στάδιο της επιθεώρησης.
ζ) ανασκοπείται η παροχή των πόρων για το 2ο στάδιο της επιθεώρησης και συμφωνούνται με τον οργανισμό οι λεπτομέρειες του σταδίου αυτού.

Για τα συστήματα διαχείρισης προσωπικών δεδομένων δύναται να εκτελείται το σύνολο του 1ου σταδίου εκτός της έδρας του οργανισμού, εκτός αν αποφασιστεί διαφορετικά.

Τα ευρήματα του 1ου σταδίου καταγράφονται στην έκθεση επιθεώρησης και κοινοποιούνται στον οργανισμό, συμπεριλαμβανομένου του εντοπισμού τυχόν σημείων που θα μπορούσαν κατά το 2ο στάδιο της επιθεώρησης να στοιχειοθετηθούν ως μη συμμορφώσεις.

Η έκθεση επιθεώρησης του πρώτου σταδίου ανασκοπείται από την BQC πριν αποφασιστεί η διενέργεια του 2ου σταδίου και επιβεβαιώνεται η καταλληλόλητα των μελών της ομάδας επιθεώρησης που έχει επιλεγεί για τη διενέργεια του 2ου σταδίου.

Κατά τον καθορισμό του διαστήματος που μεσολαβεί μεταξύ των δύο σταδίων της επιθεώρησης, λαμβάνονται υπόψη οι ανάγκες του πελάτη για την επίλυση προβληματικών σημείων που εντοπίστηκαν κατά το 1ο στάδιο της επιθεώρησης και η σημαντικότητα των ευρημάτων.

#### 3.5.2 Δεύτερο στάδιο επιθεώρησης

Σκοπός του 2ου σταδίου της επιθεώρησης είναι η αξιολόγηση του συστήματος διαχείρισης του οργανισμού, καθώς και της αποτελεσματικότητας αυτού. Το 2ο στάδιο της επιθεώρησης λαμβάνει χώρα

στις εγκαταστάσεις του οργανισμού και περιλαμβάνει κατ' ελάχιστο:

α) πληροφορίες και αντικειμενικές αποδείξεις αναφορικά με την συμμόρφωση του οργανισμού προς όλες τις απαιτήσεις του προτύπου ή άλλου κανονιστικού εγγράφου του εφαρμόσιμου συστήματος διαχείρισης, καθώς επίσης της πολιτικής, των στόχων και των διαδικασιών που ο ίδιος έχει ορίσει,

β) παρακολούθηση, μέτρηση, αναφορά και ανασκόπηση ως προς σημαντικούς αντικειμενικούς σκοπούς και στόχους,

γ) το σύστημα διαχείρισης και την επίδοση του οργανισμού αναφορικά με την συμμόρφωση με νομικές απαιτήσεις,

δ) το λειτουργικό έλεγχο των διεργασιών του οργανισμού,

ε) την εσωτερική επιθεώρηση και την ανασκόπηση διοίκησης,

στ) την ευθύνη της διοίκησης για την πολιτική του οργανισμού και τη δέσμευσή της στην πολιτική ασφάλειας πληροφοριών και τους στόχους ασφάλειας πληροφοριών,

ζ) τις σχέσεις μεταξύ των κανονιστικών απαιτήσεων, τις πολιτικές, τους αντικειμενικούς σκοπούς και στόχους επίδοσης, τυχόν εφαρμόσιμες νομικές απαιτήσεις, ευθύνες, ικανότητες προσωπικού, λειτουργίες, διαδικασίες, δεδομένα επίδοσης και συμπεράσματα και ευρήματα εσωτερικών επιθεωρήσεων,

η) τις απαιτήσεις των προτύπων **ISO/IEC 27001** και **ISO/IEC 27701:2019 (όπου γίνεται συνδυασμένη επιθεώρηση)**,

θ) τις απαιτήσεις του προτύπου **ISO/IEC 27701:2019 (όπου γίνεται ξεχωριστά μόνο η επιθεώρηση του)**,

ι) την αξιολόγηση των κινδύνων που σχετίζονται με την ασφάλεια των πληροφοριών και εάν η αξιολόγηση αυτή παράγει συνεπή, έγκυρα και συγκρίσιμα αποτελέσματα εάν επαναλαμβάνονται,

κ) τον καθορισμό των στόχων και των σημείων ελέγχου (controls) βάσει της αξιολόγησης του κινδύνου ασφάλειας πληροφοριών και των διαδικασιών αντιμετώπισης κινδύνων,

