ΕΙΔΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ ΠΙΣΤΟΠΟΙΗΣΗΣ

ΣΥΣΤΗΜΑΤΩΝ ΔΙΑΧΕΙΡΙΣΗΣ

ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ

της

EP CERTIFICATION ΜΟΝΟΠΡΟΣΩΠΗ Ι.Κ.Ε

ΣΥΜΦΩΝΑ ΜΕ ISO/IEC 27001:2022

ΠΙΝΑΚΑΣ ΕΓΚΡΙΣΗΣ ΚΑΙ ΕΠΑΝΕΚΔΟΣΕΩΝ

Έκδοση	Ημερομηνία	ΣΥΝΤΑΞΗ	ΑΞΙΟΛΟΓΗΣΗ/ ΕΓΚΡΙΣΗ	Περιγραφή Αλλαγής
01	06/01/2023	ΥΔΠ	ΤΕΧΝΙΚΟΣ ΔΙΕΥΘΥΝΤΗΣ	Σύνταξη 1ης Έκδοσης Ημερομηνία έγκρισης 06/01/2023
02	10/04/2024	ΥΔΠ	ΤΕΧΝΙΚΟΣ ΔΙΕΥΘΥΝΤΗΣ	Σύνταξη 2ης Έκδοσης Ημερομηνία έγκρισης 10/04/2024

ΠΕΡΙΕΧΟΜΕΝΑ

1. Γενικά

1.1 Ταυτότητα, Σκοπός, Πεδίο Εφαρμογής

Η ΤΑΥΤΟΤΗΤΑ ΤΟΥ ΦΟΡΕΑ ΠΙΣΤΟΠΟΙΗΣΗΣ
Επωνυμία: EP CERTIFICATION ΜΟΝΟΠΡΟΣΩΠΗ Ι.Κ.Ε.
Διακριτικός τίτλος: EP CERT
Έδρα: ΚΑΠΝΙΚΑΡΕΑΣ, 19Α, ΑΘΗΝΑ, ΤΚ 10556
Τηλέφωνο: +30 2109569617
Email: info@epcert.gr
Ιστότοπος: www.epcert.gr
ΑΦΜ: 801182964
ΔΟΥ: Α ΑΘΗΝΩΝ
Αρμόδιο Πρόσωπο για τις επαφές με τον Φορέα Διαπίστευσης: Ο Διαχειριστής

Σκοπός του παρόντος Ειδικού Κανονισμού Πιστοποίησης είναι η παροχή τεκμηριωμένων πληροφοριών προς κάθε ενδιαφερόμενο μέρος ή πελάτη του Φορέα Πιστοποίησης EP CERTIFICATION ΜΟΝΟΠΡΟΣΩΠΗ Ι.Κ.Ε. σχετικά με τις απαιτήσεις πιστοποίησης του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών, όπως αυτές ορίζονται από το διεθνές πρότυπο EN ISO/IEC 27001:2022. (ΕΛΟΤ EN ISO/IEC 27001 Ε2)

Ο παρών Ειδικός Κανονισμός ισχύει σε συνδυασμό με το Γενικό Κανονισμό Πιστοποίησης Συστημάτων Διαχείρισης κατά ΕΛΟΤ EN ISO/IEC 17021-1:2015.

Εκτός από το πρότυπο ISO/IEC 27001, υπάρχουν ειδικές απαιτήσεις από τα αντίστοιχα έγγραφα που έχουν σημασία για τα συστήματα διαχείρισης της ασφάλειας πληροφοριών και τη διαπίστευση της EPCERT. Επιπρόσθετα, υπάρχει απαίτηση να καλύπτονται τυχόν νέες κατευθυντήριες γραμμές που δημοσιεύονται από την ΕΑ και/ή τον IAF σχετικά με την πιστοποίηση κατά ISO/IEC 27001. Η απαίτηση αυτή αφορά την πιο πρόσφατη δημοσιευμένη έκδοση των ανωτέρω εγγράφων, λαμβάνοντας υπόψη πιθανές μεταβατικές περιόδους. Οι παραπομπές σε παραγράφους του προτύπου ΕΛΟΤ EN ISO/IEC 17021-1 βασίζονται στην έκδοση ΕΛΟΤ EN ISO/IEC 17021-1:2015.

Ο παρών ειδικός κανονισμός πιστοποίησης αποτελείται από τα ακόλουθα τρία στοιχεία:
> Την ερμηνεία του προτύπου ISO/IEC 27001 (κεφάλαιο 2)
> Την οργάνωση της EPCERT (κεφάλαιο 3)
> Τις διαδικασίες που χρησιμοποιεί ο φορέας πιστοποίησης (κεφάλαιο 4)

1.2 Αναφορές

- Εγχειρίδιο Διαχείρισης
- Διαδικασίες
- Γενικοί Όροι και Προϋποθέσεις Πιστοποίησης Συστημάτων, Προϊόντων και Προσωπικού

• Γενικοί Όροι Σύμβασης για την Πιστοποίηση Συστημάτων, Προϊόντων
• Γενικός Κανονισμός Πιστοποίησης Συστημάτων Διαχείρισης κατά ΕΛΟΤ EN ISO/IEC 17021-1:2015
• ΕΛΟΤ EN ISO/IEC 17021-1:2015 Αξιολόγηση της συμμόρφωσης - Απαιτήσεις για φορείς επιθεώρησης και πιστοποίησης συστημάτων διαχείρισης - Μέρος 1: Απαιτήσεις
• ΕΛΟΤ EN ISO 9000:2015 Συστήματα Διαχείρισης Ποιότητας - Θεμελιώδεις Αρχές και Λεξιλόγιο.
• ΕΛΟΤ EN ISO/IEC 27000:2018 Τεχνολογία Πληροφοριών – Τεχνικές Ασφάλειας – Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών – Επισκόπηση και λεξιλόγιο
• ΕΛΟΤ EN ISO/IEC 27001:2022 Ασφάλεια πληροφοριών, κυβερνοασφάλεια και προστασία της ιδιωτικής ζωής - Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών — Απαιτήσεις
• ISO/IEC 27002:2022 Τεχνολογία πληροφοριών - Τεχνικές ασφάλειας - Κώδικας πρακτικής για τους ελέγχους ασφάλειας των πληροφοριών
• ISO/IEC 27003:2017 Τεχνολογία πληροφοριών - Τεχνικές ασφάλειας - Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών – Οδηγίες
• ISO/IEC 27004:2016 Τεχνολογία πληροφοριών - Τεχνικές ασφάλειας - Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών – Παρακολούθηση, μέτρηση, ανάλυση και αξιολόγηση
• ISO/IEC 27005:2022 Ασφάλεια πληροφοριών, κυβερνοασφάλεια και προστασία της ιδιωτικής ζωής — Οδηγίες για τη διαχείριση κινδύνων για την ασφάλεια των πληροφοριών
• ISO/IEC 27006:2015/Amd 1:2020 Τεχνολογία πληροφοριών - Τεχνικές ασφάλειας - Απαιτήσεις για Οργανισμούς που διενεργούν επιθεωρήσεις σε Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών – Amd 1
• ISO/IEC 27007:2020 Ασφάλεια πληροφοριών, κυβερνοασφάλεια και προστασία της ιδιωτικής ζωής — Οδηγίες για την επιθεώρηση συστημάτων διαχείρισης ασφάλειας πληροφοριών
• ISO/IEC TS 27008:2019 Τεχνολογία πληροφοριών - Τεχνικές ασφάλειας - Οδηγίες για την αξιολόγηση των σημείων ελέγχου ασφάλειας πληροφοριών
• ISO/IEC 17000:2020, Αξιολόγηση Συμμόρφωσης — Λεξιλόγιο και γενικές αρχές
• Κανονισμοί και Κατευθυντήριες Οδηγίες του ΕΣΥΔ:
• IAF MD Κατευθυντήριες Οδηγίες της Διεθνούς Διαπίστευσης:

- IAF MD 1:2023 Πιστοποίηση πολλαπλών χώρων βάσει δειγματοληψίας.
- IAF MD 2:2023 Μεταφορά διαπιστευμένης πιστοποίησης συστημάτων διαχείρισης.
- IAF MD 11:2023 Επιθεωρήσεις ολοκληρωμένων συστημάτων διαχείρισης.
- IAF MD 26:2022 Μεταβατικές Απαιτήσεις από το ISO/IEC 27001:2023 στο ISO/IEC 27001:2022.
- IAF ID Ενημερωτικά έγγραφα της Διεθνούς Διαπίστευσης:
- IAF ID 14:2023 Οδηγίες για τον προσδιορισμό του χρόνου επιθεώρησης ολοκληρωμένων συστημάτων διαχείρισης πολλών τοποθεσιών.
- ΚΟ ΕΣΥΔ ISMS για τη διαπιστευση φορεων πιστοποιησης συστηματων διαχειρισης της ασφάλειας πληροφοριών

1.3 Ορισμοί

Η ορολογία που χρησιμοποιείται στον παρόντα κανονισμό είναι σύμφωνη με το πρότυπο EN ISO/IEC 17000:2020, το ΕΛΟΤ EN ISO 9000:2015 Συστήματα Διαχείρισης Ποιότητας - Θεμελιώδεις Αρχές και Λεξιλόγιο, το EN ISO/IEC 27001:2022 Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών — Απαιτήσεις και οδηγίες

εφαρμογή και το ISO/IEC 27000:2018 Τεχνολογία Πληροφοριών – Τεχνικές Ασφάλειας – Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών – Επισκόπηση και λεξιλόγιο.

- ***πελάτης:*** οργανισμός ή πρόσωπο που λαμβάνει ένα προϊόν ή μία υπηρεσία**.**
- ***ικανοποίηση πελάτη:*** Η αντίληψη του πελάτη του βαθμού στον οποίο εκπληρώνονται οι απαιτήσεις των πελατών**.**
- ***προσωπικό:*** Προσωπικό εντός του οργανισμού
- ***εργαζόμενος:*** πρόσωπο που εκτελεί εργασία ή δραστηριότητες που σχετίζονται με την εργασία και οι οποίες τελούν υπό τον έλεγχο του οργανισμού
- ***υπηρεσία:*** αποτέλεσμα τουλάχιστον μία δραστηριότητας που εκτελείται αναγκαστικά στη διεπαφή μεταξύ του προμηθευτή και πελάτη, που είναι γενικά άυλη.
- ***περιουσιακό στοιχείο:*** Κάθε στοιχείο που έχει αξία για τον οργανισμό. Υπάρχουν πολλοί τύποι περιουσιακών στοιχείων, π.χ. δεδομένα, υλικό, λογισμικό, πάροχοι υπηρεσιών, προσωπικό και φυσικές τοποθεσίες
- ***επίθεση:*** Εσκεμμένη μορφή κινδύνου, π.χ. μια ανεπιθύμητη ή αδικαιολόγητη πράξη με σκοπό την απόκτηση πλεονεκτημάτων ή την πρόκληση βλάβης σε τρίτους μέσω της ανάληψης ενεργειών σε ένα σύνολο περιουσιακών στοιχείων.
- ***διαθεσιμότητα:*** Η δυνατότητα να είναι κάτι προσβάσιμο και χρησιμοποιήσιμο από μια εξουσιοδοτημένη οντότητα ανά πάσα στιγμή.
- ***έλεγχος:*** Μέτρο μείωσης κινδύνου. Έλεγχοι είναι οι διαδικασίες, οι πολιτικές, οι συσκευές, οι ενέργειες ή άλλες πράξεις που μπορούν να μειώσουν αποτελεσματικά τον κίνδυνο.
- ***ακεραιότητα:*** Η ακρίβεια και η πληρότητα.
- ***ασφάλεια πληροφοριών:*** Η διατήρηση της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των πληροφοριών.
- ***κίνδυνος (ασφάλειας πληροφοριών):*** Ένας κίνδυνος ασφάλειας πληροφοριών υφίσταται όπου είναι πιθανό ότι οι απειλές θα εκμεταλλευτούν τα τρωτά σημεία ενός περιουσιακού στοιχείου πληροφοριών και θα βλάψουν έναν οργανισμό.
- ***αξιολόγηση κινδύνου (ασφάλεια πληροφοριών):*** Η γενικότερη διαδικασία του προσδιορισμού και της ανάλυσης ενός κινδύνου.
- ***αντιμετώπιση κινδύνου (ασφάλεια πληροφοριών):*** Η διαδικασία της μείωσης κινδύνου. Συμπεριλαμβάνει συνήθως την αποφυγή, την ελάττωση, τον μετριασμό ή την αποδοχή του κινδύνου.
- ***απειλή:*** Πιθανή γενεσιουργός αιτία ανεπιθύμητου συμβάντος, το οποίο μπορεί να έχει βλαβερό αποτέλεσμα.
- ***ευπάθεια:*** Αδυναμία ενός περιουσιακού στοιχείου ή ελέγχου, η οποία μπορεί να αξιοποιηθεί από μία ή περισσότερες απειλές.
- ***απαίτηση:*** Ανάγκη ή προσδοκία που είναι δηλωμένη, γενικά σιωπηρά ή υποχρεωτικά**.**
- ***νομοθετικές και άλλες απαιτήσεις:*** οι νομικές απαιτήσεις που πρέπει να πληροί ένας οργανισμός και άλλες απαιτήσεις τις οποίες ένας οργανισμός έχει ή επιλέγει να συμμορφωθεί
- ***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.)

- ***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
- ***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
- ***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 σχεδίασμά 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

1.4 Συντομογραφίες

- ***ΥΔΠ:*** Υπεύθυνος Διαχείρισης Συστημάτων
- ***ΣΔΑΠ:*** Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών
- ***ΦΠ:*** Φορέας Πιστοποίησης
- ***ΓΚΠ***: Γενικός Κανονισμός Πιστοποίησης
- ***ΠΣΔ***: Πιστοποίηση Συστημάτων Διαχείρισης
- ***ISO:*** Διεθνής Οργανισμός Τυποποίησης (International Organization for Standardization)

2. Οδηγός και ερμηνεία του ISO/IEC 27001:2022

Εκτός εάν αναφέρεται διαφορετικά, οι αριθμοί των κεφαλαίων στο παρόν κεφάλαιο παραπέμπουν στα κεφάλαια του προτύπου ISO/IEC 27001:2022.

ΤΙΤΛΟΣ ΤΟΥ ΠΑΡΑΓΡΑΦΟΥ ΤΟΥ ΠΡΟΤΥΠΟΥ - ΟΔΗΓΟΣ ΚΑΙ ΕΡΜΗΝΕΙΑ

Γενικά

Σε διάφορα μέρη του συστήματος χρησιμοποιείται η φράση "για την καθιέρωση, την εφαρμογή και τη διατήρηση μιας διαδικασίας". Εάν απαιτείται διαδικασία, αυτό σημαίνει ότι ο οργανισμός πρέπει να καθορίσει πώς, από ποιον και πότε θα εκτελεστεί η εν λόγω δραστηριότητα. Οι διαδικασίες δεν χρειάζεται να καθορίζονται γραπτώς. Για τις 6.1, 8.1 και 8.2, πρέπει να υπάρχει τεκμηρίωση που να αποδεικνύει ότι οι διαδικασίες εκτελούνται σύμφωνα με τον προγραμματισμό, γεγονός που μπορεί να αποτελέσει τεκμηρίωση της ίδιας της διαδικασίας. Οι οργανισμοί μπορεί να επιλέξουν να τεκμηριώνουν τις διαδικασίες επειδή αυτό προσφέρει στον οργανισμό ένα πλεονέκτημα, για παράδειγμα όταν η διαδικασία ανατίθεται ή εκτελείται ξανά. Μια τεκμηριωμένη διαδικασία μπορεί επίσης να απλοποιήσει τόσο τις εσωτερικές όσο και τις εξωτερικές επιθεωρήσεις. Το παράρτημα 1 του παρόντος περιέχει μια επισκόπηση των απαιτούμενων εγγράφων και αρχείων, καθώς και των εγγράφων και αρχείων που συνιστά η EPCERT.

Για την αξιολόγηση των διαδικασιών, το πρότυπο ζητά σε διάφορα σημεία να τηρούνται έγγραφα ή αρχεία και να αποδεικνύεται ότι το σύστημα λειτουργεί αποτελεσματικά.

Παράγραφος 4: Πλαίσιο του οργανισμού

Αυτή η παράγραφος έχει την έννοια της προληπτικής δράσης και καθορίζει το πλαίσιο για το ΣΔΑΠ. Επιτυγχάνει αυτούς τους στόχους συγκεντρώνοντας τα σχετικά εξωτερικά και εσωτερικά ζητήματα, δηλαδή εκείνα που επηρεάζουν την ικανότητα του οργανισμού να επιτύχει το επιδιωκόμενο αποτέλεσμα του ΣΔΑΠ. Ο οργανισμός οφείλει να αξιολογεί αν η κλιματική αλλαγή αποτελεί σημαντικό παράγοντα για την επίτευξη των στόχων του. Πρέπει να αναγνωρίσει και να καθορίσει τα ενδιαφερόμενα μέρη που σχετίζονται με το σύστημα διαχείρισης ασφάλειας πληροφοριών, καθώς αυτά ενδέχεται να έχουν απαιτήσεις που αφορούν την κλιματική αλλαγή. Οι απαιτήσεις των ενδιαφερομένων μερών θα πρέπει να ληφθούν υπόψη κατά τον καθορισμό του πεδίου εφαρμογής του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ).Θα πρέπει να σημειωθεί ότι ο όρος "ζήτημα" καλύπτει όχι μόνο προβλήματα, τα οποία θα αποτελούσαν αντικείμενο προληπτικής δράσης, αλλά και σημαντικά θέματα που πρέπει να αντιμετωπίσει το ΣΔΑΠ, όπως οι τυχόν στόχοι διασφάλισης της αγοράς και διακυβέρνησης που μπορεί να θέσει ο οργανισμός για το ΣΔΑΠ.

Σημειώνεται ότι ο όρος "απαίτηση" είναι "ανάγκη ή προσδοκία που δηλώνεται, εν γένει υπονοείται ή είναι υποχρεωτική". Σε συνδυασμό με την παράγραφο 4.2, αυτό από μόνο του μπορεί να θεωρηθεί ως απαίτηση, καθώς, αυστηρά μιλώντας, ένα ΣΔΑΠ που δεν συμμορφώνεται με τις γενικά αποδεκτές προσδοκίες του κοινού θα μπορούσε πλέον να θεωρηθεί ότι δεν συμμορφώνεται με το πρότυπο. Πρέπει να προσδιορίζονται οι "σχετικές" απαιτήσεις των ενδιαφερομένων μερών και να καθορίζεται ποιες θα αντιμετωπιστούν μέσω του ΣΔΑΠ.

Η τελευταία απαίτηση (παράγραφος 4.4) είναι η καθιέρωση, η εφαρμογή, η διατήρηση και η συνεχής

βελτίωση του ΣΔΑΠ, συμπεριλαμβανομένων των απαιτούμενων διαδικασιών και της αλληλεπίδρασής τους σύμφωνα με τις απαιτήσεις του προτύπου.

Παράγραφος 5: Ηγεσία

Η παράγραφος αυτή θέτει απαιτήσεις για την "ανώτατη διοίκηση", η οποία είναι το πρόσωπο ή η ομάδα ατόμων που διευθύνει και ελέγχει τον οργανισμό στο υψηλότερο επίπεδο. Σημειώνεται ότι εάν ο οργανισμός που αποτελεί αντικείμενο του ΣΔΑΠ είναι μέρος ενός μεγαλύτερου οργανισμού, τότε ο όρος "ανώτατη διοίκηση" αναφέρεται στον μικρότερο οργανισμό. Ο σκοπός αυτών των απαιτήσεων είναι να επιδείξουν ηγεσία και δέσμευση με ηγεσία από την κορυφή. Ιδιαίτερη ευθύνη της ανώτατης διοίκησης είναι η καθιέρωση της πολιτικής για την ασφάλεια των πληροφοριών και το πρότυπο ορίζει τα χαρακτηριστικά και τις ιδιότητες που πρέπει να περιλαμβάνει η πολιτική αυτή. Τέλος, η παράγραφος θέτει απαιτήσεις στην ανώτατη διοίκηση για την ανάθεση αρμοδιοτήτων και εξουσιών σχετικών με την ασφάλεια των πληροφοριών, υπογραμμίζοντας συγκεκριμένους ρόλους που αφορούν τη συμμόρφωση του ΣΔΑΠ προς το ISO/IEC 27001 και την υποβολή εκθέσεων σχετικά με την απόδοση του ΣΔΑΠ.

Παράγραφος 6: Σχεδιασμός

Η παράγραφος 6.1.1 (Γενικά) συνεργάζεται με τις 4.1 και 4.2 για να ολοκληρώσει το νέο τρόπο αντιμετώπισης των προληπτικών ενεργειών. Το πρώτο μέρος (δηλαδή μέχρι και το σημείο 6.1.2) αφορά την εκτίμηση κινδύνου, ενώ το σημείο 6.1.3 αφορά την αντιμετώπιση του κινδύνου. Καθώς η αξιολόγηση και η αντιμετώπιση των κινδύνων ασφάλειας πληροφοριών εξετάζεται στις παραγράφους 6.1.2 και 6.1.3, οι οργανισμοί μπορούν να χρησιμοποιήσουν τη συγκεκριμένη παράγραφο για να εξετάσουν τους κινδύνους και τις ευκαιρίες του ΣΔΑΠ.

Η παράγραφος 6.1.2 (Αξιολόγηση κινδύνου ασφάλειας πληροφοριών) αφορά ειδικά την αξιολόγηση του κινδύνου ασφάλειας πληροφοριών. Σε ευθυγράμμιση με τις αρχές και την καθοδήγηση του ISO 31000, η παράγραφος αυτή καταργεί τον προσδιορισμό των περιουσιακών στοιχείων, των απειλών και των τρωτών σημείων ως προαπαιτούμενο για τον προσδιορισμό των κινδύνων. Αυτό διευρύνει την επιλογή των μεθόδων εκτίμησης κινδύνου που μπορεί να χρησιμοποιήσει ένας οργανισμός και εξακολουθεί να συμμορφώνεται με το πρότυπο. Η παράγραφος αναφέρεται επίσης σε "κριτήρια αποδοχής της αξιολόγησης κινδύνου", τα οποία επιτρέπουν κριτήρια εκτός από ένα μόνο επίπεδο κινδύνου. Τα κριτήρια αποδοχής κινδύνου μπορούν πλέον να εκφράζονται με άλλους όρους εκτός από τα επίπεδα, για παράδειγμα, τα είδη ελέγχου που χρησιμοποιούνται για την αντιμετώπιση του κινδύνου. Η παράγραφος αναφέρεται σε "ιδιοκτήτες κινδύνων" και όχι σε "ιδιοκτήτες περιουσιακών στοιχείων" και αργότερα απαιτεί την έγκρισή τους για το σχέδιο αντιμετώπισης κινδύνων και τους υπολειπόμενους κινδύνους. Απαιτεί επίσης από τους οργανισμούς να αξιολογούν τις συνέπειες, την πιθανότητα και τα επίπεδα κινδύνου.
Η παράγραφος 6.1.3 (Αντιμετώπιση του κινδύνου ασφάλειας πληροφοριών) αφορά την αντιμετώπιση του κινδύνου ασφάλειας πληροφοριών. Αναφέρεται στον "προσδιορισμό" των απαραίτητων ελέγχων και όχι στην επιλογή ελέγχων από το παράρτημα Α. Ωστόσο, το πρότυπο διατηρεί τη χρήση του παραρτήματος Α ως διασταύρωση για να διασφαλιστεί ότι δεν έχει παραλειφθεί κανένας απαραίτητος έλεγχος, και οι οργανισμοί εξακολουθούν να υποχρεούνται να συντάσσουν δήλωση εφαρμογής (Statement of Applicability - SOA). Η διαμόρφωση και η έγκριση του σχεδίου αντιμετώπισης των κινδύνων αποτελεί μέρος αυτής της παραγράφου.

Η παράγραφος 6.2 (Στόχοι ασφάλειας πληροφοριών και σχεδιασμός για την επίτευξή τους) αφορά τους στόχους ασφάλειας πληροφοριών. Χρησιμοποιεί τη φράση "σχετικές λειτουργίες και επίπεδα", όπου εδώ, ο όρος "λειτουργία" αναφέρεται στις λειτουργίες του οργανισμού και ο όρος "επίπεδο", τα επίπεδα διοίκησης, εκ των οποίων η "ανώτατη διοίκηση" είναι το υψηλότερο. Η παράγραφος ορίζει τις ιδιότητες που πρέπει να διαθέτουν οι στόχοι ασφάλειας πληροφοριών ενός οργανισμού. Οι στόχοι της ασφάλειας των πληροφοριών πρέπει να παρακολουθούνται και να καθίστανται "διαθέσιμοι ως τεκμηριωμένες πληροφορίες".

Η παράγραφος 6.3 (Σχεδιασμός αλλαγών) αφορά τον τρόπο με τον οποίο διασφαλίζεται ότι οι αλλαγές στο ΣΔΑΠ γίνονται με προγραμματισμένο τρόπο. Δεδομένου ότι δεν καθορίζει διαδικασίες που πρέπει να περιλαμβάνονται, θα πρέπει να καθορίζεται το πώς μπορεί να αποδειχθεί ότι οι αλλαγές στο ΣΔΑΠ έχουν πράγματι προγραμματιστεί.

Παράγραφος 7: Υποστήριξη

Αυτή η παράγραφος αρχίζει με την απαίτηση ότι οι οργανισμοί πρέπει να καθορίζουν και να παρέχουν τους απαραίτητους πόρους για την καθιέρωση, την εφαρμογή, τη διατήρηση και τη συνεχή βελτίωση του ΣΔΑΠ. Με απλά λόγια, πρόκειται για μια πολύ ισχυρή απαίτηση που καλύπτει όλες τις ανάγκες σε πόρους του ΣΔΑΠ. Η παράγραφος προσδιορίζει τι απαιτείται για την καθιέρωση, την εφαρμογή, τη διατήρηση και τη συνεχή βελτίωση ενός αποτελεσματικού ΣΔΑΠ, μεταξύ άλλων:

- Απαιτήσεις πόρων
- Επάρκεια όσον αφορά την εκπαίδευση, την κατάρτιση και την εμπειρία των ατόμων που εμπλέκονται στις επιδόσεις της ασφάλειας των πληροφοριών
- Ενημέρωση για την πολιτική ασφάλειας των πληροφοριών, την απόδοση της ασφάλειας και τις επιπτώσεις της μη συμμόρφωσης με τις απαιτήσεις του ΣΔΑΠ.
- επικοινωνία για το τι, πότε, με ποιον, πώς με τα ενδιαφερόμενα μέρη.

Τέλος, υπάρχουν απαιτήσεις για "τεκμηριωμένες πληροφορίες". Το πρότυπο αναφέρεται σε "τεκμηριωμένες πληροφορίες" και όχι σε "έγγραφα και αρχεία" και απαιτεί τη διατήρησή τους ως αποδεικτικά στοιχεία της επάρκειας. Οι απαιτήσεις αυτές αφορούν τη δημιουργία και την επικαιροποίηση των τεκμηριωμένων πληροφοριών και τον έλεγχό τους. Δεν υπάρχει πλέον κατάλογος εγγράφων που πρέπει να προσκομιστεί ή συγκεκριμένα ονόματα που πρέπει να δοθούν. Η νέα αναθεώρηση δίνει έμφαση στο περιεχόμενο και όχι στο όνομα.

Παράγραφος 8: Επιχείρηση

Ο οργανισμός πρέπει να σχεδιάζει, να εφαρμόζει και να ελέγχει τις διαδικασίες που απαιτούνται για την ικανοποίηση των απαιτήσεων ασφάλειας πληροφοριών και για την υλοποίηση των ενεργειών που καθορίζονται στο πρότυπο. Ο οργανισμός πρέπει να καθορίζει κριτήρια για τις διαδικασίες για την υλοποίηση των ενεργειών που προσδιορίζονται στην παράγραφο 6 και να ελέγχει τις εν λόγω διαδικασίες σύμφωνα με τα κριτήρια. Απαιτείται να ελέγχουν τις "εξωτερικά παρεχόμενες διαδικασίες, προϊόντα ή υπηρεσίες" που σχετίζονται με το ΣΔΑΠ. Ο οργανισμός πρέπει να διενεργεί αξιολογήσεις κινδύνου ασφάλειας πληροφοριών σε προγραμματισμένα χρονικά διαστήματα και πρέπει επίσης να εφαρμόζει το σχέδιο αντιμετώπισης του κινδύνου ασφάλειας πληροφοριών. Η παρούσα παράγραφος αφορά την εκτέλεση των σχεδίων και των διαδικασιών που αποτελούν αντικείμενο των προηγούμενων παραγράφων. Οι οργανισμοί πρέπει να

σχεδιάζουν και να ελέγχουν τις διαδικασίες που απαιτούνται για την εκπλήρωση των απαιτήσεων ασφάλειας των πληροφοριών τους, συμπεριλαμβανομένων:

- τήρηση εγγράφων
- διαχείριση της αλλαγής
- αντιμετώπιση ανεπιθύμητων συμβάντων
- την επιθεώρηση τυχόν εξωτερικών διεργασιών

Ο σχεδιασμός και ο έλεγχος της λειτουργίας επιβάλλουν επίσης τη διενέργεια αξιολογήσεων κινδύνου για την ασφάλεια των πληροφοριών σε προγραμματισμένα χρονικά διαστήματα και την εφαρμογή ενός σχεδίου αντιμετώπισης του κινδύνου για την ασφάλεια των πληροφοριών.

Η παράγραφος 8.1 αφορά την εκτέλεση των ενεργειών που προσδιορίζονται στην παράγραφο 6.1, την επίτευξη των στόχων ασφάλειας πληροφοριών και τις εξωτερικές διαδικασίες.

Η παράγραφος 8.2 αφορά τη διενέργεια αξιολογήσεων κινδύνου ασφάλειας πληροφοριών σε προγραμματισμένα διαστήματα ή όταν προτείνονται ή συμβαίνουν σημαντικές αλλαγές- και

Η παράγραφος 8.3 αφορά την εφαρμογή του σχεδίου αντιμετώπισης κινδύνων.

