FINAL
DRAFT

INTERNATIONAL
STANDARD

**ISO/IEC
FDIS
27036-3**

ISO/IEC JTC **1**/SC **27**

Secretariat: **DIN**

Voting begins on:
2023-02-08

Voting terminates on:
2023-04-05

Cybersecurity — Supplier relationships —

Part 3: Guidelines for hardware, software, and services supply chain security

Reference number
ISO/IEC FDIS 27036-3:2023(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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see https://patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

ISO/IEC 27036-3 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 27036-3:2013), which has been technically revised.

The main changes are as follows:

— the structure and content have been aligned with the most recent version of ISO/IEC/IEEE 15288;

— former Annex A has been removed;

— Annex B has been added.

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

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

Hardware and software products and information technology services are developed, integrated, and delivered globally through deep and physically dispersed supply chains. The supply chain can be a point-to-point or a many-to-many structure and can also be referred to as a supply network. Hardware and software are assembled from many components provided by many suppliers. Information technology 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" a hardware, software, 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 hardware, software and service supply chain poses risks to acquiring organizations.

This document provides guidance to hardware, software and service acquirers and suppliers to reduce or manage information security risk. This document identifies the business case for hardware, software, and service 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 life cycle approach to manage risks supported by specific controls and practices. Its application is expected to result in:

— increased hardware, software, and services 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 document is intended to be used by all types of organizations that acquire or supply hardware, software, and services. The guidance is primarily focused on the initial link of the first acquirer and supplier, but the principal steps should be applied throughout the chain, starting when the first supplier becomes an acquirer. This change of roles and applying the same steps for each new acquirer-supplier link in the chain is the essential intention of this document. By following this document, information security implications can be communicated among organizations in the chain. This helps identify 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 hardware, software, and services supply chain should define their trust boundaries. They should evaluate the risk associated with their supply chain activities, and then define and implement appropriate risk identification and mitigation techniques to reduce the vulnerabilities being introduced through their hardware, software and services supply chain.

The framework and controls outlined in ISO/IEC 27001 and ISO/IEC 27002 provide a useful starting point for identifying appropriate requirements for acquirers and suppliers. The ISO/IEC 27036 series provides further detail on how to establish and monitor supplier relationships. This document has been structured to be harmonized with ISO/IEC/IEEE 15288 and ISO/IEC/IEEE 12207.

Cybersecurity — Supplier relationships —

Part 3: Guidelines for hardware, software, and services supply chain security

1 Scope

This document 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.

This document 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.

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*

ISO/IEC 27036-1, *Cybersecurity — Supplier relationships — Part 1: Overview and concepts*

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.

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

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

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

3.1
software bill of materials
SBoM
inventory of software components, sub-components and dependencies with associated information

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

EXAMPLE Hardware, software, data, humans, processes (e.g. processes for providing service to users), procedures (e.g. operator instructions), facilities, materials, and naturally occurring entities or any combination.

Note 1 to entry: A system element is a discrete part of a system that can be implemented to fulfil specified requirements.

[SOURCE: ISO/IEC/IEEE 15288:2015, 4.1.47]

3.3
traceability
property that allows the tracking of the activity of an identity, process, or an element throughout the supply chain

3.4
transparency
property of a system or process to imply openness and accountability

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: A system is able to accomplish its intended use, goals and objectives (i.e. meet stakeholder requirements) in the intended operational environment. The right system was built.

[SOURCE: ISO/IEC/IEEE 15288:2015, 4.1.53]

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 includes, but is not limited to, specified requirements, design description and the system itself. The system was built right.

[SOURCE: ISO/IEC/IEEE 15288:2015, 4.1.54]

4 Structure

This structure of this document is harmonized with ISO/IEC/IEEE 15288 and ISO/IEC/IEEE 12207. Clause 6 mirrors life cycle processes provided in those two standards. This document is also harmonized with ISO/IEC 27002 and references relevant information security controls within the life cycle processes with the mapping provided in Annex A.

