

1. Αντικείμενο

Ο παρών ειδικός κανονισμός πιστοποίησης αφορά τις βασικές αρχές, τα βήματα, τις διαδικασίες και τις αποφάσεις που εφαρμόζει η BQC και που υλοποιούνται μέσω του **Πλαισίου Κυβερνο-Υγιεινής για Μικρομεσαίες Επιχειρήσεις (ΜμΕ) / Cyber-Hygiene Framework for Small and Medium Enterprises (SMEs)**, όπως αυτό έχει σχεδιαστεί από την **Αρχή Ψηφιακής Ασφάλειας Κύπρου (ΑΨΑ) / Digital Security Authority (DSA)** ως **Εθνικό Κέντρο Συντονισμού Κυβερνοασφάλειας στην Κυπριακή Δημοκρατία / National Cybersecurity Centre of Cyprus (NCC-CY)**.

Η BQC έχει εγκριθεί από την Αρχή Ψηφιακής Ασφάλειας (ΑΨΑ) για τη διενέργεια επιθεωρήσεων και πιστοποιήσεων σύμφωνα με το Πλαίσιο Κυβερνο-Υγιεινής για ΜμΕ, ενώ έχει διαπιστευτεί σύμφωνα με το **ISO/IEC 17021-1** και **ISO/IEC 27006** για τη διενέργεια επιθεωρήσεων και πιστοποιήσεων συστημάτων διαχείρισης ασφάλειας πληροφοριών σύμφωνα με τα πρότυπα **ISO/IEC 27001**.

2. Σχετικά έγγραφα αναφοράς

Το Πλαίσιο Κυβερνο-Υγιεινής για ΜμΕ αποτελείται από τα ακόλουθα έγγραφα:

1. Τη **διαδικασία-κανονισμό επιθεώρησης και πιστοποίησης** μέσω του Πλαισίου Κυβερνο-Υγιεινής για ΜμΕ (ήτοι το παρόν έγγραφο). Στο έγγραφο περιγράφονται και αναλύονται οι βασικές αρχές, τα βήματα, οι αποφάσεις που πρέπει να υλοποιηθούν και τα έγγραφα που πρέπει να συμπληρωθούν για να εξασφαλίσει μια ΜμΕ την πιστοποίηση κυβερνοασφάλειας. Τα περιεχόμενα του εγγράφου είναι συμβατά με τις βασικές αρχές και απαιτήσεις διεθνώς αναγνωρισμένων προτύπων διαπίστευσης όπως είναι το ISO 17021.

2. Το **έγγραφο των κριτηρίων** του προτύπου ISO/IEC 17021-1 χρησιμοποιείται ως βάση για τη διεξαγωγή της επιθεώρησης. Σε περίπτωση συμμόρφωσης εκδίδεται το Πιστοποιητικό Πιστοποίησης.

3. Την **περιγραφή θέσης εργασίας του επιθεωρητή** η οποία περιέχει τις αρμοδιότητες, υπευθυνότητες και την επαγγελματική επάρκεια των επιθεωρητών, οι οποίοι διενεργούν τις επιθεωρήσεις επί των κριτηρίων του Πλαισίου Κυβερνο-Υγιεινής για ΜμΕ.

4. Το **ερωτηματολόγιο της επιθεώρησης** αποτελεί βασικό εργαλείο υποστήριξης και λογοδοσίας των επιθεωρητών. Το ερωτηματολόγιο περιέχει σημεία ελέγχου βασιζόμενα στα κριτήρια του Πλαισίου Κυβερνο-Υγιεινής για ΜμΕ. Μετά την αποπεράτωση της επιθεώρησης, το ερωτηματολόγιο περιέχει για κάθε σημείο ελέγχου ένδειξη για την συμμόρφωση, επαληθεύσιμες αποδείξεις και (όπου έχουν αναδειχτεί) σχετικές αποκλίσεις.

5. Την **έκθεση επιθεώρησης**, η οποία περιέχει το αποτέλεσμα της επιθεώρησης και την εισήγηση προς τον φορέα πιστοποίησης σχετικά με την έκδοση ή την μη αποδοχή έκδοσης του πιστοποιητικού πιστοποίησης.

6. Την **μεθοδολογία υπολογισμού διάρκειας της επιθεώρησης**, η οποία περιέχει τις σχετικές οδηγίες για τον τρόπο υπολογισμού της.

3. Όροι – Ορισμοί

Επιθεώρηση: Η συστηματική, ανεξάρτητη και τεκμηριωμένη διεργασία για την απόκτηση τεκμηρίων και την αξιολόγησή τους αντικειμενικά για τον προσδιορισμό του βαθμού στον οποίο πληρούνται τα κριτήρια επιθεώρησης

Πιστοποίηση: Η βεβαίωση ενός τρίτου μέρους σχετικά με το αντικείμενο της διαδικασίας αξιολόγησης συμμόρφωσης με την εξαίρεση της διαπίστευσης

Διαπίστευση: Η βεβαίωση ενός τρίτου μέρους, ενός οργανισμού αξιολόγησης της συμμόρφωσης, η οποία αποδεικνύει επίσημα την ικανότητά του να εκτελεί συγκεκριμένα καθήκοντα αξιολόγησης της συμμόρφωσης

Κυβερνοασφάλεια: Οι δραστηριότητες που απαιτούνται για την προστασία των συστημάτων

δικτύου και πληροφοριών, των χρηστών των εν λόγω συστημάτων και άλλων επηρεαζόμενων από κυβερνοαπειλές προσώπων

ΜΜΕ: Ο ορισμός των «Μικρομεσαίων Επιχειρήσεων» (ΜμΕ) ορίζεται με βάση το πλήθος απασχολούμενων ατόμων (απασχολούν <250 άτομα) και τον κύκλο εργασιών ή το σύνολο του ισολογισμού (έχουν $\leq$ € 50 εκατ. ετήσιου κύκλου εργασιών ή $\leq$ € 43 εκατ. ετήσιου συνολικού ισολογισμού.)