Παράγραφος 9: Αξιολόγηση επιδόσεων

Ο οργανισμός αξιολογεί την απόδοση της ασφάλειας των πληροφοριών και την αποτελεσματικότητα του συστήματος διαχείρισης της ασφάλειας των πληροφοριών. Ο οργανισμός διεξάγει εσωτερικούς ελέγχους σε προγραμματισμένα χρονικά διαστήματα για να παρέχει πληροφορίες σχετικά με το κατά πόσον το σύστημα διαχείρισης της ασφάλειας των πληροφοριών συμμορφώνεται με τις απαιτήσεις του ίδιου του οργανισμού και με τις απαιτήσεις του διεθνούς προτύπου.
Η παράγραφος 9.1 (Παρακολούθηση, μέτρηση, ανάλυση και αξιολόγηση) αναφέρει τους γενικούς στόχους. Ως γενική σύσταση, θα πρέπει να καθορίζονται ποιες πληροφορίες χρειάζονται ώστε να αξιολογηθούν οι επιδόσεις της ασφάλειας πληροφοριών και η αποτελεσματικότητα του ΣΔΑΠ. Από αυτή την "ανάγκη πληροφόρησης", καθορίζεται τι πρέπει να μετρηθεί και να παρακολουθηθεί, πότε, ποιος και πώς.
Ένας οργανισμός μπορεί να έχει διάφορες ανάγκες πληροφόρησης και οι ανάγκες αυτές μπορεί να αλλάζουν με την πάροδο του χρόνου. Για παράδειγμα, όταν ένα ΣΔΑΠ είναι σχετικά νέο, μπορεί να είναι σημαντικό να παρακολουθείται απλώς η συμμετοχή σε εκδηλώσεις ευαισθητοποίησης για την ασφάλεια των πληροφοριών. Μόλις επιτευχθεί το επιδιωκόμενο ποσοστό, ο οργανισμός μπορεί να εξετάσει περισσότερο την ποιότητα της εκδήλωσης ευαισθητοποίησης. Αυτό μπορεί να γίνει με τον καθορισμό συγκεκριμένων στόχων ευαισθητοποίησης και τον προσδιορισμό του βαθμού στον οποίο οι συμμετέχοντες έχουν κατανοήσει αυτά που έμαθαν. Αργότερα, η ανάγκη πληροφόρησης μπορεί να επεκταθεί για να προσδιοριστεί ο αντίκτυπος που έχει αυτό το επίπεδο ευαισθητοποίησης στην ασφάλεια των πληροφοριών για τον οργανισμό. Θα πρέπει να επιλεγεί μια συγκρίσιμη και αναπαραγώγιμη μέθοδος παρακολούθησης, μέτρησης, ανάλυσης και αξιολόγησης για να δώσει ένα έγκυρο αποτέλεσμα.

Οι εσωτερικοί έλεγχοι και η ανασκόπηση από τη διοίκηση εξακολουθούν να αποτελούν βασικές μεθόδους ανασκόπησης της απόδοσης του ΣΔΑΠ και εργαλεία για τη συνεχή βελτίωσή του. Οι απαιτήσεις περιλαμβάνουν τη διενέργεια εσωτερικών ελέγχων σε προγραμματισμένα διαστήματα, τον σχεδιασμό, την

καθιέρωση, την εφαρμογή και τη διατήρηση προγράμματος(ων) ελέγχου(ων), την επιλογή επιθεωρητών και τη διενέργεια ελέγχων που διασφαλίζουν την αντικειμενικότητα και την αμεροληψία της ελεγκτικής διαδικασίας.
Στην παράγραφο 9.3 (Ανασκόπηση από τη διοίκηση), αντί να προσδιορίζει ακριβείς εισροές και εκροές, η εν λόγω παράγραφος θέτει τώρα απαιτήσεις σχετικά με τα θέματα που πρέπει να εξεταστούν κατά την ανασκόπηση. Η απαίτηση για την πραγματοποίηση των ανασκοπήσεων σε προγραμματισμένα διαστήματα παραμένει, αλλά η απαίτηση για την πραγματοποίηση των ανασκοπήσεων τουλάχιστον μία φορά ετησίως έχει καταργηθεί.

Παράγραφος 10: Βελτίωση

Λόγω του νέου τρόπου χειρισμού των προληπτικών ενεργειών, δεν υπάρχουν απαιτήσεις προληπτικών ενεργειών στην παρούσα παράγραφο. Ωστόσο, υπάρχουν ορισμένες νέες απαιτήσεις διορθωτικών ενεργειών. Η πρώτη είναι η αντίδραση στη μη συμμόρφωση και η ανάληψη δράσης, ανάλογα με την περίπτωση, για την επιθεώρηση και τη διόρθωση της μη συμμόρφωσης και την αντιμετώπιση των συνεπειών. Ο δεύτερος είναι να προσδιοριστεί αν υπάρχουν ή θα μπορούσαν ενδεχομένως να εμφανιστούν παρόμοιες μη συμμορφώσεις. Αν και η έννοια της προληπτικής δράσης έχει εξελιχθεί, εξακολουθεί να υπάρχει ανάγκη να εξετάζεται η πιθανή μη συμμόρφωση, έστω και ως συνέπεια μιας πραγματικής μη συμμόρφωσης. Υπάρχει επίσης μια νέα απαίτηση να διασφαλίζεται ότι οι διορθωτικές ενέργειες είναι κατάλληλες για τις επιπτώσεις της μη συμμόρφωσης που διαπιστώθηκε. Η απαίτηση για συνεχή βελτίωση έχει επεκταθεί ώστε να καλύπτει την καταλληλότητα και την επάρκεια του ΣΔΑΠ καθώς και την αποτελεσματικότητά του, αλλά δεν διευκρινίζει πλέον πώς ένας οργανισμός το επιτυγχάνει αυτό.

Παράρτημα Α Αναφορά ελέγχων ασφάλειας πληροφοριών

Οι έλεγχοι ασφάλειας πληροφοριών μπορούν να κατηγοριοποιηθούν σε 4 ομάδες ή θέματα. Αυτά είναι:

1. ανθρώπους, αν αφορούν μεμονωμένους ανθρώπους,
2. φυσικές, εάν αφορούν φυσικά αντικείμενα,
3. τεχνολογικές, εάν αφορούν την τεχνολογία,
4. διαφορετικά κατηγοριοποιούνται ως οργανωτικά.

Οι έλεγχοι ασφαλείας αναλύονται αναλυτικότερα στο παράρτημα 2 του παρόντος.

3. ΟΡΓΑΝΩΣΗ, ΥΠΕΥΘΥΝΟΤΗΤΕΣ ΚΑΙ ΑΡΜΟΔΙΟΤΗΤΕΣ

3.1 Αρχές και γενικές απαιτήσεις (κεφάλαια 4 και 5 του ISO 17021-1)

3.1.1 Αμεροληψία (ISO 17021-1 παράγραφοι 4.2, 5.2 και 5.3)

Το προσωπικό δεν μπορεί να έχει εμπλακεί ως σύμβουλος για τον οργανισμό που πρόκειται να πιστοποιηθεί είτε για το σύστημα διαχείρισης ασφάλειας πληροφοριών είτε για άλλα συστήματα διαχείρισης.
Η διενέργεια "προ-επιθεώρησης" δεν θεωρείται συμβουλευτική εφόσον περιλαμβάνει μόνο την αξιολόγηση του εφαρμοζόμενου συστήματος και δεν παρέχονται συμβουλές για τη διόρθωση ενδεχόμενων παραβάσεων ή μη συμμόρφωσης.
Περισσότερα αναφορικά με τη διασφάλιση της αμεροληψίας ορίζονται στον ΓΚΠ της EPCERT.

3.1.2 Ανταπόκριση σε παράπονα (ISO 17021-1 παράγραφος 9.6.7)

Η EPCERT πρέπει να ενημερώνει το ΕΣΥΔ το συντομότερο δυνατό, αλλά σε κάθε περίπτωση εντός δύο εβδομάδων, για τις καταγγελίες που υποβάλλονται από τρίτους (όπως η αρμόδια αρχή) στην EPCERT σχετικά με πιστοποιητικό που έχει εκδώσει (όχι για ενστάσεις από οργανισμούς που έχουν πιστοποιηθεί από την EPCERT). Η EPCERT θα δημοσιεύει τον αριθμό και τη φύση των καταγγελιών στην ετήσια έκθεσή της.
Περισσότερα αναφορικά με τη διαχείριση των παραπόνων ορίζονται στον ΓΚΠ της EPCERT.

3.2 Οργανωτική δομή (κεφάλαιο 6 του ISO 17021-1)

Υπεύθυνος εφαρμογής του παρόντος ειδικού κανονισμού είναι ο Υπεύθυνος Διαχείρισης Ποιότητας του Φορέα Πιστοποίησης σε συνεργασία με τους Αναπληρωτές του. Ο ΥΔΠ είναι αρμόδιος για την έκδοση και αναθεώρηση του παρόντος με την έγκριση της Ανώτατης Διοίκησης.

3.3 Προσωπικό εντός της EPCERT (κεφάλαιο 7 του ISO 17021-1)

Το πρότυπο ISO/IEC 27006:2015/Amd 1:2020 Τεχνολογία πληροφοριών - Τεχνικές ασφάλειας - Απαιτήσεις για Οργανισμούς που διενεργούν επιθεωρήσεις σε Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών – Amd 1 προσδιορίζει τις απαιτήσεις επάρκειας του προσωπικού που εμπλέκεται στη διαδικασία της πιστοποίησης, όπως ορίζει το διεθνές πρότυπο ΕΛΟΤ ΕΝ ISO/IEC 17021-1:2015. Ο Φορέας Πιστοποίησης εφαρμόζει ένα σύστημα για τον καθορισμό της διαχείρισης των ικανοτήτων του εμπλεκόμενου προσωπικού, όπως αυτό περιγράφεται στη διαδικασία Δ03 Διαχείριση Προσωπικού.

Ειδικά, το προσωπικό που εμπλέκεται στη διαδικασία πιστοποίησης ενός οργανισμού κατά ISO/IEC 27001:2022 πρέπει να πληροί τις απαιτήσεις επάρκειας όπως αυτές προσδιορίζονται στο παράρτημα Α, πίνακας Α.1 του προτύπου ISO/IEC 27006:2015 συμπεριλαμβανομένων τυχόν διευκρινίσεων του Amd 1:2020 που εφαρμόζονται, όπως αυτός ισχύει.

Ο κατάλογος νομοθεσίας, που τηρεί επικαιροποιημένο ο ΥΔΠ, ορίζει τις γνώσεις της νομοθεσίας και των κανονισμών για την πιστοποίηση που είναι απαραίτητες για τις διάφορες θέσεις πιστοποίησης (βλέπε παράρτημα νομοθεσίας).

3.4 Επιθεωρητές/ Εμπειρογνώμονες ISO/IEC 27001:2022 (κεφάλαιο 7 του ISO 17021-1)

Το Μητρώο Επιθεωρητών/Εμπειρογνωμόνων Πιστοποίησης ΣΔ του Φορέα αποτελείται από μέλη ικανά να ανταποκριθούν στις απαιτήσεις της επιθεώρησης ενός ΣΔΑΠ.

Αρχική αξιολόγηση επιθεωρητών

Οι επιθεωρητές των συστημάτων διαχείρισης ασφάλειας πληροφοριών οφείλουν να διαθέτουν τις ακόλουθες γνώσεις και εμπειρία:

- Ειδικά χαρακτηριστικά του ΣΔΑΠ,
- Ενταγμένος επιθεωρητής σε άλλον φορέα EA-MLA αν είναι δυνατόν,
- Συμμετοχή σε εκπαιδευτικά προγράμματα ΣΔΑΠ και λήψη σχετικών προσωπικών στοιχείων ταυτοποίησης,
- Τρέχοντα αρχεία επαγγελματικής κατάρτισης,
- Συμμετοχή σε επιθεωρήσεις ΣΔΑΠ.

Εκτός των παραπάνω, διασφαλίζεται ότι τα κριτήρια επιλογής επιθεωρητών εγγυώνται ότι κάθε επιθεωρητής παρέχει τα ακόλουθα:

a) Πτυχίο τριτοβάθμιας εκπαίδευσης,
b) Πλήρης απασχόληση, τουλάχιστον τέσσερα έτη εργασιακής εμπειρίας στον τομέα της τεχνολογίας των πληροφοριών- για τουλάχιστον δύο έτη πρέπει να υπάρχει ρόλος ή λειτουργία σχετική με την ασφάλεια των πληροφοριών,
c) Επιτυχής ολοκλήρωση τουλάχιστον πενθήμερης κατάρτισης που καλύπτει το πεδίο εφαρμογής των ελέγχων του ΣΔΑΠ και τη διενέργεια των επιθεωρήσεων. Το εκπαιδευτικό πρόγραμμα για την οργάνωση και διενέργεια επιθεωρήσεων μπορεί να καλυφθεί και από πενθήμερο σεμινάριο επιθεωρητών άλλου προτύπου.
d) Πριν εργαστεί ως επιθεωρητής που διενεργεί επιθεωρήσεις ΣΔΑΠ, θα πρέπει να αποκτήσει εμπειρία στην επιθεώρηση ΣΔΑΠ. Η εμπειρία αυτή θα αποκτηθεί ως εκπαιδευόμενος επιθεωρητής, υπό την επίβλεψη επικεφαλής επιθεωρητή ΣΔΑΠ (βλέπε ISO/IEC 17021-1:2015, 9.2.2.1.4) σε τουλάχιστον μια επιθεώρηση αρχικής πιστοποίησης ΣΔΑΠ (στάδιο 1 και στάδιο 2) ή επαναπιστοποίησης και τουλάχιστον μια επιθεώρηση επιτήρησης. Η εμπειρία αυτή θα αποκτηθεί σε τουλάχιστον 10 ημέρες επιτόπιας επιθεώρησης του ΣΔΑΠ και πρέπει να έχει πραγματοποιηθεί τα τελευταία 5 έτη. Η συμμετοχή περιλαμβάνει ανασκόπηση της τεκμηρίωσης και αξιολόγηση των κινδύνων, αξιολόγηση της εφαρμογής και υποβολή εκθέσεων επιθεώρησης.
e) Σχετική και επικαιροποιημένη εμπειρία τα τελευταία πέντε έτη (τουλάχιστον 1 έτος εργασιακή εμπειρία στο IT ή στο IS, ή ανάπτυξη/ επιθεώρηση συστημάτων δύο ΣΔΑΠ ή ISO 9001 στο EA33 κ.ά.). Συνδυασμός αυτός θα εκτιμηθεί ανά περίπτωση.

f) Διατήρηση των τρεχουσών γνώσεων και δεξιοτήτων με συνεχή επαγγελματική ανάπτυξη. Αποδεικνύεται με την παρακολούθηση τουλάχιστον ενός επαγγελματικού σεμιναρίου σχετικό με το IT και το IS τα τελευταία δύο (2) έτη, ή την παρακολούθηση εκπαίδευσης/ ενημέρωσης από την EPCert σχετικά με τις εξελίξεις στα σχετικά πρότυπα και επιθεωρήσεις, ή την συμμετοχή στη συγγραφή συγγραμμάτων ή άρθρων σχετικών με το αντικείμενο τα τελευταία δύο (2) έτη, ή παρουσία ως εισηγητής σε σεμινάρια, ημερίδες, συνέδρια, κ.ά. σχετικά με το αντικείμενο τα τελευταία δύο (2) έτη.

g) Πρέπει να έχει την ικανότητα να επιθεωρεί ένα ΣΔΑΠ σύμφωνα με το πρότυπο ISO/IEC 27001.

Κατάταξη επιθεωρητών σε βαθμίδες:

Για τον ορισμό ενός επιθεωρητή με τη βαθμίδα του επικεφαλής λαμβάνονται υπόψη τα κάτωθι:

- Εμπειρία σε επιθεωρήσεις 3ου μέρους κατά την τελευταία τριετία:
    - τρεις (3) επιθεωρήσεις στη βαθμίδα του επικεφαλής επιθεωρητή για τη συμμόρφωση ΣΔΑΠ στην ισχύουσα έκδοση του προτύπου ISO/IEC 27001, ή στην προηγούμενη εφόσον υπήρξε κατάλληλη επιμόρφωση για τη μετάβαση στην ισχύουσα -θα πρέπει να έχει συμμετάσχει ενεργά σε όλα τα στάδια (αρχικό πεδίο εφαρμογής και προγραμματισμός, ανασκόπηση της τεκμηρίωσης και αξιολόγηση των κινδύνων, αξιολόγηση της εφαρμογής και υποβολή εκθέσεων επιθεώρησης)- για λογαριασμό διαπιστευμένου φορέα πιστοποίησης (από φορέα διαπίστευσης μέλος του MLA), **ή**
    - πέντε (5) επιθεωρήσεις στη βαθμίδα του επιθεωρητή για τη συμμόρφωση ΣΔΑΠ στην ισχύουσα έκδοση του προτύπου ISO/IEC 27001, ή στην προηγούμενη εφόσον υπήρξε κατάλληλη επιμόρφωση για τη μετάβαση στην ισχύουσα -θα πρέπει να έχει συμμετάσχει ενεργά σε όλα τα στάδια (αρχικό πεδίο εφαρμογής και προγραμματισμός, ανασκόπηση της τεκμηρίωσης και αξιολόγηση των κινδύνων, αξιολόγηση της εφαρμογής και υποβολή εκθέσεων επιθεώρησης)- για λογαριασμό διαπιστευμένου φορέα πιστοποίησης (από φορέα διαπίστευσης μέλος του MLA)

Για τον ορισμό ενός επιθεωρητή με τη βαθμίδα του επιθεωρητή (μέλος ομάδας επιθεώρησης) λαμβάνονται υπόψη τα κάτωθι:

- Εμπειρία σε επιθεωρήσεις 3ου μέρους κατά την τελευταία τριετία:
    - τρεις (3) επιθεωρήσεις στη βαθμίδα του επιθεωρητή για τη συμμόρφωση ΣΔΑΠ στην ισχύουσα έκδοση του προτύπου ISO/IEC 27001, ή στην προηγούμενη εφόσον υπήρξε κατάλληλη επιμόρφωση για τη μετάβαση στην ισχύουσα -θα πρέπει να έχει συμμετάσχει ενεργά σε όλα τα στάδια (ανασκόπηση της τεκμηρίωσης και αξιολόγηση των κινδύνων, αξιολόγηση της εφαρμογής και υποβολή εκθέσεων επιθεώρησης)- για λογαριασμό διαπιστευμένου φορέα πιστοποίησης (από φορέα διαπίστευσης μέλος του MLA), **ή**
    - κάλυψη του σημείου d ανωτέρω

Για την ολοκλήρωση της διαδικασίας κατάταξης σε βαθμίδες, απαιτείται επιπλέον επιτυχής επιτόπια αξιολόγηση του επιθεωρητή (επιτόπου επιθεώρηση στον πελάτη) με παρουσία αξιολογημένου επιθεωρητή του Φορέα ή του ΥΔΠ.

Ο Επικεφαλής Επιθεωρητής διεξάγει και τα δύο στάδια της επιθεώρησης κατά την αρχική πιστοποίηση ενός ΣΔΑΠ, την επιτήρηση της πιστοποίησης και την επαναπιστοποίηση. Για τη διασφάλιση της αμεροληψίας στη διαδικασία της επιθεώρησης και όπου είναι εφικτό, ορίζεται διαφορετικός Επικεφαλής Επιθεωρητής σε κάθε κύκλο πιστοποίησης του οργανισμού.

Στις υποχρεώσεις των Επιθεωρητών περιλαμβάνονται τα παρακάτω:

- Διαρκής ενημέρωση και επιμόρφωση σχετικά με τις μεταβολές στη νομοθεσία που διέπει την πιστοποίηση ΣΔΑΠ, αλλά και τη λειτουργία των υπό πιστοποίηση ΣΔΑΠ των οργανισμών
- Μη ύπαρξη σχέσης (οικονομικής, εμπορικής ή οποιουδήποτε άλλου είδους) με τον οργανισμό του οποίου το ΣΔΑΠ επιθεωρείται κατά τα δύο (2) τελευταία χρόνια

Ο Φορέας παρακολουθεί τις μεταβολές στη νομοθεσία που διέπει την πιστοποίηση και υποχρεούται να ανασκοπεί τα έγγραφα του ΣΔ που εφαρμόζει και να ενημερώνει ή και να εκπαιδεύει κατάλληλα τα μέλη του Μητρώου Επιθεωρητών.

Αρχική αξιολόγηση εμπειρογνωμόνων

Οι εμπειρογνώμονες των συστημάτων διαχείρισης ασφάλειας πληροφοριών πρέπει να πληρούν τα κριτήρια a, b και e ανωτέρω.

Στις υποχρεώσεις των Εμπειρογνωμόνων περιλαμβάνονται τα παρακάτω:

- Μη ύπαρξη σχέσης (οικονομικής, εμπορικής ή οποιουδήποτε άλλου είδους) με τον οργανισμό του οποίου το ΣΔΑΠ επιθεωρείται κατά τα δύο (2) τελευταία χρόνια

Δεν ορίζονται βαθμίδες στην κατηγορία των εμπειρογνωμόνων και δεν απαιτείται επιτόπια αξιολόγησή τους για την ένταξή τους στο μητρώο του Φορέα.

Πεδίο έγκρισης επιθεωρητών / εμπειρογνωμόνων

Δεν υπάρχει κατηγοριοποίηση των οργανισμών που επιθυμούν την πιστοποίηση σε πεδία.

Επέκταση / συρρίκνωση πεδίων έγκρισης

Δεν υπάρχει κατηγοριοποίηση των οργανισμών που επιθυμούν την πιστοποίηση σε πεδία.

Αξιολόγηση επίδοσης επιθεωρητών/ εμπειρογνωμόνων

Όλοι οι επιθεωρητές και οι εμπειρογνώμονες της EPCERT αξιολογούνται ανά 3ετία χρήσης από αξιολογημένο επιθεωρητή του Φορέα ή από τον ΥΔΠ και τα αποτελέσματα καταγράφονται στο έντυπο Ε-03.3 «Αξιολόγηση Προσωπικού». Ειδικά για τους επιθεωρητές, πραγματοποιείται και μια επιτόπια αξιολόγηση (επιτόπου επιθεώρηση στον πελάτη).

Σε περίπτωση που κάποιος εγγεγραμμένος στο Μητρώο επιθεωρητής δεν χρησιμοποιηθεί από το Φορέα για 2 συνεχόμενα έτη, διαγράφεται από το Μητρώο και για την επανένταξή του ακολουθείται εκ νέου η διαδικασία αρχικής αξιολόγησης.

Εκτός της ετήσιας αξιολόγησης -και εφόσον αυτό κριθεί απαραίτητο λόγω αποκλίσεων από το ΣΔ, πλήρωσης νέας θέσης ή λόγω αποχώρησης στελέχους- μπορούν να πραγματοποιηθούν και έκτακτες αξιολογήσεις.

3.5 Ανταλλαγή πληροφοριών μεταξύ EPCERT και τρίτων (ISO 17021-1 κεφάλαιο 8)

3.5.1 **Πληροφορίες που είναι προσβάσιμες από το κοινό (ISO 17021, παράγραφοι 8.1, 8.2, 8.3 και 8.4)**

Η EPCERT τηρεί και διαθέτει δημόσια όλες τις πληροφορίες που περιγράφουν τις διεργασίες επιθεώρησης και πιστοποίησης για τη χορήγηση, την άρνηση, τη διατήρηση, την ανανέωση, την αναστολή, την αποκατάσταση ή την απόσυρση της πιστοποίησης, την επέκταση ή συρρίκνωση του πεδίου πιστοποίησης, τα είδη των συστημάτων διαχείρισης και των σχημάτων πιστοποίησης τα οποία παρέχει, τη χρήση του ονόματός της και των λογοτύπων πιστοποίησης, τη διαδικασία διαχείρισης αιτημάτων αναφορικά με πληροφορίες, παράπονα ή ενστάσεις και την πολιτική αμεροληψίας που εφαρμόζει.

Η EPCERT παρέχει δημόσια ή κατόπιν σχετικού αιτήματος πληροφορίες σχετικά με τις γεωγραφικές περιοχές στις οποίες δραστηριοποιείται, την κατάσταση των πιστοποιητικών που έχει εκδώσει, καθώς και στοιχεία (επωνυμία, πρότυπο πιστοποίησης, πεδίο πιστοποίησης και γεωγραφική περιοχή) ενός συγκεκριμένου πιστοποιημένου πελάτη της.
Σε εξαιρετικές περιπτώσεις, η πρόσβαση σε συγκεκριμένες πληροφορίες μπορεί να είναι περιορισμένη έπειτα από αίτημα του πελάτη (π.χ. για λόγους ασφαλείας).

Η EPCERT παρέχει πληροφορίες προς τους πελάτες ή την αγορά, συμπεριλαμβανομένου του διαφημιστικού υλικού, οι οποίες είναι ακριβείς και όχι παραπλανητικές.

Η EPCERT πρέπει να αναγράφει στο πιστοποιητικό ότι αυτό εκδόθηκε βάσει του συστήματος διαπίστευσης του Ε.ΣΥ.Δ., εφόσον το πεδίο δραστηριότητας του οργανισμού εμπίπτει στο πεδίο διαπίστευσης του φορέα.

Οι πληροφορίες στο πιστοποιητικό πρέπει να καθιστούν σαφές στους δυνητικούς χρήστες ποιος οργανισμός είναι πιστοποιημένος για ποιες δραστηριότητες και δεν πρέπει να είναι παραπλανητικές. Ειδικότερα:

- Η ονομασία του οργανισμού, όπως εμφανίζεται στο πιστοποιητικό, πρέπει να αντιστοιχεί στο επίπεδο ιεραρχίας στο οποίο διενεργείται η ανασκόπηση από τη διοίκηση (π.χ. Οργανισμός x, επιχειρησιακή μονάδα y).

- Το πεδίο εφαρμογής του πιστοποιητικού περιέχει μια συνοπτική περιγραφή των δραστηριοτήτων του οργανισμού που καλύπτονται από το πιστοποιητικό. Το πεδίο εφαρμογής πρέπει να είναι εντός του πεδίου εφαρμογής που έχει καθοριστεί από τον οργανισμό που πρόκειται να πιστοποιηθεί (ISO/IEC

27001 παράγραφος 4.3). Η παρούσα περιγραφή δεν μπορεί να περιέχει κρίσεις.

- Τα υποκαταστήματα του οργανισμού σε άλλες διευθύνσεις ή/και πόλεις θα αναγράφονται στο πιστοποιητικό κατά τρόπο ώστε να είναι ανιχνεύσιμα.

- Εάν χορηγείται μερικό πιστοποιητικό για μια δραστηριότητα ή μια τοποθεσία που καλύπτεται από το πιστοποιητικό ενός ευρύτερου οργανισμού, πρέπει να είναι σαφές για όλους τους ενδιαφερόμενους ότι το εν λόγω μερικό πιστοποιητικό δεν αποτελεί ανεξάρτητη πιστοποίηση και δεν μπορεί να θεωρηθεί χωριστό από το πιστοποιητικό του ευρύτερου οργανισμού, ο αριθμός του οποίου πρέπει να αναγράφεται στο μερικό πιστοποιητικό.

- Εάν υπάρχει ανάγκη για λεπτομερέστερες πληροφορίες σχετικά με το τι περιλαμβάνει το πιστοποιητικό ISO/IEC 27001 (όπως διευθύνσεις άλλων χώρων, ονόματα προϊόντων ή υπηρεσιών), το πιστοποιητικό μπορεί να παραπέμπει σε παράρτημα, επικυρωμένο από την EPCERT, όπου εμφανίζονται οι πληροφορίες αυτές.

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

3.5.2 **Ανταλλαγή πληροφοριών μεταξύ EPCERT και πελατών (ISO 17021-1 παράγραφος 8.5)**

Ο οργανισμός με πιστοποιημένο σύστημα διαχείρισης ασφάλειας πληροφοριών είναι υπεύθυνος για τη συνέχιση της συμμόρφωσης με όλες τις απαιτήσεις. Εάν αυτό δεν ισχύει πλέον, ο ίδιος ο οργανισμός πρέπει να το αναφέρει στην EPCERT.

Η μη συνέχιση της συμμόρφωσης δεν αφορά για παράδειγμα μη συμμορφώσεις που εντοπίζονται σε εσωτερικές επιθεωρήσεις και οι οποίες μπορούν να επιλυθούν γρήγορα, αλλά αφορά διαρθρωτικές μη συμμορφώσεις που έχουν ή μπορούν να έχουν συνέπειες για την επίτευξη της πολιτικής ΥΑΕ, ώστε να αναμένονται καταγγελίες από το προσωπικό ή/και ενέργειες από τις αρχές. Βλέπε επίσης την ενότητα 4.5.2, η οποία εξετάζει τις μη συμμορφώσεις για τις οποίες η EPCERT πρέπει να διενεργήσει πρόσθετο ενδιάμεσο έλεγχο.

4. ΔΙΑΔΙΚΑΣΙΕΣ ΕΙΔΙΚΟΥ ΚΑΝΟΝΙΣΜΟΥ

Το κεφάλαιο 9 του προτύπου ISO/IEC 17021-1:2015 περιέχει απαιτήσεις σχετικά με τις διαδικασίες που χρησιμοποιούνται κατά τη διάρκεια της διαδικασίας πιστοποίησης.

4.1 Προετοιμασία για την πιστοποίηση (ISO 17021-1 παράγραφος 9.1)

4.1.1 Ανασκόπηση της αίτησης (ISO 17021-1, παράγραφοι 9.1.1 και 9.1.2)

Ο προς πιστοποίηση οργανισμός πρέπει να καθορίσει το πεδίο εφαρμογής του συστήματος διαχείρισης ασφάλειας πληροφοριών (ISO/IEC 27001, παράγραφος 4.3). Πρέπει να γίνεται διάκριση μεταξύ του πεδίου εφαρμογής που ορίζεται στο σύστημα διαχείρισης ασφάλειας πληροφοριών και των πληροφοριών στο πιστοποιητικό. Στο πιστοποιητικό πρέπει να υπάρχει συνοπτική περιγραφή των εργασιών και όλων των χώρων που καλύπτονται από την πιστοποίηση. Οι πληροφορίες αυτές στο πιστοποιητικό προέρχονται από την περιγραφή του πεδίου εφαρμογής στο πλαίσιο του συστήματος διαχείρισης ασφάλειας πληροφοριών.

Η EPCERT πρέπει να καθορίσει εάν το πεδίο εφαρμογής είναι σύμφωνο με τις απαιτήσεις του προτύπου ISO/IEC 27001 (ενότητα 4.3) όσον αφορά την ενσωμάτωση όλων των δραστηριοτήτων, προϊόντων και υπηρεσιών που ο οργανισμός μπορεί να ελέγξει και να επηρεάσει και που μπορούν να επηρεάσουν την επίδοσή του σε θέματα ασφάλειας πληροφοριών.

