Ενημέρωση για
«ISO/IEC 27001:2022» - Περίοδος μετάβασης

Παραλήπτης: Πελάτες ISO/IEC 27001:2013

Αγαπητέ πελάτη,

Το πρότυπο ISO/IEC 27001:2022 "Ασφάλεια Πληροφοριών, κυβερνοασφάλεια και προστασία ιδιωτικότητας – Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών - Απαιτήσεις" κυκλοφόρησε τον Οκτώβριο του 2022 και πρόκειται να αντικαταστήσει την έκδοση ISO/IEC 27001:2013.
Το «Διεθνές Φόρουμ Διαπίστευσης» (IAF) εξέδωσε ένα υποχρεωτικό έγγραφο IAF MD 26 (2η έκδοση, ημερομηνία 15.02.2023) που περιέχει τις απαιτήσεις μετάβασης για την νέα έκδοση ISO/IEC 27001:2022. Όλοι οι Φορείς Πιστοποίησης Συστημάτων Διαχείρισης Ασφάλειας Πληροφοριών (ISMS ISO/IEC 27001) απαιτείται να εφαρμόσουν τις απαιτήσεις του εγγράφου MD του IAF σύμφωνα με τις καθορισμένες σε αυτό ημερομηνίες.
Το «Διεθνές Φόρουμ Διαπίστευσης» (IAF) έχει ορίσει μια τριετή μεταβατική περίοδο και ορισμένες μεταβατικές ρυθμίσεις. Αυτό σημαίνει ότι μετά τη μεταβατική περίοδο, από 01.11.2025, οποιαδήποτε πιστοποίηση σύμφωνα με τις απαιτήσεις του ISO/IEC 27001 πρέπει να διενεργείται αποκλειστικά με την νέα έκδοση και όλα τα πιστοποιητικά που έχουν εκδοθεί με την παλιά έκδοση καθίστανται άκυρα, ανεξάρτητα από την ημερομηνία λήξης που αναφέρεται στο πιστοποιητικό.

Χρονοδιάγραμμα μετάβασης
Οι ακόλουθες γενικές προϋποθέσεις ορίζονται από το IAF:

- Κάθε αρχική επιθεώρηση ή επιθεώρηση επαναπιστοποίησης μετά την 01.05.2024 θα διενεργειται σύμφωνα με την νεα έκδοση, ISO/IEC 27001:2022.

- Όλα τα πιστοποιητικά ISO/IEC 27001:2013 θα λήξουν ή θα αποσυρθούν στο τέλος της μεταβατικής περιόδου, 31.10.2025. Τυχόν αποφάσεις πιστοποίησης για μετατροπή υφιστάμενων πιστοποιητικών ISO/IEC 27001:2013 θα ολοκληρωθούν το αργότερο έως τις 31.10.2025. Διαφορετικά, θα διενεργηθεί νέα αρχική επιθεώρηση.

Η μετάβαση μπορεί να πραγματοποιηθεί σε συνδυασμό με επιθεωρήση επιτήρησης ή επαναπιστοποίησης ή μέσω ειδικής επιθεώρησης.

Βασικές αλλαγές
Σε σύγκριση με το ISO/IEC 27001:2013, οι κύριες αλλαγές του ISO/IEC 27001:2022 περιλαμβάνουν, αλλά δεν περιορίζονται σε:

1) Το Παράρτημα Α αναφέρεται πλέον στα μέτρα ασφάλειας πληροφοριών του ISO/IEC 27002:2022.
2) Οι σημειώσεις της ρήτρας 6.1.3 γ) αναθεωρούνται συντακτικά, συμπεριλαμβανομένης της διαγραφής του όρου «μέτρα» και της αντικατάστασης του με τον όρο «μέτρα ασφάλειας πληροφοριών».
3) Η διατύπωση της ρήτρας 6.1.3 δ) αναθεωρήθηκε για την άρση πιθανής ασάφειας.
4) Προσθήκη νέας ρήτρας 4.2 γ) για τον καθορισμό των απαιτήσεων των ενδιαφερομένων μερών που εξετάζονται μέσω του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ISMS).
5) Προσθήκη νέας υποενότητας 6.3 – «Σχεδιασμός Αλλαγών», που ορίζει ότι οι αλλαγές στο ΣΔΑΠ θα πραγματοποιούνται από τον οργανισμό με προγραμματισμένο τρόπο.
6) Συνέχιση της συνοχής στο ρήμα που χρησιμοποιείται σε σχέση με τις τεκμηριωμένες πληροφορίες, για παράδειγμα, με τη χρήση της φράσης «Οι τεκμηριωμένες πληροφορίες θα είναι διαθέσιμες ως απόδειξη του XXX» στις παραγράφους 9.1, 9.2.2, 9.3.3 και 10.2.
7) Χρήση του όρου «διαδικασία, προϊόντων ή υπηρεσιών που παρέχονται εξωτερικά» για την αντικατάσταση του

Ενημέρωση για
«ISO/IEC 27001:2022» - Περίοδος μετάβασης

Παραλήπτης: Πελάτες ISO/IEC 27001:2013

όρου «διεργασιών που ανατίθενται σε εξωτερικούς συνεργάτες» στην ενότητα 8.1 και διαγραφή του όρου «εξωτερική ανάθεση».
8) Ονομασία και αναδιάταξη των επιμέρους ρητρών στην Παράγραφο 9.2 – «Εσωτερικός έλεγχος» και 9.3 – «Επισκόπηση της Διοίκησης».
9) Ανταλλαγή της σειράς των δύο υποπαραγράφων στην ενότητα 10 – «Βελτίωση».
10) Ενημέρωση της έκδοσης των σχετικών εγγράφων που παρατίθενται στη Βιβλιογραφία, όπως ISO/IEC 27002 και ISO 31000.
11) Ορισμένες αποκλίσεις στο ISO/IEC 27001:2013 ως προς τη δομή, το κείμενο, τους όρους και τους βασικούς ορισμούς των Προτύπων Συστημάτων Διαχείρισης (Management System Standards – MSS) αναθεωρούνται για λόγους συνέπειας με την εναρμονισμένη δομή για τα Πρότυπα Συστημάτων Διαχείρισης, για παράδειγμα, ενότητα 6.2 δ)

Απαιτήσεις για πελάτες

Για κάθε οργανισμό, η έκταση των αλλαγών που απαιτούνται εξαρτάται από την ωριμότητα και την αποτελεσματικότητα του τρέχοντος Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ), την οργανωτική δομή του και τις διεργασίες/διαδικασίες που εφαρμόζει.

Οι οργανισμοί που έχουν εφαρμόσει ΣΔΑΠ, προκειμένου να προσδιορίσουν τον αντίκτυπο των αλλαγών της νέας έκδοσης ISO/IEC 27001:2022, συνιστώνται να προβούν στις ακόλουθες ενέργειες:

- Διενέργεια gap analysis αναγνωρίζοντας τις αποκλίσεις που απαιτούνται να αντιμετωπιστούν για την συμμόρφωση στις νέες απαιτήσεις.
- Προετοιμασία ενός πλάνου μετάβασης.
- Επικαιροποίηση του ΣΔΑΠ.
- Εφαρμογή και έλεγχο της αποτελεσματικότητας τυχόν νέων μέτρων ασφάλειας πληροφοριών και τροποποιήσεων που εισάγονται από τον οργανισμό.
- Παροχή κατάλληλης εκπαίδευσης και ενίσχυση της επίγνωσης του προσωπικού και για όλα τα ενδιαφερόμενα μέρη που επηρεάζουν την αποτελεσματικότητα του ΣΔΑΠ.
- Υλοποίηση μιας εσωτερικής επιθεώρησης (επαληθεύοντας το ΣΔΑΠ σύμφωνα με τις απαιτήσεις της νέας έκδοσης) και μιας Ανασκόπησης Διοίκησης πριν την υλοποίηση της επιθεώρησης μετάβασης.

Παραμένουμε στη διάθεση σας για οποιαδήποτε διευκρίνιση.