INTERNATIONAL STANDARD

ISO/IEC 27036-1

Second edition
2021-09

Cybersecurity — Supplier relationships —

Part 1: Overview and concepts

Cybersécurité — Relations avec le fournisseur —

Partie 1: Aperçu général et concepts

Reference number
ISO/IEC 27036-1:2021(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 27036-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity, and privacy protection*.

This second edition cancels and replaces the first edition (ISO/IEC 27036-1:2014), of which this constitutes a minor revision.

The main changes compared to the previous edition are as follows:

— change of title;

— revision of Clause 2;

— alignment with drafting rules;

— ISO/IEC 27036 (all parts) added in Bibliography.

A list of all parts in the ISO/IEC 27036 series can be found on the ISO website

Introduction

Most (if not all) organizations around the world, whatever their size or domains of activities, have relationships with suppliers of different kinds that deliver products or services.

Such suppliers can have either a direct or indirect access to the information and information systems of the acquirer, or will provide elements (software, hardware, processes, or human resources) that will be involved in information processing. Acquirers can also have physical and logical access to the information of the supplier when they control or monitor production and delivery processes of the supplier.

Thus, acquirers and suppliers can cause information security risks to each other. These risks need to be assessed and treated by both acquirer and supplier organizations through appropriate management of information security and the implementation of relevant controls. In many instances, organizations have adopted ISO/IEC 27001 and ISO/IEC 27002 for the management of their information security. Such International Standards should also be adopted in managing supplier relationships in order to effectively control the information security risks inherent in those relationships.

This document provides further detailed implementation guidance on the controls dealing with supplier relationships that are described as general recommendations in ISO/IEC 27002.

Supplier relationships in the context of this document include 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).

Both the supplier and acquirer should take responsibility for achieving the objectives in the supplier-acquirer relationship and adequately addressing the information security risks that can occur. It is expected that they implement the requirements and guidelines of this document. Furthermore, fundamental processes should be implemented to support the supplier-acquirer relationship (e.g. governance, business management, and operational and human resources management). These processes will provide support in terms of information security as well as the accomplishment of business objectives.

Cybersecurity — Supplier relationships —

Part 1: Overview and concepts

1 Scope

This document 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. This document addresses perspectives of both acquirers and suppliers.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions in ISO/IEC 27000 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
acquirer
anybody that procures a product or service from another party

Note 1 to entry: Procurement may or may not involve the exchange of monetary funds.

[SOURCE: ISO/IEC/IEEE 15288:2015, 4.1.1, modified — Original Note was removed, the word "acquires" was removed from the definition, and Note 1 to entry was added.]

3.2
acquisition
process (3.7) for obtaining a product or service

[SOURCE: ISO/IEC/IEEE 15288:2015, 4.1.2, modified — The word "system" was removed.]

3.3
agreement
mutual acknowledgement of terms and conditions under which a working relationship is conducted

[SOURCE: ISO/IEC/IEEE 15288:2015, 4.1.4]

3.4
life cycle
evolution of a *system* (3.11), product, service, project, or other human-made entity from conception through retirement

[SOURCE: ISO/IEC/IEEE 15288:2015, 4.1.23]

3.5
downstream
handling *processes* (3.7) and movements of products and services that occur after an entity in the *supply chain* (3.10) takes custody of the products and responsibility for services

[SOURCE: ISO 28001:2007, 3.10, modified — The word "goods" was replaced by "products and services", and the definition was changed to better reflect this change in focus.]

3.6
outsourcing
acquisition (3.2) of services (with or without products) in support of a business function for performing activities using *supplier's* (3.8) resources rather than the *acquirer's* (3.1)

3.7
process
set of interrelated or interacting activities which transforms inputs into outputs

[SOURCE: ISO 9000:2015, 3.4.1, modified — Notes were removed.]

