INTERNATIONAL STANDARD

ISO/IEC 27036-3

First edition
2013-11-15

Information technology — Security techniques — Information security for supplier relationships —

Part 3: Guidelines for information and communication technology supply chain security

Technologies de l'information — Techniques de sécurité — Sécurité d'information pour la relation avec le fournisseur —

Partie 3: Lignes directrices pour la sécurité de la chaîne de fourniture des technologies de la communication et de l'information

Reference number
ISO/IEC 27036-3:2013(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web 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 27036-3 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

ISO/IEC 27036 consists of the following parts, under the general title *Information technology — Security techniques — Information security for supplier relationships*:

— *Part 1: Overview and concepts*

— *Part 2: Requirements*

— *Part 3: Guidelines for information and communication technology supply chain security*

The following part is under preparation:

— *Part 4: Guidelines for security of cloud services.*

Introduction

Information and Communication Technology (ICT) products and services are developed, integrated, and delivered globally through deep and physically dispersed supply chains. ICT products are assembled from many components provided by many suppliers. ICT services throughout the entire supplier relationship are also delivered through multiple tiers of outsourcing and supply chaining. Acquirers do not have visibility into the practices of hardware, software, and service providers beyond first or possibly second link of the supply chain. With the substantial increase in the number of organizations and people who "touch" an ICT product or service, the visibility into the practices by which these products and services are put together has decreased dramatically. This lack of visibility, transparency, and traceability into the ICT supply chain poses risks to acquiring organizations.

This standard provides guidance to ICT product and service acquirers and suppliers to reduce or manage information security risk. This standard identifies the business case for ICT supply chain security, specific risks and relationship types as well as how to develop an organizational capability to manage information security aspects and incorporate a lifecycle approach to manage risks supported by specific controls and practices. Its application is expected to result in:

— Increased ICT supply chain visibility and traceability to enhance information security capability;

— Increased understanding by the acquirers of where their products or services are coming from, and of the practices used to develop, integrate, or operate these products or services, to enhance the implementation of information security requirements;

— In case of an information security compromise, the availability of information about what may have been compromised and who the involved actors may be.

This international standard is intended to be used by all types of organizations that acquire or supply ICT products and services in the ICT supply chain. The guidance is primarily focused on the initial link of the first acquirer and supplier, but the principle steps should be applied throughout the chain, starting when the first supplier changes its role to being an acquirer and so on. This change of roles and applying the same steps for each new acquirer-supplier link in the chain is the essential intention of the standard. By following this international standard, information security implications can be communicated among organizations in the chain. This helps identifying information security risks and their causes and may enhance the transparency throughout the chain. Information security concerns related to supplier relationships cover a broad range of scenarios. Organizations desiring to improve trust within their ICT supply chain should define their trust boundaries, evaluate the risk associated with their supply chain activities, and then define and implement appropriate risk identification and mitigation techniques to reduce the risk of vulnerabilities being introduced through their ICT supply chain.

ISO/IEC 27001 and ISO/IEC 27002 framework and controls provide a useful starting point for identifying appropriate requirements for acquirers and suppliers. ISO/IEC 27036 provides further detail regarding specific requirements to be used in establishing and monitoring supplier relationships.

Information technology — Security techniques — Information security for supplier relationships —

Part 3: Guidelines for information and communication technology supply chain security

1 Scope

This part of ISO/IEC 27036 provides product and service acquirers and suppliers in ICT supply chain with guidance on:

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

b) responding to risks stemming from the global ICT supply chain to ICT products and services that can have an information security impact on the organizations using these products and services. These risks can be related to organizational as well as technical aspects (e.g. insertion of malicious code or presence of the counterfeit information technology (IT) products);

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

This part of ISO/IEC 27036 does not include business continuity management/resiliency issues involved with the ICT supply chain. ISO/IEC 27031 addresses business continuity.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. 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*

ISO/IEC 27036-1, *Information technology — Security techniques — Information security for supplier relationships — Part 1: Overview and concepts*

ISO/IEC 27036-2, *Information technology — Security techniques — Information security for supplier relationships — Part 2: Requirements*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000, ISO/IEC 27036-1 and the following apply.

3.1
reliability
property of a system and its parts to perform its mission accurately and without failure or significant degradation

3.2
system element
member of a set of elements that constitutes a system

Note 1 to entry: A system element is a discrete part of a system that can be implemented to fulfil specified requirements. A system element can be hardware, software, data, humans, processes (e.g. processes for providing required functionality to users), procedures (e.g. operator instructions), facilities, materials, and naturally occurring entities (e.g. water, organisms, minerals), or any combination.

