Περιεχόμενα

0. Σκοπός και Πεδίο Εφαρμογής

Σκοπός του παρόντος Ειδικού Κανονισμού Πιστοποίησης είναι η παροχή τεκμηριωμένων πληροφοριών προς κάθε ενδιαφερόμενο μέρος ή πελάτη του Φορέα Πιστοποίησης GLOBAL CERT σχετικά με τις απαιτήσεις πιστοποίησης του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών ISO 27001:2013.

Ο παρών Ειδικός Κανονισμός ισχύει σε συνδυασμό με το Γενικό Κανονισμό Πιστοποίησης GRC Γενικός Κανονισμός Πιστοποίησης

1. Αναφορές

- Εγχειρίδιο Ποιότητας QM
- P01 Διαδικασία Διαχείρισης Δραστηριοτήτων πριν τη πιστοποίηση
- P05 Διαδικασία Επιθεωρήσεων, έκδοσης πιστοποιητικών, αναστολής, ανάκλησης ή περιορισμού του πεδίου πιστοποίησης
- P11 Διαδικασία Χρήσης Σημάτων και Λογοτύπων
- GRC Γενικός Κανονισμός Πιστοποίησης
- ΕΛΟΤ ΕΝ ISO 27001:2013 + Cor. 1/2014: Τεχνολογία της πληροφορίας – Τεχνικές Ασφάλειας-Συστήματα διαχείρισης ασφάλειας πληροφοριών — Απαιτήσεις
- ISO/IEC 27000, Information technology — Security techniques — Information security management systems — Overview and vocabulary
- ISO/IEC 27002:2013, Information technology — Security Techniques — Code of practice for information security controls
- ISO/IEC 27003, Information technology — Security techniques — Information security management system implementation guidance
- ISO/IEC 27004, Information technology — Security techniques — Information security management — Measurement
- ISO/IEC 27005, Information technology— Security techniques— Information security risk management
- ISO 27006:2015 Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems
- ISO/IEC 27007:2011 «Guidelines for information security management systems auditing»
- ISO/IEC TR 27008:2011 «Guidelines for auditors on 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 31000:2009, Risk management — Principles and guidelines
- ΕΛΟΤ ΕΝ ISO/IEC 17021-1:2015 Αξιολόγηση της συμμόρφωσης– Απαιτήσεις για φορείς επιθεώρησης και πιστοποίησης συστημάτων διαχείρισης - Μέρος 1: Απαιτήσεις
- ΚΟ ΕΣΥΔ ISMS : Κατευθυντήρια Οδηγία για τη διαπίστευση φορέων πιστοποίησης συστημάτων διαχείρισης της ασφάλειας των πληροφοριών.
- Κανονισμοί και Κατευθυντήριες Οδηγίες του ΕΣΥΔ
- IAF MD Κατευθυντήριες Οδηγίες της Διεθνούς Διαπίστευσης

2. Όροι και Ορισμοί - Συντομογραφίες

αμεροληψία : παρουσία της αντικειμενικότητας (Αντικειμενικότητα σημαίνει ότι δεν υπάρχουν συγκρούσεις συμφερόντων ή ότι είναι επιλυμένες έτσι ώστε να μην επηρεάζουν αρνητικά τις μετέπειτα δραστηριότητες του φορέα πιστοποίησης. Άλλοι όροι που είναι χρήσιμοι σε σχέση με το στοιχείο της αμεροληψίας είναι: ανεξαρτησία, ελευθερία από σύγκρουση συμφερόντων, ελευθερία από προκατάληψη, έλλειψη ζημιάς από άδικη κρίση, ουδετερότητα, δικαιοσύνη, ευρύτητα, ομαλότητα χειρισμού, αποκόλληση, εξισορρόπηση.)

διακινδύνευση : η επίδραση της αβεβαιότητας

ενδιαφερόμενο μέρος : πρόσωπο ή ομάδα που ενδιαφέρεται ή επηρεάζεται από την επίδοση ενός οργανισμού

εμπιστευτικότητα : διατήρηση του εμπιστευτικού χαρακτήρα στοιχείων ή πληροφοριών

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.