Αριθμός απασχολούμενων: Ο αριθμός εργαζομένων πλήρους απασχόλησης που εργάστηκαν στην εξεταζόμενη επιχείρηση ή για λογαριασμό αυτής επί ολόκληρο το υπόψη έτος. Τα άτομα που δεν εργάστηκαν ολόκληρο το έτος, οι εργαζόμενοι μερικής απασχόλησης, ανεξάρτητα από τη διάρκεια, και οι εργαζόμενοι σε εποχική βάση αντιστοιχούν σε κλάσματα των ΕΜΕ. Στον αριθμό απασχολούμενων περιλαμβάνονται: α) οι μισθωτοί, β) τα άτομα που εργάζονται για την επιχείρηση έχουν σχέση εξάρτησης και εξομοιώνονται με τους μισθωτούς με βάση το εθνικό δίκαιο, γ) οι ιδιοκτήτες επιχειρηματίες, δ) οι εταίροι που ασκούν τακτική δραστηριότητα εντός της επιχείρησης και προσπορίζονται οικονομικά πλεονεκτήματα από την επιχείρηση

Α/Η: Η μονάδα μέτρησης του χρόνου της επιθεώρησης. Τυπικά, η διάρκεια μιας ανθρωπομέρας επιθεώρησης διαρκεί 8 ώρες συμπεριλαμβανομένων των διαλειμμάτων

Διάρκεια επιθεώρησης: Ο χρόνος που δαπανά η Ομάδα Επιθεώρησης για την υλοποίηση της επιθεώρησης και περιέχει τις δραστηριότητες ανάμεσα (περιλαμβανομένων των άκρων) στην εναρκτήρια συνεδρίαση και την καταληκτική συνεδρίαση

Πλάνο επιθεώρησης: Η περιγραφή των δραστηριοτήτων και των διευθετήσεων για την επιθεώρηση

Επιθεωρητής: Το άτομο με την αποδεδειγμένη επαγγελματική επάρκεια για τη διενέργεια επιθεώρησης

Απόκλιση: Η μη εκπλήρωση μιας απαίτησης

Αμεροληψία: Η αντικειμενικότητα όσον αφορά το αποτέλεσμα μιας δραστηριότητας αξιολόγησης της συμμόρφωσης

Εμπιστευτικότητα: Η ιδιότητα ότι οι πληροφορίες δεν διατίθενται ή αποκαλύπτονται σε μη εξουσιοδοτημένα άτομα, οντότητες ή διαδικασίες

Φορέας πιστοποίησης: Ένα τρίτο μέρος, ήτοι BQC, το οποίο αξιολογεί τη συμμόρφωση (ενός σχήματος πιστοποίησης)

Σημείο παρουσίας: Παρέχει υπηρεσία ή εκτελεί έργο σε συνεχή βάση που έχουν κάποια σχέση ή επίδραση στην κυβερνοασφάλεια του οργανισμού

4. Βασικές αρχές

Ο φορέας πιστοποίησης διενεργεί τις επιθεωρήσεις και πιστοποιήσεις σύμφωνα με το Πλαίσιο Κυβερνο-Υγιεινής για ΜμΕ, και ικανοποιεί τις απαιτήσεις του πρότυπου ISO/IEC 17021-1: Αξιολόγηση συμμόρφωσης — Απαιτήσεις για φορείς που παρέχουν έλεγχο και πιστοποίηση συστημάτων διαχείρισης — Μέρος 1: Απαιτήσεις.

Προς απόδειξη εκπλήρωσης των παραπάνω αρχών, ο φορέας πιστοποίησης έχει υποβάλει στο NCC-CY το Πιστοποιητικό Διαπίστευσης του ως Φορέας Πιστοποίησης Συστημάτων Διαχείρισης της Ασφάλειας Πληροφοριών και οφείλει να είναι ενεργό καθ' όλη τη διάρκεια της παροχής των υπηρεσιών επιθεώρησης και πιστοποίησης.

Σε κάθε περίπτωση, στα πλαίσια υλοποίησης της αρχής της αμεροληψίας δεν επιτρέπεται το προσωπικό που συμμετέχει με οποιοδήποτε τρόπο στην παροχή των υπηρεσιών επιθεώρησης και πιστοποίησης μέσω του Πλαισίου Κυβερνο-Υγιεινής για ΜμΕ να παρέχει συμβουλευτικές υπηρεσίες στους ελεγχόμενους οργανισμούς.

5. Δομή και Οργάνωση του Φορέα Πιστοποίησης

Ο φορέας πιστοποίησης αναλαμβάνει να διενεργεί τις επιθεωρήσεις και πιστοποιήσεις μέσω του Πλαισίου Κυβερνο-Υγιεινής για ΜμΕ, και ικανοποιεί τις απαιτήσεις καθώς και τα κριτήρια σύμφωνα με το πρότυπο ISO/IEC 17021-1: Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements, όσο αφορά την δομή και την οργάνωση. Συγκεκριμένα, ο φορέας πιστοποίησης έχει:

1. Κατάλληλη νομική υπόσταση ώστε να φέρει εις πέρας τις σχετικές δραστηριότητες
2. Προσωπικό με την κατάλληλη επαγγελματική επάρκεια και κατάρτιση **E035-14** ώστε να φέρει εις πέρας το έργο της επιθεώρησης και πιστοποίησης με ορθό και αποτελεσματικό τρόπο
3. Κατάλληλη εσωτερική οργάνωση ώστε να διαχειρίζεται συνολικά το έργο της επιθεώρησης και πιστοποίησης.

