Comparing ISO/IEC 27001:2022 to ISO/IEC 27001:2013. What are the changes?

A Guidance Document

SGS

ISO/IEC 27001:2022 published in October 2022.

This guidance document outlines the changes in ISO/IEC 27001:2022 as compared to ISO/IEC 27001:2013.

1 Title

The title of the new edition of ISO/IEC 27001 is changed to *Information security, cybersecurity and privacy protection – Information security management systems – Requirements*. It aligns with the title of ISO/IEC 27002:2022 *(Information security, cybersecurity and privacy protection – Information security controls)*.

2 Clauses numbering

2.1 NEW SUBCLAUSES ARE INTRODUCED IN ISO/IEC 27001:2022.

NEW SUBCLAUSES	
6.3	Planning of changes
9.2.1	General
9.2.2	Internal audit programme
9.3.1	General
9.3.2	Management review inputs
9.3.3	Management review results

An introduction of the new subclauses further harmonized the document structure with other management system standards, e.g., ISO 9001:2015, ISO 22301:2019.

2.2 THE ORDER OF TWO SUBCLAUSES IS INTERCHANGED.

ISO/IEC 27001:2022		ISO/IEC 27001:2013	
SUBCLAUSE		SUBCLAUSE	
10.1	Continual improvement	10.1	Nonconformity and corrective action
10.2	Nonconformity and corrective action	10.2	Continual improvement

Nevertheless, there is no change in the requirements in the subclauses.

3 New texts

3.1 NEW TEXTS ARE INTRODUCED IN ISO/IEC 27001:2022.

CLAUSE		NEW REQUIREMENT	SGS' REMARKS
4.2	Understanding the needs and expectations of interested parties	The organization shall determine: a) …… b) …… c) ***which of these requirements will be addressed through the information security management system.*** In the note to 4.2 *'may include legal and regulatory requirements' becomes 'can include legal and regulatory requirements'*.	The word "may" has been replaced in several areas of the standard with the word "can".
4.4	Information security management system	The organization shall establish, implement, maintain and continually improve an information security management system, ***including the processes needed and their interactions***, in accordance with ……	These texts are also included in other management system standards, e.g., ISO 9001:2015, ISO 22301:2019.
5.1	Leadership and Commitment	Requirements unchanged, new note added below Note – Reference to business in this document can be interpreted broadly to mean those activities that are core to the purposes of the organization's existence.	
5.3	Organizational roles, responsibilities and authorities	In the note 'top management ***may*** also' becomes 'top management ***can*** also'.	
6.2	Information security objectives and planning to achieve them	The information security objectives shall: a) ……; b) ……; c) ……; d) ***be monitored***; e) ……; f) ……; g) ***be available as documented information***.	For d), the new texts are also included in other management system standards, e.g., ISO 9001:2015, ISO 22301:2019.
6.3	Planning of changes	This is a new subclause. It does not appear in the 2013 edition. 6.3 states 'When the organization determines the need for changes to the information security management system, the changes shall be carried out in a planned manner'.	This is actually a fairly big change.
7.4	Communication	The organization shall determine the need for …… communications ……including: a) ……; b) ……; c) ……; d) ***how to communicate***.	Meanwhile, the requirements of ISO/IEC 27001:2013 clause 7.4 *d) who shall communication; and* *e) the processes by which communication shall be effected* are removed.
8.1	Operational planning and control	The organization shall plan, implement and control the processes …… by: — ***establishing criteria for the processes;*** — ***implementing control of the processes in accordance with the criteria.***	The new requirements are also included in other management system standards, e.g., ISO 9001:2015, ISO 22301:2019.

CLAUSE		NEW REQUIREMENT	SGS' REMARKS
9.1	Monitoring, measurement, analysis and evaluation	The organization shall determine: a) ……; b) …… ***The methods selected should produce comparable and reproducible results to be considered valid***; c) ……;	It was a note in ISO/IEC 27001:2013 clause 9.1.b).
9.3.2	Management review inputs	The management review shall include consideration of: a) ……; b) …… c) ***changes in needs and expectations of interested parties that are relevant to the information security management system;*** d) ……;	

Although new texts are added and some texts re-arranged, they only clarify the requirements and do not add new requirements to the standard.