επιθεωρητής : πρόσωπο που διεξάγει μια επιθεώρηση

επάρκεια : ικανότητα εφαρμογής γνώσεων και δεξιοτήτων για την επίτευξη των αναμενόμενων αποτελεσμάτων

μη συμμόρφωση : μη εκπλήρωση μιας απαίτησης

κύρια μη συμμόρφωση : Μη συμμόρφωση που επηρεάζει την ικανότητα του συστήματος διαχείρισης να επιτύχει τα επιδιωκόμενα αποτελέσματα

δευτερεύουσα μη συμμόρφωση ή παρατήρηση: Μη συμμόρφωση που δεν επηρεάζει την ικανότητα του συστήματος διαχείρισης να επιτύχει τα επιδιωκόμενα αποτελέσματα

οδηγός : πρόσωπο που ορίζεται από τον πελάτη για να βοηθήσει την ομάδα επιθεώρησης

παρατηρητής : πρόσωπο που συνοδεύει την ομάδα επιθεώρησης αλλά δεν επιθεωρεί

πελάτης : οργανισμός του οποίου το σύστημα διαχείρισης επιθεωρείται για σκοπούς πιστοποίησης

πιστοποιημένος πελάτης : οργανισμός του οποίου το σύστημα διαχείρισης έχει πιστοποιηθεί

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.

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.

πρότυπο : ονομάζεται ένα έγγραφο, που καταρτίζεται με συναίνεση και εγκρίνεται από αναγνωρισμένο φορέα, το οποίο παρέχει για κοινή και επαναλαμβανόμενη χρήση κανόνες, οδηγίες ή χαρακτηριστικά για δραστηριότητες ή τα αποτελέσματα τους, με σκοπό την επίτευξη του βέλτιστου βαθμού τάξης σε ένα συγκεκριμένο πλαίσιο εφαρμογής

συμβουλευτική συστήματος διαχείρισης : συμμετοχή στην εγκατάσταση, εφαρμογή ή τη διατήρηση ενός συστήματος διαχείρισης. (Προετοιμασία ή παραγωγή εγχειριδίων ή διαδικασιών, παροχή συγκεκριμένων συμβουλών, οδηγιών ή λύσεων προς την κατεύθυνση της ανάπτυξης και εφαρμογής ενός συστήματος διαχείρισης.)

σχήμα Πιστοποίησης : Σύστημα αξιολόγησης της συμμόρφωσης που σχετίζεται με συστήματα διαχείρισης στο οποίο εφαρμόζονται οι ίδιες εξειδικευμένες απαιτήσεις, ειδικοί κανόνες και διαδικασίες

τεχνική περιοχή : η τεχνική περιοχή χαρακτηρίζεται από ομοιότητες των διεργασιών που σχετίζονται με ένα συγκεκριμένο τύπο συστήματος διαχείρισης

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.)

χρόνος επιθεώρησης: χρόνος που απαιτείται για το σχεδιασμό και την ολοκλήρωση μιας πλήρους και αποτελεσματικής επιθεώρησης του συστήματος διαχείρισης του πελάτη

διάρκεια επιθεωρήσεων πιστοποίησης συστημάτων διαχείρισης : Μέρος του χρόνου επιθεώρησης που ξοδεύεται για τις δραστηριότητες επιθεώρησης από την εναρκτήρια συνεδρίαση έως τη καταληκτική συμπεριλαμβανομένης

προϊόν : Το αποτέλεσμα μίας διεργασίας (μπορεί να είναι υπηρεσία ή κατεργασμένο υλικό, το οποίο είναι απτό και η ποσότητά του είναι ένα μετρήσιμο ή ένα συνεχές χαρακτηριστικό)

διεργασία : Σύνολο από σχετικές μεταξύ τους εργασίες ή λειτουργίες ή δραστηριότητες, οι οποίες όταν εφαρμόζονται αποτελεσματικά και λαμβάνοντας ένα ή περισσότερα εισερχόμενα (inputs) δημιουργούν εξερχόμενα (outputs), τα οποία προσθέτουν αξία στον οργανισμό.

υπηρεσία: αποτέλεσμα τουλάχιστον μία δραστηριότητας που εκτελείται αναγκαστικά στη διεπαφή μεταξύ του προμηθευτή και πελάτη, που είναι γενικά άυλη.