3.8
supplier
organization or an individual that enters into an *agreement* (3.3) with the *acquirer* (3.1) for the supply of a product or service

Note 1 to entry: Other terms commonly used for supplier are contractor, producer, seller, or vendor.

Note 2 to entry: The acquirer and the supplier can be part of the same organization.

Note 3 to entry: Types of suppliers include those organizations that permit agreement negotiation with an acquirer and those that do not permit negotiation with agreements, e.g. end-user license agreements, terms of use, or open source products' copyright or intellectual property releases.

[SOURCE: ISO/IEC/IEEE 15288:2015, 4.1.45, modified — Note 3 to entry was added.]

3.9
supplier relationship
agreement or *agreements* (3.3) between *acquirers* (3.1) and *suppliers* (3.8) to conduct business, deliver products or services, and realize business benefit

3.10
supply chain
set of organizations with linked set of resources and *processes* (3.7), each of which acts as an *acquirer* (3.1), *supplier* (3.8), or both to form successive *supplier* (3.8) relationships established upon placement of a purchase order, *agreement* (3.3), or other formal sourcing *agreement* (3.3)

Note 1 to entry: A supply chain can include vendors, manufacturing facilities, logistics providers, distribution centres, distributors, wholesalers, and other organizations involved in the manufacturing, processing, design and development, and handling and delivery of the products, or service providers involved in the operation, management, and delivery of the services.

Note 2 to entry: The supply chain view is relative to the position of the acquirer.

[SOURCE: ISO 28001:2007, 3.24, modified — The definition was changed to focus more on the organization and relationships; Note 2 to entry was added.]

3.11
system
combination of interacting elements organized to achieve one or more stated purposes

Note 1 to entry: A system can be considered as a product or as the services it provides.

Note 2 to entry: In practice, the interpretation of its meaning is frequently clarified by the use of an associative noun, e.g. aircraft system. Alternatively, the word "system" can be substituted simply by a context-dependent synonym, e.g. aircraft, though this can then obscure a system principles perspective.

[SOURCE: ISO/IEC/IEEE 15288:2015, 4.1.46]

3.12
trust
relationship between two entities or elements, consisting of a set of activities and a security policy in which element *x* trusts element *y* if and only if *x* has confidence that *y* will behave in a well-defined way (with respect to the activities) that does not violate the given security policy

3.13
upstream
handling *processes* (3.7) and movements of products and services that occur before an entity in the *supply chain* (3.10) takes custody of the products and responsibility for information and communication technology (ICT) services

[SOURCE: ISO 28001:2007, 3.27, modified — The word "goods" was replaced by "products and services", and the definition was changed to better reflect this change in focus.]

3.14
visibility
property of a *system* (3.11) or *process* (3.7) that enables system elements and *processes* (3.7) to be documented and available for monitoring and inspection

4 Symbols and abbreviated terms

The following symbols and abbreviated terms are used in this document:

API	Application Programming Interface
ASP	Application Service Provider
BCP	Business Continuity Plan(ning)
BPaaS	Business Process as a Service
IaaS	Infrastructure as a Service
ICT	Information and Communication Technology
PaaS	Platform as a Service
R&D	Research & Development
SaaS	Software as a Service

5 Problem definition and key concepts

5.1 Motives for establishing supplier relationships

Organizations often choose to form and retain supplier relationships for a variety of business reasons to take advantage of the benefits they can provide. The following summarizes potential motivations for establishing a supplier relationship:

a) Focusing internal resources on core business functions which can result in a cost reduction and improve return on investment (e.g. outsourcing ICT services).

b) Acquiring a short-term or highly specialized competency that an organization does not already possess (e.g., hiring an advertising firm) to achieve certain business objectives.

c) Acquiring a utility or basic service that is common or readily available (e.g. electric power and telecommunications) that cannot efficiently be provided by the organization.

d) Enabling business operations in a different geographical location.

e) Acquiring new or replacement ICT equipment or services (e.g. laptops, printers, servers, routers, software applications, storage capacity, network connectivity, ICT managing services etc.) that enable workforce productivity and other business computing needs.