λ) τις επιδόσεις του συστήματος διαχείρισης ασφάλειας των πληροφοριών και την αποτελεσματικότητά του, αξιολογώντας τους στόχους ασφάλειας πληροφοριών,

μ) την αντιστοιχία μεταξύ των καθορισμένων σημείων ελέγχου (controls), της Δήλωσης Εφαρμοσιμότητας, των αποτελεσμάτων της διαδικασίας αξιολόγησης του κινδύνου ασφάλειας των πληροφοριών, της διαδικασίας αντιμετώπισης των κινδύνων και της πολιτικής και των στόχων ασφάλειας πληροφοριών,

ν) την εφαρμογή των σημείων ελέγχου - controls (σύμφωνα με το **Annex D** του **ISO/IEC 27006:2015**), λαμβάνοντας υπόψη το εξωτερικό και το εσωτερικό πλαίσιο και τους συναφείς κινδύνους, την παρακολούθηση, τη μέτρηση και την ανάλυση των διαδικασιών και του ελέγχου ασφάλειας πληροφοριών του οργανισμού, για να προσδιοριστεί εάν οι έλεγχοι εφαρμόζονται και είναι αποτελεσματικοί και ανταποκρίνονται στους δηλωμένους στόχους για την ασφάλεια των πληροφοριών, και

ξ) τα προγράμματα, τις διεργασίες, τις διαδικασίες, τα αρχεία, τις εσωτερικές επιθεωρήσεις και ανασκοπήσεις της αποτελεσματικότητας του ΣΔΠΔ ώστε να διασφαλιστεί ότι αυτά συμπεριλαμβάνονται στις αποφάσεις της ανώτερης διοίκησης και στην πολιτική και τους στόχους της ασφάλειας πληροφοριών.

Σημειώνεται πως σε περίπτωση που ο επιθεωρούμενος οργανισμός έχει αναθέσει σε υπεργολάβο, μέρος ή ολόκληρη διεργασία – που περιλαμβάνεται στο πεδίο πιστοποίησης – αυτή θα επιθεωρείται επί τόπου (on site) από την ομάδα επιθεώρησης. Η επιτόπια αυτή επιθεώρηση, μπορεί να αποφευχθεί στην περίπτωση που η υλοποίηση και τα αποτελέσματα αυτής της διεργασίας, μπορούν να επαληθευθούν με την ανασκόπηση των αρχείων και εγγράφων του Συστήματος Διαχείρισης που εφαρμόζεται.

Τουλάχιστον το 70% του συνολικού χρόνου που απαιτείται για τη διεξαγωγή της αρχικής

επιθεώρησης πιστοποίησης πραγματοποιείται στις εγκαταστάσεις του οργανισμού.

**3.5.3 Συμπεράσματα επιθεώρησης αρχικής πιστοποίησης**

Η ομάδα επιθεώρησης αναλύει όλες τις πληροφορίες και τις αντικειμενικές αποδείξεις που συλλέγονται κατά τα δύο στάδια της επιθεώρησης, ανασκοπεί τα ευρήματα της επιθεώρησης και καταλήγει στα συμπεράσματα της επιθεώρησης.

**3.5.4 Πληροφορίες για τη χορήγηση αρχικής πιστοποίησης**

Οι πληροφορίες που παρέχονται από την ομάδα επιθεώρησης στη Διεύθυνση Πιστοποίησης της BQC για τη λήψη της απόφασης πιστοποίησης περιλαμβάνουν, κατ' ελάχιστο, τα εξής:

α) τις αναφορές επιθεώρησης,

β) σχόλια για τις μη συμμορφώσεις και, όπου αυτό είναι εφικτό, τις διορθωτικές ενέργειες του οργανισμού,

γ) επιβεβαίωση των πληροφοριών που παρασχέθηκαν κατά την ανασκόπηση της αίτησης,

δ) επιβεβαίωση ότι ο σκοπός της επιθεώρησης έχει επιτευχθεί,

ε) πρόταση για την πιστοποίηση ή όχι του επιθεωρούμενου οργανισμού, μαζί με τυχόν προϋποθέσεις ή παρατηρήσεις.

Ο Επικεφαλής Επιθεωρητής, για κάθε επιθεώρηση που αναλαμβάνει, αναπτύσσει πρόγραμμα επιθεώρησης για τον πλήρη κύκλο της πιστοποίησης. Το πρόγραμμα περιλαμβάνει τις δραστηριότητες που απαιτείται να τεκμηριωθούν προκειμένου το σύστημα διαχείρισης να συμμορφώνεται με τις απαιτήσεις του εκάστοτε προτύπου. Στο πρόγραμμα σημειώνονται, επίσης, τυχόν μη συμμορφώσεις και παρατηρήσεις που καταγράφηκαν κατά τη διάρκεια της επιθεώρησης.