Η EPCERT μπορεί να εξειδικεύσει περαιτέρω τις διαδικασίες για τον προσδιορισμό του πεδίου εφαρμογής για ορισμένες ειδικές καταστάσεις:

- Πιστοποίηση μιας δραστηριότητας στο πλαίσιο ενός ευρύτερου οργανισμού με πολλαπλές δραστηριότητες
- Εάν στο πλαίσιο ενός οργανισμού, περισσότερα από ένα τμήματα, επιχειρηματικές μονάδες, θυγατρικές κ.λπ. ασκούν δραστηριότητες, τότε μια ξεχωριστή δραστηριότητα μπορεί να πιστοποιηθεί εάν:
    - έχει τη δική της διαχείριση,
    - μπορεί να ακολουθήσει την πολιτική της και διαθέτει ένα ανεξάρτητο σύστημα διαχείρισης ασφάλειας πληροφοριών,
    - έχει τις δικές της παραγωγικές ή άλλες εγκαταστάσεις και κάθε μία ξεχωριστά είναι υπεύθυνη για την τήρηση της νομοθεσίας και των κανονισμών.

4.1.2 Χρόνος επιθεώρησης (ISO 17021-1 παραγ. 9.1.4 και 9.1.5)

Το πρότυπο ISO/IEC 27006:2015, συμπεριλαμβανομένων τυχόν διευκρινίσεων του Amd 1:2020 που εφαρμόζονται, έχει κατευθυντήριες γραμμές για τον προγραμματισμό του απαιτούμενου χρόνου.

Ο χρόνος επιθεώρησης είναι άμεση συνάρτηση του αριθμού εργαζομένων ενός οργανισμού με την πολυπλοκότητα του οργανισμού, όπως ορίζεται στο Annex B και C του προτύπου ISO/IEC 27006:2015.

Ο "χρόνος επιθεώρησης" που αναφέρεται στον πίνακα εκφράζεται ως "ημέρες επιθεωρητή" που δαπανήθηκαν για τον έλεγχο. Η βάση για τον υπολογισμό του πίνακα 1 είναι μια 8ωρη εργάσιμη ημέρα.

Τα άτομα που εργάζονται με μερική απασχόληση υπό την επιθεώρηση του οργανισμού συνεισφέρουν ανάλογα με τον αριθμό των ωρών εργασίας σε σύγκριση με ένα άτομο που εργάζεται με πλήρη απασχόληση υπό την επιθεώρηση του οργανισμού.

Ως εργαζόμενοι εννοούνται όσοι εργάζονται σε τμήματα ή δραστηριότητες που καλύπτονται από το πεδίο της πιστοποίησης, όπως περιγράφεται στο αντίστοιχο Σύστημα Διαχείρισης κάθε Οργανισμού. Ο αριθμός αυτός αναφέρεται στον συνολικό αριθμό των εργαζόμενων (effective personnel) σε όλες τις βάρδιες.

Κατά τον προσδιορισμό του χρόνου που διατίθεται, πρέπει να λαμβάνονται υπόψη οι ακόλουθοι παράγοντες που σχετίζονται με την πολυπλοκότητα του ΣΔΑΠ και συνεπώς με την προσπάθεια που απαιτείται για την επιθεώρησή του:

- η πολυπλοκότητα του ΣΔΑΠ (π.χ. κρισιμότητα των συστημάτων πληροφοριών, κατάσταση κινδύνου του ΣΔΑΠ),
- τα είδη εργασιών που εκτελούνται στο πλαίσιο του ΣΔΑΠ,
- η προηγούμενη απόδοση του ΣΔΑΠ,
- το εύρος και η ποικιλομορφία της τεχνολογίας που χρησιμοποιείται για την εφαρμογή των διαφόρων στοιχείων του ΣΔΑΠ (π.χ. αριθμός διαφορετικών IT πλατφόρμων, αριθμός διαχωρισμένων δικτύων κ.λπ.)
- εύρος εξωτερικής ανάθεσης που χρησιμοποιείται εντός του πεδίου εφαρμογής του ΣΔΑΠ και του πεδίου εφαρμογής των κανονισμών για τρίτους
- αριθμός τοποθεσιών και αριθμός τοποθεσιών αποκατάστασης καταστροφών (Disaster Recovery sites),
- για επιθεωρήσεις επιτήρησης ή επαναπιστοποίησης: το μέγεθος και το εύρος των αλλαγών που σχετίζονται με το εφαρμοζόμενο ΣΔΑΠ σύμφωνα με την §8.5.3 του προτύπου ISO/IEC 17021-1.

Το Annex C παρέχει παραδείγματα για το πώς μπορούν να ληφθούν υπόψη αυτοί οι διαφορετικοί παράγοντες κατά τον υπολογισμό του χρόνου επιθεώρησης.

Επιπλέον παραδείγματα παραγόντων που μπορεί να επηρεάσουν το χρόνο επιθεώρησης καθορίζονται στο Annex B του προτύπου ISO/IEC 27006:2015. Συγκεκριμένα, παράγοντες που μπορεί να αυξήσουν τη διάρκεια της επιθεώρησης, όπως ορίζονται στο πρότυπο, είναι:

- Οι εργασίες πραγματοποιούνται σε παραπάνω από ένα κτήρια ή τοποθεσίες.
- Το προσωπικό μιλά περισσότερες της μίας γλώσσες (κατάσταση που απαιτεί μεταφραστή ή που αποτρέπει τους επιθεωρητές να δουλεύουν ανεξάρτητα) ή/και η τεκμηρίωση είναι διαθέσιμη σε περισσότερες της μίας γλώσσας.

- Δραστηριότητες που απαιτούν την επιθεώρηση προσωρινών εγκαταστάσεων ώστε να επαληθευθούν οι δραστηριότητες των μόνιμων εγκαταστάσεων των οποίων το Σύστημα Διαχείρισης υπόκειται σε πιστοποίηση.
- Μεγάλος όγκος νομοθεσίας που σχετίζεται με το εφαρμοζόμενο σύστημα διαχείρισης.

Παράγοντες που μπορεί να μειώσουν τη διάρκεια της επιθεώρησης, όπως ορίζονται στο πρότυπο, είναι:

- Χαμηλής ή μηδενικής επικινδυνότητας προϊόντα ή διεργασίες.
- Προηγούμενη γνώση του Συστήματος Διαχείρισης του πελάτη (π.χ. ήδη πιστοποιημένος από τον Φ.Π. σε άλλο πρότυπο, μετάβαση πιστοποίησης από άλλο διαπιστευμένο φορέα).
- Ετοιμότητα πελάτη για την επιθεώρηση (π.χ. ήδη πιστοποιημένο ή αναγνωρισμένο Σύστημα Διαχείρισης από άλλον Φορέα Πιστοποίησης).
- Διεργασίες που περιλαμβάνουν μία και μόνο γενική δραστηριότητα (π.χ. παροχή υπηρεσιών).
- Μεγάλο ποσοστό του προσωπικού του επιθεωρούμενου οργανισμού εκτελεί τις ίδιες δραστηριότητες.
- Ωριμότητα Συστήματος Διαχείρισης (π.χ. εφαρμογή για μεγάλο διάστημα).

Η διάρκεια της επιθεώρησης μπορεί να προσαρμοστεί ανάλογα με όσα διαπιστώθηκαν κατά την επιθεώρηση του σταδίου 1 (για παράδειγμα, διαφορετική αξιολόγηση της πολυπλοκότητας του πεδίου εφαρμογής του ΣΔΑΠ ή πρόσθετες περιοχές εντός του πεδίου εφαρμογής).

Εάν η EPCERT αναπτύξει ένα πρόγραμμα επιθεώρησης στο οποίο οι δραστηριότητες απομακρυσμένου ελέγχου αντιπροσωπεύουν περισσότερο από το 30% του προγραμματισμένου χρόνου επιτόπιας επιθεώρησης, η EPCERT θα αιτιολογήσει το πρόγραμμα επιθεώρησης και θα λάβει ειδική έγκριση από τον φορέα διαπίστευσης πριν από την εφαρμογή του.

Αναμένεται ότι ο υπολογιζόμενος χρόνος για τη διενέργεια του σταδίου 2 της αρχικής πιστοποίησης δεν θα μειωθεί σε λιγότερο από το 70% του συνολικού χρόνου επιθεώρησης. Όταν απαιτείται πρόσθετος χρόνος για το σχεδιασμό ή/και τη σύνταξη της έκθεσης, αυτό δεν μπορεί να αποτελέσει δικαιολογία για τη συντόμευση της επιτόπιας επιθεώρησης. Ο χρόνος ταξιδιού του επιθεωρητή δεν περιλαμβάνεται στον υπολογισμό αυτό και προστίθεται στο χρόνο επιθεώρησης.

Ο αριθμός των συνολικών ημερών των επιτόπιων επιθεωρητών -όπως υπολογίζεται για το πεδίο εφαρμογής- κατανέμεται στις διάφορες τοποθεσίες με βάση τη συνάφεια της τοποθεσίας με το σύστημα διαχείρισης και τους κινδύνους που εντοπίζονται. Η αιτιολόγηση της κατανομής καταγράφεται από τον φορέα πιστοποίησης.

Ο συνολικός χρόνος που δαπανάται για αρχική επιθεώρηση και την επιτήρηση είναι το συνολικό άθροισμα του χρόνου που δαπανάται σε κάθε τοποθεσία συν το κεντρικό γραφείο και δεν πρέπει ποτέ να είναι μικρότερος από αυτόν που θα είχε υπολογιστεί για το μέγεθος και την πολυπλοκότητα της επιχείρησης, εάν όλες οι εργασίες είχαν αναληφθεί σε μία μόνο τοποθεσία (δηλαδή με όλους τους υπαλλήλους της εταιρείας στην ίδια τοποθεσία).

Οι ακόλουθες κατευθυντήριες γραμμές είναι σημαντικές για τον περαιτέρω καθορισμό των χρονοδιαγραμμάτων:

- ✓ Το IAF MD 1:2023 (Πιστοποίηση πολλαπλών χώρων με βάση τη δειγματοληψία) παρέχει πιθανούς τρόπους για τη μείωση του χρόνου που δαπανάται για τη δειγματοληψία, εάν υπάρχει ένα κεντρικά συντονισμένο σύστημα διαχείρισης της ΥΑΕ που καλύπτει πολλούς χώρους με παρόμοιες δραστηριότητες.
- ✓ Το IAF MD 11:2023 (Επιθεωρήσεις ολοκληρωμένων συστημάτων διαχείρισης) παρέχει πιθανούς τρόπους για τη μείωση του χρόνου που δαπανάται με το συνδυασμό επιθεωρήσεων διαφορετικών συστημάτων διαχείρισης.
- ✓ Το IAF ID 14:2023 Οδηγίες για τον προσδιορισμό του χρόνου επιθεώρησης ολοκληρωμένων συστημάτων διαχείρισης πολλών τοποθεσιών

4.2 Αρχική πιστοποίηση (ISO 17021-1 παράγραφος 9.3)

4.2.1 Στάδιο 1 (ISO 17021-1 παράγραφος 9.3.1.2)

Η EPCERT πρέπει να προσδιορίσει κατά πόσον το πεδίο εφαρμογής που έχει επιλέξει ο οργανισμός ανταποκρίνεται στην πραγματική κατάσταση.

Ένα στοιχείο του σταδίου 1 είναι η επιθεώρηση των εγγράφων (βλέπε ISO/IEC 17021-1:2015 sec. 9.3.1.2). Ο τόπος διεξαγωγής του 1ου σταδίου επιθεώρησης μπορεί να καθοριστεί σε συνεννόηση με τον οργανισμό. Δύναται να εκτελείται το σύνολο του 1ου σταδίου της επιθεώρησης εκτός της έδρας του οργανισμού, εκτός αν αποφασιστεί διαφορετικά. Το παράρτημα 1 περιέχει κατάλογο των εγγράφων που είναι σημαντικά για την πραγματοποίηση του 1ου σταδίου.

Το πρώτο στάδιο της επιθεώρησης εκτελείται για να:
α) ανασκοπείται η τεκμηρίωση του συστήματος διαχείρισης του επιθεωρούμενου οργανισμού. Για το σκοπό αυτό, ο επιθεωρούμενος οργανισμός αποστέλλει στην EPCERT την τεκμηρίωση του ΣΔΑΠ που επιθυμεί να πιστοποιήσει.
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.

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

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.

Το στάδιο 1 πρέπει να προσδιορίζει κατά πόσον τα διάφορα στοιχεία του ΣΔΑΠ υπάρχουν και έχουν εφαρμοστεί. Η ποιότητα της εφαρμογής καθορίζεται κατά το στάδιο 2. Η εφαρμογή πρέπει να είναι αρκετά πλήρης ώστε να μπορεί να υπάρξει εύρημα στην έκθεση επιθεώρησης της φάσης 2 σχετικά με τη λειτουργία του ΣΔΑΠ (βλέπε 4.3.1 και 4.3.2 του παρόντος συστήματος πιστοποίησης). Ο σκοπός του σταδίου 1 είναι να προσδιοριστεί εάν ο οργανισμός είναι έτοιμος για την αξιολόγηση της εφαρμογής στο στάδιο 2.

Η επιθεώρηση 1ου σταδίου μπορεί να συνδυαστεί με επιθεωρήσεις άλλων συστημάτων διαχείρισης. Ωστόσο, αυτό δεν πρέπει να θέτει σε κίνδυνο την ποιότητα και το βάθος της επιθεώρησης. Σε μια συνδυασμένη επιθεώρηση, η έκθεση πρέπει να αναφέρει με σαφήνεια όλες τις πτυχές που αφορούν το σύστημα διαχείρισης της ΥΑΕ.

4.2.2 Στάδιο 2 (ISO 17021-1 παράγραφος 9.3.1.3)

Το κεφάλαιο 2 (ερμηνεία και οδηγός για το ISO/IEC 27001) εξηγεί τη σχέση μεταξύ των διαφόρων στοιχείων του προτύπου. Η σχέση αυτή αξιολογείται με την παρακολούθηση της επιθεώρησης κατά το Στάδιο 2.

Εκτός από τα σημεία που απαιτούνται από το ISO/IEC 17021-1:2015, η EPCERT αναμένει ότι το 2ο στάδιο της επιθεώρησης πιστοποίησης θα περιλαμβάνει επίσης:

- ✓ συνέντευξη με την ανώτατη διοίκηση που είναι υπεύθυνη για την εν λόγω εγκατάσταση,
- ✓ περιήγηση στο εργοτάξιο, περιλαμβανομένης της διερεύνησης της εφαρμογής του συστήματος διαχείρισης της ΥΑΕ στον χώρο εργασίας (μεταξύ άλλων με τη διεξαγωγή συνεντεύξεων).

4.3 Διενέργεια επιθεωρήσεων (ISO 17021-1 παράγραφος 9.4)

4.3.1 Αξιολόγηση της συμμόρφωσης με τη νομοθεσία και τους κανονισμούς (IAF MD 22)

Σύμφωνα με την παράγραφο 9.4.8.3 του προτύπου ISO/IEC 17021-1:2015, η έκθεση επιθεώρησης πρέπει να περιλαμβάνει δήλωση σχετικά με την αποτελεσματικότητα του συστήματος διαχείρισης ασφάλειας πληροφοριών όσον αφορά τη συμμόρφωσή του με τη νομοθεσία και τους κανονισμούς.

Τα ακόλουθα σημεία είναι σημαντικά για την αξιολόγηση του κατά πόσον το ΣΔΑΠ εφαρμόζεται με τέτοιο τρόπο ώστε ο οργανισμός να είναι σε θέση να συμμορφώνεται με τη νομοθεσία και τους κανονισμούς:

- Η EPCERT πρέπει να αξιολογήσει κατά πόσον τα διάφορα στοιχεία του προτύπου ISO/IEC 27001 που είναι σημαντικά για τη διασφάλιση της συμμόρφωσης (συμπεριλαμβανομένου του επιπέδου λεπτομέρειας της προσδιορισμένης νομοθεσίας και των κανονισμών, της διαδικασίας επικαιροποίησης του καταλόγου των προσδιορισμένων νομικών και άλλων σημείων συμμόρφωσης, του εντοπισμού και της κοινοποίησης των περιστατικών, της διαδικασίας αυτοαξιολόγησης, της διαδικασίας υποβολής εκθέσεων στη διοίκηση) είναι επεξεργασμένα με επαρκή λεπτομέρεια ώστε να είναι δυνατή η διασφάλιση της συμμόρφωσης.
- Η EPCERT πρέπει να αξιολογεί τη λειτουργία των στοιχείων χρησιμοποιώντας ένα συνδυασμό τρόπων επιθεώρησης στις οποίες ακολουθούνται όλα τα σχετικά βήματα για τη διασφάλιση της συμμόρφωσης με συγκεκριμένες απαιτήσεις της νομοθεσίας και των κανονισμών και με δειγματοληψία (δειγματοληπτικοί έλεγχοι) για την αξιολόγηση της συμμόρφωσης με συγκεκριμένες απαιτήσεις της νομοθεσίας και των κανονισμών. Σκοπός αυτών των αξιολογήσεων είναι να κατανοηθεί ο τρόπος λειτουργίας του ΣΔΑΠ και όχι να αναφερθεί η πραγματική συμμόρφωση.
- Ένα σωστά λειτουργικό σύστημα διαχείρισης ασφάλειας πληροφοριών θα παρέχει αποτελέσματα που θα δείχνουν το βαθμό συμμόρφωσης με τη νομοθεσία και τους κανονισμούς. Τα αποτελέσματα αυτά πρέπει να τεκμηριώνονται στο πλαίσιο του συστήματος διαχείρισης ασφάλειας πληροφοριών.
- Η λειτουργία του συστήματος διαχείρισης ασφάλειας πληροφοριών πρέπει να αποτελεί τη βάση για τη δικαιολογημένη εμπιστοσύνη της EPCERT ότι ο οργανισμός πράγματι συμμορφώνεται με τη νομοθεσία και τους κανονισμούς.
- Δεδομένου ότι η αξιολόγηση βασίζεται σε δειγματοληπτική επιθεώρηση και σε περιορισμένη χρονική περίοδο, η τεκμηριωμένη εμπιστοσύνη δεν σημαίνει απαραίτητα ότι μπορεί να εξασφαλιστεί η συμμόρφωση με τη νομοθεσία και τους κανονισμούς.

Εάν ο οργανισμός χρειάζεται αλλά δεν διαθέτει άδεια για μέρος ή το σύνολο των δραστηριοτήτων του, μπορεί να πιστοποιηθεί, εφόσον η απουσία δεν οφείλεται σε υπαιτιότητα. Η έλλειψη υπαιτιότητας της οργάνωσης πρέπει να είναι προφανής από την αλληλογραφία της με τις αρχές.

Εάν υπάρχουν επαρκείς λόγοι για να το πράξει, ο φορέας πιστοποίησης μπορεί να συμβουλευτεί δημόσιες πηγές προκειμένου να επαληθεύσει εάν οι πληροφορίες που παρέχονται από τον οργανισμό είναι σωστές.

Οι πηγές δημόσιας πληροφόρησης της αρμόδιας αρχής μπορούν να ερωτηθούν προκειμένου να αξιολογηθεί εάν:

- τα αρχεία επικοινωνίας του οργανισμού με την κυβέρνηση είναι πλήρη, όπως για παράδειγμα οι εκθέσεις επιθεώρησης που δημοσιοποιούνται στο Διαδίκτυο,
- όλοι οι χώροι και οι εγκαταστάσεις του προς πιστοποίηση οργανισμού καλύπτονται επίσης από την ισχύουσα άδεια,
- υπάρχουν νέες εξελίξεις σχετικά με τις διαφορές απόψεων μεταξύ του οργανισμού και των αρχών,
- ο οργανισμός δεν μπορεί να κατηγορηθεί για το γεγονός ότι δεν υπάρχουν άδειες.

Εάν η EPCERT επιθυμεί πληροφορίες από τις εποπτικές αρχές πέραν αυτών που υπάρχουν ήδη σε δημόσια διαθέσιμες πηγές, τότε καταρχήν ο ίδιος ο οργανισμός θα πρέπει να ζητήσει τις πληροφορίες αυτές, εκτός εάν έχουν συναφθεί άλλες συμφωνίες μεταξύ του οργανισμού και της EPCERT.

Σε κάθε περίπτωση, η EPCERT πρέπει να αποφασίσει κατά της πιστοποίησης ή να ανακαλέσει το πιστοποιητικό, εάν συντρέχει μία ή περισσότερες από τις ακόλουθες περιπτώσεις:

- Διαπιστώνεται ότι η διαδικασία και οι αρμοδιότητες που προβλέπονται στο σύστημα διαχείρισης ασφάλειας πληροφοριών για την υποβολή αιτήσεων για την έκδοση αδειών ή/και την απαιτούμενη κοινοποίηση ή η διαδικασία χειρισμού της συνέχισης της αίτησης ή της απαιτούμενης κοινοποίησης δεν λειτουργούν.
- Η EPCERT έχει σοβαρές αμφιβολίες για το αν ο οργανισμός μπορεί να επιτύχει την πρόθεσή του να συμμορφωθεί με τις νομικές απαιτήσεις χρησιμοποιώντας το σύστημα διαχείρισης ασφάλειας πληροφοριών.
- Οι διαδικασίες για διορθωτικές και προληπτικές ενέργειες δεν είναι αποτελεσματικές. Αυτό ισχύει εάν, για παράδειγμα, οι απαιτήσεις για σημαντικούς κινδύνους ασφάλειας πληροφοριών παραβιάζονται συστηματικά και δεν υπάρχουν γραπτές συμφωνίες με τις αρχές σχετικά με το θέμα αυτό.
- Οι διαδικασίες αναφοράς περιστατικών ή/και παραβιάσεων των νομικών απαιτήσεων στην αρμόδια αρχή δεν λειτουργούν σωστά.
- Υπάρχουν αλλαγές στη Δήλωση Εφαρμοσιμότητας (SoA) του οργανισμού. Το πιστοποιητικό παραμένει σε ανάκληση έως ότου ο οργανισμός αποστέλλει στην EPCert τη νέα έκδοση Δήλωσης Εφαρμοσιμότητας, γίνει αξιολόγηση των αλλαγών και αποφασιστεί εάν απαιτούνται περαιτέρω ενέργειες (π.χ. αποστολή επιπλέον τεκμηρίωσης, διενέργεια επιθεώρησης, κ.λπ.) για την επανέκδοση του πιστοποιητικού συμμόρφωσης.

4.3.2 Αξιολόγηση της συνεχούς βελτίωσης

Σύμφωνα με την παράγραφο 9.4.8.3 του προτύπου ISO/IEC 17021-1:2015, η έκθεση επιθεώρησης πρέπει να περιέχει δήλωση σχετικά με την αποτελεσματικότητα του συστήματος διαχείρισης ασφάλειας πληροφοριών όσον αφορά τα αναμενόμενα αποτελέσματα. Η EPCERT θεωρεί αναμενόμενο αποτέλεσμα τη συνεχή βελτίωση των επιδόσεων σχετικά με την ασφάλεια πληροφοριών. Τα ακόλουθα σημεία είναι σημαντικά για την αξιολόγηση του κατά πόσον το ΣΔΑΠ έχει εφαρμοστεί κατά τρόπο ώστε ο οργανισμός να είναι σε θέση να βελτιώνει συνεχώς τις επιδόσεις του:

- Η EPCERT πρέπει να αξιολογεί κατά πόσον τα διάφορα στοιχεία του προτύπου ISO/IEC 27001 που είναι σημαντικά για την επίτευξη συνεχούς βελτίωσης των επιδόσεων που συνδέονται με τις δραστηριότητες του οργανισμού έχουν εκπονηθεί έτσι ώστε να είναι δυνατή η συνεχής βελτίωση. Τα στοιχεία αυτά περιλαμβάνουν τον εντοπισμό ευκαιριών βελτίωσης, τη συμμετοχή της ανώτατης διοίκησης στη συνεχή βελτίωση, τον προγραμματισμό των βελτιώσεων και τη διαθεσιμότητα πόρων και ανθρώπων, την παρακολούθηση και, αν χρειαστεί, την τροποποίηση των διαδικασιών βελτίωσης.
- Η EPCERT πρέπει να αξιολογεί τη λειτουργία της διαδικασίας βελτίωσης μέσω ενός συνδυασμού μεθόδων επιθεώρησης στις οποίες περιλαμβάνονται όλα τα βήματα που σχετίζονται με την

πραγματοποίηση βελτιώσεων για συγκεκριμένους κινδύνους ή ευκαιρίες και από δειγματοληπτικούς επιθεωρήσεις που αξιολογούν τον τρόπο με τον οποίο πραγματοποιούνται συγκεκριμένες επιλογές βελτίωσης.

- Εάν το σύστημα διαχείρισης ασφάλειας πληροφοριών λειτουργεί σωστά, τα αποτελέσματα του συστήματος θα δείξουν σε ποιο βαθμό βελτιώνεται η απόδοσή τυο. Αυτό τεκμηριώνεται στη συνέχεια στο πλαίσιο του ΣΔΑΠ.

Μία ή περισσότερες από τις ακόλουθες καταστάσεις μπορούν να αποτελέσουν λόγο άρνησης χορήγησης ή ανάκλησης πιστοποιητικού:

- Ο οργανισμός δεν έχει αποκτήσει, ή έχει πολύ λίγη κατανόηση των δυνατοτήτων βελτίωσης των επιδόσεων σε θέματα ασφάλειας πληροφοριών σε σχέση με τους εντοπισμένους κινδύνους και τις ευκαιρίες βελτίωσης.
- Δεν υπάρχει σχέδιο βελτίωσης ή το σχέδιο δεν είναι τεκμηριωμένο όσον αφορά το περιεχόμενο.
- Τα σχέδια επανειλημμένα δεν υλοποιούνται και δεν παρέχονται πειστικές εξηγήσεις. Πρόκειται για τα προγράμματα διαχείρισης που περιλαμβάνουν συγκεκριμένα σχέδια δραστηριοτήτων στο πλαίσιο της διαδικασίας συνεχούς βελτίωσης.
- Υπάρχουν αλλαγές στη Δήλωση Εφαρμοσιμότητας (SoA) του οργανισμού. Το πιστοποιητικό παραμένει σε ανάκληση έως ότου ο οργανισμός αποστέλλει στην EPCert τη νέα έκδοση Δήλωσης Εφαρμοσιμότητας, γίνει αξιολόγηση των αλλαγών και αποφασιστεί εάν απαιτούνται περαιτέρω ενέργειες (π.χ. αποστολή επιπλέον τεκμηρίωσης, διενέργεια επιθεώρησης, κ.λπ.) για την επανέκδοση του πιστοποιητικού συμμόρφωσης.

Η EPCERT αναμένει ότι δεν θα εκδοθεί πιστοποιητικό ISO/IEC 27001 σε οργανισμούς με δομικά επισφαλείς καταστάσεις. Η πιστοποίηση μπορεί να εξεταστεί μόνο εάν υπάρχει σχέδιο βελτίωσης το οποίο έχει γίνει αποδεκτό από τα ενδιαφερόμενα μέρη και αποσκοπεί στη μείωση των κινδύνων βραχυπρόθεσμα (π.χ. εντός 1 έτους). Ένα τέτοιο πιστοποιητικό πρέπει να έχει πρόσθετες απαιτήσεις (ενδιάμεσες εκθέσεις σχετικά με την πρόοδο των βελτιώσεων ή/και πρόσθετη επιθεώρηση).

4.3.3 Αξιολόγηση των πληροφοριών για την ασφάλεια πληροφοριών

Το πρότυπο ISO/IEC 27001 απαιτεί οι μέθοδοι παρακολούθησης και μέτρησης να παράγουν έγκυρα αποτελέσματα και οι πληροφορίες που κοινοποιούνται για την ασφάλεια πληροφοριών να είναι αξιόπιστες.

Η επιθεώρηση πιστοποίησης πρέπει να επικεντρώνεται στις διαδικασίες που σχετίζονται με την παρακολούθηση και τις μετρήσεις και στον τρόπο με τον οποίο οι πληροφορίες αυτές μετατρέπονται σε πληροφορίες για την ασφάλεια πληροφοριών. Παρόλο που η διαδικασία πιστοποίησης δεν επικεντρώνεται στη διατύπωση δηλώσεων σχετικά με μεμονωμένα στοιχεία, σημαίνει ότι:

- κατά τη διάρκεια της επιθεώρησης πιστοποίησης, θα πραγματοποιηθούν τυχαίοι έλεγχοι για ορισμένους σημαντικούς κινδύνους, προκειμένου να αξιολογηθεί κατά πόσον το σύστημα μέτρησης και καταγραφής παράγει έγκυρα και αξιόπιστα αποτελέσματα,
- για μια σειρά θεμάτων, θα αξιολογηθεί η διαδικασία επεξεργασίας των μετρήσεων και των αρχείων και, κατά περίπτωση, ο τρόπος προσαρμογής τους σε πληροφορίες για την ασφάλεια πληροφοριών,

- θα αξιολογείται κατά πόσον οι πληροφορίες που κοινοποιούνται εσωτερικά και εξωτερικά (συμπεριλαμβανομένων των εκθέσεων προς την κυβέρνηση) συμφωνούν με τις πληροφορίες που λαμβάνονται στο σύστημα διαχείρισης της ασφάλειας πληροφοριών,
- επαληθεύεται ότι το σύστημα λειτουργεί κατά τρόπο ώστε τα αποτελέσματα να είναι αναπαραγώγιμα και ότι οι πληροφορίες για την ασφάλεια πληροφοριών μπορούν να συγκριθούν με προηγούμενες ή/και μελλοντικές περιόδους.

Το πιστοποιητικό ISO/IEC 27001 σημαίνει ότι έχουν αξιολογηθεί διάφορα στοιχεία του συστήματος που είναι σημαντικά για την παραγωγή αξιόπιστων πληροφοριών για την ασφάλεια πληροφοριών. Υπό αυτή την έννοια, προσδίδει θετική αξία στις πληροφορίες που παράγονται με τη χρήση του συστήματος διαχείρισης ασφάλειας πληροφοριών. Ωστόσο, το πιστοποιητικό ISO/IEC 27001 δεν αποτελεί αξιόλογη κρίση σχετικά με την αξιοπιστία των επιμέρους στοιχείων, δεδομένου ότι αυτά αξιολογούνται μόνο με δειγματοληπτικές επιθεωρήσεις, με στόχο την αξιολόγηση του συστήματος.

Ένας οργανισμός που δημιουργεί εσφαλμένη εικόνα παρέχοντας ελλιπείς ή εσφαλμένες πληροφορίες για την ασφάλεια πληροφοριών στις εξωτερικές του επικοινωνίες δεν πληροί τις απαιτήσεις του ISO/IEC 27001 όσον αφορά την επικοινωνία.

