ISO/IEC 27036

Search

Search this site

ISO/IEC 27036:2016-2023 — Cybersecurity — Supplier relationships — **Information security for supplier relationships** *(four parts)*

Introduction

ISO/IEC 27036 is a multi-part standard offering guidance on the management of information risks involved in the **acquisition of ICT products (goods and services) from suppliers.**

The standards avoid referring to selling and buying since the issues are much the same whether the transactions are commercial or not *e.g.* when one part of an organisation or group acquires ICT products from another, or uses free/open-source products.

ISO/IEC 27036-1:2021 — Cybersecurity — Supplier relationships — **Part 1: Overview and concepts** *(second edition)*

- **Abstract**: part 1 *"is an introductory part of ISO/IEC 27036. It provides an overview of the guidance intended to assist organizations in securing their information and information systems within the context of supplier relationships. It also introduces concepts that are described in detail in the other parts of ISO/IEC 27036. [ISO/IEC 27036] addresses perspectives of both acquirers and suppliers." [ISO/IEC 27036-1:2021]*

- **Scope & purpose:** part 1 introduces all parts of this standard, providing general background information such as the key terms and concepts around information security in supplier relationships, including "*any supplier relationship that can have information security implications, e.g. information technology, healthcare services, janitorial services, consulting services, R&D partnerships, outsourced applications (ASPs), or cloud computing services (such as software, platform, or infrastructure as a service).*"

  Part 1 outlines a number of information risks commonly arising from or relating to business relationships

ISO/IEC 27036
ISO/IEC 27037
ISO/IEC 27038
ISO/IEC 27039
ISO/IEC 27040
ISO/IEC 27041
ISO/IEC 27042
ISO/IEC 27043
ISO/IEC 27045
ISO/IEC 27046
ISO/IEC 27050
ISO/IEC 27070
ISO/IEC 27071
ISO/IEC 27090
ISO/IEC 27091
ISO/IEC 27099
ISO/IEC TS 27100
ISO/IEC 27102
ISO/IEC TR 27103
ISO/IEC TR 27109
ISO/IEC TS 27110
ISO/IEC TS 27115
ISO/IEC 27116
ISO/IEC 27400
ISO/IEC 27402
ISO/IEC 27403
ISO/IEC 27404
ISO/IEC TR 27550
ISO/IEC 27551
ISO/IEC 27553
ISO/IEC 27554
ISO/IEC 27555
ISO/IEC 27556
ISO/IEC 27557
ISO/IEC 27559
ISO/IEC TS 27560

between acquirers and suppliers, where goods/services acquired have an information content or information security relevance, or where the supplier gains access to the acquirer's internal information. [The converse situation - *i.e.* acquirers gaining access to suppliers' internal information - is not explicitly mentioned in part 1 but is noted in part 2.]

The standard primarily takes the perspective of the acquirer, covering the acquirer's information security concerns that ought to be addressed in relationships with upstream suppliers. [The supplier's information risks when supplying downstream customers, or in relationships with partners, are not explicitly covered *e.g.* disclosure and theft of sensitive intellectual property.]

- **Status:** the *first* edition of part 1 was published and made available for free in **2014.** The *second* edition was published in **2021** but is no longer free, unfortunately [don't shoot the messenger! If I were in charge, I'd make all the ISO27k standards freely available to information risk and security white-hats ... but I'm not].

ISO/IEC 27036-2:2022 — Cybersecurity — Supplier relationships — **Part 2: Requirements** *(second edition)*

- **Abstract**: part 2 *"specifies fundamental information security requirements for defining, implementing, operating, monitoring, reviewing, maintaining and improving supplier and acquirer relationships. These requirements cover any procurement and supply of products and services, such as manufacturing or assembly, business process procurement, software and hardware components, knowledge process procurement, build-operate-transfer and cloud computing services ... To meet the requirements, it is expected that an organization has internally implemented a number of foundational processes or is actively planning to do so [such as] business management, risk management, operational and human resources management, and information security." [Source: ISO/IEC 27036-2:2022]*

- **Scope & purpose:** part 2 specifies fundamental information security requirements pertaining to business relationships between suppliers and acquirers of various products (goods and services). It helps them reach a common understanding of the associated information risks, and treat them accordingly to their mutual satisfaction.

  The introduction explicitly states that part 2 is ***not* for certification** despite having "Requirements" in the title and "shall" in the content [these are normally reserved words in ISO-land].

  The controls recommended in part 2 cover various aspects of governance and business management (*e.g.* operations, HR management, IT management, relationship management, metrics) as well as information risk management (*e.g.* information risk analysis and treatment, security controls specification, security architecture/design, strategy).