Η Διεύθυνση Πιστοποίησης της BQC λαμβάνει την απόφαση πιστοποίησης επί τη βάση της αξιολόγησης των ευρημάτων και των συμπερασμάτων της επιθεώρησης και άλλων σχετικών πληροφοριών (π.χ. δημόσιες πληροφορίες, σχόλια για την αναφορά επιθεώρησης από τον πελάτη).

Όταν κατά τη διάρκεια της επιθεώρησης πιστοποίησης εντοπίζονται κύριες μη συμμορφώσεις, οι οποίες δεν επιλύονται εντός έξι (6) μηνών από την τελευταία ημέρα του 2ου σταδίου, τότε θα πρέπει να διενεργηθεί εκ νέου επιθεώρηση 2ου σταδίου προτού ληφθεί απόφαση πιστοποίησης.

**3.6 Δραστηριότητες επιτήρησης**

**3.6.1 Γενικά**

Η BQC διενεργεί ετήσιες επιθεωρήσεις επιτήρησης, ώστε να ανασκοπούνται σε τακτική βάση αντιπροσωπευτικά τμήματα και λειτουργίες του οργανισμού που καλύπτονται από τον σκοπό του πιστοποιημένου συστήματος διαχείρισης και να λαμβάνονται υπόψη αλλαγές του οργανισμού και του συστήματος διαχείρισής του.

Οι δραστηριότητες επιτήρησης περιλαμβάνουν επιτόπου επιθεωρήσεις για να αξιολογείται κατά πόσο το σύστημα διαχείρισης του οργανισμού ικανοποιεί συγκεκριμένες απαιτήσεις, ως προς το πρότυπο, βάσει του οποίου χορηγείται η πιστοποίηση. Άλλες δραστηριότητες επιτήρησης ενδέχεται να είναι οι εξής:

α) ερωτήματα της BQC προς τον πιστοποιημένο οργανισμό αναφορικά με την πιστοποίηση,

β) ανασκόπηση τυχόν δηλώσεων του οργανισμού αναφορικά με τις λειτουργίες του (π.χ. διαφημιστικό υλικό, ιστοσελίδα),

γ) αιτήματα προς τον πελάτη για παροχή εγγράφων και αρχείων (έντυπα ή σε ηλεκτρονική μορφή), και

δ) άλλα μέσα παρακολούθησης της επίδοσης του πιστοποιημένου οργανισμού.

Οι επιθεωρήσεις επιτήρησης (1η και 2η) πραγματοποιούνται πριν τη λήξη της χρονικής περιόδου των 12 και 24 μηνών αντίστοιχα από την αρχική απόφαση πιστοποίησης του οργανισμού.

**3.6.2 Επιθεώρηση επιτήρησης**

Οι επιθεωρήσεις επιτήρησης είναι επιτόπου επιθεωρήσεις, αλλά όχι απαραίτητα πλήρεις επιθεωρήσεις του συστήματος. Σχεδιάζονται σε

συνδυασμό με άλλες δραστηριότητες επιτήρησης (βλέπε §3.6.1), έτσι ώστε η BQC να μπορεί να διατηρεί την εμπιστοσύνη πως το πιστοποιημένο σύστημα διαχείρισης και να συνεχίζει να ικανοποιεί τις απαιτήσεις μεταξύ των επιθεωρήσεων επαναπιστοποίησης. Το πρόγραμμα των επιθεωρήσεων επιτήρησης περιλαμβάνει, κατ' ελάχιστο, τα εξής:

α) τροποποιήσεις στην πολιτική ασφάλειας πληροφοριών,

β) την ικανότητα του οργανισμού να αναγνωρίσει τις ισχύουσες νομικές απαιτήσεις,

γ) την εφαρμογή και αξιολόγηση της συμμόρφωσης στις νομικές και κανονιστικές απαιτήσεις,

δ) την αποτελεσματικότητα του συστήματος διαχείρισης αναφορικά με την επίτευξη των στόχων,

ε) την πρόοδο των προσχεδιασμένων δραστηριοτήτων αναφορικά με τη διαρκή βελτίωση,

στ) το διαρκή λειτουργικό έλεγχο,

ζ) την ανασκόπηση τυχόν αλλαγών,

η) τη χρήση των σημάτων ή/ και άλλων αναφορών στην πιστοποίηση,

θ) τον έλεγχο των αρχείων ενστάσεων και παραπόνων, όπου καταγράφεται τυχόν αδυναμία συμμόρφωσης ή μη τήρησης των απαιτήσεων πιστοποίησης, και οι ενέργειες του επιθεωρούμενου οργανισμού για τη διερεύνηση της αποτελεσματικότητας του ΣΔΠΔ και των διαδικασιών που εφαρμόζει, καθώς και τη λήψη των κατάλληλων διορθωτικών μέτρων.