4.3.4 Διαδικασίες για παραβιάσεις ασφάλειας πληροφοριών και επικίνδυνες καταστάσεις

Ο επιθεωρητής ασφάλειας πληροφοριών της EPCERT αναμένεται να:

- να αναφέρει παραβάσεις της νομοθεσίας και των κανονισμών με απειλητικές για τη ζωή συνέπειες τόσο στην ανώτατη διοίκηση του προς πιστοποίηση οργανισμού όσο και στην Επιθεώρηση Εργασίας ή σε οποιοδήποτε άλλο όργανο στο οποίο εκπροσωπείται το προσωπικό,
- να αναστείλει ή να ανακαλέσει την πιστοποίηση, εάν το σύστημα διαχείρισης ασφάλειας πληροφοριών δεν οδηγεί στην πρόληψη των παραβιάσεων ή στην επίλυση επικίνδυνων καταστάσεων.

Εάν υπάρχει άμεσος κίνδυνος για τα άτομα, για παράδειγμα, λόγω της παράβασης ή της επικίνδυνης κατάστασης, τότε η παραπάνω διαδικασία δεν θα είναι επαρκής. Ένας επιθεωρητής θα μπορούσε να διωχθεί για ποινικό αδίκημα, εάν άνθρωποι τίθενται σε κίνδυνο ως αποτέλεσμα της παράλειψης του επιθεωρητή να αναλάβει δράση.
Στο πλαίσιο της ευθύνης της EPCERT, είναι καταρχήν σημαντικό να μπορεί η EPCERT να αποδείξει ότι έχει κάνει ό,τι εύλογα μπορεί να αναμένεται από αυτήν για να αποτρέψει κάθε πιθανό κίνδυνο.
Η εταιρεία πρέπει να αποφασίζει κατά περίπτωση αν θα αναφέρει ή όχι την παράβαση ή την επικίνδυνη κατάσταση στις κυβερνητικές αρχές.

4.3.5 Εκθέσεις επιθεώρησης (ISO 17021-1 παράγραφος 9.4.8)

Η EPCERT οφείλει να αναφέρει τα αποτελέσματα της επιθεώρησης πιστοποίησης στον προς πιστοποίηση οργανισμό και να διατυπώνει ευκαιρίες βελτίωσης. Αυτό δεν θεωρείται σύσταση που πρέπει να ικανοποιηθεί. Η EPCERT δεν επιτρέπεται να διατυπώνει συστάσεις για την τροποποίηση του συστήματος

διαχείρισης της ΥΑΕ ή/και να διατυπώνει προτάσεις για συγκεκριμένες λύσεις με βάση τα αποτελέσματα της παρούσας έκθεσης.

Σύμφωνα με την EPCERT, η έκθεση πρέπει να περιλαμβάνει επαρκείς πληροφορίες εκ των υστέρων για να εξηγήσει τις διαδικασίες της, π.χ. εάν υπάρχουν ενστάσεις/προσφυγές. Η EPCERT πρέπει να τηρεί αρχεία με πληροφορίες σχετικά με τις επιθεωρήσεις που πραγματοποιούνται (βλέπε ISO 17021-1 παράγραφος 9.6.8). Στο πρότυπο ISO/IEC 17021:2015, παρ. 9.4.8.3 α, απαιτείται η έκθεση επιθεώρησης να περιέχει δήλωση με περίληψη των τεκμηρίων που δείχνουν το βαθμό στον οποίο το σύστημα διαχείρισης ασφάλειας πληροφοριών είναι ικανό να πληροί τις ισχύουσες απαιτήσεις και να επιτυγχάνει τα επιδιωκόμενα αποτελέσματα. Ως "αποτελέσματα" νοούνται τα επιδιωκόμενα αποτελέσματα που αποσκοπούν - τουλάχιστον - στη βελτίωση των επιδόσεων του συστήματος, στην εκπλήρωση των υποχρεώσεων συμμόρφωσης και στην επίτευξη των στόχων. Σύμφωνα με την EPCERT, η δήλωση αυτή θα πρέπει να επικεντρώνεται στην επίτευξη των επιδιωκόμενων αποτελεσμάτων και στη λειτουργία των στοιχείων του συστήματος διαχείρισης ασφάλειας πληροφοριών που είναι σημαντικά για την εξασφάλιση των υποχρεώσεων συμμόρφωσης και τη βελτίωση των επιδόσεων του ΣΔΑΠ.

Εκτός από τα παραπάνω σημεία, η έκθεση σχετικά με τις επιθεωρήσεις επιτήρησης πρέπει να δίνει ιδιαίτερη προσοχή στην εφαρμογή των σχεδίων για τη διόρθωση των μη συμμορφώσεων που εντοπίστηκαν σε προηγούμενες επιθεωρήσεις, ενώ η έκθεση σχετικά με την επιθεώρηση επαναπιστοποίησης πρέπει να δίνει ιδιαίτερη προσοχή στην εφαρμογή των σχεδίων για τη διόρθωση των μη συμμορφώσεων που εντοπίστηκαν συνολικά κατά την τρέχουσα τριετία.

4.4 Διατήρηση της πιστοποίησης (παράγραφος 9.6 του ISO 17021-1)

4.4.1 Επιθεώρηση επιτήρησης (ISO 17021-1, παράγραφος 9.6.2)

Η EPCERT αναμένει ότι σε επιθεωρήσεις επιτήρησης θα δοθεί προσοχή στα ακόλουθα σημεία, επιπλέον των στοιχείων που απαιτούνται από το ISO/IEC 17021-1:2015:

- τη συμμετοχή της ανώτατης διοίκησης,
- τη λειτουργία των διαδικασιών που σχετίζονται με την επικοινωνία με ενδιαφερόμενα μέρη (συμπεριλαμβανομένης της αλληλογραφίας με κυβερνητικές αρχές),
- τη λειτουργία των διαδικασιών για την αξιολόγηση από τον οργανισμό της συμμόρφωσής του με τη νομοθεσία και τους κανονισμούς και τα αποτελέσματα των διαδικασιών αυτών.

Οι επιθεωρήσεις επιτήρησης μπορούν να συνδυαστούν με επιθεωρήσεις άλλων συστημάτων διαχείρισης. Ωστόσο, αυτό δεν πρέπει να θέτει σε κίνδυνο την ποιότητα και το βάθος της επιθεώρησης. Σε έναν συνδυασμένο έλεγχο, η έκθεση πρέπει να αναφέρει με σαφήνεια όλες τις πτυχές που αφορούν το σύστημα διαχείρισης ασφάλειας πληροφοριών.

4.4.2 Επιθεώρηση επαναπιστοποίησης (ISO 17021-1, παράγραφος 9.6.3)

Η επιθεώρηση επαναπιστοποίησης πρέπει να σχεδιάζεται και να 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. Αυτό θα πρέπει να προγραμματιστεί και να πραγματοποιηθεί σε εύθετο χρόνο ώστε να καταστεί δυνατή η έγκαιρη ανανέωση πριν από την ημερομηνία λήξης του πιστοποιητικού.

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

Οι δραστηριότητες της επιθεώρησης επαναπιστοποίησης ενδέχεται να 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 ή της πιστοποίησης από την EPCERT ως προς περισσότερα του ενός συστήματα διαχείρισης, ο σχεδιασμός της επιθεώρησης πρέπει να διασφαλίζει επαρκείς επιτόπου επιθεωρήσεις, ώστε να ενισχύεται η εμπιστοσύνη στην πιστοποίηση.

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

- την αποτελεσματικότητα του συνόλου του συστήματος διαχείρισης αναφορικά με εσωτερικές και εξωτερικές αλλαγές, και την συνεχιζόμενη σχετικότητα και εφαρμοσιμότητα του πεδίου της πιστοποίησης,
- την αποδεδειγμένη δέσμευση για διατήρηση της αποτελεσματικότητας και της βελτίωσης του συστήματος διαχείρισης, ώστε να βελτιώνεται η συνολική επίδοση,
- το κατά πόσο η λειτουργία του πιστοποιημένου συστήματος διαχείρισης συμβάλλει στην επίτευξη των ποιοτικών και των αντικειμενικών σκοπών του οργανισμού,
- τα ευρήματα και την αποτελεσματικότητα των διορθωτικών ενεργειών που εντοπίστηκαν καθ’ όλη τη διάρκεια του τελευταίου κύκλου πιστοποίησης.

4.4.3 Ειδικές επιθεωρήσεις (ISO 17021-1 παράγραφος 9.6.4)

Η EPCERT πρέπει να εξετάζει το ενδεχόμενο διενέργειας πρόσθετης (ενδιάμεσης) επιθεώρησης κατά τη διάρκεια του κύκλου επιθεώρησης εάν:

- η EPCERT ενημερώνεται για τις αποφάσεις σχετικά με καταγγελίες (διατυπωμένες σε επίσημη επιστολή) στις οποίες οι αρχές έχει εντοπίσει παραβίαση σημαντικών κανονισμών ασφάλειας πληροφοριών,
- υπάρχουν άλλες ενδείξεις που δίνουν στην EPCERT λόγο να αμφιβάλλει για την ορθή λειτουργία του

συστήματος διαχείρισης ασφάλειας πληροφοριών,

- υπάρχουν αλλαγές στη Δήλωση Εφαρμοσιμότητας (SoA) του οργανισμού.

Η ενδιάμεση επιθεώρηση δεν είναι πάντα απαραίτητο να διενεργείται στον τόπο εγκατάστασης του πιστοποιημένου οργανισμού. Η EPCERT μπορεί μερικές φορές να την πραγματοποιήσει ζητώντας να ανασκοπήσει σχετικές πληροφορίες.

Παράρτημα 1. Διαθέσιμα έγγραφα για πιστοποίηση

Ο οργανισμός πρέπει να διαθέτει και να διατηρεί τα ακόλουθα έγγραφα/αρχεία:

- ✓ Περιγραφή του πεδίου εφαρμογής (4.3)
- ✓ Πολιτική ασφάλειας πληροφοριών (5.2)
- ✓ Κατανομή ρόλων, αρμοδιοτήτων και εξουσιών (5.3)
- ✓ Διαδικασίες και οι ενέργειες που απαιτούνται για την αξιολόγηση και την αντιμετώπιση των κινδύνων ασφάλειας πληροφοριών (6.1.2 – 6.1.3)
- ✓ Διαθέσιμοι πόροι (7.1)
- ✓ Τεκμήρια ικανοτήτων (7.2)
- ✓ Τεκμήρια των δραστηριοτήτων επικοινωνίας (7.4)
- ✓ Τεκμήρια εκτέλεσης των ενεργειών που προσδιορίζονται στην παράγραφο 6.1 (8.1 – 8.2)
- ✓ Τεκμήρια εφαρμογής του σχεδίου αντιμετώπισης κινδύνων (8.3)
- ✓ Τεκμήρια για τα αποτελέσματα της παρακολούθησης, μέτρησης, ανάλυσης και αξιολόγησης των επιδόσεων (9.1)
- ✓ Πρόγραμμα εσωτερικής επιθεώρησης και αποτελέσματα των εσωτερικών επιθεωρήσεων (9.2.2)
- ✓ Αποτελέσματα της ανασκόπησης από τη Διοίκηση (9.3)
- ✓ Αποδεικτικά στοιχεία για το αποτέλεσμα της διαδικασίας συνεχούς βελτίωσης (10.1)
- ✓ Το ιστορικό των περιστατικών και των μη συμμορφώσεων, τα μέτρα που ελήφθησαν και τα αποτελέσματα των μέτρων και των διορθωτικών ενεργειών και η αποτελεσματικότητά τους (10.2)
- ✓ Λίστα επιλεγμένων σημείων ελέγχου (Information security controls) / Δήλωση Εφαρμοσιμότητας

Τα έγγραφα/αρχεία που συνιστά η EPCERT να είναι διαθέσιμα:

- ✓ Ανάλυση πλαισίου λειτουργίας (βλ. 4.1 και 4.2)
- ✓ Περιγραφή της οργάνωσης και των αρμοδιοτήτων
- ✓ Επισκόπηση των τεκμηριωμένων πληροφοριών και αρχείων (συμπεριλαμβανομένων τυχόν περιγραφών διαδικασιών/διαδικασιών εκτός από εκείνες που απαιτούνται λίγο ή πολύ βάσει των σημείων 6.1, 8.1, 8.2 και 8.3)

Παράρτημα 2. Έλεγχοι ασφάλειας πληροφοριών

5 Οργανωτικοί έλεγχοι

5.1 Πολιτικές για την ασφάλεια των πληροφοριών

Έλεγχος

Η πολιτική για την ασφάλεια των πληροφοριών και οι ειδικές πολιτικές για κάθε θέμα θα πρέπει να ορίζονται, να εγκρίνονται από τη διοίκηση, να δημοσιεύονται, να κοινοποιούνται και να αναγνωρίζονται από το αρμόδιο προσωπικό και τα ενδιαφερόμενα μέρη και να επανεξετάζονται σε προγραμματισμένα χρονικά διαστήματα και σε περίπτωση σημαντικών αλλαγών.

Σκοπός αυτού του ελέγχου είναι να διασφαλιστεί η συνεχής καταλληλότητα, επάρκεια και αποτελεσματικότητα της κατεύθυνσης και της υποστήριξης της ασφάλειας των πληροφοριών από τη διοίκηση, σύμφωνα με τις επιχειρηματικές, νομικές, κανονιστικές, ρυθμιστικές και συμβατικές απαιτήσεις.Η διοίκηση θα πρέπει να καθορίσει ένα σύνολο πολιτικών για να αποσαφηνίσει την κατεύθυνση και την υποστήριξη της ασφάλειας των πληροφοριών. Σε ανώτατο επίπεδο, θα πρέπει να υπάρχει μια συνολική "πολιτική ασφάλειας πληροφοριών" Πρέπει να δημιουργηθεί ένα έγγραφο, το οποίο θα περιέχει τον τρόπο με τον οποίο ο οργανισμός διαχειρίζεται τους στόχους της ασφάλειας πληροφοριών. Το έγγραφο αυτό πρέπει να εγκριθεί από τη διοίκηση και να περιέχει πολιτικές τόσο υψηλού όσο και χαμηλού επιπέδου. Μόλις εφαρμοστούν οι πολιτικές, πρέπει να επανεξετάζονται τακτικά. Η καλύτερη προσέγγιση είναι να ορίσετε μια τακτική συνάντηση και να προγραμματίσετε μια επιπλέον συνάντηση ενδιάμεσα, εάν το απαιτεί η κατάσταση. Εάν γίνουν οποιεσδήποτε αλλαγές, η διοίκηση πρέπει να δώσει την έγκρισή της. Οι πολιτικές θα πρέπει να κοινοποιούνται στους εσωτερικούς και εξωτερικούς ενδιαφερόμενους φορείς.

5.2 Ρόλοι και αρμοδιότητες για την ασφάλεια των πληροφοριών

Έλεγχος

Οι *ρόλοι και οι αρμοδιότητες για την ασφάλεια των πληροφοριών θα πρέπει να καθορίζονται και να κατανέμονται σύμφωνα με τις ανάγκες του οργανισμού*.

Σκοπός αυτού του ελέγχου είναι η καθιέρωση μιας καθορισμένης, εγκεκριμένης και κατανοητής δομής για την εφαρμογή, τη λειτουργία και τη διαχείριση της ασφάλειας των πληροφοριών εντός του οργανισμού. Η πολιτική πρέπει να ορίζει ποιος είναι υπεύθυνος για ποιο περιουσιακό στοιχείο, ποια διαδικασία ή ποια δραστηριότητα κινδύνου ασφάλειας πληροφοριών. Είναι σημαντικό η ανάθεση να γίνεται με σαφήνεια και για όλες τις εργασίες. Βεβαιωθείτε ότι οι ρόλοι και οι αρμοδιότητες ταιριάζουν στον οργανισμό σας- μια μικρή ομάδα πέντε ατόμων πιθανόν να μην χρειάζεται έναν υπεύθυνο ασφαλείας πλήρους απασχόλησης.

5.3 Διαχωρισμός καθηκόντων

Έλεγχος

Τα αντικρουόμενα καθήκοντα και οι αντικρουόμενοι τομείς ευθύνης θα πρέπει να διαχωρίζονται.

Σκοπός αυτού του ελέγχου είναι η μείωση του κινδύνου απάτης, σφάλματος και παράκαμψης των ελέγχων ασφάλειας πληροφοριών. Για να αποφευχθεί οποιαδήποτε κατάχρηση των περιουσιακών στοιχείων της εταιρείας, η "εξουσία" για τον πλήρη έλεγχο μιας ευαίσθητης δραστηριότητας δεν θα πρέπει να ανήκει στο ίδιο πρόσωπο. Ο καλύτερος τρόπος για να το εφαρμόσετε αυτό είναι να καταγράφετε όλες τις δραστηριότητες και να χωρίζετε τις σημαντικές εργασίες σε εκτέλεση και έλεγχο ή έγκριση και έναρξη. Με

τον τρόπο αυτό αποφεύγεται η απάτη και το σφάλμα, π.χ. στην περίπτωση που ένα άτομο δημιουργεί και υπογράφει όλες τις επιταγές της εταιρείας.

5.4 Αρμοδιότητες διαχείρισης

Έλεγχος

Η διοίκηση θα πρέπει να απαιτεί από όλο το προσωπικό να εφαρμόζει την ασφάλεια των πληροφοριών σύμφωνα με την καθιερωμένη πολιτική ασφάλειας πληροφοριών, τις ειδικές πολιτικές και τις διαδικασίες του οργανισμού.

Σκοπός αυτού του ελέγχου είναι να διασφαλιστεί ότι η διοίκηση κατανοεί το ρόλο της στην ασφάλεια των πληροφοριών και να αναλάβει δράσεις που αποσκοπούν στο να διασφαλιστεί ότι όλο το προσωπικό γνωρίζει και εκπληρώνει τις ευθύνες του για την ασφάλεια των πληροφοριών. Η διοίκηση πρέπει να διασφαλίσει ότι όλοι οι εργαζόμενοι και οι εργολάβοι γνωρίζουν και ακολουθούν την πολιτική ασφάλειας πληροφοριών του οργανισμού. Θα πρέπει να δίνουν το παράδειγμα και να δείχνουν ότι η ασφάλεια πληροφοριών είναι χρήσιμη και αναγκαία.

5.5 Επικοινωνία με τις αρχές

Έλεγχος

Ο οργανισμός θα πρέπει να δημιουργεί και να διατηρεί επαφές με τις αρμόδιες αρχές.

Σκοπός αυτού του ελέγχου είναι να διασφαλιστεί η κατάλληλη ροή πληροφοριών όσον αφορά την ασφάλεια των πληροφοριών μεταξύ του οργανισμού και των σχετικών νομικών, ρυθμιστικών και εποπτικών αρχών. Θα πρέπει να είναι σαφές ποιος είναι υπεύθυνος για την επικοινωνία με τις αρχές (π.χ. επιβολή του νόμου, ρυθμιστικοί φορείς, εποπτικές αρχές), με ποιες αρχές θα πρέπει να γίνει η επικοινωνία (π.χ. ποια περιοχή/χώρα) και σε ποιες περιπτώσεις πρέπει να γίνει αυτό. Η γρήγορη και επαρκής ανταπόκριση σε περιστατικά μπορεί να μειώσει σημαντικά τις επιπτώσεις και μπορεί να είναι ακόμη και υποχρεωτική από το νόμο.

5.6 Επικοινωνία με ομάδες ειδικών ενδιαφερόντων

Έλεγχος

Ο οργανισμός θα πρέπει να δημιουργεί και να διατηρεί επαφές με ομάδες ειδικού ενδιαφέροντος ή άλλα εξειδικευμένα φόρουμ ασφάλειας και επαγγελματικές ενώσεις.

Ο σκοπός αυτού του ελέγχου είναι να διασφαλιστεί η κατάλληλη ροή πληροφοριών όσον αφορά την ασφάλεια των πληροφοριών. Για να διασφαλιστεί ότι παρακολουθούνται οι τελευταίες τάσεις και οι βέλτιστες πρακτικές για την ασφάλεια των πληροφοριών, το προσωπικό με καθήκοντα ISMS θα πρέπει να διατηρεί καλές επαφές με ομάδες ειδικού ενδιαφέροντος. Οι ομάδες αυτές μπορούν να ζητηθούν για συμβουλές εμπειρογνωμόνων σε ορισμένες περιπτώσεις και να αποτελέσουν μια εξαιρετική πηγή για τη βελτίωση των γνώσεων του καθενός.

5.7 Πληροφορία για απειλές

Έλεγχος

Θα πρέπει να συλλέγονται και να αναλύονται πληροφορίες σχετικά με τις απειλές για την ασφάλεια των πληροφοριών για την παραγωγή πληροφοριών σχετικά με τις απειλές.

Σκοπός αυτού του ελέγχου είναι να παρέχει επίγνωση του περιβάλλοντος απειλών του οργανισμού, ώστε να μπορούν να ληφθούν οι κατάλληλες ενέργειες μετριασμού. Η αντίδραση στις απειλές ελάχιστα συμβάλλει στην αποτροπή της πρώτης υλοποιημένης εμφάνισής τους. Συλλέγοντας και αναλύοντας πληροφορίες σχετικά με τις απειλές που απειλούν τον οργανισμό σας, έχετε καλύτερη εικόνα για το ποιοι μηχανισμοί προστασίας πρέπει να τεθούν σε εφαρμογή για την προστασία από τις απειλές που αφορούν τον οργανισμό σας. Οι κατασκευαστές τσιπ υπολογιστών πρέπει να προετοιμάζονται για στοχευμένες επιθέσεις κλοπής IP από κρατικούς φορείς, αλλά για έναν μικρό πάροχο SaaS, τα αυτοματοποιημένα μηνύματα ηλεκτρονικού "ψαρέματος" αποτελούν μεγαλύτερη απειλή.

5.8 Ασφάλεια πληροφοριών στη διαχείριση έργων

Έλεγχος

Η ασφάλεια των πληροφοριών πρέπει να ενσωματωθεί στη διαχείριση του έργου.

Σκοπός αυτού του ελέγχου είναι να διασφαλιστεί ότι οι κίνδυνοι ασφάλειας πληροφοριών που σχετίζονται με έργα και παραδοτέα αντιμετωπίζονται αποτελεσματικά στη διαχείριση έργων καθ' όλη τη διάρκεια του κύκλου ζωής του έργου. Για να διασφαλιστεί η επιτυχής εφαρμογή του ΣΔΑΠ σε ολόκληρο τον οργανισμό, η ασφάλεια των πληροφοριών θα πρέπει να λαμβάνεται υπόψη και να τεκμηριώνεται σε όλα τα έργα με τη μορφή απαιτήσεων. Οι απαιτήσεις αυτές μπορεί να απορρέουν από επιχειρηματικές, νομικές και συμμόρφωσης με άλλα πρότυπα ή κανονισμούς. Εάν έχετε εγχειρίδια ή πρότυπα διαχείρισης έργων, θα πρέπει να συμπεριλάβετε ένα Παράγραφος για την ασφάλεια των πληροφοριών.

5.9 Απογραφή των πληροφοριών και άλλων συναφών περιουσιακών στοιχείων

Έλεγχος

Θα πρέπει να καταρτιστεί και να διατηρηθεί ένας κατάλογος των πληροφοριών και άλλων συναφών περιουσιακών στοιχείων, συμπεριλαμβανομένων των ιδιοκτητών.

Ο σκοπός αυτού του ελέγχου είναι να προσδιορίσει τις πληροφορίες του οργανισμού και άλλα συναφή περιουσιακά στοιχεία προκειμένου να διαφυλάξει την ασφάλεια των πληροφοριών τους και να αποδώσει την κατάλληλη κυριότητα. Ο οργανισμός θα πρέπει να έχει εντοπίσει όλα τα περιουσιακά στοιχεία πληροφοριών και επεξεργασίας πληροφοριών. Όλα τα περιουσιακά στοιχεία πρέπει να καταγράφονται σε απογραφή, η οποία πρέπει να τηρείται δεόντως. Η γνώση των περιουσιακών στοιχείων, της σημασίας τους, της θέσης τους και του τρόπου χειρισμού τους είναι απαραίτητη για τον εντοπισμό και την πρόβλεψη των κινδύνων. Μπορεί ακόμη και να είναι υποχρεωτική για νομικές υποχρεώσεις ή ασφαλιστικούς σκοπούς. Όλα τα περιουσιακά στοιχεία της απογραφής, άρα ολόκληρης της εταιρείας, εάν η απογραφή είναι πλήρης, πρέπει να έχουν έναν ιδιοκτήτη. Χάρη στην ιδιοκτησία περιουσιακών στοιχείων, τα περιουσιακά στοιχεία παρακολουθούνται και φροντίζονται καθ' όλη τη διάρκεια του κύκλου ζωής τους. Παρόμοια περιουσιακά στοιχεία μπορούν να ομαδοποιηθούν και η καθημερινή επίβλεψη ενός περιουσιακού στοιχείου μπορεί να ανατεθεί σε έναν λεγόμενο θεματοφύλακα, αλλά ο ιδιοκτήτης παραμένει υπεύθυνος. Η ιδιοκτησία των περιουσιακών στοιχείων πρέπει να εγκριθεί από τη διοίκηση.

5.10 Αποδεκτή χρήση των πληροφοριών και άλλων συναφών περιουσιακών στοιχείων

Έλεγχος

Θα πρέπει να προσδιοριστούν, να τεκμηριωθούν και να εφαρμοστούν κανόνες για την αποδεκτή χρήση και διαδικασίες για το χειρισμό των πληροφοριών και άλλων συναφών περιουσιακών στοιχείων.

Σκοπός αυτού του ελέγχου είναι να διασφαλιστεί ότι οι πληροφορίες και άλλα συναφή περιουσιακά στοιχεία προστατεύονται, χρησιμοποιούνται και χειρίζονται κατάλληλα. Θα πρέπει να υπάρχουν καλά τεκμηριωμένοι κανόνες για την πρόσβαση στα περιουσιακά στοιχεία πληροφοριών. Οι χρήστες του περιουσιακού στοιχείου θα πρέπει να γνωρίζουν τις απαιτήσεις ασφάλειας πληροφοριών σχετικά με τη χρήση του περιουσιακού στοιχείου και να τις ακολουθούν. Για το χειρισμό των περιουσιακών στοιχείων θα πρέπει επίσης να υπάρχουν διαδικασίες. Το προσωπικό πρέπει να κατανοεί την επισήμανση των περιουσιακών στοιχείων και να γνωρίζει πώς να χειρίζεται τα διάφορα επίπεδα ταξινόμησης. Δεδομένου ότι δεν υπάρχει καθολικό πρότυπο για την ταξινόμηση, είναι επίσης σημαντικό να γνωρίζετε τα επίπεδα ταξινόμησης των άλλων μερών, δεδομένου ότι πιθανότατα θα διαφέρουν από τα δικά σας.

5.11 Επιστροφή περιουσιακών στοιχείων

Έλεγχος

Το προσωπικό και άλλα ενδιαφερόμενα μέρη, κατά περίπτωση, θα πρέπει να επιστρέφουν όλα τα περιουσιακά στοιχεία του οργανισμού που έχουν στην κατοχή τους κατά την αλλαγή ή τη λήξη της απασχόλησης, της σύμβασης ή της συμφωνίας τους.

Σκοπός αυτού του ελέγχου είναι η προστασία των περιουσιακών στοιχείων του οργανισμού στο πλαίσιο της διαδικασίας αλλαγής ή τερματισμού της απασχόλησης, της σύμβασης ή της συμφωνίας. Όταν ένας εργαζόμενος ή ένα εξωτερικό μέρος δεν μπορεί πλέον να έχει πρόσβαση σε ένα περιουσιακό στοιχείο, για παράδειγμα, λόγω λήξης της απασχόλησης ή της συμφωνίας, πρέπει να επιστρέψει το περιουσιακό στοιχείο στον οργανισμό. Θα πρέπει να υπάρχει μια σαφής πολιτική για το θέμα αυτό, η οποία θα πρέπει να είναι γνωστή σε όλους τους εμπλεκόμενους. Τα μη υλικά περιουσιακά στοιχεία που είναι σημαντικά για τις τρέχουσες δραστηριότητες, όπως οι ειδικές γνώσεις που δεν έχουν ακόμη τεκμηριωθεί, θα πρέπει να τεκμηριώνονται και να επιστρέφονται ως τέτοια.

5.12 Ταξινόμηση των πληροφοριών

Έλεγχος

Οι πληροφορίες θα πρέπει να ταξινομούνται σύμφωνα με τις ανάγκες ασφάλειας πληροφοριών του οργανισμού με βάση την εμπιστευτικότητα, την ακεραιότητα, τη διαθεσιμότητα και τις σχετικές απαιτήσεις των ενδιαφερομένων μερών.

Σκοπός αυτού του ελέγχου είναι να διασφαλιστεί ο εντοπισμός και η κατανόηση των αναγκών προστασίας των πληροφοριών σύμφωνα με τη σημασία τους για τον οργανισμό. Ορισμένες πληροφορίες θεωρούνται ευαίσθητες λόγω π.χ. νομισματικής ή νομικής αξίας και πρέπει να παραμένουν εμπιστευτικές, ενώ άλλες πληροφορίες είναι λιγότερο κρίσιμες. Ο οργανισμός θα πρέπει να διαθέτει πολιτική για τον τρόπο χειρισμού διαβαθμισμένων πληροφοριών. Η ευθύνη για την ταξινόμηση των περιουσιακών στοιχείων πληροφοριών ανήκει στον ιδιοκτήτη τους. Για να γίνει διάκριση μεταξύ της σημασίας των διαφορετικών διαβαθμισμένων περιουσιακών στοιχείων, μπορεί να είναι χρήσιμο να εφαρμοστούν διάφορα επίπεδα εμπιστευτικότητας, από ανύπαρκτα έως σοβαρά επιζήμια για την επιβίωση του οργανισμού.

5.13 Επισήμανση των πληροφοριών

Έλεγχος

Θα πρέπει να αναπτυχθεί και να εφαρμοστεί ένα κατάλληλο σύνολο διαδικασιών για την επισήμανση των πληροφοριών σύμφωνα με το σύστημα ταξινόμησης των πληροφοριών που έχει υιοθετήσει ο οργανισμός.

Σκοπός αυτού του ελέγχου είναι να διευκολύνει την επικοινωνία της ταξινόμησης των πληροφοριών και να υποστηρίξει την αυτοματοποίηση της επεξεργασίας και της διαχείρισης των πληροφοριών. Δεν εμπίπτουν όλες οι πληροφορίες στην ίδια κατηγορία, όπως αναφέρεται στο σημείο 5.12 ανωτέρω. Επομένως, είναι σημαντικό να επισημαίνονται όλες οι πληροφορίες σύμφωνα με την ταξινόμησή τους. Όταν γίνεται χειρισμός, αποθήκευση ή ανταλλαγή πληροφοριών, μπορεί να είναι ζωτικής σημασίας να γνωρίζουμε την ταξινόμηση του αντικειμένου. Οι ετικέτες πρέπει να είναι εύκολα αναγνωρίσιμες. Οι διαδικασίες θα πρέπει να παρέχουν οδηγίες σχετικά με το πού και πώς τοποθετούνται οι ετικέτες, λαμβάνοντας υπόψη τον τρόπο πρόσβασης στις πληροφορίες ή το χειρισμό των περιουσιακών στοιχείων ανάλογα με τους τύπους των μέσων αποθήκευσης.

