1. Πεδίο Εφαρμογής

Η πολιτική αφορά το χρονοδιάγραμμα μετάβασης από το ISO/IEC 27001:2013 στη νέα έκδοση του προτύπου ISO/IEC 27001:2022.

Οι κάτοχοι ενεργού πιστοποιητικού ISO/IEC 27001 θα πρέπει να οργανώσουν την αναβάθμιση του πιστοποιητικού τους στην καινούργια έκδοση του προτύπου και να προετοιμαστούν για αυτό με τον κατάλληλο τρόπο, στις συνθήκες που έχει καθορίσει ο Διεθνής Οργανισμός Τυποποίησης (ISO).

2. Εισαγωγή

Η νέα έκδοση του προτύπου ISO/IEC 27001:2022 ανακοινώθηκε από τον Διεθνή Οργανισμό Τυποποίησης ISO τον Οκτώβριο 2022.

Η ανάγκη για την αναβάθμιση του προτύπου σε νέα έκδοση προέκυψε ως συνέπεια της πολύχρονης παρουσίας του προτύπου, των τεχνολογικών εξελίξεων που τρέχουν με γρήγορους ρυθμούς και της σημαντικής διείσδυσης του προτύπου στην αγορά πιστοποίησης.

3. Πολιτική

α) Όπως συνηθίζεται στις αναθεωρήσεις των προτύπων, έχει καθοριστεί 3ετής περίοδος για την μετάβαση στο νέο πρότυπο, με τις ακόλουθες συνθήκες:

- Όλες οι πιστοποιήσεις σύμφωνα με το ISO/IEC 27001:2013 λήγουν ή ανακαλούνται μετά την λήξη της μεταβατικής περιόδου, δηλαδή με καταληκτική ημερομηνία την **31/10/2025**.

- Μετά την ημερομηνία 31/10/2025, όλες οι πιστοποιήσεις που εκδίδονται σύμφωνα με την παλιά έκδοση του προτύπου δεν θα ισχύουν πλέον. Όλες οι πιστοποιήσεις που βασίζονται στο ISO/IEC 27001:2013 θα παυθούν ή θα ανακληθούν στο τέλος της μεταβατικής περιόδου, που λήγει στις 31/10/2025.

- Επιθεωρήσεις αρχικής πιστοποίησης ή επαναπιστοποίησης σύμφωνα με το ISO/IEC 27001:2013 σταματούν να διενεργούνται από τους φορείς πιστοποίησης μετά τις **30/04/2024** (18 μήνες δηλαδή μετά την έκδοση του προτύπου ISO/IEC 27001:2022).

- Σημειώνεται ότι τα πιστοποιητικά που θα εκδίδονται κατά την διάρκεια της μεταβατικής περιόδου θα λαμβάνουν υπόψη την καταληκτική ημερομηνία 31/10/2025, (ανεξαρτήτως αν θα ολοκληρώνεται η συνήθης τριετής διάρκεια ισχύος του πιστοποιητικού ή όχι).

- Κατά τη μεταβατική περίοδο, οι πιστοποιήσεις που εκδίδονται σύμφωνα με τις απαιτήσεις του προτύπου ISO/IEC 27001:2013 ισχύουν εξίσου με τις πιστοποιήσεις που εκδίδονται σύμφωνα με το πρότυπο ISO/IEC 27001:2022.

- Μετά την 30/04/2024 θα πραγματοποιούνται επιθεωρήσεις πιστοποίησης και επαναπιστοποίησης και θα εκδίδονται πιστοποιητικά (νέες πιστοποιήσεις / επαναπιστοποιήσεις) αποκλειστικά σύμφωνα με το πρότυπο ISO/IEC 27001:2022.

- Η μετάβαση στο νέο πρότυπο ISO/IEC 27001:2022 θα πρέπει να έχει πραγματοποιηθεί μέχρι τις 31/10/2025 και μπορεί να γίνει στα πλαίσια Επιτήρησης, Επαναπιστοποίησης ή Έκτακτης Επιθεώρησης.

β) Οι κύριες αλλαγές του ISO/IEC 27001:2022 αφορούν:

- **Ονομασία του προτύπου:** Περιλαμβάνει πληροφορίες σχετικά με τον τίτλο και την περιγραφή των στοιχείων ελέγχου (security controls) "Information security, cybersecurity and privacy protection — Information security management systems — Requirement".

