

ISO/IEC 27002:2022

ISO/IEC 27002:2022 provides best-practice information security controls to help organizations select, implement, and manage protections for information assets.



What it is

ISO/IEC 27002:2022 is an international information security control framework that helps organizations select, implement, and manage controls to protect information assets and address cybersecurity risks. It provides a comprehensive set of best-practice guidelines supporting effective data protection, risk management, and operational security.

Published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), ISO/IEC 27002 is used by organizations of all sizes and industries seeking to establish or improve their information security management systems (ISMS). The standard covers topics such as organizational controls, people controls, physical controls, and technological controls, aligning closely with ISO/IEC 27001 and supporting compliance with regulatory requirements.

At a glance

PUBLISHER International Organization for Standardization (ISO)	TYPE Standard	VERSION 2022
EFFECTIVE February 2022	DOMAIN Cybersecurity	FAMILY ISO 27000 Series
REGION International	ADOPTION MODEL Certification	IMPLEMENTATION COMPLEXITY High

Source: <https://www.iso.org/standard/75652.html>

Why it matters

- **Strengthen information security governance** Enable organizations to establish clear security policies, roles, and responsibilities supporting a culture of security accountability.
- **Enhance risk management practices** Support ongoing identification, assessment, and treatment of security risks to address evolving threats and vulnerabilities.
- **Improve regulatory compliance** Align organizational controls with international standards, easing compliance with data protection laws and industry-specific regulations.
- **Increase audit readiness** Facilitate the documentation and monitoring of controls, processes, and procedures needed for successful internal and external audits.

How SmartSuite supports ISO 27002:2022

Control Catalog and Implementation Guidance Operationalize ISO 27002 controls with owners, procedures, and implementation notes.	Risk and Asset Linkage Tie controls to risks and assets to prioritize what matters most.	Control Review and Evidence Schedule Schedule recurring reviews and attach proof that controls operate consistently.
Exceptions and Compensating Controls Track exceptions, approvals, and compensating controls with clear documentation.	Cross-Framework Mapping Map controls to NIST, SOC 2, or internal standards to reduce duplicate work.	Audit and Executive Reporting Provide reporting by control domain, owner, scope, and remediation status.

Common framework mappings

Official resources

ISO/IEC 27002:2022 Standard Defines updated guidance on information security controls for organizations implementing an ISMS. iso.org/standard/75652.html	ISO/IEC 27002 Implementation Guidelines Provides detailed guidance on implementing security controls from the ISO/IEC 27002 standard. iso.org/publication/75652.html
--	--

Frequently asked questions

What is ISO/IEC 27002:2022 used for?

ISO/IEC 27002:2022 provides a structured catalog of information security controls designed to help organizations protect their information assets, mitigate cybersecurity risks, and meet regulatory requirements. It is used as a practical guide for selecting, implementing, and managing security controls within an information security management system (ISMS) or similar governance framework.

Is ISO/IEC 27002:2022 certifiable or mandatory?

ISO/IEC 27002:2022 itself is not certifiable; organizations cannot be certified against it directly. Instead, it provides detailed control guidance to support ISO/IEC 27001 certification and is generally voluntary unless adopted as a legal or regulatory requirement in specific jurisdictions or sectors.

What is the scope of ISO/IEC 27002:2022 and who should use it?

ISO/IEC 27002:2022 is applicable to any organization, regardless of size, industry, or geographic location, seeking to strengthen its information security controls. The framework covers organizational, people, physical, and technological controls, making it relevant for both public and private sector entities managing sensitive information.

What are the key concepts or artifacts required by ISO/IEC 27002:2022?

Key artifacts include documented security policies, risk assessments, control implementation plans, and evidence of control operation. The framework also emphasizes the creation and maintenance of a controls inventory, supporting documentation, and alignment with business objectives and risk appetite.

How does ISO/IEC 27002:2022 recommend organizations implement security controls?

Implementation follows a risk-based approach: organizations assess their information security risks, select relevant controls from the framework, and integrate these into operational processes and policies. Ongoing monitoring, regular reviews, and periodic control effectiveness assessments are critical components of sustained implementation.

How does ISO/IEC 27002:2022 relate to other information security frameworks?

ISO/IEC 27002:2022 closely supports ISO/IEC 27001 by providing detailed guidance for the Annex A controls required for ISMS certification. It can also be mapped to other standards such as NIST SP 800-53, CIS Controls, and national cybersecurity laws to enhance compliance and interoperability.

What are the ongoing compliance requirements for ISO/IEC 27002:2022?

To maintain compliance, organizations must continuously monitor the effectiveness of implemented controls, update risk assessments in response to changing threats, and ensure policies, training, and technical safeguards remain current. Periodic internal reviews and readiness for external audits are essential for sustained alignment.

How would SmartSuite support ISO/IEC 27002:2022?

SmartSuite enables organizations to operationalize ISO/IEC 27002:2022 by providing a centralized control library, facilitating risk tracking, and automating evidence collection for implemented controls. It streamlines remediation workflows, supports audit readiness, and delivers reporting dashboards for real-time visibility into control effectiveness and compliance status.

License included / downloadable: No ISO/IEC 27002:2022 requires purchase via the ISO catalog or authorized national standards bodies.
License not included with platform

Full framework page and mappings: smartsuite.com/frameworks/iso-iec-27002-2022-information-security-controls