protiviti®
Global Business Consulting

ISO 27002 Is Changing: What You Need To Do

Background

ISO 27002 contains details of controls required to be certified under the ISO 27001 standard. With the ever changing security threat landscape and the need to protect information assets, the International Organisation for Standardisation (ISO) has introduced several changes to the 27002 set of controls. These changes have been published in the latest version of the ISO 27002:2022 standard released in February 2022. This revision focuses on consolidating controls from the previous versions, categorising them differently and introducing attributes (hashtags) for each control which enable ease of maintenance and comparison with other security frameworks such as the National Institute of Standards and Technology – Cybersecurity Framework (NIST-CSF).

Changes in the revised version:

Title

The title of the revised standard has changed from "Information technology – Security techniques – Code of practice for information security controls" to "Information security, cybersecurity and privacy protection – Information security controls".

Controls

- The total number of controls has been reduced from 114 to 93
- 11 new controls have been introduced
- 24 controls have been consolidated
- 58 controls have been slightly rephrased to better align with the new categories.

Consolidation of existing categories

- The total number of categories have been reduced from 14 to 4. The new set of categories is now - Organisation, People, Physical and Technology. The new categorisation provides ease of classifying the controls and removes the redundancy or confusion in bucketing the controls under a specific category.

Introduction of attributes

- Each control is specified with the following attributes:
  - Control type – (Preventive, Detective, Corrective)
  - Information security properties – (Confidentiality, Integrity, Availability)
  - Cybersecurity concepts – (Identify, Protect, Detect, Respond, Recover)
  - Operational capabilities – (Governance, Asset management, Application security, Supplier relationships security etc.)
  - Security domains – (Governance and Ecosystem, Protection, Defence, Resilience)

Summary of new categories:

- **Organisation** – New controls on threat intelligence, information security for the use of cloud services and ICT readiness for business continuity has been added and most of the entity-level controls from the previous version have been consolidated under this category.
- **People** – No new controls have been added under this category. All existing controls under the human resource security and several from the confidentiality and non-disclosure agreements and information security event reporting as they relate to people have been included in this category.
- **Physical** – A new control related to physical security monitoring has been included with emphasis on the design of monitoring controls to detect unauthorised access.
- **Technology** – Several new controls have been added under the Technology category such as configuration management, information deletion, data masking, data leakage prevention, monitoring activities, web filtering and secure coding. These controls provide specific guidance as to what needs to be implemented, for example, the design and implementation of black/whitelisting of websites for web filtering.

protiviti®
Global Business Consulting

Changes your organisation needs to make:

- **Operational practices** –Existing practices and supporting tools may need to be modified to reflect the changes in the revised standard.
- **Documentation (policies and procedures)** –With the introduction of new controls, existing policies and procedures will need to be updated to address the new requirements and describe the design and implementation of the additional controls. Additionally, new procedures may need to be documented to reflect the change in process or approach.
- **Risk assessment** –The risk assessment approach needs to be revised to include all information that is required to be assessed for the new controls. For example, the risk assessment should include the risks associated with using cloud service/s if it is not already a part of the existing risk assessment.
- **Context and objective** –The context and objective of the existing Information Security Management System (ISMS) will need to be validated with the changes in the controls to incorporate any new security objectives that are deemed relevant for the organisation.
- **Statement of Applicability (SoA)** – With the changes to the list of controls, the SoA will need to be updated.
- **Gap assessment** –Organisations need to perform a gap assessment to identify the changes that need to be made along with the identification of effort and timelines to design and implement the new controls.
- **Control library** – The control library will need to be updated to ensure the correct mapping of controls to the new categories. The control attributes should also be updated for ease of comparison and validation.

How does this impact my existing certification:

You can continue to maintain your ISMS and get certified under the existing version but it is recommended to review and implement the changes from ISO 27002 as soon as possible. The ISO 27001 standard is in the final stages of review and the revision is expected to be published in the coming months. Once this revised version is published and released, it is expected that organisations will be given a grace period to implement the new controls and adopt the revised standard

How we can help:

With these new changes coming into effect, we can help you with the following:

- Provide a detailed view of the specific control level changes and the impact on your organisation.
- Uplift your existing documentation to reflect the changes in your system and control environment.
- Provide guidance and assistance in risk and gap assessments, and updates to your control library.
- Assist in the design and implementation strategy for new controls.
- Perform an internal audit to validate the updates, which can be relied upon by the certification body.

Contact us:

Ewen Ferguson
ewen.ferguson@protiviti.com.au

Krishnan Venkatraman
krishnan.venkatraman@protiviti.com.au

protiviti®
Global Business Consulting