INTERNATIONAL STANDARD

ISO/IEC 27036-3

Second edition
2023-06

Cybersecurity — Supplier relationships —

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

Cybersécurité — Relations avec le fournisseur —

Partie 3: Lignes directrices pour la sécurité de la chaîne de fourniture en matériel, logiciels et services

Reference number
ISO/IEC 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).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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.

This document 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

The 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. Specific guidance for supplier relationships can be found in ISO/IEC 27002:2022, 5.19 to 5.22. 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.

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:

   - establish information security requirements for suppliers including hardware, software, and services-related regulatory (i.e. telecommunications or IT) requirements, technical requirements, chain of custody, transparency and visibility (e.g. SBoM), 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 hardware, software, and services supply chain when appropriate;
   - define requirements for suppliers in the hardware, software, and services supply chain to provide credible evidence that they have fulfilled information security requirements;
   - define requirements for suppliers of critical elements in the hardware, software, and services 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;
   - define physical security requirements of the acquirer e.g. suppliers only utilizing data centres that meet the acquirer's expectations for security including availability;
   - define requirements for suppliers to identify the expected life span of the element to help the acquirer plan for any migration that can be required in support of continued system and mission operations;
   - define requirements for suppliers to demonstrate to the acquirer that the supplier has robust software supply chain practices;
   - define requirements for auditing of suppliers' information systems where applicable;
   - define requirements for monitoring suppliers' work processes and work products where applicable;
   - to share the acquirer's requirements throughout the supply chain, define requirements for communicating to upstream suppliers what is expected of them.

b) Advertise the acquisition and select the supplier

1) Communicate the request for the supply of a product or service to identified suppliers;

   - there should be no activity specific to hardware, software, and services supply chain.

2) Select one or more suppliers;

   - select suppliers based on an evaluation of their ability to meet specified requirements including those for hardware, software, and services supply chain,
   - use established evaluation methods and results for hardware, software, and services, components or their suppliers (e.g. ISO/IEC 15408 repositories for components or ISMS certification for suppliers) as criteria to evaluate conformance to specified requirements,
   - employ consideration of suppliers past performance regarding personnel policies, procedures, and information security practices as part of source selection requirements and processes.

c) Initiate an agreement

   1) Negotiate an agreement with the supplier;

      — negotiate an agreement with the selected supplier or suppliers and stipulate agreed requirements applicable to hardware, software, and services supply chain in the agreement.

   2) Commence the agreement with the supplier;

      — establish and maintain a plan for ensuring the integrity of acquired software and hardware products and components provided through hardware, software, and services supply chain.

d) Monitor the agreement

   1) Assess the execution of the agreement;

      — establish and maintain verification procedures and criteria for delivered products and services,

      — audit suppliers' information systems where applicable,

      — monitor and evaluate the suppliers' processes (e.g. design, delivery practices) and work products where applicable.

   2) Provide data needed by the supplier and resolve issues in a timely manner;

      — report information security weakness and vulnerabilities detected in the use of hardware, software, or services provided through the supply chain.

   3) Evaluate suppliers for their ability to meet specified hardware, software, and services supply chain requirements.

e) Accept the product or service

   1) Confirm that the delivered product or service complies with the agreement;

      — there should be no activity specific to hardware, software, and services supply chain.

   2) Make payment or provide other agreed consideration to the supplier for the product or service rendered to close of the agreement;

      — there should be no activity specific to hardware, software, and services supply chain.

6.1.2 Supply process

The purpose of the supply process is to provide an acquirer with a product or service that meets agreed requirements (see ISO/IEC/IEEE 15288). Suppliers in the hardware, software, and services supply chain should include the following as a part of the supply process to ensure and demonstrate that they are appropriately managing hardware, software, and services supply chain risks:

a) Identify opportunities

   1) Determine the existence and identity of an acquirer who has, or who represents an organization or organizations having, a need for a product or service;

      — there should be no activity specific to hardware, software, and services supply chain.

b) Respond to a tender

   1) Evaluate a request for the supply of a product or service to determine feasibility and how to respond;

      — specify a set of baseline information security requirements that apply to all relationships with acquirers with tailoring as needed.

   2) Prepare a response that satisfies the solicitation;

      — establish a way to demonstrate ability to deliver products and services that respond to the acquirer's information security requirements including hardware, software, and services-related (i.e. telecommunications or IT) regulatory requirements, technical requirements, chain of custody, transparency and visibility (e.g. SBoM), sharing information on information security incidents throughout the supply chain, rules for component disposal or retention of elements such as components, data, or intellectual property, and other relevant requirements,

      — tailor the set of baseline information security requirements for specific relationships with acquirers as needed,

      — specify requirements for providing credible evidence for adherence to the acquirer's requirements.

c) Initiate an agreement

   1) Negotiate an agreement with the acquirer;

      — there should be no activity specific to hardware, software, and services supply chain.

   2) Commence the agreement with acquirer;

      — establish and maintain a plan for ensuring the integrity of included and delivered software and hardware products and components,

      — establish and maintain a plan for ensuring the protection of intellectual property rights such as those of data and information, designs, processes, environments, etc.

d) Execute the agreement

   1) It is expected that the agreement will be executed according to the supplier's established project plans;

      — there should be no activity specific to hardware, software, and services supply chain.