4 Annex A

The title of Annex A is changed to "Information security controls reference". Also, the controls are revised to align with ISO/IEC 27002:2022.

Nevertheless, as in the case of the 2013 version, only the descriptions of the controls is derived from ISO/IEC 27002:2022. Not included in Annex A of ISO/IEC 27001:2022 are the other elements in ISO/IEC 27002:2022, such as the purpose and attributes of the controls. Organizations implementing ISO/IEC 27001 should refer to the guidance standard for a better understanding of the information security controls.

5 Other Changes

CLAUSE	ISO/IEC 27001:2022	ISO/IEC 27001:2013	SGS' REMARKS
4.1 Understanding the organization and its context	Note: Determining these issues refers to establishing the external and internal context of the organization considered in ***Clause 5.4.1 of ISO 31000:2018***	Note: Determining these issues refers to establishing the external and internal context of the organization considered in ***Clause 5.3 of ISO 31000:2009***	The reference of ISO 31000 in the note is updated for the new edition of ISO 31000.
5.1 Leadership and commitment	Note: "Reference to "business" in this document can be interpreted broadly to mean those activities that are core to the purposes of the organization's existence."	Nil.	A new note is added in ISO/IEC 27001:2022 clause 5.1.
5.3 Organizational roles, responsibilities and authorities	Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated ***within the organization***.	Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated.	ISO/IEC 27001:2022 specifies that the information security responsibilities and authorities shall be communicated within the organization. The communication with parties outside of the organization is addressed in 7.4

CLAUSE	ISO/IEC 27001:2022	ISO/IEC 27001:2013	SGS' REMARKS
6.1.3 Information security risk treatment	c) Note 2: Annex A contains ***a list of possible*** information security controls.	c) Note 1: Annex A contains ***a comprehensive list*** of control objectives and controls.	The note is rephrased that the information security controls listed in Annex A are a **list of possible** information security controls, instead of a **comprehensive list**. It clarifies that the Annex A controls are not exhaustive and additional information security controls can be included, as stated in the second note in the clause.
8.1 Operational planning and control	The organization shall plan, implement and control the processes needed to meet requirements, and to implement the actions determined in Clause 6.	The organization shall plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined in 6.1. The organization shall also implement plans to achieve information security objectives determined in 6.2.	The sentences in clause 8.1 are rephrased but the requirements are unchanged.
	The organization shall ensure that ***externally provided processes, products or services*** that are relevant to the information security management system are controlled.	The organization shall ensure that ***outsourced processes*** are determined and controlled.	Some services in information security such as data centers or cloud services are more appropriately categorized as externally provided instead of outsourced. Furthermore the new requirement explicitly mentions "products" — this includes tangible products used (e.g. printers, scanners, servers, network gear, video cameras etc.)
9.1 Monitoring, measurement, analysis and evaluation 9.2.2 Internal audit programme 9.3.3 Management review results	All three (sub-) clauses 9.1 / 9.2.2 / 9.3.3 Documented information shall be available as evidence of ……	The organization shall retain documented information as evidence of ……	The sentence related to documented information requirement is rephrased but the requirement is unchanged.

6 Conclusion

As expected, Annex A is revised to align with the information security controls in ISO/IEC 27002:2022. This is also the most significant change of ISO/IEC 27001:2022. The changes in clauses 4-10 are minor editorial changes to further harmonize the structure with other management system standards.

To transition to the new edition, moderate efforts might be needed for those organizations that are already certified to ISO/IEC 27001:2013. These efforts may include revising the internal policies in accordance with the new subclauses and the modified requirements, as well as the risk assessment results and risk treatment plan in accordance with ISO/IEC 27001:2022 Annex A.

WWW.SGS.COM

SGS SA Corporate Headquarters
P.O. Box 2152
1 Place des Alpes
1201 Genève, Switzerland
+41 22 739 91 11

WHEN YOU NEED TO BE SURE