ι) τη διατήρηση και επικαιροποίηση των στοιχείων του συστήματος, όπως είναι η αξιολόγηση του κινδύνου ασφάλειας των πληροφοριών, οι εσωτερικές επιθεωρήσεις, η ανασκόπηση διοίκησης και οι διορθωτικές ενέργειες,

κ) την ανασκόπηση των ενεργειών που εκτελέστηκαν για τις μη συμμορφώσεις που εντοπίστηκαν κατά τη διάρκεια της προηγούμενης επιθεώρησης,

λ) τις επικοινωνίες από εξωτερικά μέρη, όπως προβλέπεται στο **ISO/IEC 27701:2019** και άλλα έγγραφα που απαιτούνται για την πιστοποίηση,

μ) περιοχές που υπόκεινται σε αλλαγές,

ν) επιλεγμένες απαιτήσεις που προβλέπονται στο **ISO/IEC 27701:2019**,

ξ) άλλες επιλεγμένες περιοχές, που απαιτούνται κατά περίπτωση,

ο) αλλαγές στα σημεία ελέγχου (controls) και κατά συνέπεια αλλαγές που επηρεάζουν τη Δήλωση Εφαρμοσιμότητας, και

π) την εφαρμογή και αποτελεσματικότητα των σημείων ελέγχου (controls) σύμφωνα με το πρόγραμμα επιθεώρησης.

Η έκθεση της επιθεώρησης επιτήρησης θα πρέπει να περιλαμβάνει, κατ' ελάχιστο, τα ανωτέρω, καθώς και πληροφορίες σχετικά με την άρση των μη συμμορφώσεων που είχαν προηγουμένως καταγραφεί, την έκδοση της Δήλωσης Εφαρμοσιμότητας που είναι σε ισχύ και οποιαδήποτε σημαντική αλλαγή παρατηρήθηκε από την προηγούμενη επιθεώρηση.

### 3.7 Δραστηριότητες επαναπιστοποίησης

#### 3.7.1 Γενικά

Η επιθεώρηση επαναπιστοποίησης διενεργείται πριν από τη λήξη του πιστοποιητικού Συμμόρφωσης εκτός και εάν έχει ζητηθεί εγγράφως από τον οργανισμό 3 τουλάχιστον μήνες πριν τη λήξη του πιστοποιητικού συμμόρφωσης, διακοπή της Πιστοποίησης.

Σε περίπτωση που με ευθύνη του οργανισμού, η επιθεώρηση επαναπιστοποίησης διενεργηθεί μετά την ημερομηνία λήξης του πιστοποιητικού (χωρίς τεκμηριωμένη αιτιολόγηση), η επιθεώρηση θεωρείται επιθεώρηση αρχικής πιστοποίησης και ακολουθούνται οι κανόνες που περιγράφονται στην §3.5.

#### 3.7.2 Σχεδιασμός επιθεώρησης επαναπιστοποίησης

Μια επιθεώρηση επαναπιστοποίησης σχεδιάζεται και διεξάγεται, ώστε να αξιολογείται η διαρκής ικανοποίηση όλων των απαιτήσεων του σχετικού προτύπου του συστήματος διαχείρισης ή άλλου κανονιστικού εγγράφου. Σκοπός της επιθεώρησης επαναπιστοποίησης είναι η επιβεβαίωση της συνεχιζόμενης συμμόρφωσης και αποτελεσματικότητας του συστήματος διαχείρισης

στο σύνολό του, καθώς και της συνεχιζόμενης σχετικότητας και εφαρμοσιμότητας του πεδίου της πιστοποίησης.

Η επιθεώρηση επαναπιστοποίησης λαμβάνει υπόψη την επίδοση του συστήματος διαχείρισης κατά την περίοδο της πιστοποίησης και περιλαμβάνει την ανασκόπηση αναφορών προηγούμενων επιθεωρήσεων επιτήρησης.