   2) Assess the execution of the agreement;

      — there should be no activity specific to hardware, software, and services supply chain.

e) Deliver and support the product or service

   1) Deliver the product or service in accordance with the agreement criteria;

      — there should be no activity specific to hardware, software, and services supply chain.

   2) Provide assistance to the acquirer in support of the delivered system or service in accordance with the agreement criteria;

      — respond to inquiries about status of ongoing security obligations (e.g. audits),

      — provide assistance with incident response queries.

3) Accept and acknowledge payment or other agreed consideration;

   — there should be no activity specific to hardware, software, and services supply chain.

f) Close the agreement

1) It is expected that the responsibility for the product or service is transferred to the acquirer, or other party, as directed by the agreement to obtain closure of the agreement;

   — there should be no activity specific to hardware, software, and services supply chain.

2) Ensure that agreed security measures are executed or maintained upon termination of the agreement.

6.2 Organizational project-enabling processes

6.2.1 Life cycle model management process

The purpose of the life cycle model management process is to define, maintain, and ensure availability of policies, life cycle processes, life cycle models, and procedures for use by the organization (see ISO/IEC/IEEE 15288). Hardware, software, and services supply chain security should be considered in this process, but there is no specific guidance in addition to what is provided in ISO/IEC/IEEE 15288 and ISO/IEC 27036-2.

6.2.2 Infrastructure management process

The purpose of the infrastructure management process is to provide the enabling infrastructure to hardware, software, and services supply chain to support acquirers and suppliers throughout the life cycle (see ISO/IEC/IEEE 15288).

Acquirers and suppliers should include the following, where appropriate, as a part of infrastructure management process to address information security risks in the hardware, software, and services supply chain:

a) establish and maintain visibility into their processes, environment, third party software components (e.g. SBoM) and relevant assets for manufacturing or operating the products or services;

b) establish and maintain visibility into their development, integration, and production environments including having an inventory of assets in the environment;

c) establish physical security processes and capability for hardware components, and media, including during delivery, removal and maintenance;

d) establish code repository security including hosting all code-related assets in secure source code repositories with controlled and audited access;

e) establish design/development environment security including automated build environments, with few owners and high traceability of actions on build scripts and access to code files during build, as well as the same protections for the build scripts as other code assets (including being checked into the code repository);

f) establish a malware and application security scanning program for both the code under development and for the environment, at least to the level described in ISO/IEC 27002;

g) implement code exchange processes that ensure integrity and authenticity using e.g. hashes or digital signatures;

h) for delivery of physical goods, implement tamper evident methods and packaging;

i) specify the ways for demonstrating the existence of robust software supply chain processes.

NOTE This process defines, provides and maintains the facilities, tools, and communications and information technology assets needed for the organization’s business with respect to the scope of this document (see ISO/IEC/IEEE 15288).

6.2.3 Project portfolio management process

The purpose of the project portfolio management process is to initiate and sustain necessary, sufficient and suitable projects in order to meet the strategic objectives of the organization (see ISO/IEC/IEEE 15288). Acquirers and suppliers should consider hardware, software, and services supply chain security in this process, and suppliers should start as early as can be feasible for the supplier during the product life cycle. Otherwise, there is no specific guidance in addition to what is provided in ISO/IEC/IEEE 15288 and ISO/IEC 27036-2.

6.2.4 Human resource management process

The purpose of the human resource management process is to ensure the organization is provided with necessary human resources and to maintain their competencies, consistent with strategic needs (see ISO/IEC/IEEE 15288). In addition to implementing the human resource management process in ISO/IEC/IEEE 15288 and people controls in ISO/IEC 27002, acquirers and suppliers should educate staff on specific hardware, software, and services supply chain concerns and how to address them. Specifically, acquirers and suppliers should do the following in consideration with requirements to be shared among the acquirer and suppliers in the hardware, software, and services supply chain:

a) establish organizational policy and general contractual requirements to address awareness and training on hardware, software, and services supply chain risk management;

b) define and require roles throughout the hardware, software, and services supply chain and system/element life cycle to limit opportunities and means available to individuals performing these roles that can result in adverse consequences;

c) develop a comprehensive awareness and training programme that promotes the organization’s hardware, software, and services supply chain security policy and procedures;

d) train quality assurance and information security personnel on hardware, software, and services supply chain threat and vulnerability assessment methodologies;

e) train receiving personnel (such as technical personnel, equipment specialists, and item managers) on correct processes for receipt of elements/services (including spare parts), including any known parts anomalies (which can indicate counterfeits, subversion, or quality issues);

f) train software developers on use of secure coding practices and its importance for addressing information security risks associated with hardware, software, and services supply chain risks and reducing the number of vulnerabilities in delivered code;

g) establish and enforce requirements for personnel security reviews and assessments. These reviews and assessments should include personnel who have exposure or access to elements, element processes, or business activities that allows an opportunity to apply technical knowledge or understanding of business processes to obtain unauthorized exposure of, or access to, elements or processes that can result in compromise or loss;

h) define processes by which general hardware, software, and services supply chain information is collected, lessons learned extracted, and shared between the acquirer's and supplier's personnel as scoped within the contract;

i) implement identity management, access controls, and process monitoring to permit timely detection and classification of anomalous behaviours or personnel that can result in adverse consequences for both physical and logical access in hardware, software, and services supply chain;

j) establish and enforce requirements for the assignment of unique identities to all individuals (e.g. logon account, user ID) including requirements under what circumstances such items can be reused (e.g. employee termination, name change);

k) establish screening requirements for relevant personnel.