6. Διαδικασία Πιστοποίησης

6.1 Αρχικές επικοινωνίες

Το προσωπικό του φορέα πιστοποίησης παρέχει πληροφορίες σχετικά με το Πλαίσιο Κυβερνο-Υγιεινής για ΜμΕ στους ενδιαφερόμενους όταν αυτές ζητηθούν. Οι πληροφορίες μπορεί να αφορούν τα κριτήρια του Πλαισίου Κυβερνο-Υγιεινής για ΜμΕ ή/και τον τρόπο διενέργειας των σχετικών επιθεωρήσεων ή/και τον τρόπο λειτουργίας της πιστοποίησης ή/και τον τρόπο υποβολής της σχετικής αίτησης ή/και οποιαδήποτε άλλη σχετική πληροφορία. Το στάδιο αυτό είναι προαιρετικό και έχει ως αφετηρία την εκδήλωση ενδιαφέροντος ενός οργανισμού προς τον φορέα πιστοποίησης για το σχέδιο πιστοποίησης και επιθεώρησης για το Πλαίσιο Κυβερνο-Υγιεινής για ΜμΕ.

6.2 Αίτηση πιστοποίησης

Ο φορέας πιστοποίησης έχει δημιουργήσει σχετική πληροφοριακή αίτηση πιστοποίησης **E050-74**, μέσω της οποίας ο κάθε ενδιαφερόμενος αιτείται τεχνική

και οικονομική προσφορά **E050-76** για τη λήψη υπηρεσιών επιθεώρησης και πιστοποίησης μέσω του Πλαισίου Κυβερνο-Υγιεινής για ΜμΕ.

6.3 Αξιολόγηση αίτησης πιστοποίησης

Το κατάλληλο προσωπικό του φορέα πιστοποίησης, εξετάζει τα στοιχεία της αίτησης, προκειμένου να καταλήξει στα ακόλουθα συμπεράσματα:

1. Αν ο αιτούμενος οργανισμός είναι ΜμΕ, με έδρα την Κύπρο σύμφωνα με τον ορισμό που εμπεριέχεται στα κριτήρια του Πλαισίου Κυβερνο-Υγιεινής για ΜμΕ και συνεπάγεται ότι έχει το δικαίωμα επιθεώρησης και πιστοποίησης σύμφωνα με το σχήμα
2. Αν ο φορέας πιστοποίησης έχει την τεχνική ικανότητα να παρέχει τη συγκεκριμένη υπηρεσία επιθεώρησης και πιστοποίησης σύμφωνα με το σχήμα.

Το αποτέλεσμα της αξιολόγησης επισημαίνεται πάνω στο έγγραφο της αίτησης, συμπληρώνονται τα στοιχεία του προσωπικού του φορέα πιστοποίησης που εξήγαγε το συμπέρασμα και η σχετική ημερομηνία.

Στην συνέχεια, ο φορέας πιστοποίησης εκτιμά τη διάρκεια της επιθεώρησης σε Α/Η σύμφωνα με την σχετική οδηγία υπολογισμού Α/Η (όπως δηλώνεται στην αίτηση πιστοποίησης **E050-74**) και εκδίδει την σχετική τεχνική και οικονομική προσφορά **E050-76**.

Ως διάρκεια επιθεώρησης ορίζεται ο χρόνος που θα δαπανήσει η ομάδα επιθεώρησης για την υλοποίηση της επιθεώρησης και περιέχει τις δραστηριότητες ανάμεσα στην εναρκτήρια συνεδρίαση και την καταληκτική συνεδρίαση (περιλαμβανομένων των άκρων). Η διάρκεια της επιθεώρησης συνεπώς αφορά μόνο τη διεξαγωγή της επιθεώρησης και δεν περιλαμβάνει τυχόν επιπλέον Α/Η που μπορεί να χρειαστούν για την ανασκόπηση των διορθωτικών ενεργειών των αποκλίσεων που πιθανώς να έχουν προκύψει από την επιθεώρηση. Ο φορέας πιστοποίησης ενημερώνει στην οικονομική

προσφορά το επιπλέον κόστος Α/Η για αυτές τις περιπτώσεις (εάν απαιτείται).

Ο χρόνος επιθεώρησης, μετριέται σε ανθρωποημέρες (Α/Η) και προκύπτει από τον **συνδυασμό 2 παραμέτρων:**

1. Πλήθος απασχολούμενων ατόμων.

2. Αριθμό σημείων παρουσίας.

Σημείωση: ως σημεία παρουσίας νοούνται τα σημεία φυσικής παρουσίας του οργανισμού, (π.χ. γραφεία, αποθήκες, παραγωγικοί χώροι κλπ.) που μπορούν να επηρεάσουν την κυβερνοασφάλεια του οργανισμού (π.χ. όχι μια αποθήκη με πρώτες ύλες που δεν έχει πρόσβαση σε συστήματα πληροφορικής) και για τα οποία αιτείται ο οργανισμός να επιθεωρηθούν μέσω του Πλαισίου Κυβερνο-Υγιεινής για ΜμΕ.

Συγκεκριμένα, **ισχύουν τα ακόλουθα:**

- Μέχρι 9 απασχολούμενα άτομα – 1 ανθρωποημέρα (Α/Η) επιθεώρησης.

- Από 10 μέχρι 49 απασχολούμενα άτομα – 1,5 ανθρωποημέρα (Α/Η) επιθεώρησης.

- Από 50 μέχρι 249 απασχολούμενα άτομα – 2 ανθρωποημέρες (Α/Η) επιθεώρησης.

Οι **παραπάνω τιμές μεταβάλλονται** ως ακολούθως ανάλογα με το πλήθος σημείων παρουσίας του οργανισμού (τα οποία βρίσκονται εντός του πλαισίου της πιστοποίησης):

- 1 & 2 σημεία παρουσίας 0 (Α/Η) επιθεώρησης.

- 3 – 6 σημεία παρουσίας + 0,5 (Α/Η) επιθεώρησης.

- 7 – 12 σημεία παρουσίας + 1.0 (Α/Η) επιθεώρησης.

- 13 – 20 σημεία παρουσίας + 1.5 (Α/Η) επιθεώρησης.

- > 20 σημεία παρουσίας + 2.0 (Α/Η) επιθεώρησης.