Suppliers can provide a multitude of products or services, including IT outsourcing, professional services, basic utilities (equipment maintenance service, security guards service, cleaning and delivering services etc.), cloud computing services, information and communication technology (ICT), knowledge management, R&D, manufacturing, logistics, health care services, Internet services, and many others.

5.2 Types of supplier relationships

5.2.1 Supplier relationships for products

When an acquirer enters a supplier relationship for products, it typically purchases products with agreed specifications for a predetermined period for manufacturing the acquirer's products.

The supplier can have access to the acquirer's information when delivering and supporting the product which can result in information security risks to the acquirer's information. Failures to fulfil requirements, software vulnerabilities and malfunctions of products and inadvertent release of sensitive information can also cause information security risks to the acquirer.

To manage these information security risks, the acquirer may wish to control supplier's access to the acquirer's information. The acquirer may also wish to control elements of the supplier's production processes to maintain quality of the products and to reduce information security risks derived from vulnerabilities, malfunctions or other failures to fulfil requirements. This, in turn, can pose information security risks to the supplier because the acquirer can have access to the supplier's information when controlling elements of the supplier's processes.

Further, the acquirer may wish to have assurances regarding the specification of products, by monitoring or auditing of the production processes or requiring the supplier to obtain an independent certification to demonstrate existence of good practices and required processes. These assurance requirements need be agreed between the acquirer and supplier.

5.2.2 Supplier relationships for services

When an acquirer procures services, the supplier generally has access to the acquirer's information. This causes potential information security risks to the acquirer. In the case of business process outsourcing, e.g. that of marketing, call centre operation or the organization's ICT infrastructure, a significant portion of the acquirer's critical business information can be put under management of the

supplier. Other kinds of services have generally limited access to the acquirer's information, such as food services and janitorial services.

Delivery of some services requires the acquirer's information to be located within acquirer's premises and to be accessed onsite or remotely by the supplier. In other cases, acquirer's information is located at the supplier's site. These specific conditions can impact selection of controls applicable to the acquirer or supplier. See Table 2 for examples of how location can have an impact on supplier's accesses to the acquirer's information.

When acquiring services, acquirers should establish rules for how to control supplier access to acquirer's information. The acquirer may also wish to control the quality of the service to reduce information security risks, including the ability to meet availability requirements over time. A service level agreement is a general way of agreeing on the quality of service. For the supplier, a service level agreement can be a tool for communicating how the supplier will satisfy quality expectations to the acquirer.

The acquirer may wish to have assurance regarding the quality of the service by monitoring or auditing the supplier service processes or requiring the supplier to obtain a certification to demonstrate existence of good practices or required processes. These assurance requirements need also be agreed between the parties.

5.2.3 ICT supply chain

An ICT supply chain is a set of organizations with a linked set of resources and processes that form successive supplier relationships of ICT products and services. An ICT product or service can be composed of components, resources and processes produced by a supplier which can have been produced, in whole or in part, by another supplier. As such, an ICT service, in its entirety, may have been sourced by multiple suppliers. As depicted in Figure 1, an organization in an ICT supply chain is an acquirer in relation to the upstream organization, and a supplier in relation to the downstream organization. The adjacent downstream organization is often called a customer from the perspective of the organization that provides products or services to it. The customer at the end of the ICT supply chain is referred to as an end customer, or consumer. Generally, the end customer has limited control over their direct supplier's information security requirements and no control over information security requirements beyond the direct supplier.