δεδομένα προσωπικού χαρακτήρα: κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»)· το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου,

ΥΔΠ: Υπεύθυνος Διαχείρισης Ποιότητας

ΣΔΠ: Σύστημα Διαχείρισης Ποιότητας

ΦΠ: Φορέας Πιστοποίησης GLOBAL CERT

3. Υπευθυνότητες και Αρμοδιότητες

Υπεύθυνος εφαρμογής του παρόντος ειδικού κανονισμού είναι ο Υπεύθυνος Πιστοποίησης του Φορέα Πιστοποίησης σε συνεργασία με τον Υπεύθυνο Διαχείρισης

Ποιότητας. Ο ΥΔΠ είναι αρμόδιος για την έκδοση και αναθεώρηση με την έγκριση της Ανώτατης Διοίκησης.

4. Ανάπτυξη Ειδικού Κανονισμού

4.1 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 ISO 27006.

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.

Κατά τα άλλα ισχύουν τα προβλεπόμενα στον Γενικό Κανονισμό Πιστοποίησης.

4.2 Περιεχόμενο Επιθεώρησης

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 παρακάτω εξειδικεύεται το περιεχόμενο της επιθεώρησης και αναφέρονται συνοπτικά οι πτυχές του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών κατά ISO 27001:2013, που ελέγχονται και των οποίων αξιολογείται ο βαθμός συμμόρφωσής με τις αντίστοιχες απαιτήσεις που θέτει το διεθνές πρότυπο.

Επισημαίνεται ότι η διενέργεια αξιολόγησης της συμμόρφωσης περιλαμβάνει δύο διακριτά Στάδια (Στάδιο 1 και Στάδιο 2) τα οποία διενεργούνται υποχρεωτικά στις εγκαταστάσεις του επιθεωρούμενου οργανισμού.

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 αποτυχία του επιθεωρούμενου οργανισμού να συμμορφώνεται με βασικές απαιτήσεις, ο βαθμός συμμόρφωσης με τις οποίες διερευνάται κατά το Στάδιο 1, μπορεί να σηματοδοτήσει αδυναμία εκτέλεσης του Σταδίου 2. Τούτο καθίσταται σαφές και γραπτώς στον επιθεωρούμενο οργανισμό, ο οποίος δια του εκπροσώπου του λαμβάνει ενυπόγραφα γνώση περί των αποτελεσμάτων της επιθεώρησης 1ου Σταδίου. Το Στάδιο 1 έχει σαν κύριο αντικειμενικό σκοπό να διαπιστωθεί ο βαθμός ετοιμότητας που επιδεικνύει ο επιθεωρούμενος οργανισμός για την επιθεώρηση του Σταδίου 2, καθώς επίσης και να συλλεγούν όλα εκείνα τα αναγκαία δεδομένα και στοιχεία ώστε να σχεδιαστεί κατάλληλα και επαρκώς το πρόγραμμα της επιθεώρησης του Σταδίου 2, το οποίο σε κάθε περίπτωση θα επιβεβαιώσει και τα ευρήματα του Σταδίου1. Ειδικότερα κατά το Στάδιο 1 αξιολογούνται και ελέγχονται :

- Η συμμόρφωση του οργανισμού με το ισχύον νομοθετικό πλαίσιο που διέπει τη λειτουργία του και τα προιόντα ή/και υπηρεσίες του,

- Η καταλληλότητα του σχεδιασμού του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών σε ότι αφορά τη δυνατότητα κάλυψης των σκοπών, στόχων και της καθιερωμένης πολιτικής της επιχείρησης (Ελέγχεται η τεκμηρίωση του πελάτη που απαιτείται στο ISO/IEC 27001, επαρκής κατανόηση του σχεδιασμού του ISMS στο πλαίσιο της οργάνωσης του πελάτη, εκτίμηση κινδύνου και μετριασμός (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 της τελικής 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 αξιόπιστης εσωτερικής επιθεώρησης και ανασκόπησης από τη Διοίκηση,
- Η ανάγκη για ανασκόπηση πρόσθετης γραπτής τεκμηρίωσης και διάθεσης πρόσθετων πόρων ή τεχνογνωσίας κατά τη τελική αξιολόγηση, καθώς και η επιλογή των μελών της ομάδας επιθεώρησης για το 2ο στάδιο,
- 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 τεκμηριώνονται στο στάδιο 1 στην έκθεση επιθεώρησης, αναπτύσσεται ένα σχέδιο επιθεώρησης για τη διεξαγωγή του δεύτερου σταδίου. Εκτός από την αξιολόγηση της αποτελεσματικής εφαρμογής του ISMS, οι στόχοι του δεύτερου σταδίου είναι για να επιβεβαιώσει ότι ο πελάτης τηρεί τις δικές του πολιτικές, στόχους και διαδικασίες.