Παράδειγμα:

- Ο χρόνος επιθεώρησης για έναν οργανισμό που έχει 10 απασχολούμενα άτομα και ένα (1) σημείο παρουσίας, θα είναι: 1,5 Α/Η.

- Ο χρόνος επιθεώρησης για έναν οργανισμό που έχει 8 απασχολούμενα άτομα και οκτώ (8) σημεία παρουσίας, θα είναι: 2,0 Α/Η.

- Ο χρόνος επιθεώρησης για έναν οργανισμό που έχει 200 απασχολούμενα άτομα και δέκα (10) σημεία παρουσίας, θα είναι: 3,0 Α/Η.

- Ο χρόνος επιθεώρησης για έναν οργανισμό που έχει 200 απασχολούμενα άτομα και ένα (1) σημείο παρουσίας, θα είναι: 2,0 Α/Η.

6.4 Σύμβαση

Ως έναρξη του έργου επιθεώρησης και πιστοποίησης μέσω του Πλαισίου Κυβερνο-Υγιεινής για ΜμΕ, νοείται η ημερομηνία της υπογραφής σχετικής σύμβασης συνεργασίας **E050-77** ανάμεσα στον φορέα πιστοποίησης και τον αιτούμενο οργανισμό.

Ο φορέας πιστοποίησης έχει έγκυρη και νομικά εκτελεστή συμφωνία σύμφωνα με την ισχύουσα νομοθεσία με κάθε πελάτη για την παροχή των δραστηριοτήτων επιθεώρησης πιστοποίησης σύμφωνα με τις σχετικές απαιτήσεις του πρότυπου ISO/IEC 17021-1 και του παρόντος εγγράφου.

Στη σύμβαση περιέχεται σαφή ένδειξη ότι για την απονομή του πιστοποιητικού στα πλαίσια του σχεδίου πιστοποίησης μέσω του Πλαισίου Κυβερνο-Υγιεινής για ΜμΕ, απαιτείται η επιτυχής ολοκλήρωση της σχετικής επιθεώρησης. Επιτυχής επιθεώρηση, θεωρείται η επιθεώρηση στην οποία είτε δεν υπάρχουν αποκλίσεις είτε αυτές έχουν αντιμετωπιστεί αποτελεσματικά από τον οργανισμό στο χρονικό διάστημα που έχει χορηγηθεί προς τούτο από τον φορέα πιστοποίησης.

6.5 Επιθεώρηση

Ο φορέας πιστοποίησης, επιλέγει (από σχετική λίστα κατάλληλων καταρτισμένων επιθεωρητών) έναν ή περισσότερους επιθεωρητές για την εκτέλεση της επιθεώρησης ανά περίπτωση (δηλώνεται από τον ανασκοπητή του φορέα στο έντυπο αίτησης πιστοποίησης **E050-74**) και τους ενημερώνει σχετικά με την ανάθεση του κάθε έργου.

Με ευθύνη του φορέα πιστοποίησης γίνεται η κατάλληλη επικοινωνία τόσο με τον/τους επιθεωρητή/ές όσο και με τον υποψήφιο οργανισμό προς επιθεώρηση, ώστε να προκύψουν τα ακόλουθα:

1. Ότι δεν υπάρχει κάποιο εμπόδιο στην αμεροληψία της ομάδας επιθεώρησης.

2. Ότι δεν υπάρχει κάποια αμφισβήτηση ως προς την επάρκεια της ομάδας επιθεώρησης.

Σε περίπτωση που τίθεται κάποιο ζήτημα σε σχέση με τα παραπάνω, ο φορέας πιστοποίησης προβαίνει στις κατάλληλες διορθωτικές ενέργειες μέχρι να αποκατασταθεί. Ενώ στην συνέχεια γίνονται συνεννοήσεις για τον καθορισμό μιας κοινά αποδεκτής ημερομηνίας (ανάμεσα στην ομάδα επιθεώρησης και τον επιθεωρούμενο οργανισμό) για την διενέργεια της επιθεώρησης.

6.6 Πλάνο επιθεώρησης

Ο επιθεωρητής αποστέλλει πλάνο επιθεώρησης **E050-78** στον επιθεωρούμενο οργανισμό για την διενέργεια της επιθεώρησης στον συμφωνημένο χρόνο, καλύπτοντας όλο το εύρος των κριτηρίων του Πλαισίου Κυβερνο-Υγιεινής για ΜμΕ και αναφέροντας επίσης την προβλεπόμενη διάρκεια επιθεώρησης.

Σε περίπτωση ύπαρξης πολλαπλών σημείων παρουσίας του οργανισμού, η ομάδα επιθεώρησης θα επισκεφτεί όλα τα σημεία παρουσίας.

Το μέλος της ομάδας επιθεώρησης το οποίο θα αναλάβει κάθε σημείο και ποια θα είναι η διάρκεια της επιθεώρησης στο κάθε σημείο, καθορίζεται από την ομάδα επιθεώρησης μετά από σχετική συζήτηση με τον οργανισμό.

Το πλάνο επιθεώρησης αποστέλλεται στον επιθεωρούμενο οργανισμό πριν την διενέργεια της επιθεώρησης εντός εύλογου χρονικού διαστήματος, με σκοπό την διευκόλυνση της προετοιμασίας των δυο μερών.

6.7 Επιτόπια επιθεώρηση

Η ομάδα επιθεώρησης εισέρχεται στο χώρο του επιθεωρούμενου οργανισμού σύμφωνα με τις οδηγίες του επιθεωρούμενου οργανισμού και τηρώντας όλες τις σχετικές διαδικασίες και προβλέψεις.

6.8 Εναρκτήρια συνεδρίαση

Η επίσημη εναρκτήρια συνεδρίαση λαμβάνει χώρα με κατάλληλους εκπροσώπους του οργανισμού πριν την έναρξη της επιθεώρησης. Ο σκοπός της εναρκτήριας συνεδρίασης, είναι να παρέχει μια σύντομη επισκόπηση και επεξήγηση των βασικών αρχών, λειτουργιών και δραστηριοτήτων της επιθεώρησης που πρόκειται να διενεργηθεί.