6.2.5 Quality management process

The purpose of the quality management process is to ensure that products, services and implementations of life cycle processes of a hardware, software, and services supply chain meet organization quality objectives and achieve customer satisfaction (see ISO/IEC/IEEE 15288).

Acquirers and suppliers should include the following as a part of the quality management process to address information security risks in hardware, software, and services supply chain:

a) active vulnerability management programme at a minimum comparable to what is described in ISO/IEC 27002;

NOTE 1 General vulnerability management activities are addressed under 6.3.4.

b) integration of testing for weaknesses and vulnerabilities into quality management activities throughout the system development life cycle including design and architecture reviews, documentation reviews, and a variety of testing that software and hardware undergo before delivery and installation and whenever upgrades take place;

c) specific guidelines and timelines for addressing identified critical security vulnerabilities.

NOTE 2 Integration of testing for reliability and resilience into quality management activities can be considered, if appropriate.

6.2.6 Knowledge management process

The purpose of the knowledge management process is to create the capability and assets that enable the organization to exploit opportunities to re-apply existing knowledge (see ISO/IEC/IEEE 15288). Acquirers and suppliers should consider hardware, software, and services supply chain security in this process but there is no specific guidance in addition to what is provided in ISO/IEC/IEEE 15288 and ISO/IEC 27036-2.

6.3 Technical management processes

6.3.1 Project planning process

The purpose of the project planning process is to produce and coordinate effective and workable plans (see ISO/IEC/IEEE 15288). For projects involving hardware, software, and services created and delivered across geographically dispersed supply chains controlled by multiple entities, it is recommended that acquirers and suppliers consider and integrate the following aspects into the project plans during the project planning process:

a) how the need for securing acquirer and supplier information impacts project plans and schedules;

b) any aspects of hardware, software, and services supply chain information security risk management that should be integrated in project roles, responsibilities, accountabilities, and authorities;

c) different legal requirements of multiple jurisdictions relevant to the hardware, software, and services supply chain;

d) resources for ensuring protection of acquirer and supplier information across hardware, software, and services supply chain(s) including staffing requirements;

e) integration into continuous integration (CI)/continuous deployment (CD) pipeline, code repositories, security automation for the product or development environment, including associated costs;

f) applicable project roles, responsibilities, accountabilities, and authorities.

6.3.2 Project assessment and control process

The purpose of the project assessment and control process is to assess if the plans are aligned and feasible; determine the status of the project's technical and process performance; and direct execution to help ensure that the performance is according to plans and schedules, within projected budgets, to satisfy project objectives (see ISO/IEC/IEEE 15288). In addition to implementing the project assessment and control process in ISO/IEC/IEEE 15288 and ISO/IEC 27036-2, acquirers should implement the following:

a) Periodically perform compliance audits of supplier products or services to determine if suppliers are continuing to be compliant with the acquirer's requirements. Document results of these audits in compliance reports. Periodicity of compliance audits should be determined based on the identified hardware, software, and services supply chain security risk and risk tolerance of the acquirer.

6.3.3 Decision management process

The purpose of the decision management process is to provide a structured, analytical framework for objectively identifying, characterizing and evaluating a set of alternatives for a decision at any point in the life cycle and select the most beneficial course of action (see ISO/IEC/IEEE 15288). Acquirers and suppliers should consider hardware, software, and services supply chain security in this process but there is no specific guidance in addition to what is provided in ISO/IEC/IEEE 15288 and ISO/IEC 27036-2.

6.3.4 Risk management process

The purpose of the risk management process is to identify, analyse, treat and monitor the risks continually (see ISO/IEC/IEEE 15288). In addition to implementing the risk management process in ISO/IEC/IEEE 15288, ISO/IEC 27036-2 and information security risk management approach described in ISO/IEC 27005, acquirers and suppliers should implement the following to address information security risks in hardware, software, and services supply chain including:

a) identify threats, vulnerabilities, and consequences related to hardware, software, and services;

b) identify and document hardware, software, and services supply chain risks associated with the identified threats and vulnerabilities;

c) identify legal requirements of multiple jurisdictions relevant to the hardware, software, and services supply chain;

d) define and select strategy for management of hardware, software, and services supply chain risks due to unintentional and intentional weaknesses and vulnerabilities;

e) demarcate responsibilities in mitigating hardware, software, and services supply chain risks among acquirers and suppliers;

f) establish risk communication processes among acquirers and suppliers;

g) identify effectiveness of past corrective actions by suppliers throughout the supply chain in other products or services and apply to future activities;

h) establish a process by which SBoM can be used to identify and inform the system owner of remediation options associated with weaknesses and vulnerabilities;

i) determine root causes of weaknesses and vulnerabilities that are identified during development, delivery, and operations. Implement countermeasures and mitigations, as appropriate;

j) monitor hardware, software, and services supply chain for potential concerns, identify and analyse resulting information security risks, and update risk assessment and risk treatment strategies accordingly;

k) manage risks associated with use of open-source modules by:

   1) performing a security evaluation of each open-source module before it is incorporated into solution,

   2) where specialist methods such as cryptography are employed in the module, ensuring that the implementation of such mechanisms is reviewed by a subject matter expert,

   3) ensuring that the risks in using such modules are carefully monitored by the acquirer's ISMS, including regular checking of published vulnerability lists and industry advisories pertinent to those modules.