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

α) δέσμευση της Ανώτατης Διοίκησης για την πολιτική ασφάλειας πληροφοριών και τους στόχους της ασφάλειας πληροφοριών,

β) απαιτήσεις τεκμηρίωσης που περιλαμβάνονται στο πρότυπο ISO/IEC 27001,

γ) αξιολόγηση της ασφάλειας των πληροφοριών που σχετίζονται με τους κινδύνους και ότι οι εκτιμήσεις παράγουν συνεπή, έγκυρα και συγκρίσιμα αποτελέσματα εάν επαναληφθούν,

δ) Προσδιορισμός των στόχων ελέγχου και έλεγχοι βάσει της αξιολόγησης κινδύνου για την ασφάλεια πληροφορίες και διεργασίες μετριασμού,

ε) πληροφορίες επιδόσεων ασφαλείας και αποτελεσματικότητα του ISMS, αξιολόγηση σε σχέση με τους στόχους ασφάλειας πληροφοριών,

στ) αντιστοιχία μεταξύ των καθορισμένων ελέγχων, τη δήλωση της εφαρμογής και τα αποτελέσματα της αξιολόγησης των κινδύνων των πληροφοριών ασφαλείας και τη διεργασία μετριασμού και την πολιτική ασφάλειας πληροφοριών και τους στόχους.

ζ) εφαρμογή των ελέγχων (παράρτημα D), λαμβάνοντας υπόψη το εσωτερικό και εξωτερικό πλαίσιο λειτουργίας και τους συναφείς κινδύνους, τη παρακολούθηση, μέτρηση

και ανάλυση των διεργασιών ασφάλειας πληροφοριών της εταιρείας και τους ελέγχων, για να προσδιορισθεί αν τα στοιχεία ελέγχου είναι εφαρμοστέα και ανταποκρίνονται στους δεδηλωμένους στόχους της ασφαλείας πληροφοριών,

η) τα προγράμματα, διεργασίες, διαδικασίες, αρχεία, εσωτερικές επιθεωρήσεις και ανασκοπήσεις της αποτελεσματικότητας του ISMS για να εξασφαλιστεί ότι αυτά είναι ανιχνεύσιμα στις αποφάσεις της Ανάωτατης Διοίκησης και την πολιτική ασφάλειας πληροφοριών και τους στόχους.

Η Ομάδα Επιθεώρησης πρέπει να:

α) απαιτεί από τον πελάτη να αποδείξει ότι η αξιολόγηση της ασφάλειας των πληροφοριών που σχετίζονται με τους κινδύνους που είναι συναφείς και επαρκείς για τη λειτουργία του ISMS εντός του πεδίου του ISMS.

β) διαπιστώσει κατά πόσον 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.

Εκτός από τις απαιτήσεις για την αναφορά στο ISO/IEC 17021-1, 9.4.8, η έκθεση επιθεώρησης παρέχει τις ακόλουθες πληροφορίες ή μια αναφορά σε αυτό:

α) ένα λογαριασμό της επιθεώρησης συμπεριλαμβανομένης της σύνοψης της ανασκόπησης των εγγράφων,

β) ένα λογαριασμό της επιθεώρησης πιστοποίησης της ανάλυσης κινδύνου για την ασφάλεια πληροφοριών του πελάτη,

γ) αποκλίσεις από το πρόγραμμα επιθεώρησης (π.χ. περισσότερο ή λιγότερο χρόνο που δαπανάται σε ορισμένες τακτικές δραστηριότητες),

δ) πεδίο ISMS.