Η εναρκτήρια συνεδρίαση συμπεριλαμβάνει τουλάχιστον τα πιο κάτω:

- Παρουσίαση των μελών της ομάδας ελέγχου και σύντομη επεξήγηση του ρόλου τους στην επιθεώρηση.
- Επιβεβαίωση του πεδίου εφαρμογής της επιθεώρησης.
- Επιβεβαίωση του πλάνου επιθεώρησης.
- Επιβεβαίωση ότι υπάρχουν οι κατάλληλοι πόροι και εξοπλισμός αναγκαία από τους επιθεωρητές για τη βέλτιστη διεξαγωγή της επιθεώρησης.
- Αναφορά στην υποχρέωση για εμπιστευτικότητα του συνόλου της πληροφορίας που αφορά την επιθεώρηση, όπως προκύπτει από την σχετική σύμβαση του κάθε επιθεωρητή.
- Επιβεβαίωση ότι υπάρχουν εκ μέρους του ελεγχόμενου οργανισμού, τα άτομα τα οποία θα συνοδεύσουν τους επιθεωρητές είτε ως καθοδηγητές είτε ως παρατηρητές.
- Τη διαδικασία της επιθεώρησης και τα μετέπειτα βήματα.
- Την υποχρέωση των ελεγκτών να τεκμηριώσουν τις αποδείξεις της επιθεώρησης στα κατάλληλα ερωτηματολόγια, ως μέρος της διαδικασίας και με σκοπό την αποτελεσματικότερη υλοποίηση της

επιθεώρησης αλλά και την παροχή ικανών επαληθεύσιμων αποδεικτικών στοιχείων συμμόρφωσης του οργανισμού προς τα κριτήρια του σχήματος πιστοποίησης κυβερνοασφάλειας για ΜμΕ.

- Την μορφή της έκθεσης επιθεώρησης, τον χρόνο παράδοσής της και την ανάγκη τήρησης της από τον Φορέα Πιστοποίησης.

- Το γεγονός ότι η επιθεώρηση στηρίζεται στην εύρεση αντικειμενικών αποδείξεων με δειγματοληπτικό τρόπο, εξηγώντας επίσης και τους περιορισμούς που έχει αυτός ο τρόπος επιθεώρησης.

- Δήλωση σχετικά με το γεγονός ότι η επιθεώρηση δεν εξασφαλίζει ότι δεν μπορεί ή δεν πρόκειται να συμβεί κάποιο περιστατικό ασφαλείας και ότι δεν τους απαλλάσσει από όποια σχετική ευθύνη σύμφωνα με οποιονδήποτε σχετικό νόμο.

- Την επιβεβαίωση του χρόνου και του τόπου της καταληκτικής συνάντησης, στην οποία θα ζητηθεί και η υπογραφή της σχετικής έκθεσης ελέγχου.

Στο τέλος της εναρκτήριας συνάντησης, προβλέπεται συγκεκριμένο εύλογο χρονικό διάστημα και κάποιος χρόνος για την υποβολή ερωτήσεων και παροχή απαντήσεων από τους συμμετέχοντες. Δεν προβλέπεται η εναρκτήρια συνεδρίαση να διαρκεί περισσότερο από μια ώρα εκτός και αν συμφωνηθεί διαφορετικά.

6.9 Πραγματοποίηση της επιθεώρησης

Σκοπός του παρόντος βήματος είναι η συλλογή επαληθεύσιμων αποδείξεων της συμμόρφωσης του οργανισμού ως προς τα κριτήρια του σχήματος πιστοποίησης κυβερνοασφάλειας για ΜμΕ.

Στα πλαίσια της πραγματοποίησης του ελέγχου:

- Ο κάθε επιθεωρητής με τον συνοδό του μεταβαίνει στο χώρο της επιθεώρησης σύμφωνα με το πλάνο επιθεώρησης και πραγματοποιεί την επιθεώρηση των κριτηρίων που του έχουν ανατεθεί.

- Ο κάθε Επιθεωρητής δείχνει δέουσα επιμέλεια στην αποτελεσματική ολοκλήρωση του κάθε

ανατεθειμένου σημείου επιθεώρησης μέσα στα χρονικά περιθώρια που έχουν καθοριστεί στα πλαίσια του πλάνου επιθεώρησης.

- Κατά τη διάρκεια της επιθεώρησης, μόνο πληροφορίες που είναι σχετικές με τον σκοπό της επιθεώρησης, το πεδίο εφαρμογής της επιθεώρησης και τα σχετικά κριτήρια, επιτρέπεται να συλλεχθούν με την εφαρμογή κατάλληλης δειγματοληψίας.

- Η πληροφορία που συλλέγεται θα πρέπει να μπορεί να επαληθευτεί, στο βαθμό που αυτό είναι εφικτό, προκειμένου να είναι αποδεκτή ως αποδεικτικό της επιθεώρησης (αντικειμενική απόδειξη) (objective evidence). Η πληροφορία καταγράφεται μέσα στο ερωτηματολόγιο της επιθεώρησης **E050-75** στα κατάλληλα σημεία.

- Για κάθε κριτήριο του Πλαισίου Κυβερνο-Υγιεινής για ΜμΕ συμπληρώνονται: οι επαληθεύσιμες αποδείξεις, το συμπέρασμα σχετικά με την συμμόρφωση έναντι κάθε σημείου ελέγχου και οι αποκλίσεις (για τις περιπτώσεις που υπάρχει μερική ή πλήρης μη συμμόρφωση).

- Κανένα από τα μέλη της ομάδας επιθεώρησης δεν χειρίζεται οποιοδήποτε πληροφοριακό εξοπλισμό, ακόμα και αν είναι καταρτισμένος ή είναι εγκεκριμένος και κατάλληλα εκπαιδευμένος από τον κατασκευαστή.