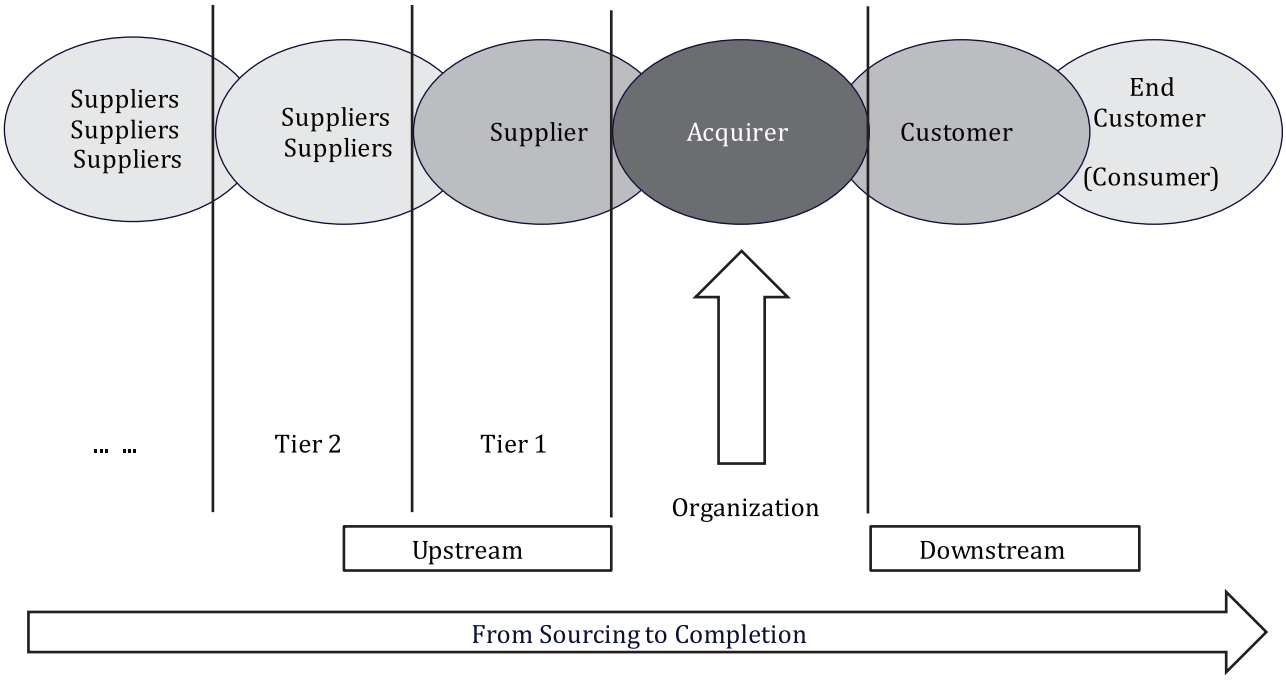

Figure 1 — Supply chain relationships

Acquirers and suppliers throughout the ICT supply chain inherit information security risks associated with individual supplier relationships for products and services (see 5.2.1 and 5.2.2). However, it is challenging for acquirers to manage these information security risks through communicating, monitoring, and enforcing their information security throughout the ICT supply chain due to limited visibility into and access to their suppliers' suppliers.

5.2.4 Cloud computing

Cloud computing is a form of a supplier relationship, in that a cloud computing service, in its entirety, may have been sourced from multiple suppliers. The purpose of cloud computing is to enable utility-based or per-use computing and storage services and capabilities based on business requirements for scalability, availability and elasticity service expectations. In a cloud computing service, a supplier is commonly referred to as the cloud service provider and the acquirer referred to as the cloud service customer. In some cases, the cloud service provider delegates the management or control over components, resources and processes to the cloud service customer in an environment potentially shared with other cloud service customers, commonly referred to as a multi-tenant cloud environment. ICT supply chain security considerations also apply when cloud computing services form an ICT supply chain, e.g., when a customer uses SaaS built on top of IaaS.

5.3 Information security risks in supplier relationships and associated threats

Information security risks in supplier relationships are a matter of concern, not only for the acquirer and supplier, but also for customers and other interested parties. It is a question of trust in business activities in society. Both the supplier and acquirer should consider the inherent and residual information security risks associated with establishing a supplier relationship.