5 Key concepts

5.1 Business case for hardware, software, and services supply chain security

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

For example, increased visibility into the hardware, software, and services 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 supply chain entities 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 hardware, software, and services supply chain risks and their possible impacts on businesses. Specifically, the 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 the acquirer's business, information, and information systems.

5.2 Hardware, software, and services 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 hardware, software, and services throughout their supply chain. The acquirer's management of the sourcing of suppliers, products or services is essential for information security.

Acquiring hardware, software, and services presents special information security risks to acquirers. As supply chains get more complex and physically dispersed and traverse multiple international and organizational boundaries, specific manufacturing and operation practices applied to individual elements (hardware, software, services, and their components) become more difficult to trace, including identifying the individuals who are accountable for the quality and security of those elements. This creates a general lack of traceability throughout the supply chain which in turn results in higher risk of compromise to the acquirers' information security and therefore to business operations, from:

— intentional events such as malicious code insertion and presence of counterfeit products in the supply chain;

— unintentional events, such as poor software development practices or software vulnerabilities.

Both intentional and unintentional events can result in a compromise to the 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

Hardware, software, and services acquirers and suppliers can involve multiple entities in a variety of supply chain-based relationships, including but not limited to:

a) information or operational system management support where systems are owned by the acquirer and managed by the supplier;

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

c) product development, design, engineering, etc. where the supplier provides all or part of the service associated with creating hardware and software;

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

e) open source product suppliers and distributors.

When acquirers grant suppliers access to acquirers' information and information systems, acquirers assume greater dependency on the supplied hardware, software, and services. By doing so, they assume more risk and therefore require greater trust from suppliers. For example, acquiring information or operational system management support has sometimes higher risk than acquiring open source or

commercial off-the-shelf products. From the supplier's perspective, any compromises to the acquirer's information can harm the supplier's 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 hardware, software, and services supply chain throughout their life cycle, acquirers and suppliers should implement an organizational capability for managing information security aspects of supplier relationships. This capability should establish and monitor hardware, software, and services 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 hardware, software, and services supply chain vulnerabilities:

   1) Establish and maintain a plan for identifying potential hardware, software, and services 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 supply chain-related threats and vulnerabilities (see 6.3.4).

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

c) Establish and adhere to baseline system and software life cycle processes and practices for establishing robust supplier relationships in regard to hardware, software, and services 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 that changes which 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 the supply chain and for sharing information about the incidents with suppliers and acquirers.

5.5 System life cycle processes

Life cycle processes can help set expectations between acquirers and suppliers for rigor and accountability with regards to information security. Acquirers can implement life cycle processes internally, to increase the rigor with which they establish and manage supplier relationships. Suppliers can implement life cycle processes to help demonstrate rigor that suppliers apply to system and software processes with respect to supplier relationships. While having those processes in place is helpful for both acquirers and suppliers to begin addressing supply chain risks, additional hardware, software, and services supply chain security activities should be integrated into those processes.

Systems and software present many of the supply chain risks. Using a life cycle approach provided in ISO/IEC/IEEE 15288 and ISO/IEC/IEEE 12207 offers an established way of managing those risks. Both ISO/IEC/IEEE 15288 and ISO/IEC/IEEE 12207 provide a set of the same processes as they apply

to the specific context of systems or software. ISO/IEC/IEEE 12207 is a special case of applying ISO/IEC/IEEE 15288. Both documents allow for the use of any life cycle or life cycle model and present a set of processes that can be used within any life cycle or any life cycle phase, as appropriate. For example, the Configuration Management process can be used both during system or software development and in operations and maintenance life cycle phases. This document adopts the same approach as ISO/IEC/IEEE 15288 and ISO/IEC/IEEE 12207, describing each process at a summary level by a statement of purpose and then decomposing each process into practices.