- Τα μέλη της ομάδας επιθεώρησης επιλέγουν και εφαρμόζουν κατάλληλες μεθόδους αναγνώρισης και συλλογής των αποδείξεων (ενδεικτικά αναφέρονται: συνεντεύξεις με αρμόδιο προσωπικό, επισκόπηση συστημάτων, επισκόπηση προβλέψεων, φυσική παρατήρηση, παρακολούθηση μιας εργασίας την ώρα που γίνεται, ανασκόπηση γραπτής τεκμηρίωσης κ.α.).

6.10 Σύσκεψη των επιθεωρητών και Συγγραφή της αναφοράς

Μετά την ολοκλήρωση της επιθεώρησης, η ομάδα επιθεώρησης πραγματοποιεί σύσκεψη χωρίς την παρουσία εκπροσώπων του οργανισμού ώστε να

υπάρχει μία συνολική εικόνα για τη συμμόρφωση του οργανισμού προς τα κριτήρια του Πλαισίου Κυβερνο-Υγιεινής για ΜμΕ.

Η ομάδα επιθεώρησης εξάγει την έκθεση επιθεώρησης **E050-79** με τη βοήθεια των σχετικών ερωτηματολογίων. Για κάθε κριτήριο του Πλαισίου Κυβερνο-Υγιεινής για ΜμΕ, αναφέρεται ευκρινώς το συμπέρασμα σχετικά με την συμμόρφωση. Για τις περιπτώσεις που υπάρχει μερική ή πλήρης μη συμμόρφωση, καταγράφεται ανά κριτήριο η σχετική απόκλιση. Για το σύνολο των αποκλίσεων δίνεται στον οργανισμό χρονικό διάστημα **30 ημερών** για να προσκομίσει κατάλληλες αποδείξεις σχετικά με την αποτελεσματική αντιμετώπιση και άρση των αποκλίσεων.

Η έκθεση επιθεώρησης **E050-79** συμπληρώνεται και υπογράφεται από όλα τα μέλη της ομάδας επιθεώρησης και περιέχει επιπλέον την εισήγηση της ομάδας επιθεώρησης σχετικά με την έκδοση πιστοποιητικού.

Έκθεση επιθεώρησης που φέρει μια ή περισσότερες ανοικτές αποκλίσεις, δεν μπορεί να συνοδεύεται με θετική εισήγηση προς τον Φορέα Πιστοποίησης για την έκδοση πιστοποιητικού.

6.11 Καταληκτική συνεδρίαση

Η καταληκτική συνεδρίαση παρουσιάζει τα αποτελέσματα της επιθεώρησης. Πρέπει να συμμετέχει η διοίκηση του οργανισμού και όποια άλλα μέλη κρίνεται απαραίτητο από τον οργανισμό.

Η καταληκτική συνεδρίαση συμπεριλαμβάνει πληροφορίες τουλάχιστον για τα πιο κάτω (σε βαθμό λεπτομέρειας κατάλληλα προσαρμοσμένου σύμφωνα με τις γνώσεις του οργανισμού για τις διαδικασίες επιθεώρησης):

- Αναφορά στο ότι η επιθεώρηση που πραγματοποιήθηκε βασίστηκε στη συλλογή αντικειμενικών στοιχείων με δειγματοληπτικό τρόπο.
- Αναφορά στην έκθεση επιθεώρησης και τα αποτελέσματά της.

- Σε περίπτωση αποκλίσεων, οι επόμενες ενέργειες που πρέπει να διενεργηθούν και το χρονικό πλαίσιο των **30 ημερών** για την εφαρμογή κατάλληλων διορθωτικών ενεργειών από την πλευρά του οργανισμού και την επιβεβαίωση τους από την ομάδα επιθεώρησης.

Στο τέλος της καταληκτικής συνεδρίασης, παρέχεται η έκθεση επιθεώρησης **E050-79** στον οργανισμό και λαμβάνεται κατάλληλα υπογεγραμμένη από την διοίκηση του οργανισμού ή από άλλο κατάλληλα εξουσιοδοτημένο άτομο.

6.12 Άρση αποκλίσεων

Η ομάδα επιθεώρησης καταγράφει στο κατάλληλο σημείο του ερωτηματολογίου επιθεώρησης **E050-75** τις αποκλίσεις (μία ή περισσότερες) ανά σημείο ελέγχου και κριτηρίου του σχεδίου πιστοποίησης μέσω του Πλαισίου Κυβερνο-Υγιεινής για ΜμΕ.

Οι αποκλίσεις δεν έχουν διαβάθμιση. Οποιοδήποτε σημείο του κριτηρίου δεν καλύπτεται από τον οργανισμό θεωρείται απόκλιση και καταγράφεται με τέτοιο τρόπο ώστε να είναι σαφές για τον οργανισμό (όταν διαβάσει την σχετική έκθεση επιθεώρησης):

- Ποιο κριτήριο αφορά η απόκλιση.
- Ποια είναι η έκταση της απόκλισης ως προς τις απαιτήσεις του κριτηρίου.
- Ποιο είναι το σχετικό αποδεικτικό στοιχείο (όπου υπάρχει) της απόκλισης.

Έκθεση επιθεώρησης που φέρει μια ή περισσότερες ανοικτές αποκλίσεις δεν μπορεί να συνοδεύεται με θετική εισήγηση για την έκδοση πιστοποιητικού.

