**ISO/IEC 27036:2013+ — Information technology — Security techniques — Information security for supplier relationships *(four parts)***

**Introduction**

ISO/IEC 27036 is a multi-part standard offering guidance on the evaluation and treatment of information risks involved in the**acquisition of goods and services from suppliers.** The implied context is business-to-business relationships, rather than retailing, and information-related products. The terms acquisition and acquirer are used rather than purchase and purchasing since the process and the risks are much the same whether or not the transactions are commercial (*e.g*. one part of an organization or group may acquire products from another part as an internal transfer without literally paying for them).

**Scope and purpose**

Being an *information*security standard, the products most obviously covered by the standards include:

* IT outsourcing and cloud computing services;
* Other professional services *e.g.*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 often has an active role in the product design (as opposed to commodities and standard off-the-shelf products);
* Utilities such as electric power and water.

The standards may cover:

* Strategic goals, objectives, business needs and compliance obligations in relation to information security 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;
  + Creating a shared responsibility for compliance 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:
* + Relationship management covering the entire lifecycle of the business relationship;
  + 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 certified compliant with [ISO/IEC 27001](https://www.iso27001security.com/html/27001.html) and/or use standards such as [ISO27k](https://www.iso27001security.com/html/iso27000.html)) 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 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 selecting, evaluating 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 step 1.

[**ISO/IEC 27036-1:2014**](https://standards.iso.org/ittf/PubliclyAvailableStandards/c059648_ISO_IEC_27036-1_2014.zip)**— Information security for supplier relationships — Part 1: Overview and concepts [FREE!]**

**Scope & purpose:** part 1 introduces all parts of this standard, providing general background information and introducing the key terms and concepts in relation to 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).”

It outlines a number of information risks commonly arising from or relating to business relationships 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.

Interestingly, 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 is primarily written from the perspective of the acquirer, covering the acquirer’s information security concerns that ought to be addressed when forming relationships with suppliers.

**Status:** published in **2014**and [downloadable **for free** from the ITTF site](https://standards.iso.org/ittf/PubliclyAvailableStandards/c059648_ISO_IEC_27036-1_2014.zip).

[**ISO/IEC 27036-2:2014**](https://www.iso.org/standard/59680.html?browse=tc)**— Information security for supplier relationships — Part 2: Requirements**

**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 **ISO/IEC 27036 Part 2 is *not*intended for certification purposes**, despite having “Requirements” in the title and “shall” in the content [these are normally reserved words in ISO-land].

The control measures 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 security management (*e.g.* information risk analysis and treatment, controls specification, 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 including consulting). Nevertheless, the standard is a useful checklist or reminder of the information security aspects that ought to be considered in most if not all business relationships.

**Status:** published in **2014**.

Oct Part 2 is being revised following changes in ISO/IEC 15288. The revised standard is at **W**orking **D**raft stage.  It is due to be published in 2023.

**Notes: although this is not meant to be a certifiable standard,**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.

[**ISO/IEC 27036-3:2013**](https://www.iso.org/standard/59688.html?browse=tc)**— Information security for supplier relationships — Part 3:- Guidelines for ICT supply chain security**

**Scope & purpose:** this part of the standard guides both suppliers and acquirers of ICT goods and services on information risk management relating to the widely dispersed and complex supply chain, including risks such as malware and counterfeit products plus ‘organizational risks’, and the integration of risk management with system and software lifecycle processes, drawing on ISO/IEC 15288, 12207 and [27002](https://www.iso27001security.com/html/27002.html).

This part of ISO/IEC 27036 does *not*cover the business continuity aspects. It specifically concerns ICT products.

**Content:** a wide range of information security controls are noted in part 3, such as: chain of custody; least privilege access; separation of duties; tamper resistance and evidence; persistent protection; compliance management; code assessment and verification; security training; vulnerability assessment and response; defined security expectations; intellectual property rights and responsibilities; avoiding the gray-market; procurement processes including anonymous and all-at-once acquisition; passing security requirements to upstream suppliers; quality management; HR management; project management; supplier/relationship management; risk and security management (*e.g.* requirements analysis should include information security requirements addressing potential risks); configuration and change management; information management; security architecture/design; ICT implementation and transition; ICT integration; ICT testing and verification (*e.g*. security/penetration testing, vulnerability scanning, stress testing, compliance testing); malware protection; ICT management, maintenance and disposal *etc.* Most of these are covered in general terms by ISO/IEC 27002: 27036-3 provides additional guidance in the specific context of ICT supplies. An annex includes a breakdown of comparable clauses in ISO/IEC 15288 and 12207, and another identifies relevant clauses from [ISO/IEC 27002](https://www.iso27001security.com/html/27002.html).

**Status:** published in **2013**.

[**ISO/IEC 27036–4:2016**](https://www.iso.org/standard/59689.html?browse=tc)**— Information security for supplier relationships — Part 4: Guidelines for security of cloud services**

**Scope & purpose:**part 4 offers information security guidance to the vendors and customers of cloud services.

The scope is to:

“provide 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.

[The standard] does not include business continuity management/resiliency issues involved with the cloud service. [ISO/IEC 27031](https://www.iso27001security.com/html/27031.html) addresses business continuity. [The standard] 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](https://www.iso27001security.com/html/27002.html) and [ISO/IEC 27017](https://www.iso27001security.com/html/27017.html). The scope of this [standard] is to define guidelines supporting the implementation of information security management for the use of cloud services.” [quoting from the FDIS version]

**Status:**published in **2016**.

**Personal comments: p**art 4 explicitly describes the information risks that the standard addresses. Full marks!

**Revision of ISO/IEC 27036**

The revision of this multi-part standard is under way. It has been proposed to revise the set to improve internal consistency, and to align with [ISO/IEC 15288](https://en.wikipedia.org/wiki/ISO/IEC_15288) (IT system lifecycles).