6.3.5 Configuration management process

The purpose of configuration management (CM) is to manage system and system elements and configurations over their life cycle. CM also manages consistency between a product and its associated configuration definition (see ISO/IEC/IEEE 15288). CM is critical for understanding what changes are made to products, systems, product and system elements, relevant documentation, and supply chain itself, including who makes these changes. To ensure that hardware, software, and services supply chain concerns are appropriately addressed, acquirers and suppliers should include the following, where appropriate, as a part of the CM process to address specific information security risks in hardware, software, and services supply chain:

a) control access and changes to all hardware and hardware elements throughout the life cycle, including design, manufacturing, testing, operations, maintenance, and disposal;

b) control access and changes to documentation associated with hardware, software, and services;

c) approve and manage changes to delivery methods, both logical and physical;

d) approve and manage changes to systems and software, including source code, database structures and values;

e) house all relevant assets in source code repositories to enable additional attention to information security and to access control;

f) house the servers that host the source code repositories securely, configure them to be secure by default (e.g. with least necessary privileges, disabled services that are not widely needed), and appropriately protect these servers to the sensitivity of housed code;

g) define and use secure baseline configurations as a starting point for supply chain components including containers, build servers, code repositories and other infrastructure or cloud components;

h) control access to source code repositories through the use of corporate identity systems with strict control maintained over access to any system account; segregation of duties principle should be observed, and elevated access only granted when necessary;

i) manage access privileges to the repositories, including access to branches, work areas or code sets; and only grant access privileges based on least privilege and need-to-know;

j) preserve changes to the code repository, including review and approval for future analysis;

k) record file names, account name of a person checking in the file, check-in time stamp, and the line that was changed in the change logs;

l) maintain and manage a manifest of all code assets contributing to a product, including those developed in house and by suppliers;

m) establish and preserve chain of custody for each element through code signing, time stamping, and other appropriate techniques.

ISO/IEC 27002 provides additional specific guidance regarding setting expectations during the Configuration management process.

6.3.6 Information management process

The purpose of the information management process is to generate, obtain, confirm, transform, retain, retrieve, disseminate and dispose of information, for designated stakeholders during and, as appropriate, after the life cycle of hardware, software, and services supply chain (see ISO/IEC/IEEE 15288).

In addition to implementing the information management process described in ISO/IEC/IEEE 15288, a number of controls outlined in ISO/IEC 27002 provide additional guidance.

6.3.7 Measurement process

The purpose of the measurement process is to collect, analyse, and report objective data and information to support effective management and demonstrate the quality of the products, services, and processes (see ISO/IEC/IEEE 15288). There are no hardware, software, and services supply chain security aspects to the measurement process. ISO/IEC 27004 provides guidance on information security measurement that can be applied to develop and implement specific measures to address information security risks in hardware, software, and services supply chain.

6.3.8 Quality assurance process

The purpose of the quality assurance process is to help ensure the effective application of the organization's quality management process to the acquired and supplied hardware, software, and services (see ISO/IEC/IEEE 15288). Acquirers and suppliers should include the following as a part of the quality assurance process to address information security risks in hardware, software, and services supply chain:

a) compare requirements in the agreement against delivered products and services;

b) assess the effectiveness of controls to confirm they are operating effectively, e.g. supporting processes are being followed by personnel;

c) conduct assurance reviews regularly.

6.4 Technical processes

6.4.1 Business or mission analysis process

The purpose of the business or mission analysis process is to define the business or mission problem or opportunity, characterize the solution space, and determine potential solution class(es) that can address a problem or take advantage of an opportunity (see ISO/IEC/IEEE 15288). Business or mission analysis process also ensures that applicable business and mission-related information security considerations are addressed by the hardware, software, or service. Acquirers and suppliers should consider hardware, software, and services supply chain security in this process but there is no specific guidance in addition to what is provided in ISO/IEC/IEEE 15288 and ISO/IEC 27036-2.

6.4.2 Stakeholder needs and requirements definition process

The purpose of the stakeholder needs and requirements definition process in the context of hardware, software, and services supply chain is to define the requirements for a hardware, software, or service that can provide the capabilities needed by users and other stakeholders in a defined environment while appropriately managing acquirer's hardware, software, and services supply chain-related information security risk (see ISO/IEC/IEEE 15288). Acquirers and suppliers should include the following as a part of stakeholder requirements definition process to address specific hardware, software, and services supply chain-related risks:

a) define and document information protection requirements based on acquirer needs, compliance requirements, and available risk assessment and risk treatment information and documentation;

b) clarify risks and threats to missions and incorporate this knowledge in defining supplier security-related requirements;

c) define and document data and information integrity requirements for suppliers, including code integrity and SBoM;

d) define and document system integrity requirements for hardware, software, and services products and services suppliers;

e) define and document information and system availability requirements for hardware, software, and services suppliers;

f) define and document information confidentiality requirements for hardware, software, and services suppliers;

g) define and document information security aspects of hardware, software, and service delivery requirements including functional (e.g. role-based access control, logging) and non-functional security requirements;

h) define and document consequences of violations of information security requirements for hardware, software, and service delivery.