Supplier relationships between acquirers and suppliers are achieved, documented, and enforced using agreements. Organizations can act simultaneously or successively as both acquirers and suppliers of hardware, software, 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 the acquisition process and the supply process (see ISO/IEC/IEEE 15288).

The organizational project-enabling processes are concerned with ensuring adequate resources so that the project meets the needs and expectations of the organization's interested parties. The organizational project-enabling processes establish the environment in which projects are conducted (see ISO/IEC/IEEE 15288). Unless specifically stated, these processes are applicable to both acquirers and suppliers.

Technical management processes are concerned with rigorous project management and project support for system and software engineering projects, including those that span across hardware, software, and services supply chain or multiple hardware, software, and services supply chains. Unless specifically stated, these processes are applicable to both acquirers and suppliers.

The technical processes define the requirements, transform the requirements into products and services, and address the use and sustainment of products and services until disposal. Unless specifically stated, these processes are applicable to both acquirers and suppliers.

5.8 provides a summary of specific hardware, software, and services supply chain security practices. Clause 6 provides a mapping of these hardware, software, and services supply chain security activities for each life cycle 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 5.1.

ISO/IEC 27002 provides additional specific guidance regarding setting expectations during the life cycle processes described in Clause 6. The mapping of Clause 6 to ISO/IEC 27002 controls is provided in Annex A.

5.6 ISMS processes in relation to system life cycle 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 helps acquirers and suppliers to begin addressing hardware, software, and services 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 hardware, software, and services 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. 5.5 addresses use of information security controls. Annex A maps specific information security controls to the individual life cycle 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 can include:

a) scope of the ISMS;

b) statement of applicability;

c) risk assessment procedures,

d) audit plan;

e) awareness programmes;

f) incident management;

g) measurement programmes;

h) information classification scheme;

i) change management;

j) other relevant specific controls applied.

5.7 ISMS controls in relation to hardware, software, and services supply chain security

ISO/IEC 27002 includes a number of controls that specifically target external parties, including suppliers. ISO/IEC 27002:2022, 5.19 to 5.22, provide specific guidance for supplier relationships. These and additional extended controls can be used within the context of the life cycle processes to help acquirers in validating specific supplier practices to ensure information security of acquirers' information and information systems.

Annex A maps specific ISO/IEC 27002 controls to individual life cycle processes.

5.8 Essential hardware, software, and services supply chain security practices

Some of the hardware, software, and services supply chain risks can be addressed by applying the standards providing life cycle processes (ISO/IEC/IEEE 15288 and ISO/IEC/IEEE 12207), requirements for establishing ISMS (ISO/IEC 27001), and information security controls (ISO/IEC 27002). Specific controls/treatments to address these practices include:

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 high-risk 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) software Bill of Materials (SBoM) that documents components of various software packages that are part of the hardware, software, or service (more information about the essential elements of SBoM can be found in Annex B);

i) hardware, software, and services 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;

j) vulnerability assessment and response: a formal understanding by the 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 time frame involved. This should include an agreement between the acquirer and supplier on systematic repeatable vulnerability response processes;

k) 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;

l) ownership and responsibilities: the 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;

m) avoidance of unauthentic and unverified components: many hardware, software, and services supply chain risks can be avoided by requiring verification of authenticity for system components;

n) anonymous acquisition: when appropriate and feasible, practice anonymous acquisition; when acquirer identity is sensitive, obscure the connection between the hardware, software, and services supply chain and the acquirer;

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

p) recursive requirements for suppliers: contracts can establish that suppliers place and validate hardware, software, and services supply chain requirements on their upstream suppliers.

6 Hardware, software, and services supply chain security in life cycle processes

6.1 Agreement processes

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. See ISO/IEC/IEEE 15288 for guidance regarding implementing an acquisition process. Acquirers should include the following as a part of the acquisition process, to ensure they are appropriately managing hardware, software, and services 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 hardware, software, and services supply chain risks,

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