Η ομάδα επιθεώρησης ενημερώνει τον οργανισμό κατά τη διάρκεια της καταληκτικής συνάντησης σχετικά με την ύπαρξη χρονικού πλαισίου **30 ημερών** (από την ημέρα της καταληκτικής συνάντησης) για την εφαρμογή κατάλληλων διορθωτικών ενεργειών για την αντιμετώπιση των αποκλίσεων. Στα πλαίσια αυτού του χρονικού διαστήματος, ο οργανισμός οφείλει να αποστείλει ή να κάνει με άλλο τρόπο διαθέσιμα τα κατάλληλα αποδεικτικά στοιχεία στον

επιθεωρητή. Η ομάδα επιθεώρησης, οφείλει να ανασκοπήσει τα σχετικά αποδεικτικά στοιχεία και να αποφανθεί σχετικά με την επάρκειά τους για την αποτελεσματική αντιμετώπιση των αποκλίσεων. Σε περίπτωση που πράγματι οι αποκλίσεις αντιμετωπίζουν αποτελεσματικά την/τις απόκλιση/αποκλίσεις, συμπληρώνονται τα στοιχεία στο κατάλληλο σημείο της αναφοράς και αλλάζει η εισήγηση της ομάδας επιθεώρησης σε θετική για την έκδοση πιστοποιητικού. Σε οποιαδήποτε άλλη περίπτωση, η ομάδα επιθεώρησης συμπληρώνει την εισήγηση για την έκδοση πιστοποιητικού ως αρνητική. Η νέα έκδοση της έκθεσης επιθεώρησης-τελική παραδίδεται στον επιθεωρούμενο οργανισμό, σε συνέχεια των παραπάνω ενεργειών.

6.13 Ολοκλήρωση της Επιθεώρησης και Παράδοση της Σχετικής Τεκμηρίωσης

Για να ολοκληρωθεί η διαδικασία της επιθεώρησης, η ομάδα επιθεώρησης παραδίδει στον φορέα πιστοποίησης τα ακόλουθα έγγραφα:

- Το πλάνο επιθεώρησης **E050-78**
- Το συμπληρωμένο ερωτηματολόγιο επιθεώρησης **E050-75**
- Τη συμπληρωμένη και υπογεγραμμένη τελική έκθεση επιθεώρησης **E050-79**
- Σχετικό υποστηρικτικό υλικό (αν και εφόσον απαιτείται)

6.14 Αξιολόγηση και απόφαση πιστοποίησης

Ο φορέας πιστοποίησης, επιλέγει άτομο/άτομα από το προσωπικό του, που έχουν την κατάλληλη επάρκεια και αρμοδιότητα για την αξιολόγηση της σχετικής τεκμηρίωσης της επιθεώρησης και την λήψη της απόφασης πιστοποίησης.

Κατά τη διάρκεια της ανασκόπησης ελέγχεται ότι:

- Τα έγγραφα, όπως αναφέρονται παραπάνω, έχουν συμπληρωθεί πλήρως.
- Οι πιθανές αποκλίσεις έχουν αρθεί και υπάρχουν στοιχεία για τον τρόπο αντιμετώπισής τους.

- Η διάρκεια της επιθεώρησης ήταν η προβλεπόμενη σύμφωνα με τους αρχικούς υπολογισμούς και όπως φαίνεται στη σχετική οικονομική προσφορά **E050-76** και στη σύμβαση συνεργασίας **E050-77**.

- Η ομάδα επιθεώρησης είχε την επαγγελματική επάρκεια που απαιτείται σύμφωνα με την σχετική περιγραφή θέσης εργασίας **E035-14**.

- Δεν συντρέχει κάποιο κόλλημα προς τη διαδικασία αξιολόγησης (π.χ. καταγγελία, παράπονο, προσφυγή κ.α.).

Με το πέρας της αξιολόγησης, συμπληρώνεται το κατάλληλο έγγραφο σύμφωνα με τις διαδικασίες του Φορέα Πιστοποίησης, στο οποίο αναφέρεται:

- Η απόφαση του Φορέα Πιστοποίησης για την έκδοση του πιστοποιητικού.
- Η ημερομηνία λήψης της απόφασης.
- Το άτομο/άτομα που έλαβαν την απόφαση.

6.15 Χορήγηση πιστοποιητικού

Σε περίπτωση θετικής αξιολόγησης ο φορέας πιστοποίησης εκδίδει το κατάλληλο πιστοποιητικό σε χρονικό διάστημα **όχι μεγαλύτερο των 15 ημερών από την ημερομηνία υπογραφής της θετικής έκθεσης επιθεώρησης**. Σε περίπτωση αποκλίσεων, δίδεται το χρονικό πλαίσιο **30 ημερών** για την εφαρμογή των κατάλληλων διορθωτικών ενεργειών.

Το πιστοποιητικό έχει τα ακόλουθα κατ' ελάχιστο περιεχόμενα:

- Την επωνυμία του πιστοποιημένου οργανισμού.
- Την διεύθυνση των σημείων παρουσίας που βρίσκονται εντός του πεδίου της παρούσας πιστοποίησης.
- Την ημερομηνία έκδοσης της πιστοποίησης και έναρξης ισχύος του πιστοποιητικού.
- Την ημερομηνία λήξης του πιστοποιητικού (1 χρόνος παρά μια μέρα από την ημερομηνία έκδοσης).
- Ένα μοναδικό αναγνωριστικό αριθμό ή άλλη σήμανση του πιστοποιητικού.
- Το όνομα και την έκδοση των κριτηρίων του Πλαισίου Κυβερνο-Υγιεινής για ΜμΕ, σύμφωνα με τα οποία έχει διενεργηθεί η επιθεώρηση και η σχετική πιστοποίηση.

- Το όνομα, την διεύθυνση και το λογότυπο του φορέα πιστοποίησης που εκδίδει το πιστοποιητικό.

Για την εξασφάλιση της ορθής λειτουργίας της αγοράς και της συγκεκριμένης πιστοποίησης, ο φορέας πιστοποίησης λαμβάνει μέτρα για την αποφυγή παραχάραξης των πιστοποιητικών.

6.17 Διατήρηση της πιστοποίησης

Ο οργανισμός οφείλει να συμμορφώνεται με τα σημεία ελέγχου του Πλαισίου Κυβερνο-Υγιεινής για ΜμΕ καθ' όλη τη διάρκεια ισχύος του σχετικού πιστοποιητικού.

