SmartSuite

Framework / Supply Chain Security / ISO 27000 Series

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

ISO/IEC 27036 is the four-part standard for information security in supplier relationships: concepts, Part 2 requirements, supply chain guidelines and cloud guidelines.



What it is

ISO/IEC 27036, Cybersecurity: Supplier relationships, is the four-part international standard series on information security in the relationships between acquirers and suppliers, published by ISO and IEC through ISO/IEC JTC 1/SC 27 for any organization that buys or supplies products and services that touch information. The current parts are Part 1:2021 (overview and concepts), Part 2:2022 (requirements), Part 3:2023 (guidelines for hardware, software, and services supply chain security) and Part 4:2016 (guidelines for security of cloud services); Parts 1 to 3 are second editions that replaced the 2013 and 2014 first editions.

Only Part 2 states requirements. Its Introduction says it is not intended for certification purposes and is meant to set defined information security objectives for a supplier and acquirer relationship that form a basis for assurance.

At a glance

PUBLISHER
International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC)

TYPE
Standard

VERSION
Part 1:2021, Part 2:2022, Part 3:2023 (second editions); Part 4:2016 (first edition)

EFFECTIVE
Part 1: September 2021; Part 2: June 2022; Part 3: June 2023; Part 4: October 2016

DOMAIN
Supply Chain Security

FAMILY
ISO 27000 Series

REGION
International

ADOPTION MODEL
Voluntary

IMPLEMENTATION COMPLEXITY
Medium

Source: iso.org/standard/82905.html

Why it matters

- **Risks managed on both sides** The risks should be managed by both acquirers and suppliers, and the requirements in Part 2 are written for both roles (Part 2 Introduction and Clause 5.1.1).
- **Mutual understanding** Part 2 facilitates understanding of the other party's approach to information security and its tolerance for information security risk (Part 2 Introduction, item b).
- **Objectives that support assurance** Clauses 6 and 7 state objectives that Annex C consolidates, which gives acquirer and supplier a basis for assurance (Part 2 Introduction, item f; Annex C).
- **Visibility beyond the first supplier** Part 3 addresses supply chains in which acquirers see only the first or second link, and aims for visibility, traceability and transparency (Part 3 Introduction and Clause 5.1).

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

How SmartSuite supports ISO/IEC 27036

Supplier Relationship Life Cycle

Track each supplier through planning, selection, agreement, management and termination, with an owner and status at each stage (Part 2, Clauses 7.1 to 7.5).

Selection and Due Diligence Evidence

Use Third Party Risk Management to record how candidate suppliers were evaluated against your security requirements, with the evidence collected (Part 2, Clause 7.2).

Agreements and Requirements

Use Procurement Operations and Compliance Management to hold contracts and the information security requirements agreed in each one (Part 2, Clauses 6.1 and 7.3).

Monitoring and Change

Schedule reviews and record changes in a supplier's services or sub-suppliers through the operating period (Part 2, Clause 7.4).

Termination and Transition

Track the closing steps for each relationship, including return or removal of information and access, as tasks with owners (Part 2, Clause 7.5).

Supply Chain Risk Reporting

Use Third Party Risk Management and Cyber & IT Risk to report supplier risk, open findings and dependencies on software components to security leadership (Part 2, Clause 6.3.4; Part 3, Annex B).

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 · Shared Assessments SIG · IEC 62443

Official resources

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

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

iso.org/standard/59689.html

Frequently asked questions

Which parts of ISO/IEC 27036 are requirements and which are guidance?

Part 2:2022 is the requirements part and uses "shall" in Clauses 6 and 7. Part 1:2021 is an introductory overview of concepts (Clause 1), Part 3:2023 gives guidance for acquirers and suppliers of hardware, software and services (Clause 1), and Part 4:2016 gives guidelines for the security of cloud services.

Can an organization be certified to ISO/IEC 27036?

No. The Introduction to Part 2 says the document is not intended for certification purposes (item e). Its objectives are meant as a basis for assurance between an acquirer and a supplier (item f), and Part 1 recommends using ISO/IEC 27001 and ISO/IEC 27002 in managing supplier relationships (Introduction).

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

What are the stages of the supplier relationship life cycle in Part 2?

Clause 7 sets five processes for a single supplier relationship: supplier relationship planning (7.1), supplier selection (7.2), supplier relationship agreement (7.3), supplier relationship management (7.4) and supplier relationship termination (7.5). Each is written as an objective, inputs, activities and outputs, and applies to both acquirer and supplier.

What does Part 3 add for hardware and software supply chains?

Part 3:2023 aims at visibility, traceability and transparency in multi-layered supply chains (Clause 5.1) and sets guidance for each 15288 life cycle process in Clause 6, including verification (6.4.9) and disposal (6.4.14). Annex B (informative) lists the essential elements of a software bill of materials, defined in Clause 3.1 as an inventory of software components, sub-components and dependencies.

Are all four parts of ISO/IEC 27036 current?

Yes, as of October 14, 2026: ISO lists Part 1:2021, Part 2:2022 and Part 3:2023 as published second editions, and Part 4:2016 as confirmed in March 2022. Part 1 entered systematic review on July 15, 2026, and ISO lists no revision project for any part.

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

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