ISO/IEC 27002 provides additional specific guidance regarding setting expectations during the stakeholder requirements definition process.

6.4.3 System requirements definition process

The purpose of the system requirements definition process in the context of hardware, software, and services supply chain is to transform the stakeholder, user-oriented view of desired capabilities into a technical view of a solution that meets operational needs of the user while appropriately managing acquirer’s hardware, software, and services supply chain-related information security risk (see ISO/IEC/IEEE 15288). Acquirers and suppliers should include the following as a part of the system requirements definition process to address specific information security risks in the hardware, software, and services supply chain:

a) ensure that elements are assigned varying degrees of criticality depending on the purpose and use of each element;

b) incorporate hardware, software, and services supply chain risk considerations and assessments into all management, operational and technical requirements and business processes to protect elements, processes, requirements, and business practices against compromise of confidentiality, integrity and availability;

c) incorporate defensive design criteria in all technical requirements to result in design options for elements, systems, and processes that protect mission capabilities, system performance, or element confidentiality, integrity, and availability;

d) protect requirements and supporting documentation from exposure or access that can result in the loss of the confidentiality, integrity or availability of the elements and systems through a hardware, software, and services supply chain-related compromise;

e) monitor and reassess evolving technical requirements and adjust, following approved change management procedures, requirements for protection of critical elements and processes throughout the element’s life cycle;

f) identify operational concepts and associated scenarios for misuse and abuse cases.

ISO/IEC 27002 provides additional specific guidance that can be used during the system requirements definition process.

6.4.4 System architecture definition process

The purpose of the system architecture definition process in the context of hardware, software, and services supply chain is to generate system architecture alternatives, to select one or more alternative(s) that frame stakeholder concerns and meet system requirements, and to express this in a consistent set of views, while appropriately managing acquirer's hardware, software, and services supply chain-related information security risk (see ISO/IEC/IEEE 15288). Acquirers and suppliers should include the following as a part of architecture design process to address specific information security risks in hardware, software, and services supply chain:

a) use defensive design techniques to anticipate maximum possible ways the hardware, software, or service can be misused and abused or to protect the product or system from such uses; ensure architecture and design address intended and unintended use scenarios; choose and implement designs based on the acquirer's stated risk tolerance and document for management sign-off acceptance of risks that are not fully mitigated;

b) limit the number, size, and privileges of critical elements;

c) reduce complexity of design, production processes, and design implementation. Complexity has multiple negative effects, including introducing effort or the possibility of effort which in turn can cause confidentiality, integrity or availability issues; cascading failures due to tight coupling of elements; and impediments to root cause analysis of faults and incidents;

d) use security mechanisms or controls to reduce opportunities to exploit hardware, software, and services supply chain vulnerabilities. Examples include encryption, access control, identity management, and detection measures such as those for discovering malware or tampering;

e) isolate elements (using techniques such as virtual machines, quarantines, jails, sandboxes, and one-way gateways) to reduce the damage one element can do to another;

f) design countermeasures and mitigations against potential exploitations of weaknesses and vulnerabilities in hardware, software, and services; design elements including programming techniques or configurations;

g) identify unique software components and their origins to ensure SBoM can be created that documents all components;

h) include the ability to configure increased system or system element isolation, even if this reduces system capability (e.g. counter attacks until a patch is available);

i) design elements to withstand out-of-bounds inputs (e.g. excessive voltages, numbers out of range, and so on);

j) design elements so they are hard to disable and, if disabled, trigger notification methods such as audit trails, tamper evidence or alarms, and so on;

k) design delivery mechanisms to avoid exposure or access to the system and element delivery processes and use of the element during the delivery process;

l) include fail-over/redundant or alternative systems or system elements where appropriate; ensure that the fail-over and redundant mechanisms are not subject to common mode failures;

m) define and/or use standards-based technical interfaces and process requirements to provide options for the modification of processes or modification/replacement of elements should a supply chain compromise occur;

n) design relevant validation controls to be used during implementation and operation;

o) design mechanisms for tracing and tracking supply chain events and incidents. These should be access controlled and tamper-resistant;

p) use certified products (where available) e.g. common criteria (CC) evaluated products which provide a level of assurance (when implemented as per the terms of evaluation);

q) follow recognized architecture principles e.g. the Open Group Architecture Framework (TOGAF) making sure the environment is documented and follows set rules;

r) separate development and production environments to minimize incidents from occurring e.g. transfer of vulnerabilities, inadvertent information disclosure.

6.4.5 Design definition process

The purpose of the design definition process is to provide sufficient detailed data and information about the system and its elements to realize the solution in accordance with the system requirements and architecture (see ISO/IEC/IEEE 15288). Design definition process is critical to ensuring that the resulting system is designed securely, including the strategy and plan for assuring security throughout the system's life cycle. To ensure that hardware, software, and services supply chain concerns are appropriately addressed, acquirers and suppliers should do the following, when appropriate, as a part of design definition process to address specific information security risks in hardware, software, and services supply chain:

a) determine security technologies required for each element composing the system;

b) determine the necessary security considerations for the design such as least privilege, least functionality, restricted access to systems or services, and defence-in-depth;

c) identify how security considerations will be addressed through the evolution of the design throughout the system life cycle to include planning for obsolescence of system elements and technologies and their replacement during the life cycle;

d) ensure that security considerations are integrated throughout design definition activities;

e) identify dependent software components through an SBoM.

