protiviti®
Global Business Consulting

ISO 27001:2022 – Key Changes and Approaches to Transition

Executive Summary:

This article will address the changes and updates to ISO 27001 standard published on October 25, 2022, and the approaches organizations can take to implement the changes introduced. There have been significant advancements in technology, as well as an increase in the complexity of security threats since the last iteration of ISO 27001 was published on September 25, 2013. The changes introduced in the ISO 27001 and the Annex A controls aim to provide guidance on improving the governance around the implemented security controls and addressing risks introduced by emerging security threats.

As organizations begin the transition process to ISO 27001:2022, they should factor in changes that may be needed across their security processes and updates to their policies, procedures and standard. Transition to the new version should be completed by October 31, 2025, and will require planning, education, staff and budget to accomplish.

What is ISO 27001:

ISO 27001 is an international standard that outlines a framework for an Information Security Management System (ISMS). The standard provides a systematic approach to implementing information security controls to manage the applicable risks to an organization. It provides guidance on the implementation of security controls and best practices for protecting information assets, including people, processes, and technology.

The standard covers the management of risks to the security of information that an organization holds. It includes requirements for risk assessment, the implementation of security controls, and regular reviews to ensure that the ISMS is effective. It also includes guidelines for incident management and business continuity planning. Organizations that adopt the standard are required to have a management system in place to protect against unauthorized access, disclosure, disruption, modification, or destruction of information.

ISO 27001 certification is the process of demonstrating to an external auditor from a certifying body, that the organization's ISMS meets the requirements outlined in the standard. Achieving certification requires the completion of an external audit, and ongoing surveillance audits to demonstrate ongoing compliance with the standard. Organizations that are certified can use the standard as a benchmark for their information security management, and it can also be used to demonstrate the company's commitment to information security to clients, stakeholders and regulatory bodies.

What are the changes to ISO 27001:

ISO 27001 was first published in 2005 and then revised on September 25, 2013, as ISO/IEC 27001:2013. The most recent revision was published on October 25, 2022, as ISO/IEC 27001:2022 "Information security, cybersecurity and privacy protection — Information security management systems".

It is important to understand the differences between ISO 27001 and ISO 27002. ISO 27001 is the main standard against which organizations are certified, whereas ISO 27002 provides guidance on implementing Annex A security controls.

The ISO 27001 management clauses (4-10) have undergone several minor changes, especially across the following clauses:

- Clause 4.2: Understanding the needs and expectations of interested parties
- Clause 6.2: Information Security objectives and planning to achieve them
- Clause 6.3: Planning of Changes
- Clause 8.1: Operational Planning and control

In terms of structural changes, Clause 9.2: Internal audit has been divided into 9.2.1: General and 9.2.2: Internal audit program. However, the requirements remain the same.

Similarly, Clause 9.3: Management review has been split into three subsections — 9.3.1: General, 9.3.2: Management review inputs, and 9.3.3: Management review results. A new mandatory item 9.3.2 c) has been added for the management review: “Changes in needs and expectations of interested parties that are relevant to the information security management system;” top management in the organization will need to ensure that this is covered at the management reviews.

The ISO 27001:2022 version also introduces a new Clause 6.3: Planning for Changes. “When the organization determines the need for changes to the information security management system, the changes shall be carried out in a planned manner.” To meet this requirement, it is important that changes to the ISMS are planned and evidence retained to show the changes were managed appropriately. Organizations should ensure they have a documented plan that includes activities completed, evidence of management review and communications based on the defined communication plan.

The major change that organizations should be aware of is the update to Annex A controls within the new ISO 27001:2022 standard. ISO 27001:2022 adopts a new structure for the Annex A controls (Information Security Controls), which has been reorganized, updated, and extended. This aligns with ISO/IEC 27002:2022, published in March 2022. ISO/IEC 27002 is to be used as a reference for selecting and implementing controls for risk treatment in an Information Security Management System (ISMS) based on ISO/IEC 27001.

Key Changes to ISO 27002 - Annex A Controls

The major changes to ISO 27002, include restructuring the original 14 control domains into 4 categories. As a result, the total number of controls has decreased from the original 114 to 93. This decrease has come mainly due to merging 57 controls into 24 controls. 58 controls remain mostly unchanged, with minor contextual updates, and 11 controls are brand new (not available in ISO/IEC 27001:2013).

