IAF Mandatory Document

TRANSITION REQUIREMENTS FOR ISO/IEC 27001:2022

Issue 2

(IAF MD 26:2023)

Issued: 15 February 2023 Application Date: 15 February 2023 IAF MD 26:2023, Issue 2

The International Accreditation Forum, Inc. (IAF) facilitates trade and supports industry and regulators by operating a worldwide mutual recognition arrangement among Accreditation Bodies (ABs) in order that the results issued by Conformity Assessment Bodies (CABs) accredited by IAF members can be accepted globally.

Accreditation reduces risk for business and its customers by assuring them that accredited CABs are competent to carry out the work they undertake within their scope of accreditation. ABs that are members of IAF and their accredited CABs are required to comply with appropriate international standards and IAF mandatory documents for the consistent application of those standards.

ABs that are signatories to the IAF Multilateral Recognition Arrangement (MLA) are evaluated regularly by an appointed team of peers to provide confidence in the operation of their accreditation programs. The structure of the IAF MLA is detailed in IAF PL 3 - Policies and Procedures on the IAF MLA Structure and for Expansion of the Scope of the IAF MLA. The scope of the IAF MLA is detailed in the IAF MLA Status document.

The IAF MLA is structured in five levels: Level 1 specifies mandatory criteria that apply to all ABs, ISO/IEC 17011. The combination of a Level 2 activity(ies) and the corresponding Level 3 normative document(s) is called the main scope of the MLA, and the combination of Level 4 (if applicable) and Level 5 relevant normative documents is called a sub-scope of the MLA.

- The main scope of the MLA includes activities e.g. product certification and associated mandated standards e.g. ISO/IEC 17065. The attestations made by CABs at the main scope level are considered to be equally reliable.
- The sub scope of the MLA includes conformity assessment requirements e.g. ISO 9001 and scheme specific requirements, where applicable, e.g. ISO 22003-1. The attestations made by CABs at the sub scope level are considered to be equivalent.

The IAF MLA delivers the confidence needed for market acceptance of conformity assessment outcomes. An attestation issued, within the scope of the IAF MLA, by a body that is accredited by an IAF MLA signatory AB can be recognized worldwide, thereby facilitating international trade.

TABLE OF CONTENTS

Issue No 2
Prepared by: IAF Technical Committee
Approved by: IAF Members Date: 03 February 2023
Issue Date: 15 February 2023 Application Date: 15 February 2023
Name for Enquiries: Elva Nilsen
IAF Corporate Secretary
Telephone: +1 613 454-8159
Email: secretary@iaf.nu

Introduction to IAF Mandatory Documents

The term “should” is used in this document to indicate recognised means of meeting the requirements of the standard. A Conformity Assessment Body (CAB) can meet these in an equivalent way provided this can be demonstrated to an Accreditation Body (AB). The term “shall” is used in this document to indicate those provisions which, reflecting the requirements of the relevant standard, are mandatory.

Transition Requirements for ISO/IEC 27001:2022

1. INTRODUCTION

All documents that provide information on transitions of normative documents will be mandatory documents to be followed by IAF MLA Accreditation Body (AB) signatories and accredited Conformity Assessment Bodies (CABs), with the scope as detailed in this document. This document is developed by an appointed Task Force of the IAF Technical Committee and in accordance with IAF PR 7:2022 *Requirements for Producing IAF Mandatory Documents on Transitions*.

This document provides transition requirements for the following and is mandatory for the related IAF MLA AB signatories and accredited CABs:

Normative Document:	ISO/IEC 27001:2022
Replacing:	ISO/IEC 27001:2013
Current Status (at time of MD publication):	IS
Transition Period:	3 Years (36 months)

2. SUMMARY OF KEY CHANGES

2.1 Background

According to the related ISO policy, ISO/IEC FDIS 27001:2022 was prepared through integrating ISO/IEC 27001:2013 with ISO/IEC 27001:2013/COR 1:2014, ISO/IEC 27001:2013/COR 2:2015 and ISO/IEC 27001:2013/DAmd1 in July 2022. Additionally, ISO required ISO/IEC FDIS 27001:2022 to align with the harmonized structure for management system standards (MSS) defined in Annex SL of the ISO/IEC Directives, Part 1, Consolidated ISO supplement, 2022. Based on the result of the FDIS ballot, ISO published ISO/IEC 27001:2022 on 25 October 2022.