- **Παράρτημα Α:** Παρόλο που η βασική δομή του προτύπου με τις 10 βασικές παραγράφους δεν έχει κάποια σημαντική αλλαγή, στο Annex A υπάρχει διαφοροποίηση τόσο στη λογική όσο και τα περιεχόμενα, οπότε επηρεάζει την προσέγγιση στο διαχειριστικό Σύστημα. Οι αναθεωρήσεις είναι κανονιστικές (normative).

  - ✓ Τα security controls έχουν μειωθεί (από 112 σε 93)

  - ✓ Τα security controls είναι χωρισμένα σε 4 γενικούς τομείς (αντί 14):

    1. People controls (8 controls)
    2. Organizational controls (37 controls)
    3. Technological controls (34 controls) (βλ. **8**)
    4. Physical controls (14 controls)

  - ✓ Προστέθηκαν καινούργια security controls που στη προηγούμενη έκδοση δεν υπήρχαν (11):

    1. Threat intelligence (βλ. **5.7**)
    2. Information security for use of cloud services (βλ. **5.23**)
    3. ICT readiness for business continuity (βλ. **5.30**)

4. Physical security monitoring (βλ. **7.4**)
5. Configuration management
6. Information deletion
7. Data masking
8. Data leakage prevention
9. Monitoring activities
10. Web filtering
11. Secure coding

- ✓ Ορισμένα security controls έχουν αναδιατυπωθεί
- ✓ Ορισμένα security controls συγχωνεύθηκαν (57 συγχωνεύτηκαν σε 24)
- ✓ Τα ονόματα των μεμονωμένων security controls έχουν αλλάξει (23)
- ✓ Νέα αρίθμηση ορισμένων security controls (35)

- Ο Διεθνής Οργανισμός Διαπίστευσης (IAF) δημοσίευσε το δεσμευτικό έγγραφο **"IAF MD 26:2022 Transition Requirements for ISO/IEC 27001:2022"** (Issue 1) στις 09/08/2022 και (Issue 2) 15/02/2023, στο οποίο καθορίζονται οι απαιτήσεις (normative) και οι προθεσμίες για την υλοποίηση των μεταβατικών δραστηριοτήτων τόσο για τους οργανισμούς πιστοποίησης όσο και για τους οργανισμούς διαπίστευσης.

- Επαναδιατύπωση του **Context of the Organization §4.2 & §4.4** ως σαφείς απαιτήσεις.

- Επαναδιατύπωση της **§5.3 Organizational roles, responsibilities and authorities** ως σαφής απαίτηση.

- Οι απαιτήσεις της **§6.1.3c** αναθεωρούνται συντακτικά με τη διαγραφή του όρου «control objectives» και αντικατάσταση από «information security controls».

- Επαναδιατύπωση της **§6.1.3d** για να αποφεύγονται οι ασάφειες.

- Αναθεώρηση της **§6.2d Information security objectives and planning to achieve them** από «communicated» σε «monitored».

- Προσθήκη της **§6.3 Planning for changes**, που ορίζει ότι οι αλλαγές στο σύστημα διαχείρισης θα πραγματοποιούνται από τον οργανισμό με προγραμματισμένο τρόπο.

- Οι απαιτήσεις της **§8.1** αναθεωρούνται συντακτικά με τη διαγραφή του όρου «outsource» και αντικατάσταση από «externally provided process, products or services».

- Αναδιάταξη των **§9.2**, **§9.3** και **§10**

γ) Συγκεκριμένα για την εφαρμογή της πολιτικής:

- Η BQC θα αποσύρει την πιστοποίηση για όλους τους πελάτες που, έως τις 31/10/2025, δεν έχουν μεταβεί στη νέα έκδοση του προτύπου.

- Η BQC έχει μεριμνήσει για τις απαραίτητες ενέργειες και μέχρι 31/10/2023 θα είναι έτοιμη να υλοποιήσει την υπηρεσία αρχικής πιστοποίησης του συστήματος διαχείρισης ασφάλειας πληροφοριών σύμφωνα με τη νέα έκδοση του προτύπου ISO/IEC 27001:2022.