Οι δραστηριότητες της επιθεώρησης επαναπιστοποίησης περιλαμβάνουν το πρώτο στάδιο της επιθεώρησης, όταν έχουν σημειωθεί σημαντικές αλλαγές στο σύστημα, τον πελάτη ή το πλαίσιο λειτουργίας του συστήματος διαχείρισης (π.χ. αλλαγές στη νομοθεσία).

Στην περίπτωση των πολλαπλών εγκαταστάσεων, ο σχεδιασμός της επιθεώρησης διασφαλίζει επαρκείς επιτόπου επιθεωρήσεις, ώστε να ενισχύεται η εμπιστοσύνη στην πιστοποίηση.

**3.7.3 Επιθεώρηση επαναπιστοποίησης**

Η επιθεώρηση επαναπιστοποίησης περιλαμβάνει μία επιτόπια επιθεώρηση, η οποία καλύπτει τα ακόλουθα ζητήματα:

α) την αποτελεσματικότητα του συνόλου του συστήματος διαχείρισης αναφορικά με εσωτερικές και εξωτερικές αλλαγές, και την συνεχιζόμενη σχετικότητα και εφαρμοσιμότητα του πεδίου της πιστοποίησης,

β) την αποδεδειγμένη δέσμευση για διατήρηση της αποτελεσματικότητας και της βελτίωσης του συστήματος διαχείρισης, ώστε να βελτιώνεται η συνολική επίδοση,

γ) το κατά πόσο η λειτουργία του πιστοποιημένου συστήματος διαχείρισης συμβάλλει στην επίτευξη των ποιοτικών και των αντικειμενικών σκοπών του οργανισμού,

δ) τα ευρήματα και την αποτελεσματικότητα των διορθωτικών ενεργειών που εντοπίστηκαν καθ' όλη τη διάρκεια του τελευταίου κύκλου πιστοποίησης.

Σε περίπτωση που έχουν ολοκληρωθεί επιτυχώς οι ενέργειες επαναπιστοποίησης πριν τη λήξη του υπάρχοντος πιστοποιητικού, η ημερομηνία έκδοσης του νέου πιστοποιητικού μπορεί να βασίζεται στην ημερομηνία λήξης του υπάρχοντος πιστοποιητικού. Η ημερομηνία έκδοσης του νέου πιστοποιητικού μπορεί να είναι την ίδια ή μεταγενέστερη ημερομηνία της απόφασης επαναπιστοποίησης.

Σε περίπτωση που η επιθεώρηση επαναπιστοποίησης δεν έχει ολοκληρωθεί ή δεν έχουν αρθεί τυχόν κύριες μη συμμορφώσεις πριν τη λήξη του υπάρχοντος πιστοποιητικού, τότε δεν μπορεί να υπάρξει εισήγηση για επαναπιστοποίηση και η ισχύς του πιστοποιητικού δεν μπορεί να επεκταθεί. Προκειμένου να αποφευχθεί κάτι τέτοιο, η BQC ενημερώνει τον οργανισμό πέντε (5) τουλάχιστον μήνες πριν τη λήξη της πιστοποίησης, ώστε να προγραμματισθεί η επιθεώρηση επαναπιστοποίησης τρεις (3) τουλάχιστον μήνες πριν την λήξη του πιστοποιητικού. Για κάθε τέτοια περίπτωση ο οργανισμός ενημερώνεται για τις συνέπειες.

Εάν το υπάρχον πιστοποιητικό ενός οργανισμού έχει λήξει, η BQC μπορεί να επαναφέρει την πιστοποίηση, εφόσον οι εκκρεμότητες της επιθεώρησης επαναπιστοποίησης έχουν ολοκληρωθεί εντός έξι (6) μηνών. Σε αντίθετη περίπτωση θα πρέπει τουλάχιστον να διενεργηθεί επιθεώρηση δεύτερου σταδίου. Η ημερομηνία του πιστοποιητικού επαναπιστοποίησης θα είναι την ημέρα της απόφασης επαναπιστοποίησης ή μεταγενέστερη και η ημερομηνία λήξης θα βασίζεται στην ημερομηνία λήξης του προηγούμενου κύκλου πιστοποίησης.

**3.7.4 Πληροφορίες για τη χορήγηση της επαναπιστοποίησης**

Η BQC λαμβάνει αποφάσεις για την ανανέωση της πιστοποίησης με βάση τα αποτελέσματα της επιθεώρησης επαναπιστοποίησης, καθώς και με βάση τα αποτελέσματα της ανασκόπησης του συστήματος κατά τη διάρκεια ισχύος της πιστοποίησης και τυχόν παράπονα που ελήφθησαν από χρήστες της πιστοποίησης.