[SOURCE: ISO/IEC 15288:2008, definition 4.32]

3.3
transparency
property of a system or process to imply openness and accountability

3.4
traceability
property that allows the tracking of the activity of an identity, process, or an element throughout the supply chain

3.5
validation
confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled

Note 1 to entry: Validation is the set of activities ensuring and gaining confidence that a system is able to accomplish its intended use, goals and objectives (i.e. meet stakeholder requirements) in the intended operational environment.

[SOURCE: ISO/IEC 15288:2008, definition 4.37]

3.6
verification
confirmation, through the provision of objective evidence, that specified requirements have been fulfilled

Note 1 to entry: Verification is a set of activities that compares a system or system element against the required characteristics. This may include, but is not limited to, specified requirements, design description and the system itself.

[SOURCE: ISO/IEC 15288:2008, definition 4.38]

4 Structure of this standard

This standard is structured to be harmonized with ISO/IEC 15288 and ISO/IEC 12207. Clause 6 mirrors lifecycle processes provided in those two standards. This standard is also harmonized with ISO/IEC 27002 and references relevant information security controls within the lifecycle processes with the mapping provided in Annex B.

The documents named in this standard are generic and do not need to be elaborate or separate documents. Organizations should use existing documents to integrate ICT supply chain security.

5 Key concepts

5.1 Business case for ICT supply chain security

Organizations acquire ICT products and services from numerous suppliers who may in turn acquire components from other suppliers. The information security risks associated with these dispersed and multi-layered ICT supply chains can be managed through the application of risk management practices and trusted relationships, thereby increasing visibility, traceability and transparency in the ICT supply chain.

For example, increased visibility into the ICT supply chain is obtained by defining adequate information security and quality requirements, and ongoing monitoring of suppliers and their products and services

once a supplier relationship is in operation. Identifying and tracking individuals accountable for quality and security for critical elements provides greater traceability. Establishing contractual requirements and expectations, as well as reviewing processes and practices provides much needed transparency.

Acquirers should establish an understanding within their organizations regarding the ICT supply chain risks and their possible impacts on businesses. Specifically, acquirer's management should be aware that practices of suppliers throughout the supply chain can have impacts on whether resulting products and services can be trusted to protect acquirer's business, information, and information systems.

5.2 ICT supply chain risks and associated threats

In a supply chain, information security management of an individual organization (acquirer or supplier) is not sufficient to maintain information security of the ICT products or services throughout their supply chain. The acquirer's management of the ICT sourcing of suppliers, products or services is essential for information security.

Acquiring ICT products and services presents special risks to acquirers in terms of managing information security risks. As global ICT supply chains get more physically dispersed and traverse multiple international and organizational boundaries, specific manufacturing and operation practices applied to individual ICT elements (products, services, and their components) become more difficult to trace including identifying individuals accountable for quality and security of those elements. This creates a general lack of traceability throughout the ICT supply chain which in turn results in higher risk of

— Compromise to acquirers' information security and therefore to business operations through intentional events such as malicious code insertion and presence of counterfeit products in the ICT supply chain

— Unintentional events, such as sloppy software development practices.

Both intentional and unintentional events may result in a compromise to acquirer's data and operations including intellectual property theft, data leakage, and reduced ability by acquirers to perform their business functions. Any of these identified concerns, if they were to occur, can harm the reputation of the organization, leading to further impacts such as loss of business.

5.3 Acquirer and supplier relationship types

ICT product and service acquirers and suppliers may involve multiple entities in a variety of supply chain based relationships, including but not limited to:

a) ICT system management support where systems are owned by acquirer and managed by supplier;

b) ICT systems or services providers where systems or resources are owned and managed by the supplier;

c) Product development, design, engineering and build where supplier provides all or parts of the service associated with creating ICT products;

d) Commercial-off-the-shelf product suppliers;

e) Open source product suppliers and distributors.

Acquirers' level of risk and need for trust in supplier relationships increases when granting a supplier a greater level of access to the acquirers' information and information systems and acquirers' dependency on the supplied ICT products and services. For example, acquiring ICT system management support has sometimes higher risk then acquiring open source or commercial off-the-shelf products. From the supplier's perspective, any compromises to the acquirer's information can harm supplier reputation and trust with the specific acquirer whose information and information systems have been compromised.

To help manage the uncertainty and risks associated with supplier relationships, acquirers and suppliers should establish a dialogue and reach an understanding regarding mutual expectations about protecting each other's information and information systems.

5.4 Organizational capability

To manage risks associated with the ICT supply chain throughout ICT products and services lifecycle, acquirers and suppliers should implement an organizational capability for managing information security aspects of supplier relationships. This capability should establish and monitor ICT supply chain security objectives for the acquirer organization and monitor achievement of these objectives including at least the following:

a) Define, select, and implement the strategy for management of information security risks caused by ICT supply chain vulnerabilities:

   1) Establish and maintain a plan for identifying potential ICT supply chain-related vulnerabilities before they are exploited; in addition, have a plan for mitigating adverse impacts.