5.14 Μεταφορά πληροφοριών

Έλεγχος

Θα πρέπει να υπάρχουν κανόνες, διαδικασίες ή συμφωνίες μεταφοράς πληροφοριών για όλους τους τύπους εγκαταστάσεων μεταφοράς εντός του οργανισμού και μεταξύ του οργανισμού και άλλων μερών.

Σκοπός αυτού του ελέγχου είναι η διατήρηση της ασφάλειας των πληροφοριών που μεταφέρονται εντός ενός οργανισμού και με κάθε εξωτερικό ενδιαφερόμενο μέρος. Οι πληροφορίες μοιράζονται εντός και εκτός του οργανισμού. Θα πρέπει να υπάρχει πρωτόκολλο για όλους τους τύπους ανταλλαγής πληροφοριών, συμπεριλαμβανομένων των ψηφιακών εγγράφων, των φυσικών εγγράφων, των βίντεο, αλλά και της προφορικής επικοινωνίας. Οι σαφείς κανόνες σχετικά με τον τρόπο με τον οποίο οι πληροφορίες μπορούν να μοιράζονται με ασφάλεια συμβάλλουν στη μείωση του κινδύνου μόλυνσης και διαρροής πληροφοριών. Των πληροφοριών που διαμοιράζονται μεταξύ του οργανισμού και εξωτερικών μερών πρέπει να προηγείται συμφωνία μεταφοράς πληροφοριών. Με αυτόν τον τρόπο, η πηγή, το περιεχόμενο, η εμπιστευτικότητα, το μέσο μεταφοράς και ο προορισμός της μεταφοράς πληροφοριών είναι γνωστά και συμφωνούνται και από τα δύο μέρη. Η επιχειρηματική επικοινωνία γίνεται συχνά μέσω ηλεκτρονικών μηνυμάτων. Συνιστάται στους οργανισμούς να έχουν μια επισκόπηση των εγκεκριμένων τύπων ηλεκτρονικών μηνυμάτων και να τεκμηριώνουν τον τρόπο με τον οποίο αυτά προστατεύονται και μπορούν να χρησιμοποιηθούν.

5.15 Έλεγχος πρόσβασης

Έλεγχος

Οι κανόνες για την επιθεώρηση της φυσικής και λογικής πρόσβασης σε πληροφορίες και άλλα συναφή περιουσιακά στοιχεία θα πρέπει να καθιερωθούν και να εφαρμοστούν με βάση τις επιχειρησιακές απαιτήσεις και τις απαιτήσεις ασφάλειας των πληροφοριών.

Σκοπός αυτού του ελέγχου είναι να διασφαλιστεί η εξουσιοδοτημένη πρόσβαση και να αποτραπεί η μη εξουσιοδοτημένη πρόσβαση σε πληροφορίες και άλλα συναφή περιουσιακά στοιχεία. Θα πρέπει να υπάρχει μια πολιτική ελέγχου πρόσβασης που να καθορίζει τον τρόπο διαχείρισης της πρόσβασης και το ποιος επιτρέπεται να έχει πρόσβαση σε τι. Οι κανόνες ανά περιουσιακό στοιχείο ανήκουν στους ιδιοκτήτες των περιουσιακών στοιχείων, οι οποίοι θέτουν απαιτήσεις, περιορισμούς και δικαιώματα για την πρόσβαση στο "δικό τους" περιουσιακό στοιχείο. Συχνά χρησιμοποιούμενοι όροι σε μια πολιτική ελέγχου πρόσβασης είναι η ανάγκη γνώσης και η ανάγκη χρήσης, όπου ο πρώτος περιορίζει τα δικαιώματα πρόσβασης μόνο σε πληροφορίες που χρειάζεται ο εργαζόμενος για να εκτελέσει το καθήκον του και ο δεύτερος περιορίζει τα δικαιώματα πρόσβασης μόνο σε εγκαταστάσεις επεξεργασίας πληροφοριών που απαιτούνται για την εκτέλεση του καθήκοντος.

5.16 Διαχείριση ταυτότητας

Έλεγχος

Θα πρέπει να γίνεται διαχείριση ολόκληρου του κύκλου ζωής των ταυτοτήτων.

Σκοπός αυτού του ελέγχου είναι να επιτρέπει τη μοναδική ταυτοποίηση των ατόμων και των συστημάτων που έχουν πρόσβαση στις πληροφορίες του οργανισμού και σε άλλα συναφή περιουσιακά στοιχεία και να επιτρέπει την κατάλληλη εκχώρηση δικαιωμάτων πρόσβασης. Για να εκχωρούνται δικαιώματα πρόσβασης σε περιουσιακά στοιχεία και δίκτυα και να παρακολουθείται ποιος πραγματικά έχει πρόσβαση, οι χρήστες πρέπει να καταχωρούνται με ένα αναγνωριστικό. Όταν ένας υπάλληλος αποχωρεί από έναν οργανισμό, το αναγνωριστικό και η πρόσβαση σε αυτό θα πρέπει να αφαιρούνται. Όταν ένας υπάλληλος χρειάζεται μόνο να μην έχει πρόσβαση, η πρόσβαση του αναγνωριστικού μπορεί να περιοριστεί. Παρόλο που η χρήση της ταυτότητας ενός άλλου υπαλλήλου μπορεί να είναι πιο γρήγορη και εύκολη για να αποκτήσετε πρόσβαση σε κάτι, αυτό δεν πρέπει να επιτρέπεται από τη διοίκηση στις περισσότερες περιπτώσεις. Η κοινή χρήση ταυτότητας καταργεί τη σύνδεση μεταξύ ενός περιορισμού πρόσβασης και ενός υπαλλήλου και καθιστά σχεδόν αδύνατο να κρατήσετε το σωστό άτομο υπεύθυνο για τις ενέργειές του. Η εκχώρηση, η τροποποίηση και τελικά η διαγραφή μιας ταυτότητας συχνά ονομάζεται κύκλος ζωής της ταυτότητας.

5.17 Πληροφορίες πιστοποίησης ταυτότητας

Έλεγχος

Η κατανομή και η διαχείριση των πληροφοριών ελέγχου ταυτότητας θα πρέπει να ελέγχεται από μια διαδικασία διαχείρισης, η οποία θα περιλαμβάνει τη συμβουλευτική του προσωπικού σχετικά με τον κατάλληλο χειρισμό των πληροφοριών ελέγχου ταυτότητας.

Ο σκοπός αυτού του ελέγχου είναι να διασφαλίσει την ορθή πιστοποίηση ταυτότητας οντοτήτων και να αποτρέψει τις αποτυχίες των διαδικασιών πιστοποίησης. Η διαχείριση της μυστικής πιστοποίησης, όπως οι κωδικοί πρόσβασης και οι κάρτες πρόσβασης, πρέπει να γίνεται στο πλαίσιο μιας επίσημης διαδικασίας. Άλλες σημαντικές δραστηριότητες που θα πρέπει να αναφέρονται στην πολιτική είναι, για παράδειγμα, η απαγόρευση της κοινής χρήσης μυστικών πληροφοριών πιστοποίησης, η παροχή στους νέους χρήστες ενός κωδικού πρόσβασης που πρέπει να αλλάζει κατά την πρώτη χρήση και η πιστοποίηση ενός χρήστη από όλα τα συστήματα με την απαίτηση των μυστικών πληροφοριών πιστοποίησης του χρήστη (κωδικός πρόσβασης στον υπολογιστή, κάρτα πρόσβασης για τις πόρτες).

Εάν χρησιμοποιούνται συστήματα διαχείρισης κωδικών πρόσβασης, πρέπει να παρέχουν καλούς κωδικούς πρόσβασης και να ακολουθούν αυστηρά την πολιτική μυστικών πληροφοριών ελέγχου ταυτότητας του οργανισμού. Οι ίδιοι οι κωδικοί πρόσβασης θα πρέπει να αποθηκεύονται και να διαβιβάζονται με ασφάλεια από το σύστημα διαχείρισης κωδικών πρόσβασης.

5.18 Δικαιώματα πρόσβασης

Έλεγχος

Τα δικαιώματα πρόσβασης σε πληροφορίες και άλλα συναφή περιουσιακά στοιχεία θα πρέπει να παρέχονται, να επανεξετάζονται, να τροποποιούνται και να αφαιρούνται σύμφωνα με την πολιτική και τους κανόνες ελέγχου πρόσβασης του οργανισμού για κάθε θέμα.

Σκοπός αυτού του ελέγχου είναι να διασφαλίσει ότι η πρόσβαση σε πληροφορίες και άλλα συναφή περιουσιακά στοιχεία ορίζεται και εξουσιοδοτείται σύμφωνα με τις επιχειρησιακές απαιτήσεις. Η διοίκηση

θα πρέπει να διαθέτει σύστημα για την παροχή και ανάκληση των δικαιωμάτων πρόσβασης. Συνιστάται να δημιουργείτε ορισμένους ρόλους με βάση τις δραστηριότητες που εκτελούν ορισμένοι τύποι εργαζομένων και να τους δίνετε τα ίδια βασικά δικαιώματα πρόσβασης. Μέρος της ύπαρξης ενός συστήματος είναι η ύπαρξη επιπτώσεων για απόπειρες μη εξουσιοδοτημένης πρόσβασης. Οι εργαζόμενοι δεν χρειάζεται να προσπαθούν να αποκτήσουν πρόσβαση σε χώρους που δεν θα έπρεπε, καθώς τα δικαιώματα πρόσβασης μπορούν εύκολα να ζητηθούν από τον ιδιοκτήτη ή/και τη διαχείριση του περιουσιακού στοιχείου. Οι οργανισμοί και οι εργαζόμενοί τους δεν είναι στατικοί. Οι ρόλοι αλλάζουν ή οι εργαζόμενοι αποχωρούν από την εταιρεία, αλλάζοντας συνεχώς τις ανάγκες πρόσβασης. Οι ιδιοκτήτες περιουσιακών στοιχείων θα πρέπει να επανεξετάζουν τακτικά ποιος μπορεί να έχει πρόσβαση στο περιουσιακό τους στοιχείο, ενώ η αλλαγή ρόλου ή η αποχώρηση θα πρέπει να προκαλεί την επανεξέταση των δικαιωμάτων πρόσβασης από τη διοίκηση. Δεδομένου ότι τα προνομιακά δικαιώματα πρόσβασης είναι πιο ευαίσθητα, θα πρέπει να επανεξετάζονται συχνότερα. Μόλις τερματιστεί μια σύμβαση ή συμφωνία, τα δικαιώματα πρόσβασης του παραλήπτη θα πρέπει να καταργηθούν.

5.19 Ασφάλεια πληροφοριών στις σχέσεις με τους προμηθευτές

Έλεγχος

Θα πρέπει να καθοριστούν και να εφαρμοστούν διαδικασίες και διαδικασίες για τη διαχείριση των κινδύνων ασφάλειας των πληροφοριών που συνδέονται με τη χρήση των προϊόντων ή υπηρεσιών του προμηθευτή.

Σκοπός αυτού του ελέγχου είναι η διατήρηση ενός συμφωνημένου επιπέδου ασφάλειας πληροφοριών στις σχέσεις με τους προμηθευτές. Δεδομένου ότι οι προμηθευτές έχουν πρόσβαση σε ορισμένα περιουσιακά στοιχεία, οι οργανισμοί πρέπει να θεσπίσουν μια πολιτική που να αναφέρει τις απαιτήσεις για τον μετριασμό των κινδύνων. Η πολιτική αυτή πρέπει να κοινοποιηθεί στους προμηθευτές και να συμφωνηθεί. Παραδείγματα τέτοιων απαιτήσεων είναι οι προκαθορισμένες διαδικασίες εφοδιασμού, οι υποχρεώσεις της διαδικασίας συμβάντων και για τις δύο πλευρές, οι συμφωνίες μη δημοσιοποίησης και η τεκμηρίωση της διαδικασίας εφοδιασμού.

5.20 Αντιμετώπιση της ασφάλειας των πληροφοριών στο πλαίσιο των συμφωνιών με τους προμηθευτές

Έλεγχος

Οι σχετικές απαιτήσεις για την ασφάλεια των πληροφοριών θα πρέπει να καθορίζονται και να συμφωνούνται με κάθε προμηθευτή με βάση τον τύπο της σχέσης με τον προμηθευτή.

Σκοπός αυτού του ελέγχου είναι η διατήρηση ενός συμφωνημένου επιπέδου ασφάλειας πληροφοριών στις σχέσεις με τους προμηθευτές. Κάθε προμηθευτής που με οποιονδήποτε τρόπο, άμεσα ή έμμεσα, έρχεται σε επαφή με τις πληροφορίες του οργανισμού πρέπει να ακολουθεί τις καθορισμένες απαιτήσεις ασφάλειας πληροφοριών και να συμφωνεί με αυτές. Παραδείγματα είναι οι απαιτήσεις σχετικά με την ταξινόμηση των πληροφοριών, την αποδεκτή χρήση και τα δικαιώματα ελέγχου. Μια εύκολα ξεχασμένη πτυχή μιας συμφωνίας είναι το τι πρέπει να γίνει όταν ο προμηθευτής δεν μπορεί ή δεν θα προμηθεύει πλέον. Είναι σημαντικό να εφαρμοστεί μια ρήτρα γι' αυτό.

5.21 Διαχείριση της ασφάλειας των πληροφοριών στην αλυσίδα εφοδιασμού ΤΠΕ

Έλεγχος

Θα πρέπει να καθοριστούν και να εφαρμοστούν διαδικασίες και διαδικασίες για τη διαχείριση των κινδύνων ασφάλειας των πληροφοριών που συνδέονται με την αλυσίδα εφοδιασμού προϊόντων και υπηρεσιών ΤΠΕ.

Σκοπός αυτού του ελέγχου είναι η διατήρηση ενός συμφωνημένου επιπέδου ασφάλειας πληροφοριών στις σχέσεις με τους προμηθευτές. Οι συμφωνίες με τους προμηθευτές θα πρέπει επίσης να αναφέρουν τις απαιτήσεις ασφάλειας πληροφοριών και τις συμφωνίες σχετικά με τις υπηρεσίες ΤΠΕ και την αλυσίδα εφοδιασμού. Παραδείγματα των απαιτήσεων που περιλαμβάνονται είναι η ανάγκη να είναι δυνατή η παρακολούθηση των αντικειμένων μέσω της αλυσίδας εφοδιασμού και ότι ένα ορισμένο ελάχιστο επίπεδο ασφάλειας διατηρείται σε κάθε επίπεδο της "αλυσίδας".

5.22 Παρακολούθηση, αναθεώρηση και διαχείριση αλλαγών στις υπηρεσίες των προμηθευτών

Έλεγχος

Ο οργανισμός θα πρέπει να παρακολουθεί, να επανεξετάζει, να αξιολογεί και να διαχειρίζεται τακτικά τις αλλαγές στις πρακτικές ασφάλειας πληροφοριών και στην παροχή υπηρεσιών των προμηθευτών.

Σκοπός αυτού του ελέγχου είναι η διατήρηση ενός συμφωνημένου επιπέδου ασφάλειας πληροφοριών και παροχής υπηρεσιών σύμφωνα με τις συμφωνίες με τους προμηθευτές. Όλοι κάνουν λάθη, το ίδιο και οι προμηθευτές. Είτε το λάθος έγινε κατά λάθος είτε σκόπιμα , το αποτέλεσμα είναι το ίδιο: ο οργανισμός δεν λαμβάνει ακριβώς αυτό που έχει συμφωνηθεί και η εμπιστοσύνη μπορεί να μειωθεί. Για το λόγο αυτό, οι οργανισμοί θα πρέπει να παρακολουθούν τους προμηθευτές και να τους ελέγχουν όπου κρίνουν απαραίτητο. Με αυτόν τον τρόπο, ένας οργανισμός είναι ενήμερος όταν ένας προμηθευτής κάνει κάτι ασυνήθιστο. Όπως ακριβώς συμβαίνει και με τις αλλαγές στο σύστημα, η διοίκηση πρέπει να ελέγχει τυχόν αλλαγές στις υπηρεσίες των προμηθευτών. Πρέπει να διασφαλίζουν ότι οι πολιτικές ασφάλειας των πληροφοριών είναι ενημερωμένες και να διαχειρίζονται τυχόν αλλαγές στην παροχή της ίδιας της υπηρεσίας. Μια μικρή αλλαγή στην παρεχόμενη υπηρεσία σε συνδυασμό με μια απαρχαιωμένη πολιτική ασφάλειας πληροφοριών μπορεί να οδηγήσει σε ένα μεγάλο νέο κίνδυνο. Οι αλλαγές από την πλευρά του προμηθευτή μπορούν εύκολα να συμβούν, για παράδειγμα όταν η υπηρεσία βελτιώνεται, παρέχεται μια νέα εφαρμογή ή ένα νέο σύστημα ή όταν αλλάζουν οι πολιτικές και οι διαδικασίες του προμηθευτή.

5.23 Ασφάλεια πληροφοριών για τη χρήση υπηρεσιών νέφους

Έλεγχος

Οι διαδικασίες για την απόκτηση, τη χρήση, τη διαχείριση και την έξοδο από τις υπηρεσίες νέφους θα πρέπει να καθιερωθούν σύμφωνα με τις απαιτήσεις ασφάλειας πληροφοριών του οργανισμού.

Σκοπός αυτού του ελέγχου είναι ο προσδιορισμός και η διαχείριση της ασφάλειας των πληροφοριών για τη χρήση υπηρεσιών νέφους. Οι πάροχοι υπολογιστικού νέφους προσφέρουν μια υπηρεσία που, όταν χρησιμοποιείται, αποτελεί τις περισσότερες φορές ζωτικό μέρος της υποδομής ενός οργανισμού. Τα έγγραφα του Office αποθηκεύονται στο cloud, αλλά πολλοί πάροχοι SaaS προσφέρουν το προϊόν τους στους πελάτες τους μέσω ενός παρόχου cloud, όπως το Amazon AWS, το Microsoft Azure ή το Google Cloud. Οι κίνδυνοι που περιβάλλουν αυτό το κρίσιμο τμήμα του οργανισμού θα πρέπει να μετριαστούν κατάλληλα. Οι οργανισμοί θα πρέπει να διαθέτουν διαδικασίες για τη χρήση, τη διαχείριση και την έξοδο (στρατηγική εξόδου) από ένα χρησιμοποιούμενο νέφος. Η διακοπή των δεσμών με έναν πάροχο νέφους συχνά σημαίνει ότι ένας νέος πάροχος νέφους βρίσκεται στον ορίζοντα, οπότε δεν πρέπει να ξεχνάμε ούτε την επιθεώρηση της αγοράς και της επιβίβασης σε ένα νέο νέφος. Ακριβώς όπως και κάθε άλλο λογισμικό τρίτων, ένα νέο περιβάλλον cloud θα πρέπει να σας επιτρέπει να διατηρείτε το επιθυμητό επίπεδο ασφάλειας των πληροφοριών σας και όχι να το θέτετε σε κίνδυνο.

5.24 Σχεδιασμός και προετοιμασία διαχείρισης περιστατικών ασφάλειας πληροφοριών

Σκοπός αυτού του ελέγχου είναι να διασφαλίσει τη γρήγορη, αποτελεσματική, συνεπή και ομαλή ανταπόκριση σε περιστατικά ασφάλειας πληροφοριών, συμπεριλαμβανομένης της επικοινωνίας σχετικά με συμβάντα ασφάλειας πληροφοριών. Οι οργανισμοί πρέπει να δημιουργήσουν και να τεκμηριώσουν διαδικασίες για τα περιστατικά ασφάλειας πληροφοριών και ποιος είναι υπεύθυνος για τι. Με αυτόν τον τρόπο, εάν συμβεί ένα περιστατικό ασφάλειας πληροφοριών, μπορεί να αντιμετωπιστεί αποτελεσματικά και γρήγορα. Τα περιστατικά ασφαλείας συμβαίνουν απροσδόκητα και μπορούν να προκαλέσουν αρκετό χάος, το οποίο μπορεί να μετριαστεί με την ύπαρξη ενός πρωτοκόλλου που ακολουθείται από ενημερωμένο και εκπαιδευμένο προσωπικό.

5.25 Αξιολόγηση και λήψη αποφάσεων σχετικά με συμβάντα ασφάλειας πληροφοριών

Έλεγχος

Ο οργανισμός θα πρέπει να αξιολογεί τα συμβάντα ασφάλειας πληροφοριών και να αποφασίζει εάν θα πρέπει να κατηγοριοποιηθούν ως συμβάντα ασφάλειας πληροφοριών.

Σκοπός αυτού του ελέγχου είναι να διασφαλίσει την αποτελεσματική κατηγοριοποίηση και ιεράρχηση των συμβάντων ασφάλειας πληροφοριών. Οι οργανισμοί θα πρέπει να διαθέτουν μια καλά τεκμηριωμένη μέθοδο αξιολόγησης των περιστατικών ασφαλείας. Όταν συμβεί ένα ύποπτο συμβάν, ο υπεύθυνος πρέπει να ελέγξει το συμβάν σε σχέση με τις απαιτήσεις και να καθορίσει αν υπήρξε πραγματικό συμβάν ασφάλειας πληροφοριών. Τα αποτελέσματα αυτής της αξιολόγησης θα πρέπει να τεκμηριώνονται, ώστε να μπορούν να χρησιμοποιηθούν για μελλοντική αναφορά.

5.26 Ανταπόκριση σε περιστατικά ασφάλειας πληροφοριών

Έλεγχος

Τα περιστατικά ασφάλειας πληροφοριών πρέπει να αντιμετωπίζονται σύμφωνα με τις τεκμηριωμένες διαδικασίες.

Σκοπός αυτού του ελέγχου είναι να διασφαλιστεί η αποτελεσματική και αποδοτική ανταπόκριση σε περιστατικά ασφάλειας πληροφοριών. Αυτό το σημείο φαίνεται απλό, αλλά εξακολουθεί να είναι σημαντικό να αναφερθεί και μερικές φορές είναι δύσκολο να γίνει στην πράξη. Μόλις συμβεί ένα περιστατικό ασφάλειας πληροφοριών, πρέπει να αντιμετωπιστεί σύμφωνα με τις διαδικασίες που έχουν οριστεί από το προσωπικό που έχει οριστεί. Θα πρέπει να λαμβάνονται οι προκαθορισμένες ενέργειες και να τεκμηριώνεται με ακρίβεια η όλη διαδικασία. Αυτό συμβάλλει στην πρόληψη μελλοντικών περιστατικών και στην εξάλειψη των σχετικών τρωτών σημείων ασφαλείας.

5.27 Μάθηση από περιστατικά ασφάλειας πληροφοριών

Έλεγχος

Οι γνώσεις που αποκτώνται από τα περιστατικά ασφάλειας πληροφοριών θα πρέπει να χρησιμοποιούνται για την ενίσχυση και τη βελτίωση των ελέγχων ασφάλειας πληροφοριών.

Σκοπός αυτού του ελέγχου είναι να μειώσει την πιθανότητα ή τις συνέπειες μελλοντικών περιστατικών. Παρόλο που τα περιστατικά είναι ανεπιθύμητα, εξακολουθούν να έχουν μεγάλη αξία. Η γνώση που αποκτάται από την επίλυση ενός περιστατικού θα πρέπει να χρησιμοποιείται για την πρόληψη παρόμοιων περιστατικών στο μέλλον και μπορεί να βοηθήσει στον εντοπισμό ενός πιθανού συστηματικού προβλήματος. Με τους

πρόσθετους ελέγχους, είναι σημαντικό να παρακολουθείτε το κόστος- ένας νέος έλεγχος δεν θα πρέπει να κοστίζει στον οργανισμό σε ετήσια βάση περισσότερο από τα περιστατικά που μετριάζει.

5.28 Συλλογή αποδεικτικών στοιχείων

Έλεγχος

Ο οργανισμός θα πρέπει να καθιερώσει και να εφαρμόσει διαδικασίες για τον εντοπισμό, τη συλλογή, την απόκτηση και τη διατήρηση αποδεικτικών στοιχείων που σχετίζονται με συμβάντα ασφάλειας πληροφοριών.

Σκοπός αυτού του ελέγχου είναι να διασφαλιστεί η συνεπής και αποτελεσματική διαχείριση των αποδεικτικών στοιχείων που σχετίζονται με περιστατικά ασφάλειας πληροφοριών για τους σκοπούς πειθαρχικών και νομικών ενεργειών. Μόλις συμβεί ένα ατύχημα, η αιτία δεν είναι συνήθως άμεσα σαφής. Όταν η αιτία είναι ένα άτομο ή ένας οργανισμός, θα πρέπει να τιμωρούνται με βάση την πρόθεση και το αποτέλεσμα. Για να συνδεθεί ένα περιστατικό με μια αιτία, πρέπει να συλλεχθούν στοιχεία. Σε περίπτωση κακόβουλης ενέργειας, τα στοιχεία αυτά και ο τρόπος απόκτησής τους ενδέχεται να χρησιμοποιηθούν σε δικαστικές διαδικασίες. Για να αποφευχθεί η τυχαία ή σκόπιμη καταστροφή αποδεικτικών στοιχείων, θα πρέπει να υπάρχει μια σαφής και ασφαλής διαδικασία αναγνώρισης αποδεικτικών στοιχείων.

5.29 Ασφάλεια πληροφοριών κατά τη διάρκεια διαταραχής

Έλεγχος

Ο οργανισμός θα πρέπει να σχεδιάσει τον τρόπο με τον οποίο θα διατηρήσει την ασφάλεια των πληροφοριών σε κατάλληλο επίπεδο κατά τη διάρκεια της διαταραχής

Σκοπός αυτού του ελέγχου είναι η προστασία των πληροφοριών και άλλων σχετικών περιουσιακών στοιχείων κατά τη διάρκεια της διακοπής. Οι οργανισμοί θα πρέπει να καθορίσουν τις απαιτήσεις τους για τη συνέχεια της ασφάλειας των πληροφοριών σε περίπτωση κρίσης. Η ευκολότερη επιλογή είναι να συνεχίσετε τις συνήθεις δραστηριότητες ασφάλειας πληροφοριών όσο το δυνατόν καλύτερα σε μια δυσμενή κατάσταση. Αφού καθοριστούν και συμφωνηθούν οι απαιτήσεις από τη διοίκηση, θα πρέπει να τεθούν σε εφαρμογή διαδικασίες, σχέδια και έλεγχοι ώστε να συνεχιστεί η λειτουργία με ένα αποδεκτό επίπεδο ασφάλειας των πληροφοριών σε περίπτωση κρίσης. Καθώς οι οργανισμοί αλλάζουν, αλλάζει και ο καλύτερος τρόπος αντιμετώπισης μιας κρίσης. Ένας οργανισμός που, για παράδειγμα, διπλασίασε το μέγεθός του μέσα σε λίγα χρόνια, είναι πολύ πιθανό να επωφεληθεί από μια διαφορετική απάντηση από ό,τι πριν από ένα χρόνο. Για το λόγο αυτό, οι έλεγχοι συνέχειας της ασφάλειας των πληροφοριών πραγματοποιούνται σε τακτική βάση.

5.30 Ετοιμότητα ΤΠΕ για επιχειρησιακή συνέχεια

Έλεγχος

Η ετοιμότητα ΤΠΕ θα πρέπει να σχεδιάζεται, να υλοποιείται, να συντηρείται και να δοκιμάζεται με βάση τους στόχους επιχειρησιακής συνέχειας και τις απαιτήσεις συνέχειας ΤΠΕ.

Σκοπός αυτού του ελέγχου είναι να διασφαλιστεί η διαθεσιμότητα των πληροφοριών του οργανισμού και άλλων σχετικών περιουσιακών στοιχείων κατά τη διάρκεια διαταραχών. Κατά τον σχεδιασμό της επιχειρησιακής συνέχειας, θα πρέπει να δοθεί ιδιαίτερη προσοχή στα σενάρια όπου τα συστήματα ΤΠ αποτυγχάνουν. Θα πρέπει να υπάρχει σαφής στρατηγική για το πώς θα αποκατασταθούν τα συστήματα, ποιος θα το κάνει και πόσος χρόνος μπορεί να χρειαστεί. Θα πρέπει επίσης να είναι σαφές τι σημαίνει "αποκατάσταση" σε ένα συγκεκριμένο σενάριο, δεδομένου ότι το να λειτουργούν μόνο τα βασικά συστήματα είναι πιθανότατα αρκετό για την πρώτη εβδομάδα μετά από μια πλήρη κατάρρευση.

5.31 Προσδιορισμός νομικών, κανονιστικών, ρυθμιστικών και συμβατικών απαιτήσεων

Έλεγχος

Οι νομικές, κανονιστικές, ρυθμιστικές και συμβατικές απαιτήσεις που σχετίζονται με την ασφάλεια των πληροφοριών και η προσέγγιση του οργανισμού για την ικανοποίηση αυτών των απαιτήσεων θα πρέπει να προσδιορίζονται, να τεκμηριώνονται και να ενημερώνονται.

Σκοπός αυτού του ελέγχου είναι η διασφάλιση της συμμόρφωσης με τις νομικές, κανονιστικές, ρυθμιστικές και συμβατικές απαιτήσεις που σχετίζονται με την ασφάλεια των πληροφοριών. Οι απαιτήσεις έρχονται από παντού και είναι εκεί για να ικανοποιηθούν. Συνεπώς, οι οργανισμοί θα πρέπει να έχουν μια επισκόπηση όλων των απαιτήσεων που σχετίζονται με την ασφάλεια των πληροφοριών, στις οποίες πρέπει να συμμορφωθούν, καθώς και του τρόπου με τον οποίο αυτό γίνεται. Δεδομένου ότι οι απαιτήσεις μπορούν να αλλάξουν ή να προστεθούν, η επισκόπηση της συμμόρφωσης με τις απαιτήσεις πρέπει να ενημερώνεται συνεχώς. Ένα παράδειγμα μεταβαλλόμενων απαιτήσεων είναι όταν ο οργανισμός σας επεκτείνεται σε μια νέα χώρα σε διαφορετική ήπειρο. Η χώρα αυτή είναι πιθανό να έχει διαφορετική νομοθεσία σχετικά με την προστασία της ιδιωτικής ζωής, την αποθήκευση πληροφοριών και την κρυπτογραφία.

