



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**



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;