



**International
Standard**

ISO/IEC 27013

**Information security, cybersecurity
and privacy protection — Guidance
on the integrated implementation of
ISO/IEC 27001 and ISO/IEC 20000-1**

AMENDMENT 1

*Sécurité de l'information, cybersécurité et protection de la vie
privée — Recommandations pour la mise en œuvre intégrée de
l'ISO/IEC 27001 et de l'ISO/IEC 20000-1*

AMENDEMENT 1

**Third edition
2021-11**

**AMENDMENT 1
2024-12**

IECNORM.COM : Click to view the full PDF of ISO/IEC 27013:2021/AMD1:2024



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2024

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Information security, cybersecurity and privacy protection — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1

AMENDMENT 1

2 Normative references

Replace reference to ISO/IEC 27001 with the following:

ISO/IEC 27001:2022, *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*

Also replace all references to ISO/IEC 27001:2013 throughout the text of the document with ISO/IEC 27001:2022.

4.2 ISO/IEC 27001 concepts

Replace the last sentence of the 2nd paragraph with the following:

Examples of requirements relevant to interested parties include business requirements, legal and regulatory requirements and contractual obligations.

Replace the reference to ISO/IEC 27001:2013 with ISO/IEC 27001:2022.

4.4 Similarities and differences

Replace the third paragraph with the following:

See Annex A for details of the correspondence between ISO/IEC 27001:2022, Clauses 1 to 10, and ISO/IEC 20000-1:2018, Clauses 1 to 10. See Annex B for a comparison of terms and definitions between ISO/IEC 27000 and ISO/IEC 20000-1.

6.2.1 Requirements and controls

Replace the entire subclause with the following:

ISO/IEC 27001:2022, Clauses 4 to 10, specifies requirements for an ISMS. In addition, ISO/IEC 27001:2022, Annex A, contains an extensive list of controls. The controls in ISO/IEC 27001:2022, Annex A, are not requirements and are not mandatory. ISO/IEC 27001:2022, 6.1.3, specifies that the organization defines and applies an information security risk treatment process to determine all controls necessary to implement information security risk treatment options chosen and then compare the necessary controls with those in ISO/IEC 27001:2022, Annex A, and verify that no necessary controls have been omitted. The statement of applicability (SoA) is then used to record which controls are relevant to the organization's ISMS. The controls listed in ISO/IEC 27001:2022, Annex A, are not exhaustive and can be substituted with others, or additional controls can be added as needed. This means it is possible for the organization's SoA to:

- a) include only a subset of the controls in ISO/IEC 27001:2022, Annex A;

- b) not include any of the ISO/IEC 27001:2022, Annex A, controls;
- c) include alternative controls;
- d) include a combination of controls from ISO/IEC 27001:2022, Annex A, and other sources.

Any control within ISO/IEC 27001:2022, Annex A, that would not modify one or more unacceptable risks, is unnecessary for the organization. Similarly, controls not included in ISO/IEC 27001:2022, Annex A, can be determined as necessary to modify risk. Organizations can design controls as required or identify them from any source.

ISO/IEC 20000-1 specifies requirements for the SMS but does not list any controls and does not specify a requirement for a Statement of Applicability, so there is no direct correlation between ISO/IEC 27001:2022, Annex A, and ISO/IEC 20000-1. However, ISO/IEC 20000-1:2018, 8.7.3.2, includes a requirement to determine controls to address information security risks to the SMS and the services, and to document the decisions about these controls. In addition, there is a requirement to monitor and review the effectiveness of these controls, and to take action if required.

Organizations wishing to integrate an ISMS and an SMS should distinguish between the requirements specified in ISO/IEC 27001 and ISO/IEC 20000-1, and the information security controls specified in ISO/IEC 27001:2022, Annex A. Even if it appears that there is a common topic area between a requirement specified in ISO/IEC 20000-1 and a control included in ISO/IEC 27001:2022, Annex A, the distinction between requirements and controls should be understood and communicated to avoid confusion within the organization.

6.2.2 *Assets and configuration items*

Replace the reference to ISO/IEC 27001:2013 with ISO/IEC 27001:2022.

Add the following as a new final paragraph to 6.2.2:

ISO/IEC 27001:2022, Annex A includes control 8.9 for "configuration management". This term is also used in ISO/IEC 20000-1, but not in the same sense, so care should be taken to not assume any relationship between these concepts. The purpose of control 8.9 is to ensure that hardware, software, services and networks function correctly with required security settings, and that the configuration is not altered by unauthorized or incorrect changes.

