



The key changes in the ISO/IEC 27002:2022

WHITE PAPER



SGS



Introduction

ISO/IEC 27002 is a guidance document and is designed to be used as a reference for selecting controls while implementing an Information Security Management System (ISMS) based on ISO/IEC 27001 or as a guidebook for organizations implementing commonly accepted information security controls. The current ISO/IEC 27002:2013 edition had been under review since 2018¹ by ISO/IEC JTC 1/SC27 and the new edition was officially published on 15 Feb 2022. While part of controls remains

unchanged, there are significant changes in control layout and other controls. Since the Annex A of ISO/IEC 27001:2013 is designed to align with ISO/IEC 27002, ISO/IEC 27001 is being revised and the amendment version is estimated to be published in Q2 2022.

This article highlights the key changes in the 2022 edition as compared to the 2013 edition of ISO/IEC 27002.

Key changes

Number of Controls | 93

There are 93 controls in the 2022 edition vs 114 controls in the 2013 edition.

Control Categories | 4

Controls are regrouped into 4 categories, instead of 14 themes and 35 categories in the 2013 edition.

The four-categories layout emphasizes the protection of information and data is more than merely technological means. To achieve the information security outcomes, technological controls are just the remedies to prevent or mitigate the information security risks.

More importantly, the top management of organizations needs to set out the information security management framework and direction, as well as to identify and communicate the importance and impacts of different information to the business and the organization.

Besides, this new control layout can facilitate management to assign responsibilities within the organization for information security enhancement.

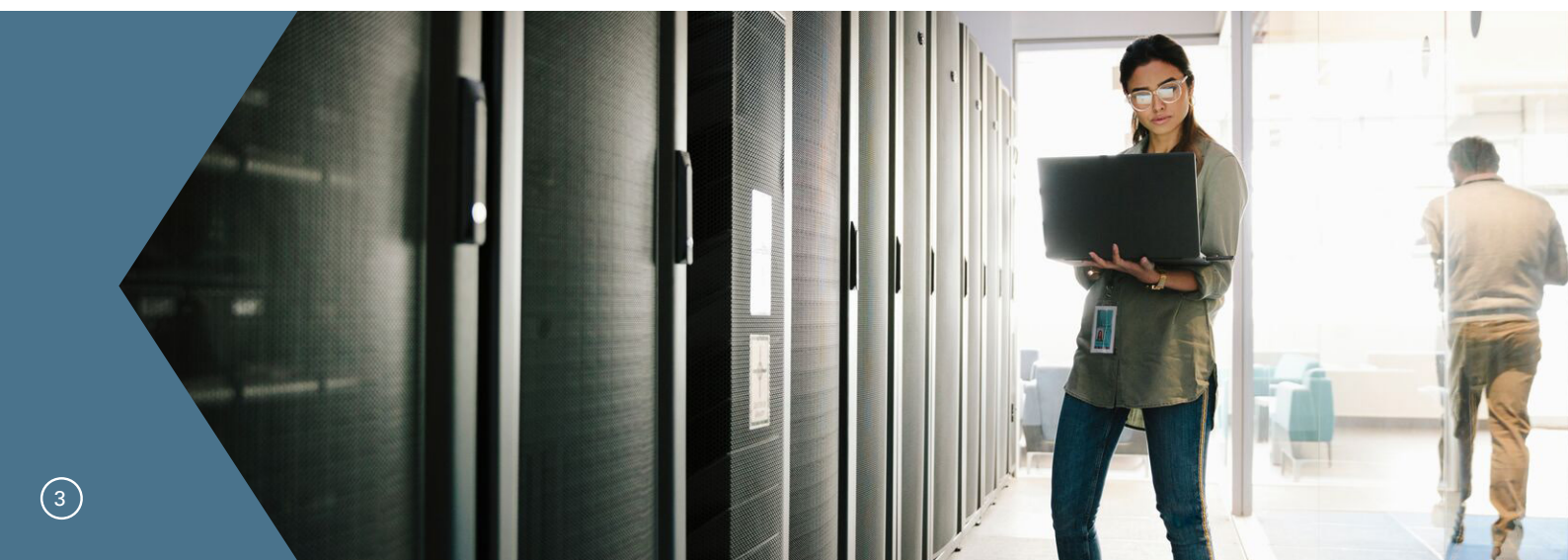
ISO/IEC 27002:2022	
5	Organizational controls
6	People controls
7	Physical controls
8	Technological controls

ISO/IEC 27002:2013		
5 Information security policies	6 Organization of information security	7 Human resource security
8 Asset management	9 Access control	10 Cryptography
11 Physical and environmental security	12 Operations security	13 Communications security
14 System acquisition, development and maintenance	15 Supplier relationships	16 Information security incident management
17 Information security aspects of business continuity management		18 Compliance

¹ Every ISO standard is subject to review every five years. Starting in Mar 2018, the ISO JTC1/SC27 proposed to update the standard, taking into account evolution of new technologies, emerging risks, and the changing industrial practices.