- Οι εν ισχύ πιστοποιημένοι οργανισμοί θα είναι σε θέση να αποδείξουν τη συμμόρφωση του συστήματος διαχείρισης ασφάλειας πληροφοριών με τη νέα έκδοση του προτύπου ISO/IEC 27001:2022 στο πλαίσιο των ετήσιων επιθεωρήσεων επιτήρησης ή επιθεωρήσεων με σκοπό την ανανέωση της πιστοποίησης (επαναπιστοποίησης) ή μέσω ξεχωριστής επιθεώρησης μετάβασης. Όταν ένας πιστοποιημένος οργανισμός συμμορφώνεται με τις απαιτήσεις του νέου συστήματος διαχείρισης, θα πρέπει να το αναφέρει στη BQC με πρότερη γραπτή ενημέρωση (μέσω ηλεκτρονικού ταχυδρομείου). Η αίτηση ελέγχου για τη μετάβαση στη νέα έκδοση του προτύπου πρέπει να υποβληθεί εγκαίρως προκειμένου να διασφαλιστεί ότι η διαδικασία πιστοποίησης σύμφωνα με τη νέα έκδοση του προτύπου ολοκληρώνεται πριν από τη λήξη της μεταβατικής περιόδου.

- Μετά την επιτυχή μετάβαση στη νέα έκδοση του προτύπου ISO/IEC 27001:2022, η BQC εκδίδει νέο πιστοποιητικό στον πελάτη. Η σημασία της πιστοποίησης συνδέεται με τον ισχύοντα κύκλο πιστοποίησης και παραμένει αμετάβλητη.

δ) Προετοιμασία των οργανισμών για τη μετάβαση στη νέα έκδοση του προτύπου:

- Εάν ο έλεγχος μετάβασης διενεργείται μαζί με επιθεώρηση επιτήρησης ή επιθεώρηση με σκοπό την ανανέωση της πιστοποίησης, ο χρόνος επιθεώρησης θα αυξηθεί κατά τουλάχιστον **0,5 ανθρωποημέρα** για σκοπούς συμμόρφωσης του ελέγχου με τις νέες/τροποποιημένες απαιτήσεις του ISO/IEC 27001:2022. Σε περίπτωση που η επιθεώρηση μετάβασης διεξάγεται ως ανεξάρτητη διαδικασία, τότε ο χρόνος της επιθεώρησης μετάβασης είναι τουλάχιστον **1 ανθρωποημέρα**. Οι δραστηριότητες που σχετίζονται με τη μετάβαση θα ρυθμίζονται από τη σύμβαση που ισχύει για τον τρέχοντα τριετή κύκλο πιστοποίησης.

- ✓ GAP Analysis κατά ISO/IEC 27001:2022 και αλλαγές που καθορίζονται από τον οργανισμό
- ✓ Αλλαγές που πραγματοποιούνται από τον οργανισμό στο σύστημα διαχείρισής του
- ✓ Επικαιροποίηση του Statement of Applicability (SoA)
- ✓ Επικαιροποίηση του Risk Management Plan, κατά περίπτωση
- ✓ Εφαρμογή και αποτελεσματικότητα των νέων ή/και τροποποιημένων ελέγχων (controls)
- ✓ Τροποποίηση εγγράφων πιστοποίησης

- Συνιστάται στους πιστοποιημένους οργανισμούς, όσο το δυνατόν νωρίτερα, να αρχίσουν να προετοιμάζονται για τη μετάβαση να σχεδιάσουν και να εφαρμόσουν σωστά τις απαραίτητες αλλαγές στο σύστημα διαχείρισής τους. Για αυτό, ππροτείνονται τα ακόλουθα βήματα:
  - ✓ Εξοικείωση με το περιεχόμενο και τις απαιτήσεις του νέου προτύπου εστιάζοντας παράλληλα στις αλλαγές που συνεπάγεται η νέα έκδοση του προτύπου
  - ✓ Εκπαίδευση του σχετικού προσωπικού προκειμένου να κατανοήσει τις απαιτήσεις και τις βασικές αλλαγές
  - ✓ Προσδιορισμός των ελλείψεων που πρέπει να εξαλειφθούν προκειμένου να ικανοποιηθούν οι νέες απαιτήσεις και κατάρτιση σχεδίου εφαρμογής
  - ✓ Εφαρμογή αλλαγών στο σύστημα διαχείρισης προκειμένου να ικανοποιηθούν οι απαιτήσεις της νέας έκδοσης του προτύπου

4. Σχετικές Αναφορές

ISO/IEC 27001:2022

IAF MD 26:2023 Issue 2

ISO/IEC 27701:2019

ΧΡΟΝΟΔΙΑΓΡΑΜΜΑ ΜΕΤΑΒΑΣΗΣ ΕΣΥΔ