6.4.6 System analysis process

The purpose of the systems analysis process is to provide a rigorous basis of data and information for technical understanding to aid decision-making across the life cycle (see ISO/IEC/IEEE 15288). Acquirers and suppliers should consider hardware, software, and services supply chain security in this process but there is no specific guidance in addition to what is provided in ISO/IEC/IEEE 15288 and ISO/IEC 27036-2.

6.4.7 Implementation process

The purpose of the implementation process is to realize a specified system element (see ISO/IEC/IEEE 15288). Suppliers should include the following as a part of implementation process to address information security risks in hardware, software, and services supply chain:

a) implement architecture and design that address hardware, software, and services supply chain-related requirements for products and services;

b) identify deviations from hardware, software, and services supply chain-related requirements implement appropriate mitigations and document this information;

c) when possible and appropriate, implement hardware and software design using programming languages that avoid inherently insecure coding constructs to reduce the likelihood of weaknesses and hardware, software, and services supply chain-related compromise;

d) identify and implement interface standards wherever practical to promote system and element sustainability and element reusability;

e) validate the implementation at appropriate and defined stages using the designed validation tests such as:

   1) use a variety of testing techniques including fuzz testing, static analysis testing, and dynamic testing to identify and address software weaknesses and vulnerabilities,

   2) use positive and appropriate negative tests to verify that the system or element operates in accordance with requirements and without extra functionality,

   3) monitor for unexpected or undesirable behaviour during test, such as network behaviour (e.g. a surprise “call home” or opening of network port), file system behaviour (e.g. reading or writing information to unexpected files/directories), race conditions, and deadlocks;

f) protect access to test cases and results. Store test cases and results in a source control system and protect similarly to how source code and build scripts are protected;

g) ensure availability of required elements and continued supply in the event of compromise to the system/element through diversity of supply (especially on commodity functions or in the event of compromise to or disruption of delivery mechanisms);

h) ensure the removal or disabling of any unnecessary functions, prevalent in commercial-off-the-shelf product implementations which are designed to support multiple applications or purposes. If left active, these functions can permit unauthorized access or exposure of the system or perform a function that reduces the availability of other functions;

i) change any default credentials such as usernames and passwords to minimize their vulnerability of exploitation;

j) document the system build to provide a record of the configuration that is able to be reviewed and confirmed;

k) document products and/or elements specific for the implementation according to the agreement.

ISO/IEC 27002 provides additional specific guidance regarding setting expectations during the Implementation process.

6.4.8 Integration process

The purpose of the integration process is to synthesize a set of system elements into a realized system (product or service) that satisfies the system requirements (see ISO/IEC/IEEE 15288).

Acquirers and suppliers should include the following as part of integration process to address information security risks in hardware, software, and services supply chain:

a) integration with existing systems should include activities listed in 6.4.4 depending on the characteristics of the integration;

b) documentation should be made on how the activities listed in 6.4.4 are applied during integration and the integrated existing systems that were in place prior to the implementation.

6.4.9 Verification process

The purpose of the verification process is to provide objective evidence that the system or system element fulfils its specified requirements and characteristics (see ISO/IEC/IEEE 15288).

This should include verifying the pre-acquisition information shared between the supplier and acquirer and developing verification requirements based on 6.2, 6.3 and 6.4.

Suppliers should include the following as a part of the verification process to address specific information security risks in hardware, software, and services supply chain:

a) verify and validate that hardware, software, and services supply chain security requirements have been addressed;

b) verify that supplier support activities align with the acquirer's information and product security objectives;

c) verify that sufficient supplier-required security practices are in place, and personnel are trained to implement them;

d) verify that the supplier's security features and functionality documentation links product features to architecture, design, requirements, code, tests, and test results;

e) verify the supplier's claims about their software supply chain security processes;

f) verify that the supplier implements verification and validation activities to ensure controls are in place, working as intended and that they meet the acquirer's requirements;

g) verify that chain of custody is maintained between organizations;

h) conduct code assessment and verification using a variety of tools and techniques such as peer reviews, manual code inspections, static code analysis, dynamic code analysis, binary code analysis, code coverage tools;

i) conduct network, container, and web application vulnerability scanning;

j) conduct malware scanning;

k) run compliance validation tools;

l) conduct stress testing;

m) examine attestations or certifications provided by suppliers:

   1) regarding the suppliers’ claims of conformance to security or business procedures, product integrity, or chain of custody;

   2) awarded to the product to assess the impact of the claims toward acquirer risk, or product fitness to a particular purpose relative to the acquirers intended use.

ISO/IEC 27002 provides additional specific guidance regarding setting expectations during the verification process.

6.4.10 Transition process

The purpose of the transition process is to establish a capability for a system to provide services specified by stakeholder requirements in the operational environment (see ISO/IEC/IEEE 15288).