11 new controls are introduced to address the evolvement in technologies and industrial practices.

5.7	Threat intelligence	Organizations should stay alert and maintain awareness of the ever-changing threat environment. There are different levels of threat intelligence: strategic, tactical, and operational. Information of tactical and operational threat intelligence can be from the special interest groups (control 5.6 Contact with special interest groups), the lesson learned from information security incidents (control 5.27 Learning from information security incidents), or the Security Operation Center (SOC). Meanwhile, organizations should overlook the changing threat landscape, not only in their industry but also in other industries.
5.23	Information security for use of cloud services	There is no doubt that the addition of this new control is to respond to the increasing use of cloud services by organizations since the last decade. Though it is an organizational control, the proper use of this control requires technical knowledge of cloud technology. Therefore, organizations might consider involving cloud experts while implementing this control.
5.30	ICT readiness for business continuity	The purpose of this new control is different from control 5.29 (Information security during disruption). It aims to ensure the availability of the organization's information and other associated assets during disruption. The disaster recovery plan (DRP) established by the IT department can be an implementation example of this control, provided that the plan addresses the organization's business continuity requirements. Control 5.29 (Information security during disruption) aims to maintain the CIA of information during disruption, e.g., the physical access control is temporarily unavailable due to power-supply suspension.
7.4	Physical security monitoring	Though it is a new control according to Annex B of ISO/IEC 27002:2022, many organizations should have already adopted this control in their physical premises, e.g., by installing a surveillance system, intrusion detection system, or door access control system, etc.
8.9	Configuration management	Configuration management should be an active process to manage the configurations of hardware, software, services (e.g., cloud services), and networks throughout their lifecycle. System hardening is an implementation example of this control. The configurations should be maintained to ensure they remain effective. The changes should be conducted in a controlled manner by following the change management process 8.32 (Change management) and the change records should be securely stored.
8.10	Information deletion	The addition of these three controls echoes the title of the 2022 edition (<i>Information security, cybersecurity and privacy protection – Information security controls</i>). The controls are commonly adopted in the current data privacy laws and international standards, e.g., the GDPR, ISO/IEC 27701, to protect data subjects' rights.
8.11	Data masking	
8.12	Data leakage prevention	
8.16	Monitoring activities	This new control aims to monitor networks, systems and applications for anomalous behaviours and potential information security incidents. Organizations have adopted various monitoring means to monitor their IT environment, e.g. by installing anti-virus software, firewalls, or web filters with logging.
8.23	Web filtering	This new control is relatively straightforward. Many organizations have adopted it in their IT network. Though more external websites are filtered, the less exposure to malicious content, organizations should balance the information security risk and business needs.
8.28	Secure coding	This new control aims to reduce the number of potential information security vulnerabilities in the newly developed or enhanced software. In the 2013 edition, this control was omitted.



Merged Controls | 24

24 controls in the 2022 edition are the results of merging some controls from the 2013 edition. Merging of controls results in a reduced number of controls and thus creates a leaner standard.

Note: Part of the merged controls are extracted and shown in the table below. Audiences can refer to Annex B of ISO/IEC 27002:2022 for a full list of merged controls.

ISO/IEC 27002:2022		ISO/IEC 27002:2013		REMARK
The controls which are inseparable in implementation are merged.				
5.1	Policies for information security	5.1.1	Policies for information security	Review of information security policies is not possible if there are no such policies established. While the policies should be regularly reviewed to keep up to date.
		5.1.2	Review of the policies for information security	
5.9	Inventory of information and other associated assets	8.1.1	Inventory of assets	Identification of asset ownership is not possible if there are no assets identified. While accountability and responsibility should be assigned to ensure the assets are properly managed and protected.
		8.1.2	Ownership of assets	
5.10	Acceptable use of information and other associated assets	8.1.3	Acceptable use of assets	Use of assets certainly includes handling of the assets.
		8.2.3	Handling of assets	
8.24	Use of cryptography	10.1.1	Policy on the use of cryptographic controls	Key management is not possible if there are no cryptographic controls in use, e.g., encryption. While protecting information with encryption is useless if the key is not properly protected.
		10.1.2	Key management	
Some controls are merged with scope extension.				
5.8	Information security in project management	6.1.5	Information security in project management	The merged control does not only aim to mitigate the information security risks related to projects, but also the project deliverables, e.g., a newly developed software.
		14.1.1	Information security requirements analysis and specification	
8.1	User endpoints devices	6.2.1	Mobile device policy	Almost all mobile devices are end-user devices. A workstation, however, is a user endpoint device but not a mobile device. The organizations which have established a mobile device policy according to ISO/IEC 27002:2013 should review the scope of the policy and update it to cover all user endpoints devices in use.
		11.2.8	Unattended user equipment	
8.26	Application security requirements	14.1.2	Securing application services on public networks	The merged control does not only aim to mitigate the information security risks related to application services on public networks, e.g., e-commerce, and transactions, it aims to prevent the information security risks of all types of application and application services.
		14.1.3	Protecting application services transactions	

Similar controls are harmonized to become one control.