Acquirer and supplier are both responsible for making their agreement trustworthy and for managing their information security risks which includes establishing delineated roles and responsibility for information security and implementation of controls.

Each supplier relationship within an organization is established for a specific purpose. The number of such relationships is likely to grow over time resulting in those relationships not being well managed or controlled by acquirers. Specifically, large organizations tend to have a significant number of supplier relationships that were established by different internal entities using a variety of processes and arrangements. Many of these relationships have extended supply chains with multiple layers. This multiplicity can result in making it increasingly more difficult for an organization to ensure that the information security risks created by those supplier relationships are appropriately addressed.

The supply and support of a product or service can be dependent upon either the acquirer or supplier transfer of information and information systems to the other party. This information needs to be appropriately protected through establishing an agreement among acquirers and suppliers. This agreement should state the mutually acceptable set of controls and responsibility for implementation. Lack of such agreement may have an impact on acquirers' or suppliers' information security in the following ways:

a) Disparate acquirer and supplier information security governance, risk tolerance and compliance practices or different cultural or organizational attitudes resulting in gaps in security requirements and controls between acquirer and supplier.

b) Reliance on supplier's services and capabilities designed to ensure compliance with acquirer's own information security requirements resulting in unintended controls dependencies.

c) Conflicting or different acquirer and supplier information security controls that interfere or weaken the information security of the other party.

Supplier relationships may create a number of information security risks for both acquirers and suppliers. The following are examples of such risks that should be considered throughout the life cycle of a supplier relationship – from planning to termination:

a) Lack or weakness of governance:

   1) Acquirers lose control over how their information is stored, processed, transmitted, created, modified and destroyed.

   2) Suppliers, unless specifically prohibited by the agreement, may outsource a subset of resources and processes to another supplier, thus reducing or limiting the acquirer's control, and potentially exposing the acquirer to further risks.

b) Miscommunication and misunderstanding:

   1) Controls put in place by the supplier do not address the risks identified by the acquirer, leaving the acquirer vulnerable to risks presumed to be addressed and managed by the supplier.

   2) Confidentiality, integrity and availability requirements of the acquirer may not be communicated properly to the supplier and hence not correctly met.

   3) Requirements concerning availability/BCP for information or information systems that support the on-time and on-delivery of products or services by the supplier to the acquirer cannot be specified, leading to interruptions in supply.

   4) Suppliers fail to allocate sufficient resources, including skilled staff, to protect the acquirer's information.

c) Geographical, social and cultural differences:

   1) The acquirer is inadvertently in breach of legislation or regulation, leading to reputational damage and financial penalties.

   2) Reference to a law or a standard as a requirement in an agreement allows for misinterpretation by acquirer and supplier which results in a dispute.

   3) The service is provided in a location either unknown to or not permitted by the acquirer, leading to violations of acquirer's regulatory or compliance requirements.

Specific information security risks to acquirer's and supplier's information and information systems can be directly correlated with inadequate control awareness, ownership and accountability. Such risks may be applicable to the supply of both products and services. Table 1 provides examples of information security risks related to acquiring products. Information security risks associated with services are usually caused by supplier access to information or information systems. Table 2 provides examples of risks related to supplier's access to acquirer's information and information systems.

Table 1 — Example information security risks for acquiring products

No.	Type	Description
1	Information security feature	In the case where supplied products have a vulnerability, the acquirer's derived products, services or processes will be vulnerable.
2	Quality	Poor quality of supplied products can cause information security weakness of the acquirer's derived products, services and processes.
3	Intellectual property rights	Unidentified intellectual property rights can cause later dispute in relation with the acquirer's derived products or services.
4	Authenticity	In the case where fake or fraudulent products were supplied, the acquirer's expectation for an information security feature and the quality and identification of intellectual property rights are threatened with a likelihood of an information security weakness introduced and a loss in the business relationship confidence.