Acquirers should include the following as a part of the transition process to address specific information security risks in hardware, software, and services supply chain:

a) include, in inventory management policies and processes, how to request replacements, appropriate stocking (including spare locations and protection of spares), receipt policies (knowing to whom the inventory should go, when it arrives, who handled it, where it is located, and if the received inventory is reconciled with what was ordered), and inventory counting/accounting policies.

b) incorporate products and elements into the organization’s inventory management system;

c) design mechanisms to reduce the risks of unauthorized access to the products or services during the delivery process;

d) implement delivery processes for the intended logical and physical transfer and receipt of elements to be done by authorized personnel;

e) establish non-destructive techniques or mechanisms to determine if there is any unauthorized access throughout the delivery process;

f) stipulate acceptable levels of information security and quality for monitoring logical delivery of products and services, requiring downloading from approved, verification-enhanced sites. Consider requiring encryption of elements (software, software patches, etc.) in transit and at rest throughout delivery;

g) establish a process and capability for protecting software products from malware;

h) establish a process and capability for verifying marks such as digital signatures and hologram tags for critical elements;

Suppliers should include the following as a part of the transition process to address specific information security risks in hardware, software, and services supply chain:

i) establish a process and capability for protecting software products from malware;

j) consider encrypting elements (software, software patches, etc.) in transit and at rest throughout delivery;

k) document and provide to the acquirer SBoM for all software components;

l) to reduce risks of counterfeiting and to allow verification by acquirers, use techniques such as difficult-to-forge marks (such as digital signatures and hologram tags) for critical elements, digital markings that include software vendor’s identity, or hash functions;

m) deploy specific delivery processes for both online and offline software delivery. Provide information on code signing and hash functions to the acquirer;

n) establish the products delivery process in such a way that the acquirer can confirm that the product is coming from the specific supplier;

o) establish anti-tamper mechanisms for prevention and discovery, including tamper-resistant and tamper-evident packaging (e.g. tamper tape or seals). These should not be easy to remove and replace without leaving evidence of such activity.

ISO/IEC 27002 provides additional specific guidance regarding setting expectations during the transition process.

6.4.11 Validation process

The purpose of the validation process in the context of hardware, software, and services supply chain is to provide objective evidence that the system, when in use, fulfils its business or mission objectives and stakeholders’ requirements, achieving its intended use in its intended operational environment (see ISO/IEC/IEEE 15288).

This should include determining whether the product received is genuine, and unaltered based on the supplier’s product description or requirements, and agreement between the acquirer and supplier to provide the acquirer confidence that the product is unaltered. It should also include development of tests that provide validation throughout the acquirer’s use of the product. Specifically, acquirers should include the following as a part of the validation process to address specific information security risks in hardware, software, and services supply chain:

a) verify and validate that hardware, software, and services supply chain security requirements have been addressed;

b) develop processes to use, where appropriate, practices to institute original equipment manufacturer (OEM) product and software validation tools that are non-invasive and can detect counterfeits or product intrusions;

c) conduct tests upon receipt, and during the acquirer’s system development and operations phases. Attempt to detect counterfeit or product intrusions including:

   1) conduct hardware and software inspections for genuine components using guidance and tools provided by the supplier, third parties, or the acquirer (e.g. manual code inspections),

   2) conduct anti-malware inspections,

   3) conduct vulnerability scans;

d) use product documentation and acquirer plans to identify and test critical components;

e) conduct code assessment and verification using a variety of tools and techniques such as static code analysis, dynamic code analysis, binary code analysis, code coverage tools;

f) conduct stress testing;

g) execute tools to gather evidence of changes resulting from remote maintenance activities.

6.4.12 Operation process

The purpose of the operation process is to use the system to provide its products or services (see ISO/IEC/IEEE 15288).

Acquirers and suppliers should include the following as a part of operation process to address specific hardware, software, and services supply chain-risks:

a) include applicable system integration and custom code extension activities as part of the upgrade and maintenance efforts in system operational requirements;

b) perform all applicable information security activities and implement applicable information security requirements in operations.

Suppliers should include the following as a part of operation process to address specific hardware, software, and services supply chain-risks:

c) ship elements “secured by default” at a level appropriate to acquirer’s requirements.

ISO/IEC 27002 provides additional specific guidance regarding setting expectations during the Operation process.

6.4.13 Maintenance process

The purpose of the maintenance process in the context of hardware, software, and services supply chain is to sustain the capability of the system and its hardware, software, and services components to provide a product or service while appropriately managing acquirer’s hardware, software, and services supply chain-related information security risk (see ISO/IEC/IEEE 15288). Acquirers and suppliers should include the following as a part of maintenance process to address specific information security risks in hardware, software, and services supply chain:

a) use procurement clauses to reduce hardware, software, and services supply chain risk in formal service and maintenance agreements with suppliers;

b) when acquiring OEM elements, including refurbished elements, establish a contractual relationship with the original manufacturer or originator that provides vetted, competent support where possible;

c) consider advance purchase and inventory of spare parts while they are widely available and verifiable, and can be installed by trained and knowledgeable authorized service personnel;

d) consider the risks that trained and knowledgeable authorized service personnel are not available, especially late in the element's life;

e) consider hardware, software, and services supply chain risks when acquiring replacement components or field additions/modifications/upgrades, particularly if they do not go through traditional acquisition processes that examine supply chain risks;