   2) Identify and document information security risks associated with the ICT supply chain-related threats, vulnerabilities, and consequences (see Clause 6.3.4).

b) Establish and adhere to baseline information security controls as a prerequisite to robust supplier relationships (see Annex B for a mapping of Clause 6 to ISO/IEC 27002).

c) Establish and adhere to baseline system and software lifecycle processes and practices for establishing robust supplier relationships in regards to ICT supply chain information security risk management concerns (see Clause 6).

d) Have a set of baseline information security requirements that apply to all supplier relationships and tailor them for specific suppliers as needed.

e) Establish a repeatable and testable process for establishing information security requirements associated with new supplier relationships, managing existing supplier relationships, verifying and validating that suppliers are complying with acquirer's information security requirements, and ending supplier relationships.

f) Establish change management processes to ensure changes that potentially affect information security are approved and applied in a timely manner.

g) Define methods for identifying and managing incidents related to or caused by ICT supply chain and for sharing information about the incidents with suppliers and acquirers.

5.5 System lifecycle processes

Lifecycle processes can help set expectations between acquirers and suppliers for rigor and accountability with regards to information security. Acquirers can implement lifecycle processes internally, to increase the rigor with which they establish and manage supplier relationships. Suppliers can implement lifecycle processes to help demonstrate rigor that suppliers apply to system and software processes with respect to supplier relationships. While having those processes in place will be helpful for both acquirers and suppliers in beginning to address ICT supply chain risks, additional ICT supply chain security activities should be integrated into those processes.

Systems and software present many of the ICT supply chain risks. Using a lifecycle approach provided in ISO/IEC 15288 and ISO/IEC 12207 offers an established way of managing those risks. Both standards provide a set of the same processes as they apply to the specific context of systems or software. ISO/IEC 12207 is a special case of applying ISO/IEC 15288. Both standards allow for the use of any lifecycle or lifecycle model and present a set of processes that can be used within any lifecycle or any lifecycle phase as appropriate. For example, the Configuration Management process can be used both during system or software development and in operations and maintenance lifecycle phases. This standard adopts the same approach as those two standards, describing each process at a summary level by a statement of purpose and then decomposing each process into practices.

Clause 5.8 provides a summary of specific ICT supply chain security practices. Clause 6 provides a mapping of these ICT supply chain security activities for each lifecycle process. Acquirers and suppliers should select those activities that are relevant to their organization's supplier relationship capabilities,

as well as to individual supplier relationships, based on the level of risk presented by suppliers or acquirers described in Clause 5.1.

5.6 ISMS processes in relation to system lifecycle processes

ISO/IEC 27001 provides a risk-based process for implementing an information security management system (ISMS) within a defined scope. Existence of an ISMS within both acquirer and supplier organizations will help acquirers and suppliers begin addressing ICT supply chain risks and realizing the need for specific information security controls and processes needed to address these risks.

NOTE This assumes that the scope of the ISMS includes the specific part of the organization that establishes and maintains acquirer and supplier relationships.

If an organization defines risks inherent in the ICT supply chain, specific controls that mitigate these risks should be selected, potentially with extended controls added to ensure that the organization fully addresses these risks. Clause 5.5 addresses use of information security controls. Annex B maps specific information security controls to the individual lifecycle processes in Clause 6.

Suppliers can demonstrate to acquirers that they have a certain level of rigor through demonstrating ISO/IEC 27001 conformance.

When acquirers and suppliers establish ISMSs according to ISO/IEC 27001, the information generated should be used to communicate the status of information security management between an acquirer and a supplier. This may include:

a) scope of the ISMS;

b) statement of applicability;

c) risk assessment procedures,

d) audit plan;

e) awareness programs;

f) incident management;

g) measurement programs;

h) information classification scheme;

i) change management;

j) other relevant specific controls applied.

5.7 ISMS information security controls in relation to ICT supply chain security

ISO/IEC 27002 includes a number of controls that specifically target external parties, including suppliers. Clause 15 of ISO/IEC 27002 provides specific guidance for supplier relationships. These and additional extended controls can be used within the context of the lifecycle processes to help acquirers in validating specific supplier practices to ensure information security of acquirers' information and information systems.

Annex B maps specific ISO/IEC 27002 controls to individual lifecycle processes.