The controls are restructured into 4 clauses:

- A.5 Organizational - contains 37 controls
- A.6 People - contains 8 controls
- A.7 Physical - contains 14 controls
- A.8 Technological - contains 34 controls

The 11 new controls added to Annex A include:

- A.5.7 Threat intelligence
- A.5.23 Information security for the use of cloud services
- A.5.30 ICT readiness for business continuity
- A.7.4 Physical security monitoring
- A.8.9 Configuration management
- A.8.10 Information deletion
- A.8.11 Data masking
- A.8.12 Data leakage prevention
- A.8.16 Monitoring activities
- A.8.23 Web filtering
- A.8.28 Secure coding

Key Transition Points for ISO 27001:2022

Organizations that are currently certified to ISO 27001:2013 will have three years to transition to ISO/IEC 27001:2022. The transition period began on October 31, 2022 and ends on October 31, 2025. Certifications based on ISO 27001:2013 will expire or be withdrawn at the end of the transition period.

Organizations pursuing ISO 27001 for the first time (both Stage 1 and Stage 2 audits) can be certified on the 27001:2013 version until October 2023. Transition audits can either be done at the same time as the organization's next audit (e.g., surveillance audit and transition audit), or separately.

All organizations that wish to remain certified to ISO 27001 will have to transition to the 2022 version of the standard within the set transition period which ends on October 31,2025. During the transition period both versions of the ISO 27001 standard remain valid and audits to either version of the standard may be conducted subject to the rules noted below, but plans should be made for an organization's transition to fully occur prior to the transition period ending.

- All new certifications starting Nov 1, 2023 should be to the new ISO 27001:2022 version, after this date all recertification audits are recommended to utilize the ISO 27001:2022 version.
- All transition audits should be conducted by July 31, 2025.
- Transition period ends on October 31, 2025, ISO 27001:2013 certificates will no longer be valid after this date.

Certification Timeline

- Entities that hold an ISO 27001:2013 will have to complete transition within 36 months.
    - During transition, existing ISO 27001:2013 certificates will remain valid.
    - ISO 27001:2022 certificates will be issued based on the 3-year re-certificate cycle.
- Transition audits to the ISO 27001:2022 are based on any one of the following:
    - Surveillance audit.
    - Recertification audit.
    - Special audit.
    - Initial certification does not require a transition audit.
- Transition audits must consider and include:
    - Gap analysis against ISO 27001:2002, and any needed changes to the auditee's ISMS.
    - Update of the Statement of Applicability (SoA).
    - Update of the risk treatment plan, as applicable.

A detailed report of the transition requirements can be found here.

How can organizations approach the transition to the revised Annex A in ISO 27001:2022.

Changes in Annex A will require organizations to realign their controls. There are two ways to transition to the new requirements. The first option would be to perform a comparison of the existing risk assessment for coverage against the Annex A controls. The new controls introduced in Annex A should be considered for applicability and risk treatment plans may need to be updated. The Statement of Applicability (SOA) would need to be updated to reflect any new controls added or modified.

The second option would be to perform a fresh risk assessment and identify relevant controls from the new Annex A, which may be considered to manage the risk. As a part of this process, coverage of all applicable Annex A controls should be ensured. Risk Treatment plans will likely require an amendment to reflect any new risks that require a treatment plan. A new SOA should be created which is aligned to the new controls. The final step would be to update any documents that reference the old set of controls.

How can Protiviti help

Whether you are currently certified to ISO/IEC 27001 or new to the standard, Protiviti provides an extensive array of services to prepare you for successful certification.

Our services include:

- ISO 27001 gap assessments and remediation support to prepare you for the certification audit. We can support all aspects of remediation activities required, from design of processes and architecture, implementation of solutions, and development of documentation to project and program management and subject matter expert support in specific areas.
- ISO 27001 internal audits as required by clause 9.2.
- Prepare your team and provide support during the certification process.

Contacts

Chip Wolford
+1.513.362.1716
Chip.wolford@protiviti.com

Anil Chacko

Anil.chacko@protiviti.com