5.14	Information transfer	13.2.1	Information transfer policies and procedures	<ul style="list-style-type: none"> Some controls in the 2013 edition are buried in the detailed guidance of the 2022 edition after the merge. Most of the absorbed controls, however, remain significant to prevent and mitigate information security risks, e.g., regular review of access rights, regular testing of information security continuity plan. Users of the 2022 edition are recommended to read through the guidance of each control for effective implementation. Though according to Annex B of ISO/IEC 27002:2022, control 8.3.3 (Physical media transfer) in the 2013 edition is merged to control 7.10 (Storage media) in the 2022 edition, the guidance of physical media transfer is identified in control 5.14 (Information transfer). All change-related controls in the 2013 edition are merged to one change management control in the 2022 edition. Not only that but the scope of control 8.32 (Change management) is also narrowed to the changes to information processing facilities and information systems. Unlike other absorbed controls, a significant part of guidance of the change-related controls in the 2013 edition is deleted.
		13.2.2	Agreements on information transfer	
		13.2.3	Electronic messaging	
5.17	Authentication information	9.2.4	Management of secret authentication information of users	
		9.3.1	Use of secret authentication information	
		9.4.3	Password management system	
5.18	Access rights	9.2.2	User access provisioning	
		9.2.5	Review of user access rights	
		9.2.6	Removal or adjustment of access rights	
5.29	Information security during disruption	17.1.1	Planning information security continuity	
		17.1.2	Implementing information security continuity	
		17.1.3	Verify, review and evaluate information security continuity	
7.10	Storage media	8.3.1	Management of removable media	
		8.3.2	Disposal of media	
		8.3.3	Physical media transfer	
		11.2.5	Removal of assets	
8.15	Logging	12.4.1	Event logging	
		12.4.2	Protection of log information	
		12.4.3	Administrator and operator logs	
8.32	Change management	12.1.2	Change management	
		14.2.2	System change control procedures	
		14.2.3	Technical review of applications after operating platform changes	
		14.2.4	Restrictions on changes to software packages	





Attributes

Apart from the new controls, the 2022 edition introduces “attributes” for each control. Each control is associated with five attributes with corresponding attribute values.

ATTRIBUTE	ATTRIBUTE VALUE	REMARK
Control types	Preventive, detective, corrective	To view control from the perspective of when and how the control modifies the risk with regard to the occurrence of an information security incident.
Information security properties	Confidentiality, integrity, availability	To view control from the perspective of which characteristic of information the control will contribute to preserving.
Cybersecurity concepts	Identify, protect, detect, respond and recover	To view control from the perspective of the association of the control to cybersecurity concepts defined in ISO/IEC TS 27110 and NIST Cybersecurity Framework.
Operational capabilities	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	To view control from the practitioner’s perspective of information security capabilities. There are in total 15 attribute values. Most of them are similar to the control themes of the 2013 edition.
Security domains	Governance_and_ecosystem, protection, defence, and resilience	To view control from the perspective of information security domains, expertise, services and products.

Annex A of ISO/IEC 27002:2022 demonstrates the use of the attributes as a way of creating different views of the controls. Nevertheless, it is certain that the use of the attributes is not mandatory. Organizations can choose to disregard one or more of the attributes or select other attributes, e.g., the maturity model.

From “Objective” to “Purpose”

As aforementioned, there are 14 domains and 35 security control categories in the 2013 edition. Under the 2013 edition, a control objective is defined under each security category to state what is to be achieved.

One or more controls are contained which can be applied to achieve the intended control objective.

In the 2022 edition, “objective” is replaced with “purpose”. Besides, each control has a purpose defined to illustrate why the control should be implemented.

Other changes

TITLE

The title of the 2022 edition is modified to *Information security, cybersecurity and privacy protection – Information security controls*. The term “Code of Practice” is removed to reflect that the document is a reference to generic information security controls.

TERMS AND DEFINITIONS

ISO/IEC 27000 is no longer the normative reference of the 2022 edition. Instead, the terms and definitions defined in clause 3 of ISO/IEC 27002:2022 apply. Users of the 2022 edition are recommended to refer to the terms and definitions to facilitate their understanding of the controls and the guidance in the document.

Summary

While the explanation and justification of the changes in the 2022 edition are not released outside of JTC 1/SC27, it is apparent that the changes are to reflect the advancement of technologies and evolving industrial practices.

As mentioned in the introduction, the amendment version of ISO/IEC 27001:2013 is on the way.

The Annex A will be replaced by the controls in ISO/IEC 27002:2022. SGS will keep on top of changes and will keep our clients and the certification community abreast of the transition plan to the new edition of ISO/IEC 27001 as soon as they come out.



WWW.SGS.COM

WHEN YOU NEED TO BE SURE