5.8 Essential ICT supply chain security practices

Some of the ICT supply chain risks can be addressed by applying the standards providing lifecycle processes (ISO/IEC 15288 and ISO/IEC 12207), requirements for establishing ISMS (ISO/IEC 27001),

and information security controls (ISO/IEC 27002). More detailed practices are required to fully address these risks, such as:

a) Chain of custody: the acquirer and supplier have the confidence that each change and handoff made during the element's lifetime is authorized, transparent and verifiable;

b) Least privilege access: personnel can access critical information and information systems with only the privileges needed to do their jobs;

c) Separation of duties: control the process of creation, modification, or deletion of data or the process of development, operation, or removal of hardware and software by ensuring that no one person or role alone can complete a task;

d) Tamper resistance and evidence: attempts to tamper are obstructed, and when they occur they are evident and reversible;

e) Persistent protection: critical data and information are protected in ways that remain effective even if the data or information are transferred from the location where it was created or modified;

f) Compliance management: the success of the protections within the agreement can be continually and independently confirmed;

g) Code assessment and verification: methods for code inspection are applied and suspicious code is detected;

h) ICT supply chain security training: organization's ability to effectively train relevant personnel on information security practices. This should include secure development practices, recognition of tampering, etc., as appropriate;

i) Vulnerability assessment and response: a formal understanding by acquirer of how well their suppliers are equipped with the capability to collect input on vulnerabilities from researchers, customers, or sources, and produce a meaningful impact analysis and appropriate remedies in the short timeframe involved. This should include acquirer and supplier agreement on systematic repeatable vulnerability response processes;

j) Defined expectations: clear language regarding the requirements to be met by the element and design/development environment is set forth in the agreement. This should include commitment to provide information security testing, code fixes and warranties about the development, integration, and delivery processes used;

k) Ownership and responsibilities: acquirer's and supplier's ownership of intellectual property rights and the other party's responsibilities for protecting the intellectual property rights are identified in the agreement;

l) Avoidance of gray-market components: many ICT supply chain risks can be avoided by requiring verification of authenticity for system components;

m) Anonymous acquisition: when appropriate and feasible, practice anonymous acquisition; when acquirer identity is sensitive, obscure the connection between the ICT supply chain and the acquirer;

n) All-at-once acquisition: components for long-life systems (durable automatic controls) can become obsolete and increase ICT supply chain risk, acquiring all spare parts within a specified time-frame reduces these risks;

o) Recursive requirements for suppliers: contracts can establish that suppliers place and validate ICT supply chain requirements on their upstream suppliers.

6 ICT supply chain security in Lifecycle Processes

6.1 Agreement Processes

Supplier relationships between acquirers and suppliers are achieved using agreements. Organizations can act simultaneously or successively as both acquirers and suppliers of ICT products and services. For those occasions when acquirer and supplier are within the same organization it is recommended to still use Agreement Processes but with less formality. Agreement Processes include Acquisition Process and Supply Process.[1)]

ISO/IEC 27002 provides additional specific guidance regarding setting expectations during the Agreement Processes. Mapping of ISO/IEC 27036-3, Clause 6 to ISO/IEC 27002 controls is provided in Annex B.

6.1.1 Acquisition Process

The purpose of the Acquisition Process is to obtain a product or service in accordance with the acquirer's requirements.[2)] ISO/IEC 15288 provides guidance regarding implementing an Acquisition Process. Acquirers should include the following activities as a part of the Acquisition Process to ensure they are appropriately managing ICT supply chain risks:

a) Prepare for the acquisition.

   1) Establish a strategy for how the acquisition will be conducted.

      — Establish sourcing strategies based on information security risk tolerance regarding ICT supply chain risks.

      — Specify a set of baseline information security requirements that apply to all relationships with suppliers.

   2) Tailor the set of baseline information security requirements for specific relationships with suppliers to prepare a request for the supply of a product or service that includes the following definition of requirements.

      — Establish information security requirements for suppliers including ICT-related regulatory (i.e. telecommunications or IT) requirements, technical requirements, chain of custody, transparency and visibility, sharing information on information security incidents throughout the supply chain, rules for disposal or retention of elements such as components, data, or intellectual property, and other relevant requirements.

      — Establish requirements for the suppliers managing their suppliers in the ICT supply chain when appropriate.

      — Define requirements for suppliers in the ICT supply chain to provide credible evidence that they have fulfilled information security requirements.

      — Define requirements for suppliers of critical elements in the ICT supply chain to demonstrate a capability to remediate emerging vulnerabilities based on information gathered from acquirers and other sources and to respond to incidents and remediate the underlying vulnerabilities that led to the incident.

      — Identify requirements for intellectual property ownership and responsibilities of the acquirer and suppliers for elements such as software code, data and information, the manufacturing/development/integration environment, designs, and proprietary processes.

1) Paraphrased from ISO/IEC 15288.

2) ISO/IEC 15288.

