AVRV's policy for transition to ISO 27001: 2022

Πολιτική της AVRV για την μετάβαση στο ISO 27001: 2022

A. Introduction

The International Organization for Standardization" (ISO) has published a new version of ISO 27001:2022 on 25/10/2022.
ISO/IEC 27001 is the world's best-known standard for information security management systems (ISMS), it defines requirements an ISMS must meet. The ISO/IEC 27001 standard provides companies of any size and from all sectors of activity with guidance for establishing, implementing, maintaining and continually improving an information security management system.
Conformity with ISO/IEC 27001 means that an organization or business has put in place a system to manage risks related to the security of data owned or handled by the company, and that this system respects all the best practices and principles enshrined in this International Standard.
The ISO 27001:2022 cancels and replaces the ISO 27001:2013.

B. Key Changes

Compared with ISO/IEC 27001:2013, the main changes of ISO/IEC 27001:2022 include, but are not limited to:

1. Annex A references the information security controls in ISO/IEC 27002:2022, which includes the information of control title and control.
2. The notes of Clause 6.1.3 c) are revised editorially, including deleting the control objectives and using "information security control" to replace "control".
3. The wording of Clause 6.1.3 d) is re-organized to remove potential ambiguity.
4. Adding a new item 4.2 c) to determine the requirements of the interested parties addressed through an information security management system (ISMS).
5. Adding a new subclause 6.3 - Planning for changes, which defines that the changes to the ISMS shall be carried out by the organization in a planned manner.
6. Keeping the consistency in the verb used in connection with documented information, for example, using "Documented information shall be available as evidence of XXX" in clauses 9.1, 9.2.2, 9.3.3 and 10.2.
7. Using "externally provided process, products or services" to replace "outsourced processes" in Clause 8.1 and deleting the term "outsource".
8. Naming and reordering the subclauses in Clause 9.2 - Internal audit and 9.3 - Management review.
9. Exchanging the order of the two subclauses in Clause 10 - Improvement.
10. Updating the edition of the related documents listed in Bibliography, such as ISO/IEC 27002 and ISO 31000.
11. Some deviations in ISO/IEC 27001:2013 to the high-level structure, identical core text, common terms and core definitions of MSS are revised for consistency with the harmonized structure for MSS, for example, Clause 6.2 d).

C. Timescale for transition of Certified Organizations

AVRV will follow the IAF MD 26:2023 issued on 15/2/2023 and instruction of ESYD issued on 20/4/2023 for the transition to ISO 27001:2022.

The time scale for the transition of certification of certified clients against ISO 27001:2022 is:

- April 2024: Initial and recertification audits will be permitted only against ISO 27001:2022
- October 2025: Due period for completion of the transition of certified clients

D. Transition audit to Certified Organizations

AVRV will perform transition audit to the clients within the time frame of the above paragraph following the rules of IAF MD 26:2023 as described below:

Audit execution

1. AVRV may conduct the transition audit in conjunction with the surveillance audit, recertification audit or through a separate audit.
2. The transition audit shall not only rely on the document review, especially for reviewing the technological information security controls.
3. The transition audit shall include, but not be limited to the following:
   - The gap analysis of ISO/IEC 27001:2022, as well as the need for changes to the client's ISMS.
   - The updating of the statement of applicability (SoA).
   - If applicable, the updating of the risk treatment plan.
   - The implementation and effectiveness of the new or changed information security controls chosen by the clients.
4. AVRV may conduct the transition audit remotely if they ensure the transition audit objectives is met.

Extra time for the transition

1. Minimum of 0.5 auditor day for the transition audit when it is carried out in conjunction with a recertification audit.
2. Minimum of 1.0 auditor day for the transition audit when it is carried out in conjunction with a surveillance audit or as a separate audit.