Table 1 *(continued)*

No.	Type	Description
5	Assurance	Without assurance of appropriate information security features, product quality, and identification of intellectual property rights and authenticity, the acquirer lacks confidence in reliance upon the supplier's products.

Table 2 — Example information security risks for acquiring services

No.	Type	Description	Example Use Case(s)
1	Physical access onsite	Supplier has physical access to the information processing facilities of the acquirer but does not have logical access	Security guard service, delivery services, a cleaning service or an equipment maintenance service
2	Access to information and information systems onsite	Supplier personnel are onsite and have logical access to information and information systems of the acquirer, through the use of acquirer's equipment	Outsourced expertise working onsite and integrated in acquirer's teams
3	Remote access to in-house information and information systems	Supplier has remote access to information and information systems of the acquirer	Remote development and maintenance activities, remote information system and equipment management, logistics, call centre operation, automated facilities management systems
4	Processing of information offsite	Information under the responsibility of the acquirer is processed by the supplier offsite, using applications and systems under the control and the management of the supplier	Consulting (market research, sales promotion, technical studies, etc.), information processing, R&D, manufacturing , storage and archival, application service (ASP), Business Process as a Service (BPaaS) such as travel or financial services, Infrastructure as a Service (IaaS) or Software as a Service (SaaS) providers
5	Applications offsite	Applications operated by the acquirer are running PaaS or IaaS	Platform as a Service (PaaS) providers if supplier provides development platform or IaaS providers if supplier provides network, compute and storage services
6	Equipment offsite	Equipment dedicated to the acquirer and owned by the acquirer are hosted offsite, on the supplier site	Offsite hosting of information systems housing or IaaS
7	Storage of information offsite	Acquirer outsources the storage of information to a supplier for offsite retention or archive	Use of storage service to maintain backup copies of information generated by in-house information processing
8	Source code escrow	Services involving supplier artefacts used by the acquirer are held in escrow by a trusted third party and are made available to the acquirer under defined circumstances	Source code held by an independent third party to maintain usefulness of software by the acquirer in the case that the supplier of the software goes out of business

5.4 Managing information security risks in supplier relationships

In the supplier relationship, acquirer's or supplier's access to or handling of the other organization's information can introduce information security risks for both the acquirer and supplier. The acquirer and supplier evaluate risks, and select, implement and maintain controls to mitigate them. In the context of supplier relationships, the controls consist of:

a) Those that directly address information security risks associated with access to or handling of each organization's information;

b) Those that address quality of supplier products that impacts the acquirer‘s and its customer‘s information security risks; and

c) Those enforcing a) or b) above on the other organization, e.g. by managing and reporting requirements, monitoring, auditing and certification.

The agreement between the acquirer and supplier binds both organizations in implementing and maintaining those controls.

Regardless of the nature of the provided product or service, visibility of information security should be considered as an important part of establishing a supplier relationship to ensure information security risks to the acquirer’s information and information systems are managed. In order to identify and manage these information security risks, the acquirer should obtain assurance that the supplier has implemented adequate information security management and controls. In the case where these are not negotiable, the acquirer should select a supplier’s product or service based on criteria which include requirements for information security management and controls to avoid or mitigate risks to an acceptable level.

5.5 ICT supply chain considerations

The acquirer’s acceptance of a supplier’s production, delivery and operation of products and services should be based on criteria which ensures levels of information security which the acquirer wishes to have within its own organization. These could include any of the following:

— Management of political, legal and information security risks relating to the local environment which impact the acquirer’s information security, including continuity of information, information systems and services.

— Management of confidentiality of physical and electronic documents and other information relating to the supplied products and services.

— Management of integrity of materials and elements to ensure proper handling, i.e., unique markings and protective labelling.

