SmartSuite

Framework / Cybersecurity / ISO 27000 Series

ISO/IEC 27002:2013

ISO/IEC 27002 provides guidance on selecting and implementing information security controls to protect data and support risk management.

What it is

ISO/IEC 27002:2013 is an international code of practice for information security controls that helps organizations select, implement, and manage security measures to protect sensitive information and support risk management efforts.

Published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), ISO/IEC 27002 provides guidance on a broad set of cybersecurity controls covering areas such as access management, cryptography, physical security, operations security, and incident response. The framework is widely adopted across various industries by organizations seeking to strengthen their cybersecurity posture and align with best practices for data protection and regulatory compliance.

At a glance

PUBLISHER International Organization for Standardization (ISO)	TYPE Standard	VERSION 2013
EFFECTIVE 2013	DOMAIN Cybersecurity	FAMILY ISO 27000 Series
REGION International	ADOPTION MODEL Risk Management	IMPLEMENTATION COMPLEXITY High

Source: https://www.iso.org/standard/54533.html

Why it matters

- **Strengthen information security governance** Enable organizations to systematically manage and oversee cybersecurity risks through structured control selection and management processes.
- **Enhance compliance readiness** Support alignment with global regulatory requirements and industry standards, simplifying compliance reporting and external audit processes.
- **Improve incident response capabilities** Facilitate timely identification and effective management of security incidents, reducing potential impact on business operations.
- **Support continuous improvement** Encourage ongoing assessment and refinement of security practices as threats evolve and organizational needs change.

© 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports ISO 27002:2013

Control Catalog and Implementation Guidance

Organize ISO 27002 control domains with defined owners, procedures, and implementation documentation.

Risk and Asset Linkage

Connect security controls to risks, assets, and mitigation strategies to prioritize security investments.

Evidence Collection and Review Cadence

Capture evidence demonstrating control operation and schedule recurring reviews across security processes.

Exception and Compensating Control Tracking

Document control exceptions, approvals, and compensating safeguards with full traceability.

Cross-Framework Control Mapping

Map ISO 27002 controls to frameworks such as NIST, CIS Controls, and SOC reporting requirements.

Security Governance and Reporting

Generate dashboards showing control coverage, open issues, remediation progress, and overall security posture.

Common framework mappings

CIS Controls v8.1 | ISO 27001:2022 | ISO 27017 | ISO 27018 | ISO 27701 | NIST CSF 2.0 | NIST 800-53 Rev.5 | SOC 2

Official resources

ISO/IEC 27002:2013 Standard

Provides a comprehensive set of guidelines for information security controls.

iso.org/standard/54533.html

ISO/IEC 27001 and ISO/IEC 27002 Overview

Describes the relationship and purpose of key ISO information security standards.

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

Frequently asked questions

What is ISO/IEC 27002:2013 used for?

ISO/IEC 27002:2013 is used to guide organizations in selecting, implementing, and managing information security controls to protect sensitive data and mitigate security risks. It serves as a detailed reference for best practices in developing an effective information security management system.

Is ISO/IEC 27002:2013 certifiable or mandatory?

ISO/IEC 27002:2013 itself is not certifiable and is not legally mandatory, but it is often used alongside ISO/IEC 27001, which is certifiable. Organizations use ISO/IEC 27002 to inform their control selection and implementation when seeking ISO/IEC 27001 certification.

Who should use ISO/IEC 27002:2013, and what is its scope?

ISO/IEC 27002:2013 is applicable to organizations of all sizes and sectors that need to manage information security risks. Its scope includes guidance on controls across 14 security domains, making it relevant for organizations seeking to formalize or benchmark their security strategies.

What are the key concepts and artifacts required by ISO/IEC 27002:2013?

Key concepts within ISO/IEC 27002:2013 include control objectives, security control selection, risk treatment, and continual improvement. Artifacts typically required include documented policies, risk assessments, control implementation records, and evidence of ongoing monitoring.

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How should organizations implement ISO/IEC 27002:2013?

Implementation involves mapping the controls in ISO/IEC 27002:2013 to identified risks within the organization, developing and enforcing appropriate policies and procedures, and performing regular reviews and updates. Ongoing employee training and technical security measures are required for effective adoption.

How does ISO/IEC 27002:2013 relate to ISO/IEC 27001 and other security frameworks?

ISO/IEC 27002:2013 provides detailed implementation guidance for the controls referenced in ISO/IEC 27001, supporting its ISMS requirements. It can be cross-mapped with other frameworks like NIST CSF or SOC 2 to facilitate integrated compliance strategies.

What are the ongoing compliance requirements for ISO/IEC 27002:2013?

Ongoing compliance requires continuous monitoring of controls, regular reviews and updates to policies, periodic risk assessments, and documenting evidence of control effectiveness. Periodic internal audits and management reviews help ensure sustained alignment with ISO/IEC 27002:2013 guidance.

How would SmartSuite support ISO/IEC 27002:2013?

SmartSuite supports ISO/IEC 27002:2013 by providing control libraries, configurable risk registers, and automated evidence collection tools, enabling organizations to map controls to risks and track compliance. The platform facilitates audit readiness with policy management modules, real-time dashboards, and reporting features, streamlining control management and compliance tracking across teams.

Framework text is licensed by its publisher and is included only where stated above.

Full framework page and mappings: smartsuite.com/frameworks/iso-iec-27002-2013-code-of-practice-for-information-security-controls