Examining Changes in the ISO 27001 and ISO 27002 Standards

UPDATE

ISO 27001

DEKRA On the safe side.

Due to growing cybersecurity challenges, ISO/IEC 27001 (with supporting voluntary ISO 27002 guidelines) mandates new requirements be implemented to ensure compliant information security management efforts in line with digitalized business practices and subsequent threats to digital data and systems.

Revisions to ensure effective information security

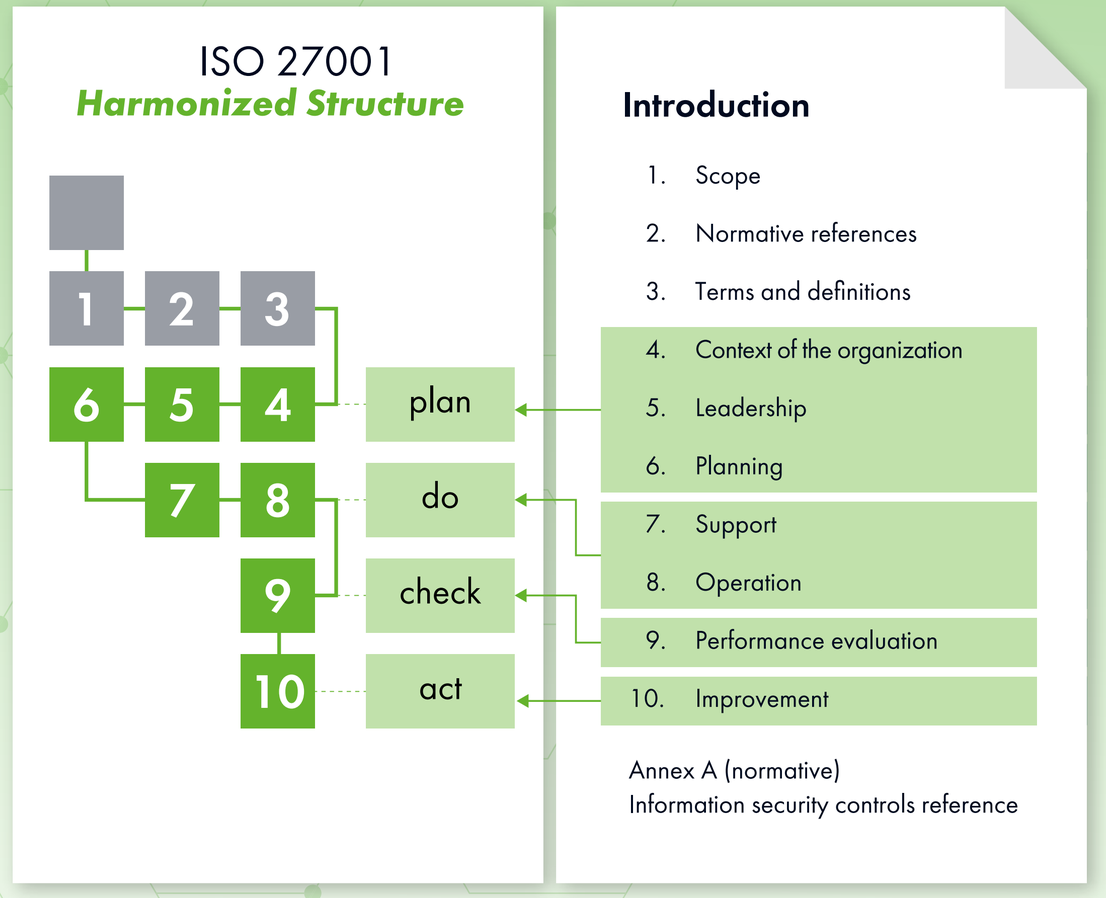
Companies working in the digital business landscape must adopt resilient security strategies and implement control measures to reduce breaches, protect intellectual property and safeguard confidential data in order to demonstrate a commitment to establishing a trusted brand built to succeed. Flexible and effective information security management plays a vital role in minimizing risk and defending against cyberattack.

ISO 27001 was revised in 2022 to reflect the previously updated ISO 27002:2022 guide for information security controls. Modifications to the ISO 27001 standard and ISO 27002 guidelines have been made to ensure information security measures are in line with current technological advancements and strengthen overall company resilience.

Main changes to the ISO 27001 standard

Revision to the ISO 27001 standard includes changes to the Harmonized Structure (HS) requiring processes and their interactions to be part of the information security management system (ISMS) and updates to the catalogue of security categories and measures listed in Annex A.