**3.8 Κύριες διεργασίες εκτέλεσης επιθεώρησης**

**3.8.1 Εναρκτήρια σύσκεψη**

Η εναρκτήρια σύσκεψη συγκαλείται από τον Επικεφαλής της ομάδας επιθεώρησης αμέσως μετά την άφιξη της ομάδας επιθεώρησης στο χώρο της επιθεώρησης.

Συμμετέχουν:

- Από την πλευρά της BQC, όλα τα μέλη της ομάδας επιθεώρησης
- Από την πλευρά του οργανισμού, τουλάχιστον, ο εκπρόσωπος της Διοίκησης και ο Υπεύθυνος Ασφάλειας Πληροφοριών του οργανισμού.

Σκοπός:

- επιβεβαίωση του σχεδίου επιθεώρησης,
- συστάσεις της ομάδας επιθεώρησης και των ρόλων των επιθεωρητών
- διασφάλιση πως μπορούν να εκτελεστούν όλες οι προγραμματισμένες ενέργειες
- αναφορά στον τρόπο διενέργειας της επιθεώρησης,
- επιβεβαίωση των διαύλων επικοινωνίας,
- ερωτήματα από τους επιθεωρούμενους.

ΔΙΕΞΑΓΩΓΗ ΕΝΑΡΚΤΗΡΙΑΣ ΣΥΣΚΕΨΗΣ

Λαμβάνονται υπόψη τα εξής:

α) συστάσεις μεταξύ των παρευρισκόμενων και περιγραφή των ρόλων τους,

β) επιβεβαίωση του πεδίου πιστοποίησης,

γ) επιβεβαίωση του σχεδίου της επιθεώρησης (συμπεριλαμβανομένου του είδους, σκοπού και κριτηρίων της επιθεώρησης), τυχόν αλλαγών και άλλες σχετικές συμφωνίες με τον πελάτη, όπως η ημερομηνία και ο χρόνος της καταληκτικής σύσκεψης και έκτακτες συσκέψεις μεταξύ της ομάδας επιθεώρησης και του εκπροσώπου του πελάτη,

δ) επιβεβαίωση των διαύλων επίσημης επικοινωνίας,

ε) επιβεβαίωση ότι οι πόροι και οι εγκαταστάσεις που απαιτούνται από την ομάδα επιθεώρησης είναι διαθέσιμοι,

στ) επιβεβαίωση των θεμάτων εμπιστευτικότητας,

ζ) επιβεβαίωση ασφαλούς εργασίας, διαδικασιών εκτάκτου ανάγκης της ομάδας επιθεώρησης,

η) επιβεβαίωση της διαθεσιμότητας, ρόλων και ταυτότητας των συνοδών και παρατηρητών,

θ) μέθοδος αναφοράς, καθώς και αξιολόγηση των μη συμμορφώσεων,

ι) τις περιπτώσεις που μπορεί μια επιθεώρηση να τερματιστεί πρόωρα,

κ) επιβεβαίωση ότι ο επικεφαλής επιθεωρητής και η ομάδα επιθεώρησης, εκπροσωπώντας την BQC, είναι υπεύθυνοι για τη διεξαγωγή της επιθεώρησης και της τήρησης του σχεδίου επιθεώρησης,

λ) επιβεβαίωση της κατάστασης των ευρημάτων προγενέστερων επιθεωρήσεων,

μ) μέθοδοι και διεργασίες που θα χρησιμοποιηθούν κατά την επιθεώρηση,

ν) επιβεβαίωση της γλώσσας που θα χρησιμοποιηθεί κατά την επιθεώρηση,

ξ) επιβεβαίωση ότι κατά τη διάρκεια της επιθεώρησης, ο πελάτης θα ενημερώνεται για την πρόοδο της επιθεώρησης,

ο) δυνατότητα του πελάτη να κάνει ερωτήσεις.