Σε περιπτώσεις που:

- έχει γίνει σχετική καταγγελία
- έχει ζητηθεί αρμοδίως από τις αντίστοιχες αρχές
- υπάρχουν άλλα στοιχεία (π.χ. παράπονα, παραβάσεις που έχουν διαπιστωθεί από αρμόδιες αρχές, κ.α.),

ο φορέας πιστοποίησης έχει το δικαίωμα να διενεργήσει έκτακτη επιθεώρηση και σε περίπτωση που προκύψουν αποκλίσεις, να προβεί στις ακόλουθες ενέργειες:

- **Αναστολή πιστοποιητικού:** Ο φορέας πιστοποίησης μετά τη συλλογή αποδείξεων στα πλαίσια έκτακτων επιθεωρήσεων και εξαγωγή συμπεράσματος ότι δεν τηρούνται ένα ή περισσότερα κριτήρια του Πλαισίου Κυβερνο-Υγιεινής για ΜμΕ, θέτει το πιστοποιητικό σε αναστολή και ζητάει από τον οργανισμό να λάβει άμεσα σε διάστημα **30 ημερών** διορθωτικές ενέργειες. Σε αναστολή πιστοποιητικού τίθεται για τον οργανισμό για την μη συμμόρφωση του οποίου υπάρχουν σοβαρές και καταγεγραμμένες υπόνοιες, αλλά δεν δέχεται την υλοποίηση έκτακτης επιθεώρησης μετά από επικοινωνία του φορέα πιστοποίησης για ένα μήνα.

- **Ανάκληση πιστοποιητικού:** Σε περίπτωση που ο οργανισμός δεν λάβει διορθωτικές ενέργειες για την απενεργοποίηση της αναστολής πιστοποιητικού εντός του προδιαγεγραμμένου διαστήματος των **30 ημερών**, το πιστοποιητικό ανακαλείται. Σε ανάκληση τίθεται επίσης το πιστοποιητικό του οργανισμού το οποίο έχει αποδειχθεί ότι είναι ψευδές ή παραποιημένο, ή ο οργανισμός έχει παραβιάσει τους

όρους της σύμβασης ή ο οργανισμός έχει προβεί σε παραπλανητική χρήση του πιστοποιητικού ή των σχετικών λογοτύπων.

Όλες οι σχετικές επικοινωνίες μεταξύ του φορέα πιστοποίησης και του πιστοποιημένου οργανισμού γίνονται **γραφώς**.

Για όσο χρονικό διάστημα το πιστοποιητικό βρίσκεται σε κατάσταση αναστολής, ο οργανισμός δεν επιτρέπεται να λέει ή με οποιονδήποτε τρόπο να υπονοεί ότι έχει ενεργή σχετική πιστοποίηση.

Η ανάκληση πιστοποιητικού συνοδεύεται και από επικαιροποίηση της κατάστασης στην βάση δεδομένων του φορέα πιστοποίησης και σε ανάρτηση σχετικής ενημέρωσης στο διαδικτυακό χώρο του φορέα πιστοποίησης.

6.18 Ανανέωση της πιστοποίησης

Το Πιστοποιητικό που χορηγείται με τον παραπάνω τρόπο, έχει **διάρκεια ισχύος ενός (1) έτους**. Με την πάροδο του ενός (1) έτους, το Πιστοποιητικό λήγει και παύει να έχει ισχύ και ο οργανισμός πρέπει να διενεργήσει τη διαδικασία πιστοποίησης από την αρχή, όπως αναφέρεται στην ενότητα Πιστοποίηση παραπάνω.

6.19 Καταγγελίες / Προσφυγές / Παράπονα

Σε συμφωνία με τα αναφερόμενα στην ενότητα Βασικές Αρχές, ο φορέας πιστοποίησης οφείλει να τηρεί διαδικασίες για την λήψη και ανταπόκριση σε καταγγελίες, προσφυγές και οποιεσδήποτε άλλες σχετικές διαδικασίες (από τους επιθεωρούμενους, τους πιστοποιημένους οργανισμούς, το ευρύτερο κοινό, ενώπιον των Κυπριακών Δικαστηρίων κ.α.) και παράπονα.

Ο φορέας πιστοποίησης δημοσιοποιεί πληροφορίες προς το ευρύτερο κοινό σχετικά με τον τρόπο και τα μέσα, μέσω των οποίων μπορεί να υποβληθούν καταγγελίες, προσφυγές και παράπονα.

Ο φορέας πιστοποίησης ανταποκρίνεται στις καταγγελίες, προσφυγές και παράπονα με αποτελεσματικό τρόπο. Οι πληροφορίες που ανταλλάσσονται ανάμεσα στα εμπλεκόμενα μέρη είναι πάντα γραπτές (φυσικές ή ηλεκτρονικές) και διατηρούνται σε κατάλληλα προστατευμένο σημείο

για χρονικό διάστημα τουλάχιστον **5 ετών**. Πρόσβαση στις πληροφορίες αυτές έχει μόνο το εξουσιοδοτημένο προσωπικό του φορέα πιστοποίησης.

6.20 Αλλαγές στα κριτήρια του Πλαισίου Κυβερνο-Υγιεινής για ΜμΕ

Σε περίπτωση αλλαγών στα κριτήρια του Πλαισίου Κυβερνο-Υγιεινής για ΜμΕ, όπως αυτά εκδίδονται από την Αρχή Ψηφιακής Ασφάλειας (ΑΨΑ) ως το

Εθνικό Κέντρο Συντονισμού Κυβερνοασφάλειας (NCC-CY), διενεργείται εκ νέου η διαδικασία επιθεώρησης και πιστοποίησης σύμφωνα με τα οριζόμενα της διαδικασίας πιστοποίησης.

Το χρονικό διάστημα για τη μετάβαση στη νέα έκδοση καθορίζεται κάθε φορά από το Εθνικό Κέντρο Συντονισμού Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας (NCC-CY).