6.2.3 *Service design and transition*

Replace the second sentence of the first paragraph with the following:

There are no directly equivalent requirements in ISO/IEC 27001, although significant planned changes to the organization or management system require an information security risk assessment to be performed (ISO/IEC 27001:2022, 8.2) and some aspects of service design, transition and delivery are covered in controls listed in ISO/IEC 27001:2022, Annex A.

6.2.4 *Risk assessment and management*

Replace the references to ISO/IEC 27001:2013 with ISO/IEC 27001:2022.

6.2.11 *Change management*

Replace the first paragraph with the following:

ISO/IEC 27001:2022, 6.3 requires that when the organization determines the need for changes to the ISMS, the changes shall be carried out in a planned manner. ISO/IEC 27001:2022, 7.5.3 requires changes

to documented information relating to the ISMS to be controlled. ISO/IEC 27001:2022, 8.1 requires the organization to control planned changes and to review the consequences of unintended changes. ISO/IEC 27001:2022, Annex A also includes control 8.32 concerning change management procedures for information processing facilities and information systems.

6.3.1 Service level management and reporting

Replace the reference to ISO/IEC 27001:2013 with ISO/IEC 27001:2022.

6.3.2 Management commitment and continual improvement

Replace the references to ISO/IEC 27001:2013 with ISO/IEC 27001:2022.

Replace the 5th paragraph with the following:

Both ISO/IEC 27001:2022, 10.1 and ISO/IEC 20000-1:2018, 10.2 refer to the organization managing various aspects of continual improvement, stating that the organization should carry out continual improvement of its management system. ISO/IEC 20000-1:2018 specifies that continual improvement is applicable to both the SMS and the services.

6.3.3 Capacity management

Replace the references to ISO/IEC 27001:2013 with ISO/IEC 27001:2022.

Add the following to the end of paragraph 2:

The purpose of control 8.6 in ISO/IEC 27001:2022, Annex A is to ensure the required capacity of information processing facilities, human resources, offices and other facilities, so while it is similar, it does not include financial resources.

6.3.5 Continuity and availability management

Replace the references to ISO/IEC 27001:2013 with ISO/IEC 27001:2022.

6.3.6 Release and deployment management

Replace the reference to ISO/IEC 27001:2013 with ISO/IEC 27001:2022.

Annex A

Replace the references to ISO/IEC 27001:2013 with ISO/IEC 27001:2022.

Make the following modifications in Table A.1:

Add additional row 6.3 "Planning of changes" (not highlighted in grey) to "ISO/IEC 27001:2013" column after 6.2.

Change row 10.1 in the "ISO/IEC 27001:2013" column to say "Continual improvement".

Change row 10.2 in the "ISO/IEC 27001:2013" column to say "Nonconformity and corrective action".

Retain the "ISO/IEC 20000-1:2018" rows as they are, so that "Nonconformity and corrective action" and "Continual improvement" correspond with the relevant row in the "ISO/IEC 27001:2013" column, even though the subclause numbers for each standard are now different.

Remove Annex B.

Change Annex C and all references to Annex C to say Annex B. Replace the references in Annex B (previously Annex C) to ISO/IEC 27001:2013 with ISO/IEC 27001:2022.

Rename Table C.1 as Table B.1.

Make the following modifications in Table C.1 (now Table B.1):

In the row entitled "external supplier", under the column titled "Comments on the usage of the term in both standards", replace the reference to A.15 in last sentence with "controls 5.19 to 5.22 in Annex A".

In the row entitled "record", under the column entitled "Comments on the usage of the term in both standards", replace the reference to A.18.1.3 with "control 5.3.3 in Annex A".

In the row entitled "request for change", under the column entitled "Comments on the usage of the term in both standards", replace all the text in that cell with "Control 8.32 in ISO/IEC 27001:2022, Annex A, refers to the management of changes."

In the row entitled "service continuity", under the column titled "Comments on the usage of the term in both standards", replace the 2nd sentence with the following: "Service continuity is normally seen as a subset of business continuity. ISO/IEC 27001:2022, Annex A includes control 5.29, information security during disruption, and control 5.30, ICT readiness for business continuity."

In the row entitled "service level agreement SLA", under the column titled "Comments on the usage of the term in both standards", replace all the text in that cell with "No direct equivalent".

In the row entitled "Transition", under the column titled "Comments on the usage of the term in both standards", replace the 2nd paragraph (including bullets) with the following: "ISO/IEC 27001:2022, Annex A includes control 8.32 for Change management."