5.32 Δικαιώματα πνευματικής ιδιοκτησίας

Έλεγχος

Ο οργανισμός θα πρέπει να εφαρμόζει κατάλληλες διαδικασίες για την προστασία των δικαιωμάτων διανοητικής ιδιοκτησίας.

Σκοπός του παρόντος ελέγχου είναι να διασφαλιστεί η συμμόρφωση με τις νομικές, καταστατικές, κανονιστικές και συμβατικές απαιτήσεις που σχετίζονται με τα δικαιώματα διανοητικής ιδιοκτησίας και τη χρήση προϊόντων ιδιοκτησίας Τα δικαιώματα διανοητικής ιδιοκτησίας (ΔΠ), που αποτελούν επίσης μέρος της νομικής συμμόρφωσης, είναι ένας τομέας που χρήζει ιδιαίτερης προσοχής. Η διανοητική ιδιοκτησία μπορεί να έχει μεγάλη αξία, γι' αυτό είναι σημαντικό να τεκμηριώνει κανείς καλά τη δική του διανοητική ιδιοκτησία και τη χρήση της διανοητικής ιδιοκτησίας άλλων. Η (τυχαία) λανθασμένη χρήση της πνευματικής ιδιοκτησίας άλλων μπορεί να οδηγήσει σε μεγάλες αγωγές και θα πρέπει να αποφεύγεται με κάθε κόστος.

5.33 Προστασία των αρχείων

Έλεγχος

Τα αρχεία πρέπει να προστατεύονται από απώλεια, καταστροφή, παραποίηση, μη εξουσιοδοτημένη πρόσβαση και μη εξουσιοδοτημένη δημοσιοποίηση.

Σκοπός αυτού του ελέγχου είναι να διασφαλιστεί η συμμόρφωση με τις νομικές, κανονιστικές και συμβατικές απαιτήσεις, καθώς και με τις προσδοκίες της κοινότητας ή της κοινωνίας σχετικά με την προστασία και τη διαθεσιμότητα των αρχείων. Οποιαδήποτε αρχεία, είτε πρόκειται για λογιστικά αρχεία είτε για αρχεία ελέγχου, θα πρέπει να προστατεύονται. Τα αρχεία κινδυνεύουν να χαθούν, να παραβιαστούν ή να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση. Οι απαιτήσεις για την προστασία των αρχείων μπορεί να προέρχονται από τον ίδιο τον οργανισμό ή από άλλες πηγές, όπως η νομοθεσία ή οι ασφαλιστικές εταιρείες. Για το σκοπό αυτό, θα πρέπει να δημιουργηθούν και να τηρηθούν αυστηρές κατευθυντήριες γραμμές.

5.34 Ιδιωτικότητα και προστασία των προσωπικών πληροφοριών που μπορούν να αναγνωριστούν (PII)

Έλεγχος

Ο οργανισμός θα πρέπει να προσδιορίζει και να πληροί τις απαιτήσεις σχετικά με τη διατήρηση της ιδιωτικής ζωής και την προστασία των προσωπικών δεδομένων σύμφωνα με τους ισχύοντες νόμους και κανονισμούς και τις συμβατικές απαιτήσεις.

Σκοπός αυτού του ελέγχου είναι να διασφαλιστεί η συμμόρφωση με τις νομικές, κανονιστικές, κανονιστικές και συμβατικές απαιτήσεις που σχετίζονται με τις πτυχές της ασφάλειας των πληροφοριών όσον αφορά την προστασία των προσωπικών πληροφοριών. Ανάλογα με τη χώρα ή τον οικονομικό χώρο στον οποίο βρίσκεται ένας οργανισμός, ενδέχεται να ισχύει διαφορετική νομοθεσία για την προστασία των προσωπικών δεδομένων. Για τους οργανισμούς που βρίσκονται στο Κατάρ ή/και επεξεργάζονται δεδομένα προσωπικού χαρακτήρα στο Κατάρ, το Κατάρ έχει εφαρμόσει τον νόμο αριθ. (13) του 2016 σχετικά με την προστασία δεδομένων προσωπικού χαρακτήρα. Οι οργανισμοί πρέπει να διασφαλίζουν ότι γνωρίζουν τις απαιτήσεις που θέτει η εν λόγω νομοθεσία και να τις ακολουθούν πιστά. Ο νόμος, για παράδειγμα, επιβάλλει τη σύναψη συμφωνιών επεξεργασίας δεδομένων, την τήρηση μητρώου δραστηριοτήτων επεξεργασίας και τη διαφάνεια της επεξεργασίας δεδομένων.

5.35 Ανεξάρτητος έλεγχος της ασφάλειας των πληροφοριών

Έλεγχος

Η προσέγγιση του οργανισμού για τη διαχείριση της ασφάλειας των πληροφοριών και η εφαρμογή της, συμπεριλαμβανομένων των ανθρώπων, των διαδικασιών και των τεχνολογιών, θα πρέπει να επανεξετάζονται ανεξάρτητα σε προγραμματισμένα χρονικά διαστήματα ή όταν συμβαίνουν σημαντικές αλλαγές.

Σκοπός αυτού του ελέγχου είναι να διασφαλίσει τη συνεχή καταλληλότητα, επάρκεια και αποτελεσματικότητα της προσέγγισης του οργανισμού για τη διαχείριση της ασφάλειας των πληροφοριών. Είναι αδύνατο για τους οργανισμούς να επανεξετάσουν αντικειμενικά το δικό τους σύστημα ασφάλειας πληροφοριών. Για το λόγο αυτό, οι οργανισμοί θα πρέπει να ελέγχουν την ασφάλεια των πληροφοριών τους από ανεξάρτητο φορέα σε τακτική βάση ή όταν συμβαίνουν μεγάλες αλλαγές. Αυτό διατηρεί την άποψη ενός οργανισμού για την ασφάλεια των πληροφοριών του σωστή και διαφανή. Ένα ανεξάρτητο μέρος μπορεί επίσης να είναι ένας εσωτερικός επιθεωρητής πλήρους απασχόλησης, ο οποίος έχει ως αποκλειστικό καθήκον τη διενέργεια των εσωτερικών ελέγχων και δεν έχει άλλα αντικρουόμενα καθήκοντα και ευθύνες.

5.36 Συμμόρφωση με τις πολιτικές και τα πρότυπα για την ασφάλεια των πληροφοριών

Έλεγχος

Η συμμόρφωση με την πολιτική ασφάλειας των πληροφοριών του οργανισμού, τις ειδικές πολιτικές, τους κανόνες και τα πρότυπα θα πρέπει να επανεξετάζεται τακτικά.

Σκοπός αυτού του ελέγχου είναι να διασφαλίσει ότι η ασφάλεια των πληροφοριών εφαρμόζεται και λειτουργεί σύμφωνα με την πολιτική ασφάλειας πληροφοριών του οργανισμού, τις πολιτικές, τους κανόνες και τα πρότυπα που αφορούν συγκεκριμένα θέματα. Με όλες αυτές τις πολιτικές, τα πρότυπα και τις διαδικασίες ασφαλείας, είναι σημαντικό για τους διαχειριστές να εξετάζουν τακτικά κατά πόσον οι δραστηριότητες ή/και οι διαδικασίες για τις οποίες είναι υπεύθυνοι συμμορφώνονται πλήρως. Για να γίνει αυτό σωστά, θα πρέπει να γνωρίζουν ακριβώς ποιοι κανόνες και απαιτήσεις πρέπει να τηρούνται και να το ελέγχουν αυτό χειροκίνητα ή με ένα αυτόματο εργαλείο αναφοράς. Τα συστήματα πληροφοριών πρέπει επίσης να επανεξετάζονται τακτικά ως προς τη συμμόρφωση. Ο ευκολότερος και συνήθως πιο οικονομικός τρόπος για να γίνει αυτό είναι η χρήση αυτοματοποιημένων εργαλείων. Αυτό το εργαλείο μπορεί να ελέγξει

γρήγορα όλες τις γωνίες ενός συστήματος και να αναφέρει ακριβώς τι πήγε/μπορεί να πάει στραβά. Οι δοκιμές ευπάθειας, όπως οι δοκιμές διείσδυσης, μπορούν να δείξουν αποτελεσματικά τυχόν αδυναμίες, αλλά μπορεί να βλάψουν το σύστημα όταν γίνονται χωρίς προσοχή.

5.37 Τεκμηριωμένες διαδικασίες λειτουργίας

Έλεγχος

Οι διαδικασίες λειτουργίας των εγκαταστάσεων επεξεργασίας πληροφοριών πρέπει να τεκμηριώνονται και να διατίθενται στο προσωπικό που τις χρειάζεται.

Σκοπός του ελέγχου αυτού είναι να διασφαλιστεί η ορθή και ασφαλής λειτουργία των εγκαταστάσεων επεξεργασίας πληροφοριών. Οι διαδικασίες λειτουργίας του εξοπλισμού πρέπει να τεκμηριώνονται και να διατίθενται σε όσους χρησιμοποιούν τον εξοπλισμό. Από την απλή διαδικασία χρήσης του υπολογιστή (από την εκκίνηση έως την απενεργοποίηση) έως τη χρήση πιο περίπλοκου εξοπλισμού θα πρέπει να υπάρχει ένας οδηγός για τον ασφαλή και σωστό χειρισμό του. Λόγω της σπουδαιότητάς τους, οι διαδικασίες θα πρέπει να αντιμετωπίζονται ως επίσημα έγγραφα, πράγμα που σημαίνει ότι τυχόν αλλαγές θα πρέπει να εγκρίνονται από τη διοίκηση.

6. Έλεγχος ατόμων

6.1 Διαλογή

Έλεγχος

Οι έλεγχοι ελέγχου του ιστορικού όλων των υποψηφίων που πρόκειται να γίνουν προσωπικό θα πρέπει να διενεργούνται πριν από την ένταξή τους στον οργανισμό και σε συνεχή βάση, λαμβάνοντας υπόψη τους ισχύοντες νόμους, κανονισμούς και δεοντολογία, και να είναι ανάλογοι με τις επιχειρηματικές απαιτήσεις, τη διαβάθμιση των πληροφοριών στις οποίες πρόκειται να αποκτήσουν πρόσβαση και τους αντιλαμβανόμενους κινδύνους.

Σκοπός αυτού του ελέγχου είναι να διασφαλιστεί ότι όλο το προσωπικό είναι κατάλληλο και κατάλληλο για τους ρόλους για τους οποίους εξετάζεται και παραμένει κατάλληλο και κατάλληλο κατά τη διάρκεια της απασχόλησής του Ένα σύστημα διαχείρισης της ασφάλειας των πληροφοριών χρειάζεται μια πολιτική για την επιθεώρηση όλων των νέων ή προαγόμενων υπαλλήλων, συμπεριλαμβανομένων των συμβούλων και του έκτακτου προσωπικού. Αυτό γίνεται για να διασφαλιστεί ότι οι εργαζόμενοι είναι ικανοί και αξιόπιστοι. Η πολιτική πρέπει να λαμβάνει υπόψη τόσο την τοπική νομοθεσία και τους κανονισμούς όσο και τον ρόλο του νέου υπαλλήλου, ώστε να διασφαλίζεται ότι ο έλεγχος είναι επαρκής αλλά όχι δυσανάλογος. Ορισμένοι ρόλοι σε έναν οργανισμό μπορεί να απαιτούν υψηλότερο επίπεδο ελέγχου, για παράδειγμα εάν οι εργαζόμενοι χειρίζονται εμπιστευτικές πληροφορίες. Ειδικά για τους ρόλους ασφάλειας πληροφοριών, ο έλεγχος θα πρέπει επίσης να περιλαμβάνει τις απαραίτητες ικανότητες και την αξιοπιστία, και αυτό θα πρέπει να τεκμηριώνεται αναλόγως.

6.2 Όροι και προϋποθέσεις απασχόλησης

Έλεγχος

Οι συμβατικές συμφωνίες απασχόλησης θα πρέπει να αναφέρουν τις ευθύνες του προσωπικού και του οργανισμού για την ασφάλεια των πληροφοριών.

Σκοπός αυτού του ελέγχου είναι να διασφαλιστεί ότι το προσωπικό κατανοεί τις ευθύνες του για την ασφάλεια των πληροφοριών για τους ρόλους για τους οποίους προορίζεται. Πριν από την έναρξη της εργασίας του, ο εργαζόμενος πρέπει να γνωρίζει την πολιτική ασφάλειας πληροφοριών του οργανισμού, συμπεριλαμβανομένων των ρόλων και των αρμοδιοτήτων του. Αυτό θα μπορούσε να κοινοποιηθεί μέσω υπογεγραμμένου κώδικα δεοντολογίας ή παρόμοιας μεθόδου. Οι συμβάσεις των εργαζομένων θα πρέπει επίσης να περιλαμβάνουν τη σχετική πολιτική ασφάλειας πληροφοριών του οργανισμού, συμπεριλαμβανομένης μιας συμφωνίας εμπιστευτικότητας, εάν ο εργαζόμενος θα έχει πρόσβαση σε εμπιστευτικές πληροφορίες.

6.3 Ευαισθητοποίηση, εκπαίδευση και κατάρτιση για την ασφάλεια των πληροφοριών

Έλεγχος

Το προσωπικό του οργανισμού και τα σχετικά ενδιαφερόμενα μέρη θα πρέπει να λαμβάνουν την κατάλληλη ενημέρωση, εκπαίδευση και κατάρτιση σε θέματα ασφάλειας πληροφοριών και τακτική ενημέρωση της πολιτικής ασφάλειας πληροφοριών του οργανισμού, των ειδικών πολιτικών και διαδικασιών, όπως αυτές σχετίζονται με τα καθήκοντα εργασίας τους.

Σκοπός αυτού του ελέγχου είναι να διασφαλιστεί ότι το προσωπικό και τα σχετικά ενδιαφερόμενα μέρη γνωρίζουν και εκπληρώνουν τις ευθύνες τους για την ασφάλεια των πληροφοριών. Οι εργαζόμενοι χρειάζονται εκπαίδευση για την ασφάλεια των πληροφοριών όταν εντάσσονται στον οργανισμό ή αλλάζουν ρόλο. Το προσωπικό που υπηρετεί επί μακρόν πρέπει επίσης να διατηρεί την ευαισθητοποίησή του με τακτική εκπαίδευση και επικοινωνία. Η κατάρτιση πρέπει να είναι σχετική με τον ρόλο. Για πολλά μέλη του προσωπικού, αυτό θα περιλαμβάνει βασικά στοιχεία, όπως υπενθυμίσεις σχετικά με την ασφάλεια των κωδικών πρόσβασης και τις επιθέσεις κοινωνικής μηχανικής. Για το τεχνικό προσωπικό ή για όσους χειρίζονται εμπιστευτικό υλικό απαιτείται πιο εμπεριστατωμένη εκπαίδευση για τον συγκεκριμένο ρόλο τους.

6.4 Πειθαρχική διαδικασία

Έλεγχος

Θα πρέπει να επισημοποιηθεί και να κοινοποιηθεί μια πειθαρχική διαδικασία για τη λήψη μέτρων κατά του προσωπικού και άλλων σχετικών ενδιαφερομένων μερών που έχουν διαπράξει παραβίαση της πολιτικής για την ασφάλεια των πληροφοριών.

Σκοπός αυτού του ελέγχου είναι να διασφαλιστεί ότι το προσωπικό και τα άλλα ενδιαφερόμενα μέρη κατανοούν τις συνέπειες της παραβίασης της πολιτικής ασφάλειας πληροφοριών, να αποτρέψουν και να αντιμετωπίσουν κατάλληλα το προσωπικό και τα άλλα ενδιαφερόμενα μέρη που διέπραξαν την παραβίαση. Θα πρέπει να υπάρχει πολιτική για την πειθαρχική διαδικασία μετά από επιβεβαιωμένη παραβίαση της πολιτικής για την ασφάλεια των πληροφοριών. Η πειθαρχική διαδικασία θα πρέπει να είναι αναλογική και κλιμακωτή, με ενέργειες που εξαρτώνται από τη σοβαρότητα του περιστατικού, την πρόθεση, το κατά πόσον πρόκειται για επαναλαμβανόμενο αδίκημα και, κυρίως, το κατά πόσον ο εργαζόμενος είχε εκπαιδευτεί επαρκώς. Πολλά καταγεγραμμένα περιστατικά ασφαλείας θα είναι αποτέλεσμα παραβίασης της πολιτικής και θα πρέπει να οδηγήσουν σε πειθαρχικά μέτρα. Αυτό είναι σημαντικό να το θυμάστε, διότι το προσωπικό θα πρέπει να αποφεύγει να αναφέρει περιστατικά ασφαλείας υπό το φόβο πειθαρχικής δίωξης.

6.5 Ευθύνες μετά τη λήξη ή την αλλαγή της απασχόλησης

Έλεγχος

Οι ευθύνες και τα καθήκοντα για την ασφάλεια των πληροφοριών που εξακολουθούν να ισχύουν μετά τη λήξη ή την αλλαγή της απασχόλησης θα πρέπει να καθορίζονται, να επιβάλλονται και να κοινοποιούνται στο σχετικό προσωπικό και σε άλλα ενδιαφερόμενα μέρη.

Σκοπός αυτού του ελέγχου είναι η προστασία των συμφερόντων του οργανισμού στο πλαίσιο της διαδικασίας αλλαγής ή τερματισμού της απασχόλησης ή των συμβάσεων. Οι ευθύνες για την ασφάλεια των πληροφοριών δεν λήγουν με την αλλαγή ή τον τερματισμό της απασχόλησης. Οι όροι και οι προϋποθέσεις απασχόλησης του εργαζομένου θα πρέπει να περιλαμβάνουν συμφωνίες εμπιστευτικότητας, οι οποίες απαιτούν από τον εργαζόμενο να τηρεί το απόρρητο των πληροφοριών μετά την αποχώρησή του από τον οργανισμό. Όταν ένας υπάλληλος αποχωρεί, μπορεί επίσης να αφήσει κενό ρόλο στην ασφάλεια πληροφοριών. Για να διατηρηθεί η συνέχεια της ασφάλειας, η διοίκηση πρέπει να προσδιορίσει αυτούς τους ρόλους, ώστε να μπορούν να μεταφερθούν.

6.6 Συμφωνίες εμπιστευτικότητας ή μη δημοσιοποίησης

Έλεγχος

Οι συμφωνίες εμπιστευτικότητας ή μη αποκάλυψης που αντικατοπτρίζουν τις ανάγκες του οργανισμού για την προστασία των πληροφοριών θα πρέπει να προσδιορίζονται, να τεκμηριώνονται, να επανεξετάζονται τακτικά και να υπογράφονται από το προσωπικό και άλλα σχετικά ενδιαφερόμενα μέρη.

Σκοπός αυτού του ελέγχου είναι η διατήρηση της εμπιστευτικότητας των πληροφοριών στις οποίες έχει πρόσβαση το προσωπικό ή εξωτερικά μέρη. Εάν η εμπιστευτικότητα των πληροφοριών είναι επαρκώς υψηλή, ενδέχεται να χρειαστεί να προστατευθεί με νομικά εκτελεστούς όρους. Στην περίπτωση αυτή, μπορούν να χρησιμοποιηθούν συμφωνίες εμπιστευτικότητας, οι οποίες καθορίζουν τις πληροφορίες που καλύπτονται, τις ευθύνες όλων των μερών, τη διάρκεια της συμφωνίας και τις κυρώσεις σε περίπτωση παραβίασης της συμφωνίας. Αυτές προστατεύουν τις πληροφορίες από την αποκάλυψη μετά την αποχώρηση του εργαζομένου από τον οργανισμό για συγκεκριμένο χρονικό διάστημα.

6.7 Απομακρυσμένη εργασία

Έλεγχος

Θα πρέπει να εφαρμόζονται μέτρα ασφαλείας όταν το προσωπικό εργάζεται εξ αποστάσεως για την προστασία των πληροφοριών στις οποίες έχει πρόσβαση, τις οποίες επεξεργάζεται ή αποθηκεύει εκτός των εγκαταστάσεων του οργανισμού.

Ο σκοπός αυτού του ελέγχου είναι να διασφαλιστεί η ασφάλεια των πληροφοριών όταν το προσωπικό εργάζεται εξ αποστάσεως. Η εξ αποστάσεως εργασία έχει γίνει πρότυπο σε πολλούς οργανισμούς, προσφέροντας τόσο στους οργανισμούς όσο και στους εργαζομένους μεγαλύτερη ευελιξία. Ωστόσο, η απομακρυσμένη εργασία έχει επιπτώσεις στην ασφάλεια των πληροφοριών, οι οποίες θα πρέπει να εξετάζονται και να τεκμηριώνονται. Η πολιτική απομακρυσμένης εργασίας θα πρέπει να περιγράφει πού και πότε επιτρέπεται η απομακρυσμένη εργασία, την παροχή συσκευών και εξοπλισμού, την εξουσιοδοτημένη πρόσβαση και τις πληροφορίες στις οποίες μπορεί να έχει πρόσβαση από απόσταση. Ιδιαίτερη σημασία έχουν οι πολιτικές που διέπουν τη χρήση ξένων δικτύων και τον κίνδυνο να ακούσουν ή να δουν εμπιστευτικές πληροφορίες φίλοι, συγγενείς ή άγνωστοι.

6.8 Αναφορά συμβάντων ασφάλειας πληροφοριών

Έλεγχος

Ο οργανισμός θα πρέπει να παρέχει στο προσωπικό μηχανισμό για την έγκαιρη αναφορά παρατηρούμενων ή ύποπτων συμβάντων ασφάλειας πληροφοριών μέσω των κατάλληλων διαύλων.

Σκοπός αυτού του ελέγχου είναι η υποστήριξη της έγκαιρης, συνεπούς και αποτελεσματικής αναφοράς συμβάντων ασφάλειας πληροφοριών που μπορούν να εντοπιστούν από το προσωπικό. Οι εργαζόμενοι αντιμετωπίζουν μερικές φορές περιστατικά ασφάλειας πληροφοριών κατά τη διάρκεια της καθημερινής τους εργασίας. Τα περιστατικά μπορεί να περιλαμβάνουν ανθρώπινα λάθη, παραβιάσεις της εμπιστευτικότητας, δυσλειτουργίες, υποψίες μόλυνσης από κακόβουλο λογισμικό και μη συμμόρφωση με την πολιτική ΔΠ ή το νόμο. Το πρώτο βήμα για τον εντοπισμό, τη διόρθωση και την πρόληψη της επανεμφάνισης περιστατικών είναι η αναφορά. Συνεπώς, οι εργαζόμενοι χρειάζονται ένα κανάλι αναφοράς και πρέπει να γνωρίζουν την ύπαρξή του.

7. Φυσικοί έλεγχοι

7.1 Φυσική περίμετρος ασφαλείας

Έλεγχος

Θα πρέπει να ορίζονται και να χρησιμοποιούνται περιμετρικές ζώνες ασφαλείας για την προστασία των περιοχών που περιέχουν πληροφορίες και άλλα συναφή περιουσιακά στοιχεία.

Σκοπός αυτού του ελέγχου είναι να αποτρέψει τη μη εξουσιοδοτημένη φυσική πρόσβαση, ζημία και παρεμβολή στις πληροφορίες του οργανισμού και σε άλλα συναφή περιουσιακά στοιχεία. Το πρώτο βήμα για την προστασία ενός φυσικού χώρου είναι ο καθορισμός της περιμέτρου του. Στη συνέχεια, μπορούν να εντοπιστούν οι ευαίσθητες ή κρίσιμες περιοχές εντός της περιμέτρου. Η περίμετρος πρέπει να είναι επαρκώς ασφαλής για την προστασία του περιεχομένου, με συναγερμούς και συστήματα ανίχνευσης εισβολέων. Εάν είναι απαραίτητο, μια ελεγχόμενη υποδοχή μπορεί να ελέγχει την πρόσβαση. Η εικόνα στην κορυφή αυτού του άρθρου είναι ένα παράδειγμα σχεδίου ζώνης που δείχνει την περίμετρο και τις ασφαλείς περιοχές.

7.2 Φυσικοί έλεγχοι εισόδου

Έλεγχος

Οι ασφαλείς χώροι θα πρέπει να προστατεύονται από κατάλληλους ελέγχους εισόδου και σημεία πρόσβασης.

Σκοπός αυτού του ελέγχου είναι να διασφαλιστεί ότι υπάρχει μόνο εξουσιοδοτημένη φυσική πρόσβαση στις πληροφορίες του οργανισμού και σε άλλα συναφή περιουσιακά στοιχεία. Μόνο εξουσιοδοτημένα άτομα θα πρέπει να μπορούν να έχουν πρόσβαση σε περιουσιακά στοιχεία και πληροφορίες. Το επίπεδο των περιορισμών εξαρτάται από τις οργανωτικές απαιτήσεις. Τα πράγματα που πρέπει να εξετάσετε περιλαμβάνουν την προσωπική ταυτοποίηση και την καταγραφή των ατόμων που έχουν πρόσβαση στις εγκαταστάσεις. Θα πρέπει να υπάρχει μια διαδικασία για την υποδοχή των επισκεπτών ώστε να διαπιστώνεται η ταυτότητά τους, πού μπορούν να πάνε και αν πρέπει να συνοδεύονται. Οι παραδόσεις αποτελούν επίσης κίνδυνο, τόσο επειδή οι χώροι παράδοσης πρέπει να ασφαλίζονται όσο και για να αποτρέπεται η είσοδος του προσωπικού παράδοσης σε απαγορευμένους χώρους.

7.3 Ασφάλιση γραφείων, χώρων και εγκαταστάσεων

Έλεγχος

Θα πρέπει να σχεδιαστεί και να εφαρμοστεί η φυσική ασφάλεια των γραφείων, των χώρων και των εγκαταστάσεων.

Σκοπός αυτού του ελέγχου είναι να αποτρέψει τη μη εξουσιοδοτημένη φυσική πρόσβαση, τη ζημία και την παρέμβαση στις πληροφορίες του οργανισμού και σε άλλα συναφή περιουσιακά στοιχεία σε γραφεία, χώρους και εγκαταστάσεις. Τα γραφεία πρέπει να ασφαλίζονται με ψηφιακά ή φυσικά κλειδιά. Γενικά, οι λεπτομερείς κατάλογοι και οι χάρτες δεν πρέπει να είναι ανοικτά προσβάσιμοι, καθώς μπορούν να αναδείξουν τη θέση ευαίσθητων περιουσιακών στοιχείων.

7.4 Παρακολούθηση της φυσικής ασφάλειας

Έλεγχος

Οι χώροι θα πρέπει να παρακολουθούνται συνεχώς για μη εξουσιοδοτημένη φυσική πρόσβαση.

Σκοπός αυτού του ελέγχου είναι να ανιχνεύει και να αποτρέπει τη μη εξουσιοδοτημένη φυσική πρόσβαση. Η παρακολούθηση μπορεί να αποτρέψει τους εισβολείς και να ανιχνεύσει την εισβολή. Φρουροί, κάμερες και συναγερμοί παρακολουθούν την μη εξουσιοδοτημένη πρόσβαση. Ο σχεδιασμός οποιουδήποτε συστήματος παρακολούθησης θα πρέπει να θεωρείται εμπιστευτικός. Απαιτούνται τακτικές δοκιμές για να διασφαλιστεί η λειτουργία του συστήματος. Τα συστήματα παρακολούθησης με κάμερες και άλλα συστήματα παρακολούθησης που συλλέγουν προσωπικές πληροφορίες ή μπορούν να χρησιμοποιηθούν για την παρακολούθηση ατόμων μπορεί να απαιτούν ιδιαίτερη προσοχή σύμφωνα με τους νόμους περί προστασίας δεδομένων. Για παράδειγμα, η επιτήρηση με κάμερες μπορεί να απαιτεί εκτίμηση αντικτύπου για την προστασία των δεδομένων σύμφωνα με τη νομοθεσία GDPR.

7.5 Προστασία από φυσικές και περιβαλλοντικές απειλές

Έλεγχος

Θα πρέπει να σχεδιαστεί και να εφαρμοστεί η προστασία από φυσικές και περιβαλλοντικές απειλές, όπως φυσικές καταστροφές και άλλες σκόπιμες ή ακούσιες φυσικές απειλές για τις υποδομές.

Σκοπός αυτού του ελέγχου είναι η πρόληψη ή η μείωση των συνεπειών των γεγονότων που προέρχονται από φυσικές και περιβαλλοντικές απειλές Φυσικές ή ανθρωπογενείς καταστροφές και φυσικές επιθέσεις απειλούν την ασφάλεια των πληροφοριών και την επιχειρησιακή συνέχεια. Το επίπεδο αυτών των κινδύνων εξαρτάται σε μεγάλο βαθμό από την τοποθεσία. Οι πλημμύρες, οι πυρκαγιές και οι μεγάλες καταιγίδες είναι οι πιο πιθανοί κίνδυνοι, αλλά ο κίνδυνος από σεισμούς, πολιτικές αναταραχές και τρομοκρατικές επιθέσεις μπορεί επίσης να ληφθεί υπόψη στις εκτιμήσεις κινδύνου.

7.6 Εργασία σε ασφαλείς χώρους

Έλεγχος

Θα πρέπει να σχεδιαστούν και να εφαρμοστούν μέτρα ασφαλείας για την εργασία σε ασφαλείς χώρους.

Σκοπός αυτού του ελέγχου είναι η προστασία των πληροφοριών και άλλων συναφών περιουσιακών στοιχείων σε ασφαλείς χώρους από ζημιές και μη εξουσιοδοτημένες παρεμβάσεις από το προσωπικό που εργάζεται στους χώρους αυτούς. Η ύπαρξη και ο σκοπός των ασφαλών περιβαλλόντων θα πρέπει να κοινοποιούνται μόνο όταν υπάρχει ανάγκη για γνώση. Θα πρέπει να φυλάσσονται κλειδωμένα, με πρόσβαση μόνο σε εξουσιοδοτημένα άτομα. Γενικά, η μοναχική εργασία θα πρέπει να αποθαρρύνεται, τόσο για λόγους ασφαλείας όσο και για λόγους προστασίας.

7.7 Καθαρό γραφείο και καθαρή οθόνη

Έλεγχος

Θα πρέπει να καθοριστούν και να εφαρμοστούν κατάλληλα σαφείς κανόνες γραφείου για τα έγγραφα και τα αφαιρούμενα μέσα αποθήκευσης και σαφείς κανόνες οθόνης για τις εγκαταστάσεις επεξεργασίας πληροφοριών.