E. Flow of Actions

Typical flow of actions related to the transition of certification against ISO 27001:2022 required by AVRV and certified clients is as follows:

1. AVRV will communicate the new certification requirements to its certified clients using the present document
2. AVRV is waiting for the completion of the accreditation transition by ESYD; at the completion of the transition by ESYD, the actions 3-8 will take place
3. AVRV will communicate with the clients in order to define the preferable period for planning the transition audit according to the provisions of the paragraph C above
4. Certified clients will inform AVRV about the preferable period for planning the transition audit according to the provisions of the paragraph C above, submitting relevant written application.
5. AVRV will modify accordingly the audit program for the next period of the current certification cycle or plan accordingly the recertification audit
6. Certified clients will modify its Information Security Management system accordingly, AVRV is recommending the clients to plan and commence required actions at the earliest opportunity
7. AVRV will prepare and submit to the client the audit plan containing provisions for the transition
8. AVRV will decide about the transition based on the results of the audit and update the certification documents for the certified client accordingly.

All certifications based on ISO/IEC 27001:2013 shall expire or be withdrawn at the end of the transition period, October 2025. The expiration of the current certification cycle will not be changed if the transition audit is a separate audit in the middle of a certification cycle or combined with a surveillance audit.

Sources

- https://iaf.nu/iaf_system/uploads/documents/IAF_MD26_Issue_2_15012023.pdf
- https://esyd.gr/main/wp-content/uploads/2023/05/%CE%A7%CE%A1%CE%9F%CE%9D%CE%9F%CE%94%CE%99%CE%91%CE%93%CE%A1%CE%91%CE%9C%CE%9C%CE%91_ISO-27001_2022.pdf

AVRV's policy for transition to ISO 27001: 2022

Πολιτική της AVRV για την μετάβαση στο ISO 27001: 2022

Α. Εισαγωγή

Ο Διεθνής Οργανισμός Τυποποίησης (ISO) δημοσίευσε την έκδοση του ISO 27001:2022 στις 25/10/2022.

Το ISO/IEC 27001 είναι το πιο γνωστό πρότυπο στον κόσμο για συστήματα διαχείρισης ασφάλειας πληροφοριών (ISMS) και καθορίζει τις απαιτήσεις που πρέπει να πληροί ένα σύστημα διαχείρισης ασφάλειας πληροφοριών. Το πρότυπο ISO/IEC 27001 παρέχει σε εταιρείες, οποιουδήποτε μεγέθους και από όλους τους τομείς δραστηριότητας, καθοδήγηση για τη δημιουργία, την εφαρμογή, τη συντήρηση και τη συνεχή βελτίωση του συστήματος διαχείρισης ασφάλειας πληροφοριών.

Η συμμόρφωση με το ISO/IEC 27001 σημαίνει ότι ένας οργανισμός ή επιχείρηση έχει θέσει σε εφαρμογή ένα σύστημα για τη διαχείριση κινδύνων που σχετίζονται με την ασφάλεια των δεδομένων που κατέχει ή διαχειρίζεται η εταιρεία και ότι αυτό το σύστημα σέβεται όλες τις βέλτιστες πρακτικές και αρχές που κατοχυρώνονται σε αυτό το Διεθνές Πρότυπο.

Το ISO 27001:2022 ακυρώνει και αντικαθιστά το ISO 27001:2013.

Β. Βασικές Αλλαγές

Οι κύριες διαφοροποιήσεις που εισάγονται από το ISO/IEC 27001:2022 σε σύγκριση με το ISO/IEC 27001:2013 είναι στα παρακάτω σημεία:

1. Στο Παράρτημα Α όπου αναφέρονται οι έλεγχοι ασφάλειας πληροφοριών που καθορίζονται από το ISO/IEC 27002:2022.
2. Φραστικές αλλαγές στις σημειώσεις της παραγράφου 6.1.3 γ), συμπεριλαμβανομένων της διαγραφής της έννοιας "στόχος ελέγχου" και της χρήσης του όρου "έλεγχος ασφάλειας πληροφοριών" αντικαθιστώντας το όρο "έλεγχος" .
3. Αναδιατύπωση της παραγράφου 6.1.3 δ) για την άρση πιθανής ασάφειας.
4. Προσθήκη νέου στοιχείου 4.2 γ) για τον καθορισμό των απαιτήσεων των ενδιαφερομένων μερών που αντιμετωπίζονται μέσω συστήματος διαχείρισης ασφάλειας πληροφοριών (ISMS).
5. Προσθήκη νέας υπο-παραγράφου 6.3 - Σχεδιασμός αλλαγών, η οποία ορίζει ότι οι αλλαγές στο ISMS θα πραγματοποιούνται από τον οργανισμό με προγραμματισμένο τρόπο.
6. Διατήρηση της συνέπειας στο ρήμα που χρησιμοποιείται σε σχέση με τεκμηριωμένες πληροφορίες, για παράδειγμα, με τη χρήση "Τεκμηριωμένες πληροφορίες θα είναι διαθέσιμες ως απόδειξη του XXX" στις παραγράφους 9.1, 9.2.2, 9.3.3 και 10.2.
7. Στην παράγραφο 8.1 χρήση του όρου "εξωτερικά παρεχόμενες διεργασίες, προϊόντα ή υπηρεσίες" σε αντικατάσταση του "διεργασίες που ανατίθενται υπεργολαβικά" και διαγραφή του όρου "υπεργολαβική ανάθεση".
8. Ονομασία και αναδιάταξη των υπο-παραγράφων της παραγράφου 9.2 – Εσωτερικές επιθεωρήσεις και 9.3 – Ανασκόπηση από την Διοίκηση.
9. Ανταλλαγή της σειράς των δύο υπο-παραγράφων της παραγράφου 10 - Βελτίωση.
10. Ενημέρωση της έκδοσης των σχετικών εγγράφων που παρατίθενται στη Βιβλιογραφία, όπως το ISO/IEC 27002 και το ISO 31000.
11. Διόρθωση αποκλίσεων στην δομή για την εναρμόνιση με την προσέγγιση "high-level structure", για παράδειγμα στην παράγραφο 6.2 δ).

Γ. Χρονοδιάγραμμα μετάβασης πιστοποιημένων οργανισμών

Η AVRV θα ακολουθήσει την IAF MD 26:2023 που εκδόθηκε στις 15/2/2023 και την οδηγία του ΕΣΥΔ που εκδόθηκε στις 20/4/2023 για τη μετάβαση στο ISO 27001:2022.

Το χρονοδιάγραμμα για τη μετάβαση της πιστοποίησης των πιστοποιημένων οργανισμών έναντι του ISO 27001:2022 έχει ως εξής

- Από τον Απρίλιο του 2024 οι αρχικές πιστοποιήσεις και οι επαναπιστοποιήσεις θα πραγματοποιούνται μόνο σύμφωνα με το ISO 27001:2022
- Μέχρι τον Οκτώβριο του 2025 θα πρέπει να έχει ολοκληρωθεί η μετάβαση όλων των πιστοποιημένων οργανισμών

Δ. Επιθεώρηση μετάβασης των Πιστοποιημένων Οργανισμών

Η AVRV θα πραγματοποιήσει την επιθεώρηση μετάβασης στους Οργανισμούς που πιστοποιεί εντός του χρονικού πλαισίου της παραπάνω παραγράφου ακολουθώντας τους κανόνες της IAF MD 26:2023 όπως συνοπτικά περιγράφεται παρακάτω:

<u>Υλοποίηση επιθεώρησης</u>

1. Η AVRV μπορεί να πραγματοποιήσει την επιθεώρηση μετάβασης σε συνδυασμό με τον μία τακτική επιθεώρηση επιτήρησης, με την επιθεώρηση επαναπιστοποίησης ή μέσω ειδικής έκτακτης επιθεώρησης
2. Η επιθεώρηση μετάβασης δεν θα περιοριστεί μόνο στην επιθεώρηση εγγράφων του συστήματος ειδικά κατά την εξέταση των τεχνολογικών πληροφοριών για τους ελέγχους ασφάλειας πληροφοριών.

3. Ο έλεγχος μετάβασης περιλαμβάνει, αλλά δεν περιορίζεται στα ακόλουθα:
   - Την ανάλυση αποκλίσεων από το ISO/IEC 27001:2022, καθώς και τις αλλαγές στο ISMS του οργανισμού για την αντιμετώπιση των αποκλίσεων.
   - Την επικαιροποίηση του statement of applicability (SoA) του οργανισμού.
   - Την επικαιροποίηση του σχεδίου αντιμετώπισης κινδύνων, αν αυτό απαιτείται.
   - Την εφαρμογή και την αποτελεσματικότητα των νέων ή τροποιημένων ελέγχων ασφάλειας πληροφοριών που έχουν επιλεγεί από τον οργανισμό.
4. Η AVRV μπορεί να διενεργήσει την επιθεώρηση μετάβασης εξ αποστάσεως, εάν διασφαλίζεται ότι επιτυγχάνονται οι στόχοι της επιθεώρησης μετάβασης.

