SmartSuite

Framework / Cybersecurity / ISO 27000 Series

ISO/IEC 27001:2022

ISO/IEC 27001:2022 specifies requirements for an information security management system: Clauses 4 to 10, risk treatment, the Statement of Applicability and 93 Annex A controls.



What it is

ISO/IEC 27001:2022 is the international standard that specifies requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS), including the assessment and treatment of information security risks. ISO and IEC published this third edition on October 25, 2022, prepared by ISO/IEC JTC 1/SC 27; it replaced ISO/IEC 27001:2013, and Amendment 1:2024 added climate change considerations to Clauses 4.1 and 4.2. Any organization can implement it, and accredited certification bodies certify against it.

The requirements are generic and apply to all organizations regardless of type, size or nature, and excluding any of the requirements in Clauses 4 to 10 is not acceptable when an organization claims conformity (Clause 1). Annex A (normative) references 93 information security controls in four themes, taken from ISO/IEC 27002:2022. The transition from the 2013 edition ended on October 31, 2025, when certifications based on it were to have expired or been withdrawn (IAF MD 26:2023).

At a glance

PUBLISHER International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC)	TYPE Standard	VERSION Third edition (ISO/IEC 27001:2022; Amendment 1:2024)
EFFECTIVE October 25, 2022 (2013 edition transition ended October 31, 2025)	DOMAIN Cybersecurity	FAMILY ISO 27000 Series
REGION International	ADOPTION MODEL Certification	IMPLEMENTATION COMPLEXITY High

Source: iso.org/standard/27001

Why it matters

- **Controls follow risk** The organization defines risk criteria, identifies risks and owners, and selects treatment options and controls from the results (Clauses 6.1.2 and 6.1.3).
- **Top management is accountable** Clause 5.1 lists eight things top management must do, from ensuring the policy and objectives fit the strategy to supporting other managers' leadership, and Clause 9.3 requires a management review.
- **Every control decision is recorded** The Statement of Applicability states each necessary control, why it is included, whether it is implemented, and why any Annex A control is excluded (Clause 6.1.3 d).
- **Changes are planned** Clause 6.3 requires that changes to the ISMS be carried out in a planned manner.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports ISO 27001:2022

Scope, Policy and Interested Parties

Record the ISMS scope, the information security policy and the requirements of interested parties with owners and review dates (Clauses 4.2, 4.3 and 5.2).

Risk Assessment and Treatment

Use Cyber & IT Risk to log risks with owners, criteria, treatment plans and the risk owners' acceptance of residual risk (Clauses 6.1.2 and 6.1.3).

Statement of Applicability

Use Compliance Management to hold the Annex A controls with applicability, justification and implementation status for each (Clause 6.1.3 d).

Evidence and Documented Information

Attach evidence to each control and keep the documented information the standard requires, with reviewers and dates (Clause 7.5).

Internal Audit and Corrective Action

Use Internal Audit Management to plan and run internal audits and to track nonconformities and corrective actions to closure (Clauses 9.2 and 10.2).

Management Review and Reporting

Record management review inputs and results and report control status, open risks and audit readiness to top management (Clause 9.3).

Common framework mappings

CIS Controls v8.1 | ISO 27002:2022 | ISO 27017 | ISO 27018 | ISO 27701 | NIST CSF 2.0 | NIST 800-53 Rev.5

Official resources

ISO/IEC 27001:2022 Standard

Official ISO publication defining requirements for an Information Security Management System (ISMS).

iso.org/standard/27001

ISO/IEC 27002 Security Controls Guidance

Provides implementation guidance supporting ISO 27001 Annex A security controls.

iso.org/standard/75652.html

ISO 27001 Implementation Resources

Official guidance explaining how organizations implement ISO 27001 and prepare for certification.

iso.org/iso-27001-information-security.html

ISO 27000 Family Overview

Describes the structure and relationship of ISO information security standards.

iso.org/isoiec-27001-information-security.html

Frequently asked questions

Which requirements of ISO/IEC 27001:2022 can an organization leave out?

None of those in Clauses 4 to 10: excluding any of them is not acceptable when an organization claims conformity (Clause 1). The organization decides which Annex A controls it needs, but it must justify the exclusion of any Annex A control in its Statement of Applicability (Clause 6.1.3 d).

What must the Statement of Applicability contain?

Clause 6.1.3 d) requires the necessary controls, the justification for including them, whether they are implemented, and the justification for excluding any Annex A control. It follows the comparison of the organization's chosen controls with Annex A in Clause 6.1.3 c).

How many Annex A controls are there and how are they grouped?

Annex A references 93 information security controls in four themes: organizational (5.1 to 5.37), people (6.1 to 6.8), physical (7.1 to 7.14) and technological (8.1 to 8.34), using the numbering of ISO/IEC 27002:2022. Eleven are new compared with the 2013 edition, and the Annex is a reference list that the organization may add to.

What changed from ISO/IEC 27001:2013 and in Amendment 1:2024?

The 2022 edition aligned the text with the harmonized structure and ISO/IEC 27002:2022, added Clause 4.2 c) and Clause 6.3 on planning of changes, and replaced the 2013 Annex A. Amendment 1:2024 added a sentence to Clause 4.1 that the organization shall determine whether climate change is a relevant issue, and a note to Clause 4.2 that interested parties can have climate-related requirements.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How is certification done and what happened to the 2013 edition?

An accredited certification body audits against the standard using the requirements of ISO/IEC 27006-1:2024 and ISO/IEC 17021-1. IAF MD 26:2023 gave certification bodies until October 31, 2025 to transition certified clients, and certifications based on the 2013 edition were to expire or be withdrawn at the end of that period.

License included / downloadable: No ISO/IEC 27001:2022 is a paid standard sold by ISO and national standards bodies, and the text is not included with the platform.

Full framework page and mappings: smartsuite.com/frameworks/iso-iec-27001-2022-information-security-management-system-isms