### 3.8.2 Ρόλος και ευθύνη των συνοδών και των παρατηρητών

Οι συνοδοί και οι παρατηρητές μπορούν να συνοδεύουν την ομάδα επιθεώρησης κατόπιν έγκρισης από τον επικεφαλής της ομάδας επιθεώρησης ή/και από τον επιθεωρούμενο, εφόσον απαιτείται. Δεν πρέπει να επηρεάζουν ή να παρεμβαίνουν στη διεξαγωγή της επιθεώρησης. Για τους παρατηρητές, οι ρυθμίσεις για την πρόσβαση, την υγεία και ασφάλεια, το περιβάλλον, την ασφάλεια και την εμπιστευτικότητα πρέπει να ρυθμίζονται με τον επιθεωρούμενο οργανισμό. Οι συνοδοί, που ορίζονται από τον επιθεωρούμενο, θα πρέπει να βοηθούν την ομάδα επιθεώρησης και να ενεργούν κατόπιν αιτήματος του επικεφαλής της ομάδας επιθεώρησης ή του επιθεωρητή στον οποίο έχουν ανατεθεί. Οι υπευθυνότητές τους περιλαμβάνουν τα κάτωθι:

- βοήθεια προς τους επιθεωρητές ώστε να εντοπίσουν τα άτομα που θα συμμετάσχουν σε συνεντεύξεις και να επιβεβαιώσουν τον τόπο και το χρόνο της συνέντευξης,

- διευθέτηση της πρόσβασης σε συγκεκριμένες τοποθεσίες του επιθεωρούμενου οργανισμού
- διασφάλιση ότι κανόνες σχετικά με τις ρυθμίσεις για την πρόσβαση, την υγεία και ασφάλεια, το περιβάλλον, την ασφάλεια και εμπιστευτικότητα και άλλα θέματα είναι γνωστά και τηρούνται από τα μέλη της ομάδας επιθεώρησης και τους παρατηρητές και αντιμετωπίζονται οι ενδεχόμενοι κίνδυνοι
- παρατήρηση της επιθεώρησης για λογαριασμό του επιθεωρούμενου
- παροχή διευκρινήσεων ή βοήθεια στη συλλογή πληροφοριών, όταν απαιτηθεί.

*Σημείωση: Ο επικεφαλής επιθεωρητής έχει δικαίωμα να ζητήσει από τον οργανισμό την αλλαγή του συνοδού ή του παρατηρητή όταν αποδεδειγμένα και κατ' επανάληψη παρεκκλίνουν από το ρόλο τους και εμποδίζουν το έργο της ομάδας επιθεώρησης.*

**3.8.3 Συμπεράσματα επιθεώρησης – Συμπλήρωση εντύπων επιθεώρησης**

**3.8.3.1 Συμπεράσματα επιθεώρησης**

Κατά τη διάρκεια της επιθεώρησης, με ευθύνη του Επικεφαλής Επιθεωρητή, η ομάδα επιθεώρησης θα πρέπει να αξιολογεί την πορεία της επιθεώρησης και να ανταλλάσσει πληροφορίες. Ο Επικεφαλής Επιθεωρητής είναι υπεύθυνος, εφόσον κρίνεται απαραίτητο, να τροποποιήσει το αρχικό πλάνο της επιθεώρησης και να αναθέσει νέες εργασίες στα μέλη της ομάδας επιθεώρησης. Κατά τη διάρκεια της επιθεώρησης, ο Επικεφαλής Επιθεωρητής θα πρέπει να ενημερώνει για την εξέλιξη αυτής και τυχόν ανησυχίες, τον ορισμένο εκπρόσωπο του επιθεωρούμενου οργανισμού.

Η ομάδα επιθεώρησης, με ευθύνη του Επικεφαλής Επιθεωρητή, οφείλει να συνεδριάσει πριν από την καταληκτική σύσκεψη, ώστε να:

- υποβάλλει σε ανασκόπηση τα ευρήματα της επιθεώρησης και άλλες σχετικές πληροφορίες που συλλέχθηκαν κατά τη διάρκεια της επιθεώρησης με βάση τους αντικειμενικούς στόχους της επιθεώρησης,
- συμφωνήσει τα συμπεράσματα της επιθεώρησης, λαμβάνοντας υπόψη την εγγενή αβεβαιότητα της διεργασίας της επιθεώρησης,
- συμφωνήσει στις απαραίτητες ακόλουθες ενέργειες που απαιτούνται,
- κατηγοριοποιήσει τις τυχόν εντοπισθείσες μη συμμορφώσεις,
- επιβεβαιώσει την καταλληλότητα του σχεδίου επιθεώρησης και εντοπίσει τυχόν τροποποιήσεις που απαιτούνται για επόμεΒνες επιθεωρήσεις.