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

α) σημαντικά μονοπάτια επιθεώρησης που ακολουθήθηκαν και τη χρησιμοποιούμενη μεθοδολογία επιθεώρησης,

β) παρατηρήσεις που έγιναν, τόσο θετικές (π.χ. αξιοσημείωτα χαρακτηριστικά) όσο και αρνητικές (π.χ. πιθανές μη συμμορφώσεις)

γ) σχόλια σχετικά με τη συμμόρφωση του ISMS του πελάτη με τις απαιτήσεις πιστοποίησης με μια σαφή δήλωση της μη συμμόρφωσης, μια αναφορά στην έκδοση της δήλωσης της εφαρμογής και, ενδεχομένως, οποιαδήποτε χρήσιμη σύγκριση με τα αποτελέσματα της προηγούμενης επιθεώρησης πιστοποίησης του πελάτη. Συμπλήρωση ερωτηματολογίων, λιστών ελέγχου, παρατηρήσεις, καταλόγων ή σημειώσεων επιθεωρητών μπορεί να αποτελούν αναπόσπαστο μέρος της έκθεσης ελέγχου. Τα έγγραφα αυτά υποβάλλονται στον Φορέα πιστοποίησης ως αποδεικτικά στοιχεία προς υποστήριξη της απόφασης 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 δώσει εμπιστοσύνη στο ISMS. Εκτός από τις απαιτήσεις για την αναφορά στο ISO/IEC 17021-1, η έκθεση καλύπτει:

— μια περίληψη από τις πιο σημαντικές παρατηρήσεις, θετικές καθώς και αρνητικές, όσον αφορά την εφαρμογή και την αποτελεσματικότητα απαιτήσεων και των ελέγχων του ISMS

— συστάσεις της ομάδας επιθεώρησης ως προς το κατά πόσον θα πρέπει να πιστοποιείται το ISMS του πελάτη ή όχι, με πληροφορίες για να τεκμηριωθεί αυτή τη σύσταση.

Επιτήρηση

Σκοπός της επιτήρησης είναι να επιβεβαιώσει ότι το εγκεκριμένο ISMS 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:

α) τα στοιχεία συντήρησης του συστήματος όπως η αξιολόγηση των διακινδυνεύσεων και ο έλεγχος των απειλών για την ασφάλεια πληροφοριών, η εσωτερική επιθεώρηση του ISMS, η ανασκόπηση από τη Διοίκηση και η διορθωτική δράση,

β) επικοινωνία με τα εξωτερικά μέρη όπως απαιτείται από το πρότυπο ISO/IEC 27001 και άλλα έγγραφα που απαιτούνται για την πιστοποίηση,

γ) αλλαγές στη τεκμηρίωση του συστήματος,

δ) περιοχές που υπόκεινται σε αλλαγές,

ε) επιλεγμένες απαιτήσεις του ISO/IEC 27001,

στ) άλλες επιλεγμένες περιοχές ανάλογα με την περίπτωση.

Ως ελάχιστο, σε κάθε επιτήρηση η ομάδα επιθεώρησης ανασκοπεί τα εξής:

α) την αποτελεσματικότητα του ISMS όσον αφορά την επίτευξη των στόχων της πολιτικής ασφάλειας πληροφοριών του πελάτη,

β) τη λειτουργία των διαδικασιών για την περιοδική αξιολόγηση και επανεξέταση της συμμόρφωσης με τις σχετικές πληροφορίες ασφαλείας νομοθεσία και κανονισμούς,

γ) αλλαγές στους ελέγχους που καθορίζονται, και τα αποτελέσματα των αλλαγών,

δ) εφαρμογή και αποτελεσματικότητα των ελέγχων σύμφωνα με το πρόγραμμα επιθεώρησης.

ε) προσφυγές και καταγγελίες

στ) τυχόν μη συμμορφώσεις και παρατηρήσεις από προηγούμενη επιθεώρηση του ISMS

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

Επαναπιστοποίηση

Αν κριθεί σκόπιμη η υλοποίηση πλήρους επαναξιολόγησης είτε λόγω χαμηλού βαθμού συμμόρφωσης του Συστήματος Διαχείρισης ISMS 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 συμβεί σημαντικές μεταβολές στο εφαρμοζόμενο σύστημα Διαχείρισης ISMS 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 Έντυπα

Για τις ανάγκες της τεκμηρίωσης του ΦΠ χρησιμοποιούνται τα έντυπα σε ηλεκτρονική ή φυσική μορφή, που αναφέρονται στις Διαδικασίες P01 και P05 του Συστήματος της GLOBAL CERT.