Construction of the *ISO 27001 Standard (Harmonized Structure)*



Changes to plan, do, check, act sections of the ISO 27001 Harmonized Structure

In adding the application of the Harmonized Structure to the ISO/IEC 27001:2022 revision, some sections and their contents had to be adapted. The changes fall in the plan, do, check, act (PDCA) sections and include:

- **Section 4.4: Information security management system**
  Requires determination of necessary processes and their interactions in the ISMS
- **Section 5.3: Organizational roles, responsibilities and authorities**
  Requires mandatory disclosure of organizational responsibilities and authorities for roles related to information security
- **Section 6.1.3: Information security risk treatment**
  Enables more flexible selection, design and expansion of reference measure listed in Annex A and emphasizes opening the management system framework for organization-specific measures
- **Section 6.3: Planning of changes**
  Requires mastery of ISMS-related change processes
- **Section 7.4: Communication**
  Previously “what about”, “when”, “with whom” and “who”, the section has been expanded to include the “how” of communication
- **Section 8.1: Operational planning and control**
  Requires processes within operational planning and control implementing measures to manage information security risks (with process criteria for process control)
- **Section 9.2 / 9.3: Internal audit / management review**
  Newly adapted to and further subdivided in the revised Harmonized Structure
- **Section 10.1 / 10.2: Continual improvement / Nonconformity and corrective action**
  Places prospective continuous improvement before retrospective handling of nonconformities and corrective action with no change in content.

Revision to Annex A of the ISO 27001 standard

In contrast to 114 information security measures divided into 14 categories in the 27001:2013 standard, only 93 measures listed in 4 key areas (organizational, people, physical, technological) are provided in Annex A of the new 27001:2022 update. Although some security measures have been deleted, 11 new measures have been added:

- **Threat intelligence –** Intelligence collection and analysis to determine protective measures
- **Information security for use of cloud services –** Secure processes for onboarding, use, management and exit from cloud providers
- **ICT readiness for business continuity –** Requirements for recovery measures with a new focus on technical measures
- **Physical security monitoring (PSM) –** Monitoring measures, intrusion alarms, etc. to deter and protect against unauthorized access
- **Data masking –** Restriction, anonymization and pseudonymization of data
- **Data leakage prevention –** Detection and monitoring of data loss/disclosure/data leakage
- **Monitoring of activities –** Proactive tracking of deviant activities
- **Web filtering –** Removing dangerous web pages that spread malware or read unauthorized data
- **Secure coding –** Eliminating vulnerabilities or susceptibility to attacks
- **Configuration management –** Correctly setting security measures and securing configuration
- **Information deletion –** Requirements for data storage with regard to DSGVO and GDPR

Updated ISO 27002 guidelines

Unlike the ISO 27001 standard that simply defines security measures, ISO 27002 is a supporting standard or code of practice. Although ISO 27001 Annex A lists security controls, for example, the newly named ISO 27002 "Information security, cybersecurity and privacy protection – Information security controls" provides guidance on how to implement those controls. Companies are free to use applicable ISO 27002 recommendations as they see fit.

Changes to ISO 27002 include a name change identifying the standard as a stand-alone set of information security controls and the introduction of 5 attributes designed to increase transparency and reduce application misinterpretations. These attributes include:

- **Control type**
  Indicates "controls" from the perspective of when and how they modify risk with respect to an information security incident
- **Impact on security objectives /IS properties (Information security properties)**
  Takes perspective of what information property the "control" is involved with
- **Classification of cybersecurity concepts**
  Indicates "controls" from cybersecurity perspective (cf. cybersecurity framework according to ISO/IEC TS 27110)
- **Operational capabilities**
  Considers "controls" from a practitioner/ISB perspective
- **Security domains**
  Indicates "controls" from the perspective of four IS domains

The aim of the revision was to improve the standard with a reference set of information security control objectives and provide a broader scope to encompass context-specific information security and privacy as well as cybersecurity risk management.

The 5 attributes of the *ISO 27002 structure* and their respective values

Control type	***Information security properties***	***Cybersecurity concepts***	***Operational capabilities***	***Security domains***
• Prevention • Discovery • Correction	• Confidentiality • Integrity • Availability	• Identify • Protect • Detect • Respond • Recover	• Governance • Asset management • Information protection • Human resource security • Physical security • System and network security • Application security • Secure configuration • Identity and access management • Threat and vulnerability management • Continuity • Supplier relationships security • Legal and compliance • Information security event management • Information security assurance	• Governance / Ecosystem • Protection • Defense • Resilience

Benefits of the revised standards

The new ISO 27001 and ISO 27002 standards focus on information security technology and address contemporary measures aligned to current organizational methods and the threats associated with the information security management system (ISMS). ISO 27001 has been simplified and now, with the help of ISO 27002, provides security measures with related attributes. Categorization has been streamlined and divided into topic blocks. Special attention has been paid to process orientation, emphasizing its importance and illustrating both its criteria and interactions. The Harmonized Structure has been revised to reflect process orientation status in effectively managing information security.

Transition timeline

As with all ISO revisions, there are deadlines for transition from the old to new certification standards. A transition period of three years started at the time of publishing in October 2022. During this grace period, companies have the opportunity to prepare for certification or recertification according to the new standard. As of October 31, 2025, all existing certificates must have already been converted to the revised ISO 27001 requirements. Initial or recertification audits can still be conducted according to ISO 27001:2013 for 18 months after publication of the new standard. Although the official date for certification under the revised ISO 27001:2022 should begin no later than November 2023, start times depend on the German Accreditation Body (DAkkS).

Call to learn more about how the revisions affect your company!

→ Contact us!