**3.8.3.2 Συμπλήρωση εντύπων επιθεώρησης**

Ο Επικεφαλής Επιθεωρητής συμπληρώνει την έκθεση επιθεώρησης **E050-2**, το ερωτηματολόγιο επιθεώρησης **E050-52B**, το πρόγραμμα επιθεώρησης τριετίας **E050-51 ή E050-51B** και προαιρετικά το έντυπο σημειώσεων επιθεωρητή **E050-7**.

**3.8.4 Καταληκτική σύσκεψη**

Συμμετέχουν:

- Από την πλευρά της BQC, όλα τα μέλη της ομάδας επιθεώρησης.
- Από την πλευρά του οργανισμού, τουλάχιστον, ο εκπρόσωπος της Διοίκησης και ο Υπεύθυνος Ασφάλειας Πληροφοριών του οργανισμού.

Σκοπός:

- Τυπικότητες.
- Δήλωση απάρνησης.
- Σύσταση στον επιθεωρούμενο ότι ο έλεγχος συμμόρφωσης είναι δειγματοληπτικός και συνεπώς εμπεριέχει ένα ποσοστό αβεβαιότητας.
- Παρουσίαση ευρημάτων επιθεώρησης.
- Συζήτηση σχετικά με τα ευρήματα της επιθεώρησης.
- Μεθοδολογία αναφοράς και το χρονοδιάγραμμα, συμπεριλαμβανομένης της κατηγοριοποίησης τυχόν ευρημάτων.
- Ενημέρωση από τον Επικεφαλής Επιθεωρητή για τη διαδικασία χειρισμού των μη συμμορφώσεων και των επιπτώσεών τους στο καθεστώς πιστοποίησης του πελάτη.

- Χρονοδιάγραμμα που θα πρέπει να αποσταλεί πλάνο διορθώσεων και διορθωτικών ενεργειών των μη συμμορφώσεων που εντοπίστηκαν.
- Τις ενέργειες της BQC μετά την πιστοποίηση.
- Πληροφορίες σχετικά με τη διαδικασία χειρισμού παραπόνων και ενστάσεων.
- Πρόταση για πιστοποίηση.

Στο τέλος της καταληκτικής σύσκεψης, ο εκπρόσωπος της Διοίκησης υπογράφει την έκθεση επιθεώρησης **E050-2** και λαμβάνει αντίγραφο αυτής. Σε περίπτωση που αρνηθεί να αποδεχθεί τα ευρήματα της επιθεώρησης και να υπογράψει την έκθεση επιθεώρησης, ο Επικεφαλής Επιθεωρητής καταγράφει τη διαφωνία ή την επιφύλαξη και δίνει αντίγραφο της έκθεσης επιθεώρησης στον επιθεωρούμενο.

**3.9 Χορήγηση πιστοποιητικού**

Η έκδοση ή μη του πιστοποιητικού συμμόρφωσης αποφασίζεται από το πρόσωπο που ορίζεται στο BQC Decision Making Matrix μετά από σχετική εισήγηση του Επικεφαλής Επιθεωρητή. Η απόφαση αξιολογεί, εκτός των άλλων, την έκθεση επιθεώρησης και την τεκμηρίωση της διενέργειας διορθωτικών ενεργειών για την άρση των μη συμμορφώσεων που παρατηρήθηκαν κατά την επιθεώρηση. Η απόφαση γνωστοποιείται εγγράφως στον οργανισμό.

Η απόφαση πιστοποίησης ή μη του επιθεωρούμενου οργανισμού λαμβάνεται από το πρόσωπο που δεν έχει εμπλακεί στη διαδικασία διενέργειας της πιστοποίησης.

Ο οργανισμός υποχρεούται να ενημερώνει την BQC για κάθε αλλαγή της έκδοσης Δήλωσης Εφαρμοσιμότητας, η οποία πρέπει να αναγράφεται στο πιστοποιητικό συμμόρφωσης. Πιστοποιητικό συμμόρφωσης με αναφορά σε παρωχημένη έκδοση της σχετικής δήλωσης δεν ισχύει και πρέπει να αποσύρεται.

Για τη διατήρηση της ισχύος του πιστοποιητικού, ο οργανισμός αποστέλλει στην BQC τη νέα έκδοση Δήλωσης Εφαρμοσιμότητας, γίνεται αξιολόγηση των αλλαγών και αποφασίζεται εάν απαιτούνται περαιτέρω ενέργειες (π.χ. αποστολή επιπλέον τεκμηρίωσης, διενέργεια επιθεώρησης, κ.λπ.) για την επανέκδοση του πιστοποιητικού συμμόρφωσης.