Note 1: ISO/IEC 27001:2013/DAmd1 was prepared to align with ISO/IEC 27002:2022, which updated Annex A and the notes of Clause 6.1.3 c). DAmd is the abbreviation of Draft Amendment.

Note 2: No more than two separate documents in the form of amendments shall be published modifying a current International Standard (see ISO/IEC Directive Part 1, 2022, Clause 2.10.3), therefore, the new edition of ISO/IEC 27001 had to be published after the preparation of ISO/IEC 27001:2013/DAmd1.

2.2 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).

Note 1: The first two items come from ISO/IEC 27001:2013/DAmd1, the third item is from ISO/IEC 27001:2013/COR 2:2015 and the other changes result from the harmonized structure for MSS.

Note 2: Compared with the old edition, the number of information security controls in ISO/IEC 27002:2022 decreases from 114 controls in 14 clauses to 93 controls in 4 clauses. For the controls in ISO/IEC 27002:2022, 11 controls are new, 24 controls are merged from the existing controls, and 58 controls are updated. Moreover, the control structure is revised, which introduces “attribute” and “purpose” for each control and no longer uses “objective” for a group of controls.

Note 3: ISO/IEC 27001:2013/COR 1:2014 is related to Annex A and overlapped by ISO/IEC 27001:2013/DAMD1.

2.3 The Impact

The impact of the changes in ISO/IEC 27001:2022 includes, but is not limited to the introduction of a new Annex A and Clause 6.3 - Planning for changes because:

1) ISO/IEC 27001:2013/COR 2:2015 has already been published and implemented.
2) Annex A is normative.
3) The harmonized structure for MSS is considered as a minor revision for the high-level structure, identical core text, common terms and core definitions of MSS, in which most of the changes are considered editorial.

The requirements in ISO/IEC 27001 that use the reference control set in Annex A are the comparison process between the information security controls determined by the organization and those in Annex A (6.1.3 c)) and the production of a Statement of Applicability (6.1.3 d)). By comparing the necessary information security controls to those in Annex A, the organization may confirm that any necessary information security control from the reference set in Annex A of ISO/IEC 27001:2022 is not inadvertently omitted.

Such comparison might not lead to the discovery of any necessary information security control that has been inadvertently omitted. However, if inadvertently omitted necessary information security controls are discovered, the organization shall update its risk treatment plans to accommodate the additional necessary information security controls and implement them.

As implied above, the impact of ISO/IEC 27001:2022 on the organizations that have implemented ISMS need not be significant.

3. KEY TIMESCALE

Activity	Due Date
AB	
AB to be ready to assess to ISO/IEC 27001:2022 no later than	6 months from the last day of publication month of ISO/IEC 27001:2022 (i.e. 30 April 2023)
Initial assessment by AB to ISO/IEC 27001:2022 only, to begin no later than	6 months from the last day of publication month of ISO/IEC 27001:2022 (i.e. 30 April 2023)
AB transitions of CABs completed by	12 months from the last day of publication month of ISO/IEC 27001:2022 (i.e. 31 October 2023)
CAB	
Initial certification and recertification by CAB to ISO/IEC 27001:2022 only, to begin no later than	18 months from the last day of publication month of ISO/IEC 27001:2022 (i.e. 30 April 2024)
CAB transitions of certified clients completed by	36 months from the last day of publication month of ISO/IEC 27001:2022 (i.e. 31 October 2025)

4. TRANSITION PROCESS ACTIONS

4.1 AB Actions

Activity	Y/N	Notes
AB's Arrangements	*Y*	1) AB shall establish its transition arrangement for ISO/IEC 27001:2022 considering the requirements of this document. 2) The transition arrangement shall address what the AB shall do and what the CABs shall do. The AB may have several separate documents to address the transition arrangement. 3) The transition arrangement shall include at least the consideration of the following: • The changes in ISO/IEC 27001 and the gap analysis.