Επιπλέον χρόνος για τη μετάβαση

1. Τουλάχιστον 0,5 ανθρωποημέρα για την επιθεώρηση μετάβασης όταν αυτή διενεργείται σε συνδυασμό με επιθεώρηση επαναπιστοποίησης .
2. Τουλάχιστον 1,0 ημέρα ελεγκτή για τον έλεγχο μετάβασης όταν αυτός διενεργείται σε συνδυασμό με έλεγχο επιτήρησης ή ως χωριστός έλεγχος.

Ε. Ροή Ενεργειών

Η τυπική ροή ενεργειών που σχετίζονται με τη μετάβαση της πιστοποίησης σύμφωνα με το ISO 27001:2022 που απαιτείται από την AVRV και τους πιστοποιημένους πελάτες της είναι η εξής:

1. Η AVRV θα κοινοποιήσει τις νέες απαιτήσεις πιστοποίησης στους πιστοποιημένους πελάτες της χρησιμοποιώντας το παρόν έγγραφο
2. Η AVRV περιμένει την ολοκλήρωση της μετάβασης διαπίστευσης από το ΕΣΥΔ, με την ολοκλήρωση της μετάβασης από το ΕΣΥΔ θα γίνουν οι ενέργειες 3-8
3. Η AVRV θα επικοινωνήσει με τους πελάτες προκειμένου να καθορίσει την προτιμώμενη περίοδο για τον προγραμματισμό του ελέγχου μετάβασης σύμφωνα με τις διατάξεις της παραγράφου Γ παραπάνω
4. Οι πιστοποιημένοι πελάτες θα ενημερώσουν την AVRV για την προτιμώμενη περίοδο για τον προγραμματισμό του ελέγχου μετάβασης σύμφωνα με τις προβλέψεις της παραγράφου Γ παραπάνω, υποβάλλοντας σχετικό γραπτό αίτημα
5. Η AVRV θα τροποποιήσει ανάλογα το πρόγραμμα ελέγχου για την επόμενη περίοδο του τρέχοντος κύκλου πιστοποίησης ή θα προγραμματίσει αναλόγως την επιθεώρηση επαναπιστοποίησης.
6. Οι πιστοποιημένοι πελάτες θα τροποποιήσουν το σύστημα διαχείρισης ασφάλειας πληροφοριών ανάλογα, η AVRV συνιστά στους πελάτες της να σχεδιάσουν και να πραγματοποιήσουν τις απαιτούμενες ενέργειες το συντομότερο δυνατό
7. Η AVRV θα προετοιμάσει και θα υποβάλει στον πελάτη πρόγραμμα επιθεώρησης που περιέχει τις προβλέψεις για τη μετάβαση
8. Η AVRV θα αποφασίσει για τη μετάβαση με βάση τα αποτελέσματα της επιθεώρηση μετάβασης και θα επικαιροποιήσει κατάλληλα τα πιστοποιητικά.

Όλες οι πιστοποιήσεις που βασίζονται στο ISO/IEC 27001:2013 θα λήξουν ή θα αποσυρθούν στο τέλος της μεταβατικής περιόδου, τον Οκτώβριο του 2025. Η λήξη του τρέχοντος κύκλου πιστοποίησης δεν θα αλλάξει εάν η επιθεώρηση μετάβασης είναι ειδική επιθεώρηση στη μέση ενός κύκλου πιστοποίησης ή επιθεώρηση μετάβασης σε συνδυασμό με επιθεώρηση επιτήρησης.

Πηγές:

- https://iaf.nu/iaf_system/uploads/documents/IAF_MD26_Issue_2_15012023.pdf
- https://esyd.gr/main/wp-content/uploads/2023/05/%CE%A7%CE%A1%CE%9F%CE%9D%CE%9F%CE%94%CE%99%CE%91%CE%93%CE%A1%CE%91%CE%9C%CE%9C%CE%91_ISO-27001_2022.pdf