— Management of integrity of software or other electronic information related to the supplied product or service to ensure it is not compromised, e.g. using cryptographic hash functions or digital watermarks.

— Management of physical security of facilities from which products and services are delivered.

— Management of information security relating to any aspect of the suppliers’ business and as it relates to other clients.

— Management of information security relating to the suppliers’ interactions with suppliers, and the suppliers’ interaction with other acquirers.

To appropriately manage information security in supplier relationships throughout the ICT supply chain, acquirers should adopt a framework with the following set of standardized organization-wide processes for the acquisition of products and services:

a) Establish information security and compliance requirements for the secure exchange or sharing of information and information systems.

b) Prior to acquisition, assess and monitor the information security risks associated with the supply chain.

c) Establish a process for negotiation or re-negotiation of the ICT supply chain agreement or agreements incorporating the information security and compliance requirements, including conditions for right to audit and restricting upstream suppliers throughout the multiple layers of the ICT supply chain.

d) Continuously monitor and report on the performance of suppliers within the ICT supply chain adhering to information security and compliance requirements, especially as a result of a supplier relationship change.

This framework should be flexible to allow for a range of ICT supply chain agreements that may be tailored based on the nature of the product or service being acquired and the risks that it is expected to create.

6 Overall ISO/IEC 27036 structure and overview

6.1 Purpose and structure

ISO/IEC 27036 is a multi-part document that provides requirements and guidance for acquirers and suppliers on how to secure information in supplier relationships. Figure 2 provides notional architecture of this multipart document.

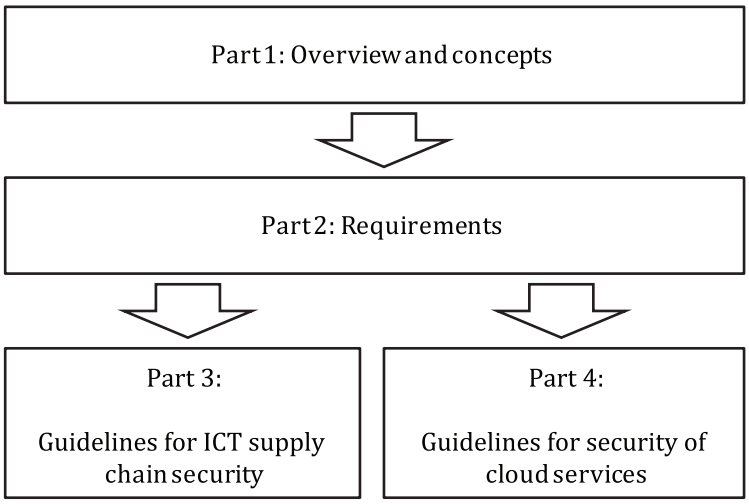

Figure 2 — ISO/IEC 27036 architecture

ISO/IEC 27036-3 and ISO/IEC 27036-4 address specific aspects of information security supplier relationships including challenges associated with those related to ICT products and services (ISO/IEC 27036-3) and cloud services (ISO/IEC 27036-4).

6.2 Overview of ISO/IEC 27036-1: Overview and concepts

This document provides overview and concepts of information security in supplier relationships. This document is an informative document.

6.3 Overview of ISO/IEC 27036-2: Requirements

ISO/IEC 27036-2 provides a high level framework for establishing information security requirements and expectations in supplier relationships. This framework includes governance, life cycle processes, and relevant high-level requirements statements. ISO/IEC 27036-2 is a normative document that acquirers can use as a source of agreement requirements to define, manage, and monitor supplier agreements. The requirements from ISO/IEC 27036-2 may also serve as additional certification criteria for the purpose of ISO/IEC 27001 certification or other certification schemas as deemed pertinent to the acquirer. For example, an acquirer may require that a supplier be certified in accordance with ISO/IEC 27001 and include additional requirements and applicable controls in accordance with ISO/IEC 27036 with respect to the products or services being offered. Acquirers may either use the entire document or extract individual portions for use as requirement statements.