Σκοπός αυτού του ελέγχου είναι να μειωθούν οι κίνδυνοι μη εξουσιοδοτημένης πρόσβασης, απώλειας και καταστροφής των πληροφοριών στα γραφεία, στις οθόνες και σε άλλα προσβάσιμα σημεία κατά τη διάρκεια των κανονικών ωρών εργασίας και εκτός αυτών. Οι ευαίσθητες πληροφορίες που παραμένουν στα γραφεία, τις οθόνες, τους εκτυπωτές και τους πίνακες μπορούν να προσπελαστούν από οποιονδήποτε.Μια σαφής πολιτική για τα γραφεία και τις οθόνες ορίζει πώς και πού μπορεί να γίνει πρόσβαση στις πληροφορίες. Μια βασική πολιτική περιλαμβάνει την απαγόρευση εκτυπωμένων εγγράφων που αφήνονται χωρίς επιτήρηση, είτε στους χώρους εργασίας είτε στους εκτυπωτές (καθαρό γραφείο) και κλειδωμένες οθόνες συσκευών (καθαρή οθόνη). Για ευαίσθητες πληροφορίες μπορεί να απαιτούνται πιο λεπτομερείς πολιτικές, για παράδειγμα ότι οι πληροφορίες δεν μπορούν να προβληθούν σε οθόνη σε ανοιχτό περιβάλλον.

7.8 Τοποθέτηση και προστασία του εξοπλισμού

Έλεγχος

Ο εξοπλισμός πρέπει να τοποθετείται με ασφάλεια και να προστατεύεται.

Σκοπός αυτού του ελέγχου είναι η μείωση των κινδύνων από φυσικές και περιβαλλοντικές απειλές, καθώς και από μη εξουσιοδοτημένη πρόσβαση και ζημία. Η προσεκτική παραπομπή του εξοπλισμού μπορεί να ελαχιστοποιήσει πολλούς κινδύνους: όχι μόνο τη μη εξουσιοδοτημένη πρόσβαση, αλλά και τους κινδύνους που οφείλονται σε περιβαλλοντικούς παράγοντες, χυμένα τρόφιμα και ποτά, βανδαλισμούς και υποβάθμιση λόγω φωτός ή υγρασίας. Η απαιτούμενη προστασία εξαρτάται από την ευαισθησία του εξοπλισμού.

7.9 Ασφάλεια περιουσιακών στοιχείων εκτός εγκαταστάσεων

Έλεγχος

Τα περιουσιακά στοιχεία εκτός του τόπου εγκατάστασης πρέπει να προστατεύονται.

Σκοπός αυτού του ελέγχου είναι να αποτρέψει την απώλεια, τη ζημία, την κλοπή ή τη διακινδύνευση των συσκευών εκτός του χώρου εγκατάστασης και τη διακοπή των λειτουργιών του οργανισμού. Οι συσκευές, συμπεριλαμβανομένων των ιδιωτικών συσκευών (φέρτε τις δικές σας συσκευές), εξακολουθούν να χρειάζονται προστασία όταν φεύγουν από τις εγκαταστάσεις. Τα βασικά στοιχεία περιλαμβάνουν κατάλληλη φυσική προστασία, όπως καλύμματα, και πρόληψη κλοπής με το να μην αφήνετε τις συσκευές αφύλακτες. Ο οργανισμός θα πρέπει να γνωρίζει ποιες συσκευές χρησιμοποιούνται εκτός των εγκαταστάσεων, από ποιον και σε ποιες πληροφορίες έχει πρόσβαση ή ποιες χρησιμοποιούνται όταν βρίσκονται εκτός εγκαταστάσεων.

7.10 Μέσα αποθήκευσης

Έλεγχος

Η διαχείριση των αποθηκευτικών μέσων θα πρέπει να γίνεται κατά τη διάρκεια του κύκλου ζωής τους: απόκτηση, χρήση, μεταφορά και απόρριψη, σύμφωνα με το σύστημα ταξινόμησης και τις απαιτήσεις χειρισμού του οργανισμού.

Σκοπός αυτού του ελέγχου είναι να διασφαλίζεται ότι οι πληροφορίες στα μέσα αποθήκευσης αποκαλύπτονται, τροποποιούνται, αφαιρούνται ή καταστρέφονται μόνο κατόπιν εξουσιοδότησης. Οι πληροφορίες που είναι αποθηκευμένες σε οποιαδήποτε μορφή μέσων ενημέρωσης ενέχουν τον κίνδυνο μη εξουσιοδοτημένης πρόσβασης και απώλειας της ακεραιότητας των πληροφοριών μέσω τροποποίησης ή υποβάθμισης, απώλειας, καταστροφής ή αφαίρεσης. Συνεπώς, τα μέσα θα πρέπει να αποθηκεύονται με ασφάλεια και τελικά να καταστρέφονται με ασφάλεια. Οι πολιτικές που διέπουν τη διαχείριση των αφαιρούμενων μέσων θα πρέπει να καλύπτουν ποιες πληροφορίες μπορούν να αποθηκευτούν σε αφαιρούμενα μέσα, την καταχώριση και τον εντοπισμό αυτών των μέσων, τον τρόπο ασφαλούς αποθήκευσης για την αποτροπή μη εξουσιοδοτημένης πρόσβασης ή υποβάθμισης και τον τρόπο μεταφοράς τους. Όταν η αποθήκευση δεν απαιτείται πλέον, είναι απαραίτητη η ασφαλής καταστροφή. Αυτό μπορεί να γίνει από εξωτερικό μέρος.

7.11 Υποστηρικτικές υπηρεσίες κοινής ωφέλειας

Έλεγχος

Οι εγκαταστάσεις επεξεργασίας πληροφοριών θα πρέπει να προστατεύονται από διακοπές ρεύματος και άλλες διαταραχές που προκαλούνται από βλάβες στις υποστηρικτικές υπηρεσίες κοινής ωφέλειας.

Σκοπός αυτού του ελέγχου είναι να αποτρέψει την απώλεια, τη ζημία ή τη διακινδύνευση των πληροφοριών και άλλων σχετικών περιουσιακών στοιχείων ή τη διακοπή των λειτουργιών του οργανισμού λόγω βλάβης και διακοπής των υποστηρικτικών υπηρεσιών κοινής ωφέλειας. Οι διακοπές ρεύματος μπορούν να θέσουν άμεσα σε κίνδυνο τις δραστηριότητες μιας επιχείρησης. Λιγότερο προφανώς, οι τηλεπικοινωνίες και ο κλιματισμός θα διακόψουν τις ψηφιακές δραστηριότητες και οι βλάβες στην παροχή αερίου, αποχέτευσης ή νερού θα εμποδίσουν τους εργαζόμενους να εργαστούν στο χώρο. Τα συστήματα επιθεώρησης και συναγερμού μπορούν να εντοπίσουν πραγματικές ή πιθανές βλάβες. Τα σχέδια συνέχειας θα πρέπει να προσδιορίζουν τις επιλογές εφεδρείας και τα στοιχεία επικοινωνίας έκτακτης ανάγκης για τους παρόχους υπηρεσιών.

7.12 Ασφάλεια καλωδίωσης

Έλεγχος

Τα καλώδια που μεταφέρουν ενέργεια, δεδομένα ή υποστηρικτικές υπηρεσίες πληροφοριών πρέπει να προστατεύονται από υποκλοπές, παρεμβολές ή ζημιές.

Σκοπός αυτού του ελέγχου είναι να αποτρέψει την απώλεια, τη ζημία, την κλοπή ή τη διακινδύνευση πληροφοριών και άλλων συναφών περιουσιακών στοιχείων και τη διακοπή των λειτουργιών του οργανισμού που σχετίζονται με την καλωδίωση ισχύος και επικοινωνιών. Οι πληροφορίες και τα δεδομένα μεταφέρονται μέσω καλωδίων, ενώ οι υπολογιστές, τα συστήματα ασφαλείας και οι περιβαλλοντικοί έλεγχοι απαιτούν ρεύμα, το οποίο παρέχεται μέσω καλωδίων. Το πρώτο μπορεί να υποκλαπεί και οι διακοπές και των δύο μπορούν να θέσουν σε κίνδυνο την ασφάλεια των πληροφοριών και την επιχειρησιακή συνέχεια. Ο απαιτούμενος βαθμός ασφάλειας εξαρτάται από τον οργανισμό και σε πολλές περιπτώσεις η διαχείρισή του γίνεται από παρόχους κτιριακών εγκαταστάσεων ή εταιρείες τηλεπικοινωνιών και κοινής ωφέλειας. Οι βασικές προστασίες περιλαμβάνουν τη χρήση αγωγών καλωδίωσης ή καλυμμάτων δαπέδου καλωδίων για την αποφυγή ζημιών, καθώς και κλειδωμένη πρόσβαση σε σημεία πρόσβασης και εισόδου βοηθητικών εγκαταστάσεων.

7.13 Συντήρηση εξοπλισμού

Έλεγχος

Ο εξοπλισμός πρέπει να συντηρείται σωστά για να διασφαλίζεται η διαθεσιμότητα, η ακεραιότητα και η εμπιστευτικότητα των πληροφοριών.

Σκοπός αυτού του ελέγχου είναι να αποτρέψει την απώλεια, τη ζημία, την κλοπή ή τη διακινδύνευση πληροφοριών και άλλων σχετικών περιουσιακών στοιχείων και τη διακοπή των λειτουργιών του οργανισμού λόγω έλλειψης συντήρησης. Η συντήρηση του εξοπλισμού εισάγει δύο ζητήματα ασφάλειας πληροφοριών: ο κακώς συντηρούμενος εξοπλισμός ενέχει τον κίνδυνο απώλειας πληροφοριών, ενώ η συντήρηση ή η συντήρηση του εξοπλισμού μπορεί να εκθέσει πληροφορίες σε εξωτερικά ή μη εξουσιοδοτημένα μέρη. Ο τακτικά συντηρούμενος και ενημερωμένος εξοπλισμός είναι λιγότερο πιθανό να χρειαστεί πιο επικίνδυνες επισκευές ή να οδηγήσει σε διακοπές λειτουργίας. Όταν απαιτούνται επισκευές, θα πρέπει να δίνεται προσοχή στην επιλογή των παρόχων υπηρεσιών και στην επιθεώρηση των εργασιών τους.

7.14 Ασφαλής διάθεση ή επαναχρησιμοποίηση του εξοπλισμού

Έλεγχος

Τα είδη εξοπλισμού που περιέχουν αποθηκευτικά μέσα θα πρέπει να επαληθεύονται ώστε να διασφαλίζεται ότι τυχόν ευαίσθητα δεδομένα και αδειοδοτημένο λογισμικό έχουν αφαιρεθεί ή αντικατασταθεί με ασφάλεια πριν από την απόρριψη ή την επαναχρησιμοποίηση.

Ο σκοπός αυτού του ελέγχου είναι να αποτραπεί η διαρροή πληροφοριών από τον εξοπλισμό που πρόκειται να διατεθεί ή να επαναχρησιμοποιηθεί. Ο εξοπλισμός που δεν χρησιμοποιείται πλέον μπορεί να έχει ακόμη εγκατεστημένο λογισμικό με άδεια χρήσης ή αποθηκευμένα ευαίσθητα δεδομένα. Αυτό ισχύει και για τον εξοπλισμό που απαιτεί επισκευή και θα πρέπει να λαμβάνεται υπόψη όταν αποφασίζεται αν θα χρησιμοποιηθούν εξωτερικές υπηρεσίες επισκευής. Οι τυπικές λειτουργίες διαγραφής ενδέχεται να μην είναι επαρκείς για την αφαίρεση ευαίσθητων πληροφοριών. Αντίθετα, οι εξειδικευμένες μέθοδοι καταστροφής, διαγραφής ή αντικατάστασης μειώνουν τον κίνδυνο παραμονής υπολειπόμενων πληροφοριών στα μέσα αποθήκευσης. Θυμηθείτε να αφαιρέσετε και τις φυσικές ετικέτες ή σημάνσεις!

8. Τεχνολογικοί έλεγχοι

8.1 Συσκευές τελικού σημείου χρήστη

Έλεγχος

Οι πληροφορίες που είναι αποθηκευμένες, υποβάλλονται σε επεξεργασία ή είναι προσβάσιμες μέσω των τελικών συσκευών των χρηστών θα πρέπει να προστατεύονται.

Ο σκοπός αυτού του ελέγχου είναι η προστασία των πληροφοριών από τους κινδύνους που ενέχει η χρήση τελικών συσκευών των χρηστών. Οι συσκευές τελικού σημείου χρήστη είναι οποιεσδήποτε συσκευές από τις οποίες μπορεί να γίνει πρόσβαση σε πληροφορίες, να υποβληθούν σε επεξεργασία ή να αποθηκευτούν πληροφορίες. Περιλαμβάνουν φορητούς υπολογιστές, smartphones και PC. Μια πολιτική για τις συσκευές τελικών σημείων των χρηστών θα πρέπει να περιλαμβάνει την εγγραφή, τη φυσική προστασία, τον κωδικό πρόσβασης και την κρυπτογραφική προστασία, καθώς και την υπεύθυνη χρήση. Η υπεύθυνη χρήση περιλαμβάνει την επιθεώρηση των ατόμων που έχουν πρόσβαση στη συσκευή, την εγκατάσταση λογισμικού, την τακτική ενημέρωση του λειτουργικού συστήματος και τη δημιουργία αντιγράφων ασφαλείας της συσκευής. Ένας οργανισμός μπορεί να απαιτεί μια ειδική πολιτική για το bring-your-own-device για την πρόληψη των διαφορών και των σχετικών κινδύνων για την ασφάλεια των πληροφοριών.

8.2 Προνομιακά δικαιώματα πρόσβασης

Έλεγχος

Η κατανομή και η χρήση προνομιακών δικαιωμάτων πρόσβασης πρέπει να περιορίζεται και να διαχειρίζεται.

Ο σκοπός αυτού του ελέγχου είναι να διασφαλιστεί ότι μόνο εξουσιοδοτημένοι χρήστες, στοιχεία λογισμικού και υπηρεσίες έχουν προνομιακά δικαιώματα πρόσβασης.Η χορήγηση προνομιακών ή διαχειριστικών δικαιωμάτων πρόσβασης σε χρήστες, στοιχεία λογισμικού και συστήματα πρέπει να γίνεται κατά περίπτωση και μόνο όταν χρειάζεται. Αυτό σημαίνει ότι πρέπει να υπάρχει πολιτική που να καθορίζει πότε μπορούν να χορηγηθούν δικαιώματα πρόσβασης και πότε πρέπει να λήξουν ή να ανακληθούν.Όταν χορηγούνται προνομιακά δικαιώματα πρόσβασης, ο χρήστης πρέπει να κατανοεί για ποιο λόγο και πότε πρέπει να τα χρησιμοποιεί. Το πρώτο βήμα είναι ότι οι προνομιούχοι χρήστες θα πρέπει πάντα να γνωρίζουν ότι έχουν δικαιώματα πρόσβασης διαχειριστή. Αυτά τα δικαιώματα δεν θα πρέπει να χρησιμοποιούνται για καθημερινές εργασίες, οι οποίες θα πρέπει πάντα να γίνονται με λογαριασμούς τυπικής πρόσβασης. Η προνομιακή πρόσβαση θα πρέπει να χρησιμοποιείται μόνο όταν εκτελούνται εργασίες διαχειριστή.

8.3 Περιορισμός πρόσβασης σε πληροφορίες

Έλεγχος

Η πρόσβαση στις πληροφορίες και σε άλλα συναφή περιουσιακά στοιχεία θα πρέπει να περιορίζεται σύμφωνα με την καθιερωμένη πολιτική ελέγχου πρόσβασης ανά θέμα.

Ο σκοπός αυτού του ελέγχου είναι να διασφαλίζεται μόνο η εξουσιοδοτημένη πρόσβαση και να αποτρέπεται η μη εξουσιοδοτημένη πρόσβαση σε πληροφορίες και άλλα συναφή περιουσιακά στοιχεία. Η πρόσβαση στις πληροφορίες και σε άλλα περιουσιακά στοιχεία θα πρέπει να βασίζεται στις επιχειρηματικές ανάγκες, με την πρόσβαση να περιορίζεται σε συγκεκριμένους χρήστες. Οι πληροφορίες δεν θα πρέπει να είναι προσβάσιμες σε ανώνυμους χρήστες, ώστε να αποφεύγεται η μη ανιχνεύσιμη και μη εξουσιοδοτημένη πρόσβαση. Αυτό είναι σημαντικό για τη διατήρηση της εμπιστευτικότητας των πληροφοριών, την παρακολούθηση της χρήσης τους και την αποτροπή της τροποποίησης και της διανομής τους.

8.4 Πρόσβαση στον πηγαίο κώδικα

Έλεγχος

Η *πρόσβαση ανάγνωσης και εγγραφής στον πηγαίο κώδικα, τα εργαλεία ανάπτυξης και τις βιβλιοθήκες λογισμικού θα πρέπει να τυγχάνουν κατάλληλης διαχείρισης*.

Σκοπός αυτού του ελέγχου είναι να αποτρέψει την εισαγωγή μη εξουσιοδοτημένων λειτουργιών, να αποφύγει ακούσιες ή κακόβουλες αλλαγές και να διατηρήσει την εμπιστευτικότητα της πολύτιμης πνευματικής ιδιοκτησίας. Ο πηγαίος κώδικας πρέπει να διατηρείται ασφαλής για την αποφυγή ανεπιθύμητων αλλαγών και για να διατηρείται ο κώδικας εμπιστευτικός. Ο ρόλος του υπαλλήλου και η επιχειρηματική ανάγκη καθορίζουν αν έχει πρόσβαση ανάγνωσης και εγγραφής. Ο περιορισμός της πρόσβασης μόνο για ανάγνωση για την πλειοψηφία του προσωπικού συμβάλλει στην προστασία της ακεραιότητας του κώδικα. Για τον ίδιο λόγο, οι προγραμματιστές θα πρέπει να χρησιμοποιούν εργαλεία ανάπτυξης που ελέγχουν τις δραστηριότητες, αντί να έχουν άμεση πρόσβαση στο αποθετήριο πηγαίου κώδικα.

8.5 Ασφαλής έλεγχος ταυτότητας

Έλεγχος

Οι *τεχνολογίες και οι διαδικασίες ασφαλούς ελέγχου ταυτότητας θα πρέπει να εφαρμόζονται με βάση τους περιορισμούς πρόσβασης στις πληροφορίες και την πολιτική ελέγχου πρόσβασης σε συγκεκριμένο θέμα*.

Ο σκοπός αυτού του ελέγχου είναι να διασφαλιστεί ότι ένας χρήστης ή μια οντότητα πιστοποιείται με ασφάλεια, όταν χορηγείται πρόσβαση σε συστήματα, εφαρμογές και υπηρεσίες Η ασφαλής πιστοποίηση ταυτότητας συμβάλλει στην εγγύηση ότι ένας χρήστης είναι αυτός που λέει ότι είναι. Η απαιτούμενη ισχύς του ελέγχου ταυτότητας εξαρτάται από την ταξινόμηση των πληροφοριών. Τα ονόματα χρήστη και οι κωδικοί πρόσβασης παρέχουν ένα βασικό επίπεδο ελέγχου ταυτότητας, το οποίο μπορεί να ενισχυθεί με τη χρήση κρυπτογραφικών ή βιομετρικών ελέγχων, έξυπνων καρτών ή μαρκών ή άλλου πολυπαραγοντικού ελέγχου ταυτότητας. Οι οθόνες σύνδεσης πρέπει να εμφανίζουν το ελάχιστο δυνατό ποσό πληροφοριών, ώστε να αποφεύγεται η παροχή βοήθειας σε μη εξουσιοδοτημένα άτομα. Όλες οι προσπάθειες σύνδεσης πρέπει να καταγράφονται, επιτυχείς ή μη, ώστε να μπορούν να εντοπιστούν επιθέσεις ή μη εξουσιοδοτημένη χρήση.

8.6 Διαχείριση χωρητικότητας

Έλεγχος

Η χρήση των πόρων θα πρέπει να παρακολουθείται και να προσαρμόζεται σύμφωνα με τις τρέχουσες και αναμενόμενες απαιτήσεις δυναμικότητας.

Σκοπός του ελέγχου αυτού είναι να διασφαλιστεί η απαιτούμενη ικανότητα των εγκαταστάσεων επεξεργασίας πληροφοριών, των ανθρώπινων πόρων, των γραφείων και άλλων εγκαταστάσεων. Η διαχείριση της χωρητικότητας καλύπτει το σύνολο των ανθρώπινων πόρων, των χώρων γραφείων και άλλων εγκαταστάσεων, όχι μόνο την επεξεργασία και αποθήκευση πληροφοριών. Οι μελλοντικές απαιτήσεις θα πρέπει να λαμβάνονται υπόψη στον επιχειρηματικό σχεδιασμό και στον σχεδιασμό ασφάλειας, ιδίως εάν η απόκτηση περιουσιακών στοιχείων έχει μεγάλο χρονικό διάστημα. Το υπολογιστικό νέφος συχνά επιτρέπει ευέλικτη διαχείριση της χωρητικότητας. Αντίθετα, οι φυσικές εγκαταστάσεις και το προσωπικό μπορεί να απαιτούν περισσότερο στρατηγικό σχεδιασμό. Η βελτιστοποίηση της φυσικής και ψηφιακής αποθήκευσης πληροφοριών, η διαγραφή παλαιών δεδομένων και η βελτιστοποίηση της επεξεργασίας παρτίδων και των εφαρμογών θα σημαίνει ότι η υπάρχουσα χωρητικότητα χρησιμοποιείται πιο αποτελεσματικά.

8.7 Προστασία από κακόβουλο λογισμικό

Έλεγχος

Η προστασία από κακόβουλο λογισμικό πρέπει να εφαρμόζεται και να υποστηρίζεται από την κατάλληλη ευαισθητοποίηση των χρηστών.

Σκοπός αυτού του ελέγχου είναι να διασφαλιστεί ότι οι πληροφορίες και άλλα σχετικά περιουσιακά στοιχεία προστατεύονται από κακόβουλο λογισμικό. Το λογισμικό ανίχνευσης κακόβουλου λογισμικού (π.χ. σαρωτές ιών) παρέχει κάποια προστασία, αλλά δεν είναι ο μόνος τρόπος προστασίας από το κακόβουλο λογισμικό. Η προστασία περιλαμβάνει επίσης ευαισθητοποίηση σε θέματα ασφάλειας πληροφοριών, ελέγχους πρόσβασης και ελέγχους διαχείρισης αλλαγών για την αποτροπή εγκατάστασης κακόβουλου λογισμικού ή πρόκλησης προβλημάτων. Ως πρώτη γραμμή άμυνας, το λογισμικό ανίχνευσης κακόβουλου λογισμικού πρέπει να εγκαθίσταται και να ενημερώνεται τακτικά. Ωστόσο, μια πολιτική για την αποτροπή της μη εξουσιοδοτημένης εγκατάστασης λογισμικού, της χρήσης ύποπτων ιστότοπων, της λήψης αρχείων από απομακρυσμένες πηγές και της ανίχνευσης ευπαθειών είναι εξίσου σημαντικές. Τέλος, οι κίνδυνοι ασφαλείας μπορούν να μειωθούν με τον ενεργό σχεδιασμό για μια επίθεση κακόβουλου λογισμικού. Η ενημέρωση για

το νέο κακόβουλο λογισμικό, η απομόνωση κρίσιμων περιβαλλόντων και η κατάρτιση σχεδίων συνέχισης της λειτουργίας σε περίπτωση επίθεσης θα συμβάλουν στη διατήρηση της συνέχειας της επιχείρησης σε περίπτωση επίθεσης.

8.8 Διαχείριση των τεχνικών τρωτών σημείων

Έλεγχος

Θα πρέπει να λαμβάνονται πληροφορίες σχετικά με τα τεχνικά τρωτά σημεία των χρησιμοποιούμενων συστημάτων πληροφοριών, να αξιολογείται η έκθεση του οργανισμού στα εν λόγω τρωτά σημεία και να λαμβάνονται τα κατάλληλα μέτρα.

Σκοπός αυτού του ελέγχου είναι να αποτρέψει την εκμετάλλευση των τεχνικών τρωτών σημείων.Η διαχείριση των τεχνικών τρωτών σημείων μπορεί να χωριστεί σε τρεις κατηγορίες: εντοπισμός, αξιολόγηση και δράση. Για τον εντοπισμό τρωτών σημείων, τα περιουσιακά στοιχεία πρέπει να καταγράφονται με λεπτομέρειες σχετικά με τον προμηθευτή, την έκδοση, την κατάσταση ανάπτυξης και τον υπεύθυνο ιδιοκτήτη. Ο πωλητής μπορεί να παρέχει πληροφορίες σχετικά με τα τρωτά σημεία, αλλά ο ιδιοκτήτης θα πρέπει να εντοπίσει πρόσθετους πόρους που παρακολουθούν και δημοσιεύουν πληροφορίες σχετικά με τα τρωτά σημεία και τις μεθόδους εντοπισμού τρωτών σημείων, όπως το pen-testing. Όταν εντοπιστεί μια ευπάθεια, πρέπει να εκτιμηθεί ο κίνδυνος και ο επείγων χαρακτήρας της, καθώς και οι πιθανοί κίνδυνοι από την εφαρμογή μιας ενημέρωσης ή επιδιόρθωσης. Οι ενημερώσεις μπορούν συχνά να χρησιμοποιηθούν για την αντιμετώπιση των ευπαθειών, αλλά μπορεί να μην επιλύουν πάντα επαρκώς το πρόβλημα και να εισάγουν νέα ζητήματα. Εάν δεν υπάρχει διαθέσιμη ενημέρωση ή η ενημέρωση θεωρείται ανεπαρκής, μέτρα όπως η παράκαμψη, η απομόνωση από το δίκτυο και η αυξημένη παρακολούθηση μπορεί να είναι επαρκή για τον μετριασμό του κινδύνου.

8.9 Διαχείριση ρυθμίσεων

Έλεγχος

Οι διαμορφώσεις, συμπεριλαμβανομένων των διαμορφώσεων ασφαλείας, του υλικού, του λογισμικού, των υπηρεσιών και των δικτύων θα πρέπει να καθορίζονται, να τεκμηριώνονται, να εφαρμόζονται, να παρακολουθούνται και να επανεξετάζονται.

Σκοπός αυτού του ελέγχου είναι να διασφαλιστεί ότι το υλικό, το λογισμικό, οι υπηρεσίες και τα δίκτυα λειτουργούν σωστά με τις απαιτούμενες ρυθμίσεις ασφαλείας και ότι η διαμόρφωση δεν αλλοιώνεται με μη εξουσιοδοτημένες ή εσφαλμένες αλλαγές. Το λογισμικό, το υλικό, οι υπηρεσίες και τα δίκτυα πρέπει να ρυθμιστούν ώστε να λειτουργούν σωστά με τις ρυθμίσεις ασφαλείας που θεωρούνται απαραίτητες για την προστασία του οργανισμού. Η διαμόρφωση θα πρέπει να βασίζεται στις επιχειρηματικές ανάγκες και τις γνωστές απειλές. Όπως συμβαίνει με όλα τα ασφαλή συστήματα, η προνομιακή πρόσβαση θα πρέπει να περιορίζεται και οι περιττές λειτουργίες να απενεργοποιούνται. Οι αλλαγές διαμόρφωσης πρέπει να ακολουθούν τη διαδικασία διαχείρισης αλλαγών και να εγκρίνονται και να τεκμηριώνονται πλήρως.

8.10 Διαγραφή πληροφοριών

Έλεγχος

Οι πληροφορίες που είναι αποθηκευμένες σε συστήματα πληροφοριών, συσκευές ή σε οποιοδήποτε άλλο μέσο αποθήκευσης πρέπει να διαγράφονται όταν δεν χρειάζονται πλέον.

Σκοπός αυτού του ελέγχου είναι να αποτρέψει την άσκοπη έκθεση ευαίσθητων πληροφοριών και να συμμορφωθεί με τις νομικές, καταστατικές, κανονιστικές και συμβατικές απαιτήσεις για τη διαγραφή πληροφοριών. Οι πληροφορίες δεν θα πρέπει να διατηρούνται για περισσότερο χρόνο από ό,τι είναι απαραίτητο προκειμένου να μειωθεί ο κίνδυνος έκθεσης στην ασφάλεια των πληροφοριών, να βελτιστοποιηθεί η χρήση των πόρων και να συμμορφωθούν με τους νόμους . Θα πρέπει να χρησιμοποιείται εγκεκριμένο λογισμικό ασφαλούς διαγραφής για να διασφαλίζεται η μόνιμη διαγραφή και να χρησιμοποιούνται πιστοποιημένοι πάροχοι διάθεσης για τα φυσικά μέσα. Η μέθοδος διαγραφής που χρησιμοποιούν οι πάροχοι υπηρεσιών νέφους θα πρέπει να ελέγχεται από τον οργανισμό για να διασφαλίζεται ότι είναι επαρκής. Η τήρηση αρχείου διαγραφής είναι χρήσιμη σε περίπτωση διαρροής δεδομένων.

8.11 Κάλυψη δεδομένων

Έλεγχος

Η απόκρυψη δεδομένων θα πρέπει να χρησιμοποιείται σύμφωνα με την πολιτική του οργανισμού σχετικά με την επιθεώρηση πρόσβασης και άλλες συναφείς πολιτικές σχετικά με το θέμα, καθώς και τις επιχειρησιακές απαιτήσεις, λαμβάνοντας υπόψη την ισχύουσα νομοθεσία.

Σκοπός αυτού του ελέγχου είναι να περιοριστεί η έκθεση ευαίσθητων δεδομένων, συμπεριλαμβανομένων των προσωπικών πληροφοριών, και να συμμορφωθεί με τις νομικές, καταστατικές, κανονιστικές και συμβατικές απαιτήσεις. Μόνο η ελάχιστη ποσότητα δεδομένων που απαιτείται για μια εργασία θα πρέπει να είναι διαθέσιμη στα αποτελέσματα αναζήτησης. Για να επιτευχθεί αυτό, τα προσωπικά δεδομένα πρέπει να καλύπτονται (ή να ανωνυμοποιούνται ή να ψευδωνυμοποιούνται) για να αποκρύπτεται η ταυτότητα των υποκειμένων. Αυτό μπορεί να απαιτείται από τη νομοθεσία.

8.12 Πρόληψη της διαρροής δεδομένων

Έλεγχος

Τα *μέτρα πρόληψης της διαρροής δεδομένων θα πρέπει να εφαρμόζονται σε συστήματα, δίκτυα και οποιεσδήποτε άλλες συσκευές που επεξεργάζονται, αποθηκεύουν ή μεταδίδουν ευαίσθητες πληροφορίες*.