		• The relevant personnel are competent for ISO/IEC 27001:2022 and transition process. Note: The assessment team, as a whole, shall have knowledge of information security technologies and practices (see IAF MD 13:2020, 4.2). As we all know, ISO/IEC 27002 provides a reference set of generic information security controls including implementation guidance. • The AB's related processes and documents affected by the change in ISO/IEC 27001 are identified, as well as IT systems for managing accreditation activities, if applicable. • The transition assessment programme. • There is a timely communication to CABs on the transition assessment programme, such as the timeline and transition assessment approach, and the consequences for not completing the transition by the deadline. 4) ABs are encouraged to plan and commence required actions at the earliest opportunity.
CAB Document Review	N	
CAB Technical Document Review	Y	1) AB shall conduct the technical document review to confirm whether or not CABs are competent for ISO/IEC 27001:2022. 2) AB shall determine the suitability of the CAB's transition arrangement and, if applicable, the effectiveness of its implementation through reviewing the following information submitted by CABs: • The gap analysis of the changes in ISO/IEC 27001:2022. • The transition arrangement and its implementation evidence. • The authorization of the related personnel. • The other relevant information deemed necessary by AB.

Technical Assessment at CAB Head Office (on-site or remote)	If applicable	If AB is able to obtain sufficient evidence through the CAB technical document review, then a CAB head office assessment is not required. If AB is not able to verify the effective implementation and conformance with the CAB's transition arrangement, then an office assessment is required.
CAB Witnessed Assessment(s)	N	
Is extra time likely to be needed for the transition?	Y	As a minimum, the assessment shall include an additional 0.5 assessment day to confirm transition of the CAB when the transition is done as a separate assessment.
Other	Y	1) AB may define the timeline for submitting the transition application by CABs in the transition assessment programme. 2) AB shall make the transition decision based on the result of transition assessment(s). 3) If applicable, AB shall update the accreditation information of the accredited CABs (e.g. accreditation certificate) if their competence for ISO/IEC 27001:2022 has been demonstrated. 4) If the accredited CAB does not successfully complete the transition assessment before the related due date listed in Clause 3, the expiry date of their accreditation for ISO/IEC 27001:2013 shall not be later than the end of the transition period.

4.2 CAB Actions

Activity	**Y/N**	**Notes**
CAB's Arrangements	Y	1) CAB shall establish its transition arrangement for ISO/IEC 27001:2022 considering the requirements of this document and the transition arrangement of the related AB. 2) The transition arrangement shall address what the CAB shall do and what the client shall do. The CAB may have several separate documents to address the transition arrangement.

		3) The transition arrangement shall include at least the consideration of the following: • The changes in ISO/IEC 27001 and the gap analysis. • The need to modify the related certification processes, documents and, if applicable, IT systems for managing certification activities. • The relevant personnel are competent for ISO/IEC 27001:2022 and transition process. • The audit team, as a whole, shall have knowledge of all information security controls contained in ISO/IEC 27002:2022 and their implementation (see ISO/IEC 27006:2015, 7.1.2.1.3 b)). • The transition audit programme. • There is a timely communication to the clients on the transition programme, such as the timeline, transition audit approach, and the consequences if the client fails to transition prior to the end of the transition period. 4) CABs are encouraged to plan and commence required actions at the earliest opportunity.
Transition audit	Y	1) CAB 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) CAB may conduct the transition audit remotely if they ensure the transition audit objectives is met.
Is extra time likely to be needed for the transition?	Y	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.
Other	Y	1) CAB may define the timeline for submitting the transition application by the certified clients in the transition audit programme. 2) CAB shall make the transition decision based on the result of transition audit. 3) CAB shall update the certification documents for the certified client if its ISMS meets the requirements of ISO/IEC 27001:2022. Note: When the certification document is updated because the client successfully completed only the transition audit, the expiration of its current certification cycle will not be changed. 4) All certifications based on ISO/IEC 27001:2013 shall expire or be withdrawn at the end of the transition period.

4.3 Other

4.3.1 The CAB office assessment following the transition decision shall focus on the verification of the implementation of the transition arrangement before the CAB's transition arrangement was totally completed. This office assessment shall include the following, at a minimum:

- The implementation of the CAB's revised processes and procedures.
- The competence of the related personnel is demonstrated before they were involved in the ISO/IEC 27001:2022 certification activities.
- The progress of the transition for the certified clients to ISO/IEC 27001:2022.

4.3.2 All witness assessments selected following the transition decision shall be based on ISO/IEC 27001:2022 and focus on the CAB's competence for conducting an audit based on ISO/IEC 27001:2022.

End of IAF Mandatory Document Transition Requirements for ISO/IEC 27001:2022

Further Information

For further information on this document or other IAF documents, contact any member of IAF or the IAF Secretariat.

For contact details of members of IAF see the IAF website: http://www.iaf.nu.

Secretariat:

Elva Nilsen
IAF Corporate Secretary
Telephone: +1 (613) 454-8159
Email: secretary@iaf.nu