6.4 Overview of ISO/IEC 27036-3: Guidelines for information and communication technology (ICT) supply chain security

In supplier relationships, an ICT product or service procured by the acquirer is not necessarily manufactured or operated solely by a supplier. For example, a product often contains parts that are made by other suppliers and provided to the supplier as an indirect relationship with the acquirer. Or, an information processing service can be built on other information processing services as its underlying infrastructure. For instance, the supplier has an agreement with another supplier to maintain the hardware, to store backups on an external location or even have the entire backup process outsourced. Thus, ICT supply chains are formed by successive supplier relationships with inherent interdependencies.

In a supply chain, information security management and controls implemented by the supplier in direct relationship with the acquirer are not always sufficient to manage information security risks of a product or service. The acquirer's management of an indirect supplier's (supplier of the supplier) product or service can be essential for information security: this requires visibility into the supply chain.

Conversely, suppliers can also experience increased information security risks caused by the interconnectedness of acquirer and supplier systems that sometimes results from the ICT supply chain. For example, acquirer can require invasive audits of the supplier's systems that can result in the acquirer's access to supplier's intellectual property.

ISO/IEC 27036-3 provides guidelines to acquirers and suppliers for managing information security risks associated with the ICT products and services supply chain. It builds on the requirements in ISO/IEC 27036-2 and provides additional practices that augment high-level requirements from ISO/IEC 27036-2.

6.5 Overview of ISO/IEC 27036-4: Guidelines for security of cloud services

Organizations use cloud computing services to take advantage of the economies of scale provided by elastic computing and storage service capabilities. These capabilities are made available on a utility-based or per-usage model. Cloud computing can be provided in a number of different cloud service delivery models, e.g., IaaS, PaaS and SaaS. However, this has introduced information security risks associated with greater complex interconnectedness of acquirer and supplier systems. Similar to ICT supply chain information security risks, there is potential for lack of clarity on roles and responsibilities for information security management and controls implementation.

For example, if information within cloud computing service workloads traverses national boundaries or the cloud service customer is unable to control how the cloud service is delivered, this may result in the risks of legal, statutory or regulatory infringement of compliance obligations by either acquirer or supplier. Additionally, multi-tenancy and the use of technologies, e.g., virtualization and application programming interfaces (APIs), can introduce new information security risks of cloud customer confidentiality as a consequence from inadequate access controls and lack of cloud service customer segregation.

ISO/IEC 27036-4 provides guidelines for information security of cloud computing services which are often provided through a supply chain from the perspective of both the acquirer and supplier of such services. Specifically, it involves managing the information security risks associated with cloud computing services throughout the supplier relationship life cycle. It builds on the requirements in ISO/IEC 27036-2 and provides additional practices that can augment high-level requirements from ISO/IEC 27036-2 and guidance from ISO/IEC 27036-3.

Bibliography

[1] ISO 9000:2015, *Quality management systems — Fundamentals and vocabulary*

[2] ISO/IEC/IEEE 15288:2015, *Systems and software engineering — System life cycle processes*

[3] ISO/IEC 12207, *Systems and software engineering — Software life cycle processes*

[4] ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

[5] ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

[6] ISO/IEC 27002, *Information technology — Security techniques — Code of practice for information security controls*

[7] ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*

[8] ISO/IEC 27014, *Information security, cybersecurity and privacy protection — Governance of information security*

[9] ISO/IEC 27035, *Information technology — Security techniques — Information security incident management*

[10] ISO/IEC 27036 (all parts), *Cybersecurity — Supplier relationships*

[11] ISO 28000, *Specification for security management systems for the supply chain*

[12] ISO 28001, *Security management systems for the supply chain — Best practices for implementing supply chain security, assessments and plans — Requirements and guidance*

ICS 35.030

Price based on 12 pages