  Given the presumptions, style, structure, depth, breadth, rigour and documentation requirements laid out in part 2, following the standard in detail would impose a significant burden of red-tape in the case of commodity supplies but may be entirely appropriate for those with strong information security implications (*e.g.* military and government procurement of classified ICT systems and services, or commercial procurement of safety- or business-critical ICT systems and services including cloud computing support for core business processes, plus information services such as consulting, legal or HR services). Nevertheless, the standard is a useful checklist or reminder of the information security aspects that ought at least to be considered in most if not all business relationships.

- **Status:** the *first* edition of part 2 was published in **2014**. Following changes in ISO/IEC 15288, the *second* edition was published in **2022**.

- **Personal comments:** although this is not intended to be a certifiable standard with formally-specified requirements that are mandatory for certification, wording along the lines of "*The following minimum activities shall be executed by the acquirer to meet the objective defined at [a specific clause]*" leaves little latitude for organisations to interpret, adapt and apply the standard according to their particular business situations and needs, despite an explanatory note:

  > *"The user of [ISO/IEC 27036-2] needs to correctly interpret each of the forms of the expression of provisions (e.g. "shall", "shall not", should" and "should not") as being either requirements to be satisfied or recommendations where there is a certain freedom of choice."*

  It comes down to the business and legal arrangements in place between supplier and acquirer as to how much 'freedom of choice' there is in interpreting and applying this standard. In the absence of explicit, perfectly worded, unambiguous and binding contractual clauses, lawyers smile wryly and rub their hands together ...

ISO/IEC 27036-3:2023 — Cybersecurity — Supplier relationships — **Part 3: Guidelines for hardware, software, and services supply chain security** *(second edition)*

ISO/IEC 27561
ISO/IEC 27562
ISO/IEC TR 27563
ISO/IEC 27564
ISO/IEC 27565
ISO/IEC 27566
ISO/IEC 27568
ISO/IEC 27569
ISO/IEC TS 27570
ISO/IEC 27573
ISO/IEC 27701
ISO/IEC 27706
ISO 27799

- **Abstract:** part 3 *"provides guidance for product and service acquirers, as well as suppliers of hardware, software and services, regarding:*

  a) gaining visibility into and managing the information security risks caused by physically dispersed and multi-layered hardware, software, and services supply chains;

  b) responding to risks stemming from this physically dispersed and multi-layered hardware, software, and services supply chain that can have an information security impact on the organizations using these products and services;

  c) integrating information security processes and practices into the system and software life cycle processes, as described in ISO/IEC/IEEE 15288 and ISO/IEC/IEEE 12207, while supporting information security controls, as described in ISO/IEC 27002.

  [ISO/IEC 27036-3] does not include business continuity management/resiliency issues involved with the hardware, software, and services supply chain. ISO/IEC 27031 addresses information and communication technology readiness for business continuity." [Source: ISO/IEC 27036-3:2023]

- **Scope & purpose:** part 3 guides both suppliers and acquirers of **ICT** products (goods and services) on information risk management relating to complex supply chains, including risks such as malware and counterfeit products plus 'organisational risks', and the integration of information risk management into ICT development lifecycles.

- **Content:** a wide range of information security controls are noted in part 3, such as:
  - Assurance;
  - Avoiding the gray-market;
  - Chain of custody (provenance and **S**oftware **B**ill **o**f **M**aterials);
  - Code assessment and verification;
  - Compliance management;
  - Configuration and change management;
  - Defined security expectations (specifications);
  - HR management;
  - ICT implementation and transition;
  - ICT integration;
  - ... and more ....

  Most of these controls are covered in general terms by ISO/IEC 27002: this standard provides additional guidance for their application in the context of supply and acquisition of **ICT** products *e.g.* maintaining a detailed SBoM (defined as an "*inventory of software components, sub-components and dependencies with associated information*") to keep up with vulnerabilities and patches even in obscure library functions *etc*. buried deep within end products.

  The bulk of the standard provides information security guidance for ICT suppliers and acquirers, as a set of processes for each stage of the typical ICT system lifecycle.

  Annexes reference applicable clauses from ISO/IEC 27002:2022 and describe the essential elements of an SBoM.

- **Status:** the *first* edition of part 3 was published in **2013**. The *second* edition was published in **2023**.

- **Personal comments**: the standard remains myopically focused on IT *e.g.* it concerns *IT* services, specifically, rather than professional services in general, even though they often have significant information content and substantial information risks. Organisations should therefore consider their supply chain information risks broadly (*e.g.* theft of intellectual property, misprepresentation, misappropriation, fraud ...) as well as commercial, financial and other kinds of risks (including business continuity aspects such as supply chain disruptions). Aside from supplier-acquirer relationships, information risks associated with business partners may also be of concern, where multiple organisations combine their efforts in the production process - for example, the use of contractors on an ICT production line. There may be yet more information risks in the logistics parts of the supply chain, plus related services such as installation, configuration, support and maintenance of ICT equipment, commercial data centre facilities, communications services and more.