Σκοπός αυτού του ελέγχου είναι να ανιχνεύει και να αποτρέπει τη μη εξουσιοδοτημένη αποκάλυψη και εξαγωγή πληροφοριών από άτομα ή συστήματα. Η παρακολούθηση και ο εντοπισμός μη εξουσιοδοτημένων προσπαθειών αποκάλυψης ή εξαγωγής δεδομένων είναι το κλειδί για την πρόληψη. Όταν ανιχνεύεται μια απόπειρα, μπορούν να ενεργοποιηθούν μέτρα όπως η καραντίνα ηλεκτρονικού ταχυδρομείου ή ο αποκλεισμός πρόσβασης. Για την αντιμετώπιση των κινδύνων διαρροής δεδομένων από το προσωπικό θα πρέπει να χρησιμοποιούνται και άλλες μέθοδοι, όπως πολιτικές και εκπαίδευση σχετικά με τη μεταφόρτωση, την κοινή χρήση ή την πρόσβαση σε δεδομένα.

8.13 Δημιουργία αντιγράφων ασφαλείας πληροφοριών

Έλεγχος

Τα αντίγραφα ασφαλείας των πληροφοριών, του λογισμικού και των συστημάτων θα πρέπει να διατηρούνται και να ελέγχονται τακτικά σύμφωνα με τη συμφωνηθείσα θεματική πολιτική για τα αντίγραφα ασφαλείας.

Ο σκοπός αυτού του ελέγχου είναι να καταστεί δυνατή η ανάκτηση μετά από απώλεια δεδομένων ή συστημάτων. Ο οργανισμός χρειάζεται ειδική πολιτική για τα εφεδρικά αντίγραφα ασφαλείας, η οποία να καλύπτει τη μέθοδο, τη συχνότητα και τις δοκιμές. Κατά την ανάπτυξη της πολιτικής, ο οργανισμός θα πρέπει

να εξετάζει σημεία όπως η διασφάλιση της πληρότητας των αντιγράφων ασφαλείας και των επαναφορών, οι επιχειρηματικές ανάγκες των αντιγράφων ασφαλείας, ο τόπος και ο τρόπος αποθήκευσης και ο τρόπος δοκιμής του συστήματος αντιγράφων ασφαλείας. Το εφεδρικό σύστημα θα πρέπει να εξετάζεται ως μέρος των σχεδίων επιχειρησιακής συνέχειας και να είναι επαρκές για την ικανοποίηση των απαιτήσεων συνέχειας.

8.14 Πλεονασμός των εγκαταστάσεων επεξεργασίας πληροφοριών

Έλεγχος

Οι *εγκαταστάσεις επεξεργασίας πληροφοριών θα πρέπει να υλοποιούνται με πλεονασμό επαρκή για την ικανοποίηση των απαιτήσεων διαθεσιμότητας*.

Σκοπός του ελέγχου αυτού είναι να διασφαλιστεί η συνεχής λειτουργία των εγκαταστάσεων επεξεργασίας πληροφοριών. Κάθε οργανισμός χρειάζεται μια αρχιτεκτονική συστήματος που να είναι επαρκής για να ικανοποιεί τις απαιτήσεις διαθεσιμότητας της επιχείρησης. Ο πλεονασμός διασφαλίζει τη διαθεσιμότητα με την ύπαρξη εφεδρικής χωρητικότητας σε περίπτωση βλάβης του συστήματος και συχνά απαιτεί διπλά συστήματα, όπως τροφοδοτικά. Ο επαρκής πλεονασμός που μπορεί να ενεργοποιηθεί όταν είναι απαραίτητο αποτελεί σημαντικό μέρος του σχεδιασμού επιχειρησιακής συνέχειας και θα πρέπει να ελέγχεται τακτικά.

8.15 Καταγραφή

Έλεγχος

Θα πρέπει να παράγονται, να αποθηκεύονται, να προστατεύονται και να αναλύονται αρχεία καταγραφής δραστηριοτήτων, εξαιρέσεων, σφαλμάτων και άλλων σχετικών συμβάντων.

Σκοπός αυτού του ελέγχου είναι η καταγραφή συμβάντων, η δημιουργία αποδεικτικών στοιχείων, η διασφάλιση της ακεραιότητας των πληροφοριών καταγραφής, η πρόληψη μη εξουσιοδοτημένης πρόσβασης, ο εντοπισμός συμβάντων ασφάλειας πληροφοριών που μπορεί να οδηγήσουν σε συμβάν ασφάλειας πληροφοριών και η υποστήριξη ερευνών. Η καταγραφή καταγράφει συμβάντα, παράγει αποδεικτικά στοιχεία, διασφαλίζει την ακεραιότητα των πληροφοριών καταγραφής, μπορεί να βοηθήσει στην αποτροπή μη εξουσιοδοτημένης πρόσβασης, εντοπίζει συμβάντα ασφάλειας πληροφοριών και υποστηρίζει έρευνες. Ένα σχέδιο καταγραφής πρέπει να προσδιορίζει ποιες πληροφορίες πρέπει να καταγράφονται (π.χ. αναγνωριστικό χρήστη) και μπορεί να καλύπτει συμβάντα όπως προσπάθειες πρόσβασης στο σύστημα, αλλαγές, συναλλαγές ή πρόσβαση σε αρχεία, μεταξύ άλλων. Τα αρχεία καταγραφής πρέπει να προστατεύονται ακόμη και από προνομιούχους χρήστες, ώστε να μην μπορούν να διαγραφούν ή να τροποποιηθούν. Τα αρχεία καταγραφής πρέπει να παρακολουθούνται και να αναλύονται για τον εντοπισμό μοτίβων ή περιστατικών που μπορεί να αποτελούν περιστατικά ασφάλειας πληροφοριών.

8.16 Δραστηριότητες παρακολούθησης

Έλεγχος

Τα δίκτυα, τα συστήματα και οι εφαρμογές θα πρέπει να παρακολουθούνται για ανώμαλη συμπεριφορά και να λαμβάνονται οι κατάλληλες ενέργειες για την αξιολόγηση πιθανών περιστατικών ασφάλειας πληροφοριών.

Σκοπός αυτού του ελέγχου είναι να ανιχνεύει ανώμαλη συμπεριφορά και πιθανά περιστατικά ασφάλειας πληροφοριών. Ο στόχος της παρακολούθησης είναι να ανιχνεύει ανώμαλη συμπεριφορά και να εντοπίζει πιθανά περιστατικά ασφάλειας πληροφοριών. Το σύστημα παρακολούθησης θα μπορούσε να καλύπτει την κυκλοφορία του δικτύου, την πρόσβαση στο σύστημα, τα αρχεία καταγραφής και τη χρήση των πόρων. Η

παρακολούθηση μπορεί να βοηθήσει στον εντοπισμό αποτυχιών ή συμφορήσεων του συστήματος, δραστηριοτήτων που σχετίζονται με κακόβουλο λογισμικό, μη εξουσιοδοτημένη πρόσβαση, ασυνήθιστη συμπεριφορά και επιθέσεις όπως επιθέσεις άρνησης παροχής υπηρεσιών.

8.17 Συγχρονισμός ρολογιού

Έλεγχος

Τα ρολόγια των συστημάτων επεξεργασίας πληροφοριών που χρησιμοποιούνται από τον οργανισμό πρέπει να συγχρονίζονται με εγκεκριμένες πηγές χρόνου.

Σκοπός αυτού του ελέγχου είναι να καταστεί δυνατή η συσχέτιση και η ανάλυση των συμβάντων που σχετίζονται με την ασφάλεια και άλλων καταγεγραμμένων δεδομένων και να υποστηριχθούν οι έρευνες για περιστατικά ασφάλειας πληροφοριών. Ο συγχρονισμός του ρολογιού είναι σημαντικός για να διασφαλιστεί ότι ο χρόνος ενός περιστατικού ασφάλειας πληροφοριών καταγράφεται αξιόπιστα. Τα συστήματα στις εγκαταστάσεις θα πρέπει να χρησιμοποιούν ένα πρωτόκολλο χρόνου δικτύου (NTP) για να εξασφαλίζουν το συγχρονισμό. Οι πάροχοι υπηρεσιών νέφους χειρίζονται γενικά το χρονοδιάγραμμα για την καταγραφή. Ωστόσο, τα ρολόγια στις εγκαταστάσεις ενδέχεται να μην είναι απόλυτα συγχρονισμένα με το ρολόι του παρόχου Cloud. Στην περίπτωση αυτή, η διαφορά πρέπει να καταγράφεται και να παρακολουθείται.

8.18 Χρήση προνομιακών βοηθητικών προγραμμάτων

Έλεγχος

Η χρήση βοηθητικών προγραμμάτων που μπορούν να παρακάμψουν τους ελέγχους του συστήματος και των εφαρμογών θα πρέπει να περιορίζεται και να ελέγχεται αυστηρά.

Σκοπός αυτού του ελέγχου είναι να διασφαλιστεί ότι η χρήση βοηθητικών προγραμμάτων δεν βλάπτει τους ελέγχους του συστήματος και των εφαρμογών για την ασφάλεια των πληροφοριών. Ένα βοηθητικό πρόγραμμα μπορεί να είναι ικανό να παρακάμπτει τους ελέγχους του συστήματος και της εφαρμογής. Η χρήση και η πρόσβαση σε προγράμματα κοινής ωφέλειας θα πρέπει επομένως να είναι αυστηρά περιορισμένη, με μοναδική ταυτοποίηση του χρήστη και καταγραφή της χρήσης.

8.19 Εγκατάσταση λογισμικού σε λειτουργικά συστήματα

Έλεγχος

Θα πρέπει να εφαρμοστούν διαδικασίες και μέτρα για την ασφαλή διαχείριση της εγκατάστασης λογισμικού στα λειτουργικά συστήματα.

Σκοπός αυτού του ελέγχου είναι να διασφαλιστεί η ακεραιότητα των λειτουργικών συστημάτων και να αποτραπεί η εκμετάλλευση τεχνικών τρωτών σημείων Η εγκατάσταση λογισμικού μπορεί να εισάγει τρωτά σημεία στα λειτουργικά συστήματα. Για να ελαχιστοποιηθεί αυτός ο κίνδυνος, το λογισμικό πρέπει να εγκαθίσταται μόνο από εξουσιοδοτημένα άτομα. Το λογισμικό θα πρέπει να προέρχεται από αξιόπιστες και συντηρούμενες πηγές ή να είναι πλήρως δοκιμασμένο εάν έχει αναπτυχθεί εσωτερικά. Οι προηγούμενες εκδόσεις θα πρέπει να διατηρούνται και όλες οι αλλαγές να καταγράφονται, ώστε να είναι δυνατή η επαναφορά, αν χρειαστεί.

8.20 Ασφάλεια δικτύου

Έλεγχος

Τα δίκτυα και οι δικτυακές συσκευές θα πρέπει να εξασφαλίζονται, να διαχειρίζονται και να ελέγχονται για την προστασία των πληροφοριών στα συστήματα και τις εφαρμογές.

Σκοπός αυτού του ελέγχου είναι η προστασία των πληροφοριών στα δίκτυα και στις υποστηρικτικές εγκαταστάσεις επεξεργασίας πληροφοριών από παραβίαση μέσω του δικτύου. Τα δίκτυα πρέπει να είναι αρκετά ασφαλή ώστε να προστατεύουν τις πληροφορίες που διακινούνται μέσω αυτών. Για να διατηρηθούν ασφαλή, πρέπει να ενημερώνονται και να παρακολουθούνται, με τη δυνατότητα να περιορίζονται τόσο οι συνδέσεις σε συσκευές που έχουν πιστοποιηθεί όσο και η κυκλοφορία που μπορεί να περάσει από το δίκτυο. Μια μέθοδος απομόνωσης του δικτύου μπορεί να είναι χρήσιμη σε περίπτωση που το δίκτυο δεχθεί επίθεση.

8.21 Ασφάλεια των υπηρεσιών δικτύου

Έλεγχος

Θα πρέπει να προσδιορίζονται, να εφαρμόζονται και να παρακολουθούνται οι μηχανισμοί ασφαλείας, τα επίπεδα υπηρεσιών και οι απαιτήσεις υπηρεσιών των δικτυακών υπηρεσιών.

Σκοπός αυτού του ελέγχου είναι να διασφαλιστεί η ασφάλεια στη χρήση των υπηρεσιών δικτύου. Οι υπηρεσίες ασφάλειας δικτύου καλύπτουν τα πάντα, από την παροχή μιας απλής σύνδεσης και εύρους ζώνης έως σύνθετες υπηρεσίες όπως τείχη προστασίας και συστήματα ανίχνευσης εισβολών. Το απαιτούμενο επίπεδο ασφάλειας εξαρτάται από τις επιχειρηματικές ανάγκες. Όταν προσδιοριστεί η απαιτούμενη ασφάλεια, πρέπει να εφαρμοστεί και να παρακολουθείται. Αυτό γίνεται συχνά από τρίτους παρόχους υπηρεσιών δικτύου. Οι διαδικασίες εξουσιοδότησης πρόσβασης και τα μέσα πρόσβασης, όπως τα VPN, θα πρέπει να λαμβάνονται υπόψη κατά τη δημιουργία υπηρεσιών ασφάλειας δικτύου.

8.22 Διαχωρισμός στα δίκτυα

Έλεγχος

Οι ομάδες υπηρεσιών πληροφοριών, χρηστών και συστημάτων πληροφοριών θα πρέπει να διαχωρίζονται στα δίκτυα του οργανισμού.

Σκοπός αυτού του ελέγχου είναι να χωρίσει το δίκτυο σε όρια ασφαλείας και να ελέγχει την κυκλοφορία μεταξύ τους με βάση τις επιχειρηματικές ανάγκες. Τα μεγάλα δίκτυα μπορούν να χωριστούν σε διάφορους τομείς. Αυτό σημαίνει ότι μπορούν να εφαρμοστούν διαφορετικά επίπεδα ασφαλείας σε κάθε τομέα, με περιορισμένη πρόσβαση σε διαφορετικά τμήματα του επιχειρηματικού δικτύου. Τα δίκτυα μπορούν να διαχωρίζονται πλήρως με φυσικό τρόπο ή ψηφιακά με τη χρήση λογικών δικτύων. Τα ασύρματα δίκτυα δεν έχουν φυσικά όρια και επομένως θα πρέπει να θεωρούνται ως εξωτερικές συνδέσεις μέχρι να περάσει μια πύλη, όπως ένα VPN, όταν υπάρχει πρόσβαση σε ευαίσθητα δεδομένα.

8.23 Φιλτράρισμα στο διαδίκτυο

Έλεγχος

Η πρόσβαση σε εξωτερικούς ιστότοπους θα πρέπει να διαχειρίζεται ώστε να μειώνεται η έκθεση σε κακόβουλο περιεχόμενο.

Ο σκοπός αυτού του ελέγχου είναι να προστατεύει τα συστήματα από την παραβίαση από κακόβουλο λογισμικό και να αποτρέπει την πρόσβαση σε μη εξουσιοδοτημένους διαδικτυακούς πόρους. Δεν είναι όλοι οι ιστότοποι στο διαδίκτυο αθώοι. Ορισμένα περιέχουν παράνομες πληροφορίες και άλλα διανέμουν κακόβουλο λογισμικό. Ο αποκλεισμός των διευθύνσεων IP ύποπτων ιστότοπων μπορεί να μειώσει τους

κινδύνους. Ωστόσο, δεν μπορεί να αποκλειστεί κάθε κακόβουλος ιστότοπος, οπότε το φιλτράρισμα πρέπει να συνοδεύεται από κανόνες και εκπαίδευση ευαισθητοποίησης σχετικά με την κατάλληλη και υπεύθυνη χρήση του διαδικτύου.

8.24 Χρήση κρυπτογραφίας

Έλεγχος

Θα πρέπει να καθοριστούν και να εφαρμοστούν κανόνες για την αποτελεσματική χρήση της κρυπτογραφίας, συμπεριλαμβανομένης της διαχείρισης των κρυπτογραφικών κλειδιών.

Σκοπός αυτού του ελέγχου είναι η διασφάλιση της ορθής και αποτελεσματικής χρήσης της κρυπτογραφίας για την προστασία της εμπιστευτικότητας, της αυθεντικότητας ή της ακεραιότητας των πληροφοριών σύμφωνα με τις επιχειρησιακές απαιτήσεις και τις απαιτήσεις ασφάλειας των πληροφοριών και λαμβάνοντας υπόψη τις νομικές, κανονιστικές, ρυθμιστικές και συμβατικές απαιτήσεις που σχετίζονται με την κρυπτογραφία. Η χρήση της κρυπτογραφίας πρέπει να διαχειρίζεται προσεκτικά, λαμβάνοντας υπόψη το απαιτούμενο επίπεδο προστασίας, τη διαχείριση των κλειδιών, την κρυπτογράφηση των συσκευών τελικού σημείου και τον τρόπο με τον οποίο η κρυπτογραφία μπορεί να επηρεάσει την επιθεώρηση του περιεχομένου (π.χ. σάρωση κακόβουλου λογισμικού). Η διαχείριση κλειδιών απαιτεί μια διαδικασία παραγωγής, αποθήκευσης, αρχειοθέτησης, ανάκτησης, διανομής, απόσυρσης και καταστροφής κρυπτογραφικών κλειδιών.

8.25 Κύκλος ζωής ασφαλούς ανάπτυξης

Έλεγχος

Θα πρέπει να θεσπιστούν και να εφαρμοστούν κανόνες για την ασφαλή ανάπτυξη λογισμικού και συστημάτων.

Σκοπός αυτού του ελέγχου είναι να διασφαλιστεί ότι η ασφάλεια των πληροφοριών σχεδιάζεται και εφαρμόζεται στο πλαίσιο του ασφαλούς κύκλου ζωής της ανάπτυξης του λογισμικού και των συστημάτων. Η ασφαλής ανάπτυξη καλύπτει την κατασκευή υπηρεσιών, αρχιτεκτονικής, λογισμικού και συστημάτων. Μια βασική πτυχή είναι ο διαχωρισμός των περιβαλλόντων ανάπτυξης, δοκιμής (έγκρισης) και παραγωγής με ασφαλή αποθετήρια για τον πηγαίο κώδικα. Η ασφάλεια θα πρέπει να λαμβάνεται υπόψη ήδη από τη φάση των προδιαγραφών και του σχεδιασμού, με σημεία ελέγχου ενσωματωμένα στο σχέδιο έργου και τις προγραμματισμένες δοκιμές. Οι προγραμματιστές πρέπει επίσης να γνωρίζουν τις οδηγίες ασφαλούς κωδικοποίησης και να είναι σε θέση να προλαμβάνουν, να βρίσκουν και να διορθώνουν ευπάθειες.

8.26 Απαιτήσεις ασφάλειας εφαρμογών

Έλεγχος

Οι απαιτήσεις ασφάλειας πληροφοριών πρέπει να προσδιορίζονται, να εξειδικεύονται και να εγκρίνονται κατά την ανάπτυξη ή την απόκτηση εφαρμογών.

Σκοπός αυτού του ελέγχου είναι να διασφαλιστεί ότι όλες οι απαιτήσεις ασφάλειας πληροφοριών προσδιορίζονται και αντιμετωπίζονται κατά την ανάπτυξη ή την απόκτηση εφαρμογών. Οι οργανισμοί πρέπει να προσδιορίσουν και να προσδιορίσουν τις απαιτήσεις ασφαλείας για τις εφαρμογές, και στη συνέχεια να τις προσδιορίσουν χρησιμοποιώντας μια αξιολόγηση κινδύνου. Οι απαιτήσεις καθορίζονται από το επίπεδο διαβάθμισης ασφαλείας των πληροφοριών που διέρχονται από την εφαρμογή. Οι απαιτήσεις μπορεί να περιλαμβάνουν ελέγχους πρόσβασης, επίπεδο προστασίας, κρυπτογράφηση, ελέγχους εισόδου και εξόδου,

καταγραφή, χειρισμό μηνυμάτων σφάλματος, ανθεκτικότητα έναντι επιθέσεων και νομικές απαιτήσεις. Η ασφάλεια απαιτεί ιδιαίτερη προσοχή εάν η εφαρμογή εκτελεί συναλλαγές πληροφοριών ή εντολών και πληρωμών.

8.27 Αρχές αρχιτεκτονικής και μηχανικής ασφαλούς συστήματος

Έλεγχος

Οι αρχές για την ανάπτυξη ασφαλών συστημάτων πρέπει να καθιερωθούν, να τεκμηριωθούν, να διατηρηθούν και να εφαρμοστούν σε κάθε δραστηριότητα ανάπτυξης πληροφοριακών συστημάτων.

Σκοπός αυτού του ελέγχου είναι να διασφαλιστεί ότι τα πληροφοριακά συστήματα σχεδιάζονται, υλοποιούνται και λειτουργούν με ασφάλεια στο πλαίσιο του κύκλου ζωής της ανάπτυξης. Οι αρχές αρχιτεκτονικής και μηχανικής διασφαλίζουν ότι τα συστήματα σχεδιάζονται, υλοποιούνται και λειτουργούν με ασφάλεια καθ' όλη τη διάρκεια του κύκλου ζωής τους. Οι αρχές του ασφαλούς συστήματος αναλύουν ποιοι έλεγχοι ασφαλείας απαιτούνται και πώς πρέπει να εφαρμόζονται. Θα πρέπει επίσης να ληφθούν υπόψη οι ορθές πρακτικές, οι πρακτικές εκτιμήσεις σχετικά με το κόστος και την πολυπλοκότητα και ο τρόπος με τον οποίο τα νέα χαρακτηριστικά μπορούν να ενσωματωθούν στα υπάρχοντα συστήματα.

8.28 Ασφαλής κωδικοποίηση

Έλεγχος

Οι αρχές ασφαλούς κωδικοποίησης πρέπει να εφαρμόζονται στην ανάπτυξη λογισμικού.

Ο σκοπός αυτού του ελέγχου είναι να διασφαλίσει ότι το λογισμικό γράφεται με ασφάλεια, μειώνοντας έτσι τον αριθμό των πιθανών τρωτών σημείων ασφάλειας πληροφοριών στο λογισμικό. Η εξάσκηση ασφαλούς κωδικοποίησης συμβάλλει στη διασφάλιση ότι ο κώδικας είναι γραμμένος με στόχο την ελαχιστοποίηση των ευπαθειών. Οι αρχές ασφαλούς κωδικοποίησης μπορούν να χρησιμοποιηθούν για την προώθηση βέλτιστων πρακτικών και τον καθορισμό ελάχιστων προτύπων στον οργανισμό. Αυτές θα πρέπει να λαμβάνουν υπόψη τις τρέχουσες απειλές του πραγματικού κόσμου, τη χρήση ελεγχόμενων περιβαλλόντων για την ανάπτυξη και τη διασφάλιση της επάρκειας των προγραμματιστών. Η ασφαλής κωδικοποίηση θα πρέπει επίσης να περιλαμβάνει τη διαχείριση των ενημερώσεων και της συντήρησης, ιδίως την επιθεώρηση του υπεύθυνου για τη συντήρηση κωδικών από εξωτερικές πηγές.

8.29 Δοκιμές ασφάλειας κατά την ανάπτυξη και την αποδοχή

Έλεγχος

Οι διαδικασίες δοκιμών ασφαλείας θα πρέπει να ορίζονται και να εφαρμόζονται στον κύκλο ζωής της ανάπτυξης.

Ο σκοπός αυτού του ελέγχου είναι να επικυρώσει εάν πληρούνται οι απαιτήσεις ασφάλειας πληροφοριών όταν οι εφαρμογές ή ο κώδικας αναπτύσσονται στο περιβάλλον παραγωγής. Οι δοκιμές ασφαλείας πρέπει να αποτελούν αναπόσπαστο μέρος των δοκιμών ανάπτυξης. Αυτό περιλαμβάνει τη δοκιμή της ασφαλούς διαμόρφωσης των λειτουργικών συστημάτων (π.χ. τείχη προστασίας), της ασφαλούς κωδικοποίησης και των λειτουργιών ασφαλείας (όπως η πρόσβαση). Οι δοκιμές πρέπει να προγραμματίζονται, να τεκμηριώνονται και να διαθέτουν κριτήρια για τον καθορισμό των αποδεκτών αποτελεσμάτων.

8.30 Ανάπτυξη με εξωτερική ανάθεση

Έλεγχος

Ο οργανισμός θα πρέπει να κατευθύνει, να παρακολουθεί και να επανεξετάζει τις δραστηριότητες που σχετίζονται με την ανάπτυξη συστημάτων από εξωτερικούς συνεργάτες.

Ο σκοπός αυτού του ελέγχου είναι να διασφαλίσει ότι τα μέτρα ασφάλειας πληροφοριών που απαιτούνται από τον οργανισμό εφαρμόζονται στην ανάπτυξη εξωτερικών συστημάτων. Όταν η ανάπτυξη ανατίθεται σε εξωτερικούς συνεργάτες, οι απαιτήσεις ασφάλειας πληροφοριών πρέπει να κοινοποιούνται και να συμφωνούνται από τον εξωτερικό συνεργάτη και να παρακολουθούνται από τον οργανισμό εξωτερικής ανάθεσης. Η αδειοδότηση και η ιδιοκτησία πνευματικής ιδιοκτησίας, οι δοκιμές και τα αποδεικτικά στοιχεία των δοκιμών, καθώς και τα συμβατικά δικαιώματα ελέγχου της διαδικασίας ανάπτυξης είναι παραδείγματα θεμάτων ασφάλειας που θα πρέπει να συμφωνηθούν μεταξύ των μερών.

8.31 Διαχωρισμός των περιβαλλόντων ανάπτυξης, δοκιμής και παραγωγής

Έλεγχος

Τα περιβάλλοντα ανάπτυξης, δοκιμών και παραγωγής πρέπει να διαχωρίζονται και να διασφαλίζονται.

Σκοπός αυτού του ελέγχου είναι η προστασία του περιβάλλοντος παραγωγής και των δεδομένων από τη διακινδύνευση από τις δραστηριότητες ανάπτυξης και δοκιμής. Οι δραστηριότητες δοκιμής και ανάπτυξης μπορεί να προκαλέσουν ανεπιθύμητες αλλαγές ή αποτυχία του συστήματος, η οποία θα μπορούσε να θέσει σε κίνδυνο το περιβάλλον παραγωγής, εάν δεν προστατεύεται επαρκώς. Ο βαθμός διαχωρισμού μεταξύ δοκιμών και παραγωγής εξαρτάται από τον οργανισμό, αλλά τα περιβάλλοντα πρέπει να διαχωρίζονται και να επισημαίνονται σαφώς, έτσι ώστε οι δοκιμές ή ενέργειες όπως η μεταγλώττιση να μην μπορούν να πραγματοποιηθούν στο περιβάλλον παραγωγής. Οι αλλαγές θα πρέπει να παρακολουθούνται, με προσεκτικό έλεγχο του ποιος έχει πρόσβαση σε κάθε περιβάλλον. Κανείς δεν πρέπει να έχει τη δυνατότητα να κάνει αλλαγές τόσο στο περιβάλλον δοκιμών όσο και στο περιβάλλον παραγωγής χωρίς προηγούμενη εξέταση και έγκριση.

8.32 Διαχείριση αλλαγών

Έλεγχος

Οι αλλαγές στις εγκαταστάσεις επεξεργασίας πληροφοριών και στα συστήματα πληροφοριών θα πρέπει να υπόκεινται σε διαδικασίες διαχείρισης αλλαγών.

Σκοπός αυτού του ελέγχου είναι η διατήρηση της ασφάλειας των πληροφοριών κατά την εκτέλεση των αλλαγών. Η εμπιστευτικότητα, η διαθεσιμότητα και η ακεραιότητα των πληροφοριών μπορεί να τεθεί σε κίνδυνο κατά την εισαγωγή υποδομών ή λογισμικού ή κατά την πραγματοποίηση σημαντικών αλλαγών σε ένα υπάρχον. Μια επίσημη διαδικασία τεκμηρίωσης, δοκιμών, ελέγχου ποιότητας και εφαρμογής μπορεί να μειώσει τους κινδύνους. Η τεκμηρίωση των δοκιμών και ο σχεδιασμός έκτακτης ανάγκης είναι σημαντικά κατά την προετοιμασία της υλοποίησης, ιδίως για να διασφαλιστεί ότι το νέο λογισμικό δεν επηρεάζει αρνητικά το περιβάλλον παραγωγής. Οι οδηγοί λειτουργίας και οι διαδικασίες ενδέχεται να χρειαστεί να τροποποιηθούν μετά την πραγματοποίηση των αλλαγών.

8.33 Πληροφορίες δοκιμής

Έλεγχος

Οι πληροφορίες δοκιμής πρέπει να επιλέγονται, να προστατεύονται και να διαχειρίζονται κατάλληλα.

Σκοπός αυτού του ελέγχου είναι να διασφαλιστεί η καταλληλότητα των δοκιμών και η προστασία των επιχειρησιακών πληροφοριών που χρησιμοποιούνται για τις δοκιμές. Υπάρχουν δύο βασικές εκτιμήσεις για τις πληροφορίες δοκιμών: θα πρέπει να είναι αρκετά κοντά στις επιχειρησιακές πληροφορίες ώστε να διασφαλίζεται η αξιοπιστία των αποτελεσμάτων των δοκιμών, αλλά δεν θα πρέπει να περιέχουν εμπιστευτικές επιχειρησιακές πληροφορίες. Εάν πρέπει να χρησιμοποιηθούν ευαίσθητες πληροφορίες για δοκιμές, θα πρέπει να προστατεύονται, να τροποποιούνται ή να ανωνυμοποιούνται πριν από τη χρήση τους και να διαγράφονται αμέσως μετά τις δοκιμές.

8.34 Προστασία των συστημάτων πληροφοριών κατά τη διάρκεια του ελέγχου και των δοκιμών

Έλεγχος

Οι ελεγκτικές δοκιμές και άλλες δραστηριότητες διασφάλισης που περιλαμβάνουν αξιολόγηση των λειτουργικών συστημάτων θα πρέπει να σχεδιάζονται και να συμφωνούνται μεταξύ του επιθεωρητή και της αρμόδιας διοίκησης.

Σκοπός αυτού του ελέγχου είναι να ελαχιστοποιηθεί ο αντίκτυπος του ελέγχου και άλλων δραστηριοτήτων διασφάλισης στα λειτουργικά συστήματα και τις επιχειρησιακές διαδικασίες. Τα επιχειρησιακά συστήματα δεν θα πρέπει να επηρεάζονται αδικαιολόγητα από τους ελέγχους ή τις τεχνικές αναθεωρήσεις. Για να αποφευχθεί η υπερβολική διαταραχή, οι έλεγχοι πρέπει να προγραμματίζονται με συμφωνημένο χρονοδιάγραμμα και πεδίο εφαρμογής. Η πρόσβαση μόνο για ανάγνωση θα αποτρέψει τις τυχαίες αλλαγές στα συστήματα κατά τη διάρκεια ενός ελέγχου, και όλη η πρόσβαση θα πρέπει να παρακολουθείται.