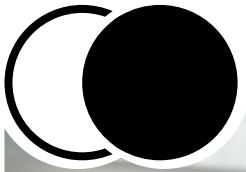


MSECB

MSECB Transition Policy on Management System Certification to ISO/IEC 27001:2022



Introduction

This policy applies to all ISO/IEC 27001 MSEC B Clients and Auditors and covers the timeline and necessary steps to be taken during the transition process from ISO/IEC 27001:2013 to ISO/IEC 27001:2022. The latest version of the standard has been published on October 25th, 2022.

MSEC B Certified Clients and Auditors are required to comply with the requirements and timelines of this policy, which is based on the IAF MD 26:2023 (Issue 2) – Transition Requirements for ISO/IEC 27001:2022.

Note: This policy has been updated on February 20, 2023, to be in alignment with Issue 2 of IAF MD 26:2023 (which has been issued on February 15, 2023).

Summary of Key Changes

As cyber threats become more advanced and the number of such threats continues to rise, the demand to update the practices for Information Security has never been more essential. At the beginning of the year 2022, ISO released [the newly revised ISO/IEC 27002:2022](#). The revision of ISO/IEC 27002 indicated that ISO/IEC 27001 will be updated as well.

Some of the key changes of the newly updated ISO/IEC 27001:2022 are as follows:

- The title of the standard has been changed to be in line with ISO/IEC 27002:2022. The new ISO/IEC 27001:2022 title is *Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements*.
- The title of Annex A has also changed from *Reference control objectives and controls* to *Information security controls reference*.
- Annex A is linked to the controls of ISO/IEC 27002:2022. The new Annex A now has 93 controls and includes the information of control title and control.
- There are minor adjustments to the vocabulary, sentence, and clause structure in clauses 4 through 10, particularly, in clauses 4.2, 6.1.3, 6.2, 6.3, 8.1, 9.2, 9.3 and 10.
- In Clause 6.1.3 c), the notes have been revised. The word “control” has been replaced with “Information security control” and the control objectives have been deleted.
- In Clause 6.1.3 d) the wording has been reorganized to avoid ambiguity.

Auditing and Key Timescale

- As of **April 30th, 2024**, all Initial (for new MSECBClients) and Recertification Audits (for existing ISO/IEC 27001:2013 MSECBCertified Clients) shall be conducted against ISO/IEC 27001:2022 and MSECBAuditors must be provided with the management system documentation addressing the requirements as per ISO/IEC 27001:2022.
- MSECBCertified Clients that have not demonstrated full conformity with ISO/IEC 27001:2022 by **October 31st, 2025**, are subject to certification withdrawal.
- All ISO/IEC 27001:2013 certificates issued after **October 31st, 2022**, will expire on **October 31st, 2025**.
- MSECBCertified Clients demonstrating full conformity with the requirements of ISO/IEC 27001:2022 will be issued a certificate with the new version of the standard.
- For MSECBCertified Clients to confirm the transition, during a surveillance audit or a separate audit, a minimum of one (1) audit day shall be included. When the transition audit is conducted in conjunction with the recertification audit a minimum of half (0.5) audit day shall be included.
- MSECBCertified Clients will be able to conduct the transition audit in conjunction with the surveillance audit, recertification audit or through a separate audit, which may be conducted remotely.
- The transition audit shall not only rely on the documentation review, especially for reviewing the technological controls. It shall include, but is not limited to the following:
 - Gap analysis of ISO/IEC 27001:2022 version and adapt the changes to their ISMS.
 - Update of the statement of applicability (SoA).
 - Ensure that their organization's risk treatment plan is updated.
 - Effective implementation of the new controls.

MSECB Auditors

All MSECB Auditors approved to conduct ISO/IEC 27001:2013 audits, will be asked to demonstrate competence on the new version of the standard prior to conducting any audits for ISO/IEC 27001:2022.

MSECB will accept Foundation, Transition, or Lead Training Courses offered by accredited personnel certification bodies, which shall include amongst others a detailed overview of ISO/IEC 27001:2022 so that auditors will be able to answer clients' questions.

Before taking any assignments, all certificates shall be submitted to the MSECB Auditor Program Coordinator at auditor@msecb.com.

MSECB



1555 boul de l'Avenir, Bureau 306,
Laval, Quebec H7S 2N5, Canada

info@msecb.com

www.msecb.com

in f