ISO/IEC 27036–4:2016 — Information security — Security techniques — Information security for

supplier relationships — **Part 4: Guidelines for security of cloud services** *(first edition)*

- **Abstract**: part 4 *"provides cloud service customers and cloud service providers with guidance on (a) gaining visibility into the information security risks associated with the use of cloud services and managing those risks effectively, and (b) responding to risks specific to the acquisition or provision of cloud services that can have an information security impact on organizations using these services.*

  [Part 4] does not include business continuity management/resiliency issues involved with the cloud service. ISO/IEC 27031 addresses business continuity.

  [Part 4] does not provide guidance on how a cloud service provider should implement, manage and operate information security. Guidance on those can be found in ISO/IEC 27002 and ISO/IEC 27017.

  The scope of [part 4] is to define guidelines supporting the implementation of information security management for the use of cloud services" [Source: ISO/IEC 27036-4:2016]

- **Scope & purpose:** part 4 guides the vendors and customers of cloud services on information security management for cloud services.
- **Status:** the *first* edition of part 4 was published in **2016** and confirmed unchanged in 2022.
- **Personal comments:** part 4 explicitly describes the information risks that it addresses. Full marks!

Personal comments on all parts of ISO/IEC 27036

Within the ISO27k *information* security standards, the products most obviously covered by ISO/IEC 27036 include:

- IT outsourcing and cloud computing services;
- Other professional services *e.g.* legal, accounting/tax and HR services, security guards, cleaners, delivery services (couriers), equipment maintenance/servicing, consulting and specialist advisory services, knowledge management, research and development, manufacturing, logistics, source code escrow and healthcare;
- Provision of ICT hardware, software and services including telecommunications and Internet services;
- Bespoke products and services where the acquirer specifies the requirements and may play an active role in the product design and development (as opposed to commodities and standard off-the-shelf products);
- Electricity to power ICT equipment.

The ISO/IEC 27036 standards therefore *could* cover:

- Strategic goals, objectives, business needs and compliance obligations in relation to information security, privacy and assurance when acquiring ICT-related or information products;
- Information risks such as:
  - Acquirer's reliance on providers, complicating the acquirer's business continuity arrangements (both resilience and recovery);
  - Physical and logical access to and protection of second and third party information assets;
  - Creating an 'extended trust' environment with shared responsibilities for information security, or conversely applying the 'zero trust' approach in this context;
  - Creating a shared responsibility for conformity with information security policies, standards, laws, regulations, contracts and other commitments/obligations;
  - Coordination between supplier and acquirer to adapt or respond to new/changed information security requirements;
  - ... and more.
- Information security controls such as:
  - Preliminary analysis, preparation of a sound business case, Invitation To Tender *etc*., taking into account the risks, controls, costs and benefits associated with maintaining adequate information security;
  - Creation of explicit shared strategic goals to align acquirer and provider on information security and other aspects (*e.g.* a jointly-owned 'relationship strategy');
  - Specification of important information security requirements (such as requiring that suppliers are ISO/IEC 27001 certified and/or use standards such as ISO27k) in contracts, Service Level Agreements *etc*.;

  - Security management procedures, including those that may be jointly developed and operated such as risk analysis, security design, identity and access management, incident management and business continuity;
  - Special controls to cater for unique risks (such as testing and fallback arrangements associated with the transition/implementation stage when an outsourcing supplier first provides services);
  - Clear ownership, accountability and responsibility for the protection of valuable information assets, including security logs, audit records and forensic evidence;
  - A 'right of audit' and other compliance/assurance controls, with penalties or liabilities in case of identified non-compliance, or bonuses for full compliance;
  - ... and more.

- The entire relationship lifecycle:
  - Initiation - scoping, business case/cost-benefit analysis, comparison of insource versus outsource options as well as variant or hybrid approaches such as co-sourcing;
  - Definition of requirements including the information security requirements, of course;
  - Procurement including evaluating, selecting and contracting with supplier/s;
  - Transition to or implementation of the supply arrangements, with enhanced risks around the implementation period;
  - Operation including aspects such as routine relationship management, compliance, incident and change management, monitoring *etc.*;
  - Refresh - an optional stage to renew the contract, perhaps reviewing the terms and conditions, performance, issues, working processes *etc.*;
  - Termination and exit *i.e.* ending a business relationship that has run its course in a controlled manner, perhaps leading back to the start.

- Some - but not all - of this is covered by ISO/IEC 27036, potentially leaving gaps to be filled by other standards plus corporate strategies, policies and procedures.

< Previous standard ^ Up a level ^ Next standard >