TECHNICAL UPDATES

ISO/IEC 27001 and ISO/IEC 27002 : 2022 UPDATES

The primary changes involve a complete overhaul of the security controls (Annex A of 27001, detailed in 27002) to align with modern threats, cloud computing, and data privacy.

Here is a summary of the key updates for both standards:

ISO/IEC 27002 is the guidance standard detailing the security controls. The primary changes are structural and focused on modernization.

1. New Structure and Fewer Controls

The total number of controls has been reduced, and the structure has been simplified into four main organizational "themes" or clauses, replacing the previous 14 domains.

Feature	ISO 27002:2013	ISO 27002:2022
Total Controls	114	93 (58 updated, 24 merged, 11 new)
Control Domains	14 categories (e.g., HR Security, Communication)	4 Themes: 1. Organizational (37 controls) 2. People (8 controls) 3. Physical (14 controls) 4. Technological (34 controls)

2. New Controls (11 Total)

11 new controls were introduced to address modern risks, technologies, and practices:

- Threat intelligence (5.7)
- Information security for use of cloud services (5.23)

- ICT readiness for business continuity (5.30)
- Physical security monitoring (7.4)
- Configuration management (8.9)
- Information deletion (8.10)
- Data masking (8.11)
- Data leakage prevention (8.12)
- Monitoring activities (8.16)
- Web filtering (8.23)
- Secure coding (8.28)

3. Introduction of Attributes

Each control now includes five attributes (tags) for filtering and sorting, which helps organizations align controls with different perspectives (like the NIST Cybersecurity Framework or the CIA Triad: Confidentiality, Integrity, Availability):

- Control Type (e.g., Preventive, Detective, Corrective)
- Information Security Properties (e.g., Confidentiality, Integrity, Availability)
- Cybersecurity Concepts (e.g., Identify, Protect, Detect, Respond, Recover)
- Operational Capabilities
- Security Domains

ISO/IEC 27001:2022 Updates

ISO/IEC 27001 is the certifiable standard for the Information Security Management System (ISMS). Its main clauses (4-10) saw minor updates, while Annex A was fully revised to align with the new ISO 27002.

1. Management System Clauses (4-10)

The core structure remains the same (High-Level Structure/Annex SL), but there are a few minor language changes for clarity and better alignment with other ISO standards:

- Clause 6.3 (Planning of Changes): This is a new subclause requiring organizations to plan changes to the ISMS in a controlled and systematic manner.
- Clause 4.2 (Interested Parties): Clarification on monitoring and reviewing the needs and expectations of interested parties.
- Clause 8.1 (Operational Planning and Control): Stronger language on controlling externally provided processes, products, or services relevant to the ISMS.

Organizations certified to ISO 27001:2013 have a three-year transition period from the publication date to update their ISMS and achieve certification to the 2022 version.

- ISO/IEC 27002:2022 Publication: February 15, 2022
- ISO/IEC 27001:2022 Publication: October 25, 2022
- Transition Deadline: October 31, 2025 (After this date, ISO 27001:2013 certificates will expire or be withdrawn.)

Should you have any questions regarding this updates, please do not hesitate to contact us at info@issg.sg.