

ISO 28000:2022

ISO 28000 is a security management standard that helps organizations assess and mitigate risks to supply chain operations.



What it is

ISO 28000 is an international supply chain security management standard that enables organizations to establish, implement, maintain, and improve security controls throughout their supply chain operations. Its primary purpose is to help organizations assess and mitigate security risks, protect assets, and ensure the continuity and resilience of supply chain activities.

Published by the International Organization for Standardization (ISO), ISO 28000 is used by manufacturers, logistics providers, transport operators, and organizations with complex supply chain dependencies across industries. The standard covers areas such as risk management, physical security, cargo integrity, incident response, and compliance with applicable legal and regulatory requirements.

At a glance

PUBLISHER International Organization for Standardization (ISO)	TYPE Standard	VERSION ISO 28000:2022
EFFECTIVE 2007	DOMAIN Supply Chain Security	FAMILY ISO Industry Standards
REGION International	ADOPTION MODEL Risk Management	IMPLEMENTATION COMPLEXITY High

Source: <https://www.iso.org/standard/79612.html>

Why it matters

- **Strengthen supply chain governance** Establish clear accountability and improve oversight of security practices throughout the entire supply chain network.
- **Improve regulatory compliance** Support compliance with national and international regulations by aligning supply chain security processes with recognized global standards.
- **Enhance risk mitigation** Enable ongoing risk identification and mitigation, reducing vulnerability to supply chain disruptions and security incidents.
- **Increase operational resilience** Bolster the organization's ability to manage and recover from security events that could impact business continuity or delivery commitments.

How SmartSuite supports ISO 28000

Supply Chain Security Governance Centralize policies, roles, and procedures governing supply chain security operations.	Risk Assessment and Threat Identification Identify and assess risks across suppliers, logistics networks, and transportation processes.	Security Control Implementation and Monitoring Track security measures protecting facilities, cargo, and supply chain activities.
Supplier and Partner Security Oversight Manage third-party security requirements, audits, and compliance status.	Supply Chain Incident and Disruption Response Track supply chain incidents, disruptions, and coordinated response actions.	Supply Chain Risk and Resilience Reporting Provide dashboards showing risk posture, control coverage, and operational resilience.

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 Catalogue Outlines related documents and standards supporting ISO 28000 framework implementation. iso.org/iso-28000-supply-chain.html	

Frequently asked questions

What is ISO 28000 used for? ISO 28000 is used to establish and maintain a structured supply chain security management system within organizations. It focuses on identifying, assessing, and mitigating risks to people, goods, and supply chain operations, aiming to ensure continuity and resilience.
Is ISO 28000 certification mandatory or voluntary? ISO 28000 certification is voluntary and not mandated by law. However, organizations may choose to pursue certification to demonstrate their compliance with internationally recognized supply chain security standards and improve stakeholder confidence.
Who does ISO 28000 apply to? ISO 28000 can be applied by manufacturers, logistics providers, shippers, transport operators, and any organization with supply chain dependencies, regardless of industry or size. Its scope covers the full spectrum of supply chain operations, including both internal processes and external suppliers.
What are the key requirements of ISO 28000? Key requirements of ISO 28000 include conducting supply chain risk assessments, developing and implementing security policies and procedures, defining roles and responsibilities, and maintaining documentation to support audits. The standard also requires incident response planning and continuous monitoring of security controls.

How should organizations implement ISO 28000?

Implementation of ISO 28000 involves establishing a management system framework, integrating risk management processes, setting security objectives, and defining operational controls across the supply chain. Regular training, internal audits, and management review are essential for ongoing effectiveness and regulatory alignment.

How does ISO 28000 relate to other ISO standards?

ISO 28000 is compatible with other management system standards, such as ISO 9001 (quality management) and ISO 27001 (information security management). Organizations often integrate ISO 28000 with these frameworks to achieve comprehensive governance and streamline compliance efforts.

What are the ongoing compliance requirements for ISO 28000?

Ongoing compliance with ISO 28000 requires continuous risk monitoring, periodic reassessment of security controls, regular internal audits, and updates to policies and procedures as supply chain risks evolve. Documentation and records must be maintained for certification and audit verification.

License included / downloadable: No ISO 28000 is published by the International Organization for Standardization. Access to the full standard typically requires purchasing official documentation through authorized standards organizations. License not included with platform

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