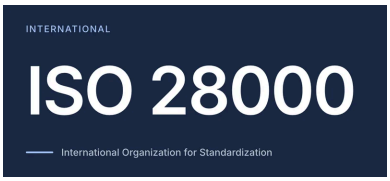
SmartSuite

Framework / Supply Chain Security / ISO Industry Standards

ISO 28000:2022 – Security and resilience – Security management systems – Requirements

ISO 28000:2022 specifies requirements for a security management system, including supply chain aspects, for any type or size of organization. ISO published it on March 15, 2022.



What it is

ISO 28000:2022, Security and resilience — Security management systems — Requirements, is the international standard that specifies requirements for a security management system, including aspects relevant to the supply chain. The International Organization for Standardization (ISO) published the second edition on March 15, 2022 through technical committee ISO/TC 292, Security and resilience. It replaces ISO 28000:2007, which ISO lists as withdrawn, and it applies to organizations of any type and size.

The standard is not industry or sector specific (Clause 1). It requires an organization to assess the security environment in which it operates, including its supply chain and the dependencies and interdependencies in it, to determine whether adequate security measures are in place to manage security-related risks, to manage compliance with statutory, regulatory and voluntary obligations, and to align its security processes and controls, including the upstream and downstream processes and controls of the supply chain, with its objectives (Introduction). An organization may verify conformity by external or internal audit.

At a glance

PUBLISHER International Organization for Standardization (ISO), ISO/TC 292	TYPE Standard	VERSION ISO 28000:2022 (second edition), with Amendment 1:2024
EFFECTIVE March 15, 2022 (publication date)	DOMAIN Supply Chain Security	FAMILY ISO Industry Standards
REGION International	ADOPTION MODEL Certification	IMPLEMENTATION COMPLEXITY High

Source: iso.org/standard/79612.html

Why it matters

- **One system across the supply chain** The organization assesses its security environment including supply chain dependencies and interdependencies, and aligns upstream and downstream processes and controls with its objectives (Introduction and Clause 4.1).
- **Obligations managed in one place** Clause 4.2.2 covers legal, regulatory and other requirements, and the Introduction requires the organization to manage compliance with statutory, regulatory and voluntary obligations.
- **Risk assessment tied to treatment** Security-related risks and opportunities are determined and addressed in Clauses 6.1.2 and 6.1.3, and carried into operation through risk assessment and treatment in Clause 8.3.
- **Plans for response and recovery** Clause 8.6 requires security plans with a response structure, warning and communication, defined content and recovery; the 2022 edition added these for consistency with ISO 22301.

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

How SmartSuite supports ISO 28000

Security Policy and Objectives

Record the security policy, security objectives, roles, responsibilities and review dates (Clauses 5.2, 5.3 and 6.2).

Context and Obligations Register

Keep interested parties, the scope and the legal, regulatory and other requirements with owners and source references (Clauses 4.2 and 4.3).

Security Risk Assessment and Treatment

Log security-related risks, opportunities, treatment actions and decisions with owners and due dates (Clauses 6.1.2, 6.1.3 and 8.3).

Controls and Supplier Dependencies

Track the controls applied under Clause 8.4 and the suppliers and partners they depend on.

Security Plans and Recovery

Hold security plans with the response structure, warning and communication steps and recovery actions (Clause 8.6).

Audit, Review and Corrective Action

Plan internal audits, record management review inputs and results and follow nonconformities to closure (Clauses 9.2, 9.3 and 10.2).

Common framework mappings

ISO 27001:2022 | ISO 27017 | NIST CSF 2.0 | NIST 800-53 Rev.5

Official resources

ISO 28000 Standard

Defines the requirements for a Supply Chain Security Management System.

iso.org/standard/79612.html

ISO 28000 Implementation Guidance

Provides practical advice for implementing and maintaining an ISO 28000 compliant system.

iso.org/iso-28000-supply-chain-security-management.html

ISO Standards Catalog

Outlines related documents and standards supporting ISO 28000 framework implementation.

iso.org/iso-28000-supply-chain.html

Frequently asked questions

What is ISO 28000:2022 and what changed from the 2007 edition?

ISO 28000:2022 is the second edition of the security management system standard, published by ISO on March 15, 2022 through ISO/TC 292. It cancels and replaces ISO 28000:2007 and, per its Foreword, adds principles in Clause 4 for better coordination with ISO 31000 and recommendations in Clause 8 for consistency with ISO 22301. Amendment 1:2024 adds climate change considerations to the context clauses.

Is ISO 28000 only for supply chain security?

No. Clause 1 says the standard specifies requirements for a security management system, including aspects relevant to the supply chain, and that it is not industry or sector specific. It applies to all types and sizes of organizations and to any activity, internal or external, at all levels.

Can an organization be certified to ISO 28000:2022?

The Introduction says conformity of the security management system to the standard may be verified by an external or internal auditing process, so certification by an accredited body is an option, not a requirement. ISO lists the 2007 edition as withdrawn. Ask your certification body which transition arrangement applies to an existing 2007 certificate.

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

What does Clause 8 require in practice?

The organization identifies its processes and activities (8.2), assesses and treats security risks (8.3), applies controls (8.4), selects security strategies and treatments and the resources they need (8.5) and maintains security plans (8.6). The plans cover the response structure, warning and communication, their content and recovery.

How does ISO 28000 relate to ISO 31000, ISO 22301 and ISO/IEC 27001?

The Foreword ties Clause 4 to ISO 31000 and Clause 8 to ISO 22301, and the Introduction names ISO 9001, ISO 14001, ISO 22301, ISO/IEC 27001 and ISO 45001 as standards it is consistent with. The shared structure lets an organization combine policies, audits and management reviews across these systems.

License included / downloadable: No ISO 28000:2022 is a copyrighted ISO standard sold by ISO and by national standards bodies; its text is not included with the platform.

Full framework page and mappings: smartsuite.com/frameworks/iso-28000-supply-chain-security-management-system