



ISO 27001:2022 INFORMATION SECURITY, CYBERSECURITY AND PRIVACY PROTECTION — INFORMATION SECURITY MANAGEMENT SYSTEMS — REQUIREMENTS

TRANSITION PLAN OF STAREGISTER

1.0 Introduction

ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements are published on 25.October.2022

Relevant document; ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls are published on 15.February.2022.

2.0 Key Changes

ISO/IEC 27001:2022 is not a fully revised edition. Its main changes include:

- Annex A references to the controls in ISO/IEC 27002:2022, which includes the information of control title and control;
- The notes of Clause 6.1.3 c) are revised editorially, including deleting the control objectives and using “information security control” to replace “control”;
- The wording of Clause 6.1.3 d) is re-organized to remove the potential ambiguity.

3.0 Transition

Initial certification by CAB to ISO/IEC 27001: 2022 to begin no later than 12 months from the last day of publication month of ISO/IEC 27001:2022 (24.October.2023)

STAREGISTER transitions of certified clients completed by 36 months from the last day of publication month of ISO/IEC 27001:2022 (24. October.2025)

4.0 STAREGISTER plan

- a. The changes in ISO/IEC 27001 and the gap analysis;
- b. The need to modify the related certification processes, documents and, if applicable, IT systems for managing certification activities;
- c. the relevant personnel are competent for ISO/IEC 27001:2022 and transition process;
- d. The audit team, as a whole, shall have knowledge of all 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;
- e. 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.
- f. update the certification documents for the certified client if its ISMS meets the requirements of ISO/IEC 27001:2022;
- g. All certifications based on ISO/IEC 27001:2013 shall expire or be withdrawn at the end of the transition period;
- h. the competence of the related personnel is demonstrated before they are involved in the ISO/IEC 27001:2022 certification activities;



ISO 27001:2022 INFORMATION SECURITY, CYBERSECURITY AND PRIVACY PROTECTION — INFORMATION SECURITY MANAGEMENT SYSTEMS — REQUIREMENTS

TRANSITION PLAN OF STAREGISTER

5.0 Transition audit

STAREGISTER may conduct the transition audit in conjunction with the surveillance audit, recertification audit or through a separate audit.

The transition audit shall not only rely on the document review, especially for reviewing the technological controls.

The transition audit shall include, but not limited to the following:

- a. the gap analysis of ISO/IEC 27001:2022, as well as the need for changes to the client's ISMS;
- b. the updating of the statement of applicability (SoA);
- c. if applicable, the updating of the risk treatment plan;
- d. the implementation and effectiveness of the new or changed controls chosen by the clients.
- e. CAB may conduct the transition audit remotely if they ensure the transition audit objectives is met.
- f. As a minimum, the audit shall include an additional 0.5 auditor day to confirm transition of the certified clients when the transition is done during a surveillance audit or as a separate audit.

6.0 STAREGISTER clients to be certified ISO 27001:2022 shall

- a. the gap analysis of ISO/IEC 27001:2022
- b. if applicable, the updating of the risk treatment plan;
- c. the implementation and effectiveness of the new or changed controls
- d. the competence of the related personnel is demonstrated before they were involved in the ISO/IEC 27001:2022 certification activities;

7.0 Reference Document

IAF MD:26:2022 Transition Requirements for ISO/IEC 27001:2022