SmartSuite

Framework / Supply Chain Security / ISO 27000 Series

ISO/IEC 27036 – Cybersecurity – Supplier Relationships (Parts 1–4)

ISO/IEC 27036 is the four-part international standard for information security in supplier relationships, covering concepts, requirements, ICT supply chain security, and cloud services.

What it is

ISO/IEC 27036, Cybersecurity – Supplier relationships, is the multi-part international standard for managing information security in the relationships between acquirers and suppliers. Part 1 (2021) gives the overview and concepts, Part 2 (2022) specifies the fundamental information security requirements for defining, implementing, operating, monitoring, reviewing, maintaining, and improving supplier and acquirer relationships, Part 3 (2023) gives guidelines for hardware, software, and services supply chain security, and Part 4 (2016) gives guidelines for the security of cloud services.

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) publish the series through ISO/IEC JTC 1/SC 27, the committee responsible for the ISO/IEC 27000 family. The standard is voluntary and applies to all organizations, regardless of type, size, and nature, in the role of acquirer, supplier, or both; Part 2 expects the organization to have foundational processes for business management, risk management, operational and human resources management, and information security already in place or in planning.

At a glance

PUBLISHER ISO and IEC	TYPE Standard	VERSION Part 1:2021, Part 2:2022, Part 3:2023, Part 4:2016
EFFECTIVE 2021-2023 (Parts 1-3); 2016 (Part 4)	DOMAIN Supply Chain Security	FAMILY ISO 27000 Series
REGION International	ADOPTION MODEL Voluntary	IMPLEMENTATION COMPLEXITY Medium

Source: https://www.iso.org/standard/82060.html

Why it matters

- **A common language for both sides** Because the standard addresses the perspectives of both acquirers and suppliers, security requirements can be written, understood, and evidenced consistently across a contract.
- **Requirements that can be audited** Part 2 states requirements rather than advice, so an organization can build supplier security into its ISO/IEC 27001 management system and have it assessed.
- **Visibility into multi-tier supply chains** Part 3 addresses the risks of physically dispersed and multi-layered hardware, software, and services supply chains, not just the direct supplier.
- **Cloud-specific guidance** Part 4 covers gaining visibility into the risks of using cloud services and responding to risks specific to acquiring or providing them.

How SmartSuite supports ISO/IEC 27036

Supplier Security Requirements Library

Hold the Part 2 requirements and the Part 3 and Part 4 guidance as reusable requirement sets applied to each supplier by type and risk tier.

Ownership, Cadence, and Accountability

Assign relationship owners across procurement, security, and the business, and schedule due diligence, reviews, and contract renewals.

Evidence Collection and Audit Trail

Attach questionnaires, certificates, audit reports, and contract clauses to each supplier with timestamps and reviewers.

Supplier Assessment and Monitoring

Run risk-tiered assessments, track findings and remediation, and record changes in the supplier's services or sub-suppliers.

Supply Chain and Cloud Alignment

Map supplier requirements to ISO/IEC 27001, NIST SP 800-161, and cloud shared-responsibility controls so one assessment serves several frameworks.

Third-Party Risk Reporting

Report supplier risk posture, open findings, and concentration across the supply chain to security leadership and the board.

Common framework mappings

ISO 27001:2022 · ISO 27002:2022 · ISO 27005:2022 · ISO 27017 · NIST SP 800-161 Rev.1 · NIST CSF 2.0 · NIST 800-53 Rev.5 · CSA CCM v4 · SIG v2024 · IEC 62443

Official resources

ISO/IEC 27036-1:2021 – Overview and concepts

The ISO catalogue entry for Part 1, the introductory part of the series that sets out its concepts.

iso.org/standard/82905.html

ISO/IEC 27036-2:2022 – Requirements

The ISO catalogue entry for Part 2, which specifies the fundamental information security requirements for supplier and acquirer relationships.

iso.org/standard/82060.html

ISO/IEC 27036-3:2023 – Hardware, software, and services supply chain security

The ISO catalogue entry for Part 3, the guidelines for multi-layered supply chain security.

iso.org/standard/82890.html

ISO/IEC 27036-4:2016 – Security of cloud services

The ISO catalogue entry for Part 4, the guidelines for cloud service customers and providers.

iso.org/standard/59689.html

Frequently asked questions

What is ISO/IEC 27036?

ISO/IEC 27036, Cybersecurity – Supplier relationships, is a four-part international standard for managing information security in the relationships between acquirers and suppliers. It covers concepts, requirements, hardware, software, and services supply chain security, and the security of cloud services.

What are the four parts of ISO/IEC 27036?

Part 1 (2021) gives the overview and concepts; Part 2 (2022) specifies the requirements; Part 3 (2023) gives guidelines for hardware, software, and services supply chain security; and Part 4 (2016) gives guidelines for the security of cloud services.

Is ISO/IEC 27036 certifiable?

The series is not certified on its own. Part 2 states requirements that organizations build into an ISO/IEC 27001 information security management system, where they can be assessed as part of that certification; Parts 1, 3, and 4 are guidance.

Who publishes ISO/IEC 27036 and who does it apply to?

ISO and IEC publish it through ISO/IEC JTC 1/SC 27. It is voluntary and applies to all organizations, regardless of type, size, and nature, whether they act as acquirer, supplier, or both.

How does ISO/IEC 27036 relate to ISO/IEC 27001 and 27002?

It elaborates the supplier relationship controls of ISO/IEC 27002 and is designed to operate within an ISO/IEC 27001 management system, using the risk management approach of ISO/IEC 27005.

What does ISO/IEC 27036 not cover?

The series does not address business continuity or resilience of the supply chain, which ISO/IEC 27031 covers, and Part 4 does not tell a cloud provider how to implement, manage, and operate its own information security, which ISO/IEC 27002 and ISO/IEC 27017 cover.

How does SmartSuite support ISO/IEC 27036?

SmartSuite manages supplier relationships as risk-tiered records with agreed security requirements, due diligence and monitoring evidence, findings, and termination tasks, mapped to ISO/IEC 27001 and NIST SP 800-161 so one supplier assessment serves several frameworks.

License included / downloadable: No The four parts of ISO/IEC 27036 are sold by ISO, IEC, and their national member bodies, and their text is not included with the platform.

Full framework page and mappings: smartsuite.com/frameworks/iso-iec-27036-cybersecurity-supplier-relationships