f) prefer formalized service/maintenance agreement(s) where possible e.g. use specified or qualified spare parts suppliers, provide a complete record of changes performed during maintenance (e.g. audit trail or change log), review changes made during maintenance;

g) establish and implement agreements for competent and suitable support including refurbished and/or salvaged elements; consider requiring the original manufacturer to certify the equipment as suitable;

h) identify methods of verifying that service personnel are authenticated and authorized to perform the service work needed at the time, as well as visitor management protocols for and monitoring of service personnel when undertaking maintenance on-site (e.g. visitor escorts);

i) develop and implement an approach for handling and processing reported hardware, software, and services supply chain anomalies while in operation; establish a method for submitting a service request and securely sharing log and error information with suppliers;

j) monitor the supplier's business health, including whether they are a candidate for merger and acquisition or in financial difficulties;

k) implement and enforce policies on software updates and patch management;

l) establish an adequate supply of trusted spare and maintenance parts for well beyond the life span of the element;

m) preserve documentation for any in-service element that is no longer supported by the supplier;

n) establish processes for purchasing of faulty elements that cannot be securely erased that would otherwise go back to the supplier (e.g. a faulty hard drive) to securely physically destroy.

ISO/IEC 27002 provides additional specific guidance regarding setting expectations during the Maintenance process.

6.4.14 Disposal process

The purpose of the disposal process in the hardware, software, and services supply chain is to end the existence of hardware, software, and services supply chain elements for a specified intended use, appropriately handle replaced or retired elements, and to properly attend to identified critical disposal needs (e.g. per an agreement, organizational policy, or environmental, legal, safety, security aspects). See ISO/IEC/IEEE 15288 for further information.

Disposal can happen at any point in the system or element life cycle and includes both electronic and non-electronic media. Acquirers and suppliers should include the following as a part of the disposal process to address information security risks in hardware, software, and services supply chain, specifically the risk of counterfeit products contaminating the supply chain:

a) preserve a chain of custody for elements to be disposed to reduce risks of compromise, for example, of personally identifiable data or intellectual property;

b) encourage the selection of elements that can be disposed of in a way that does not expose protected information, for example, elements that permit offloading of data prior to disposal or elements that are easy to wipe clean prior to disposal;

c) prohibit transmission or distribution of acquirer’s sensitive data or sensitive elements to unauthorized or unspecified parties during disposal activities;

d) when required for forensic investigation or for later comparison for detection of counterfeits, store elements for disposal to a dedicated repository and maintain the chain of custody;

e) implement procedures for the secure and permanent destruction of elements, such as using certified destruction providers and receiving a certificate of destruction after the acquirer’s information has been securely disposed;

f) engage trustworthy, trained disposal service personnel and set expectations for the procedures that conform to the disposal policy; verify through assessments that the procedures are being followed.

ISO/IEC 27002 provides additional specific guidance regarding setting expectations during the disposal process.

Annex A
(informative)

Correspondence between the controls in ISO/IEC 27002 and this document

Table A.1 shows the correspondence between the controls contained in ISO/IEC 27002 and this document.

Table A.1 — Correspondence between controls in ISO/IEC 27002 and this document

ISO/IEC 27002:2022 subclause number	ISO/IEC 27002:2022 controls	Subclause number from this document	ISO/IEC 27036-2 subclause heading
5.1	Policies for information security	6.1	Agreement processes
5.2	Information security roles and responsibilities	6.1	Agreement processes
5.21	Managing information security in the ICT supply chain	6.1	Agreement processes
5.36	Compliance with policies and standards for information security	6.1	Agreement processes
5.22	Monitoring, review and change management of supplier services	6.1	Agreement processes
5.21	Managing information security in the ICT supply chain	6.1.1	Acquisition process
5.21	Managing information security in the ICT supply chain	6.1.2	Supply process
5.8	Information security in project management	6.2	Organizational project-enabling processes
5.8	Information security in project management	6.2.1	Life cycle model management process
5.9	Inventory of information and other associated assets	6.2.2	Infrastructure management process
5.15	Access control	6.2.2	Infrastructure management process
8.24	Use of cryptography	6.2.2	Infrastructure management process
7.4	Physical security monitoring	6.2.2	Infrastructure management process
8.6	Capacity management	6.2.2	Infrastructure management process
8.21	Security of network services	6.2.2	Infrastructure management process
8.9	Configuration management	6.2.2	Infrastructure management process
5.24	Information security incident management planning and preparation	6.2.2	Infrastructure management process
5.29	Information security during disruption	6.2.2	Infrastructure management process
5.8	Information security in project management	6.2.3	Portfolio management process
6.1	Screening	6.2.4	Human resource management process
8.27	Secure system architecture and engineering principles	6.2.5	Quality management process

Table A.1 *(continued)*

ISO/IEC 27002:2022 subclause number	ISO/IEC 27002:2022 controls	Subclause number from this document	ISO/IEC 27036-2 subclause heading
8.25	Secure development life cycle	6.2.5	Quality management process
5.6	Contact with special interest groups	6.2.6	Knowledge management process
6.3	Information security awareness, education, and training	6.2.6	Knowledge management process
6.6	Confidentiality or non-disclosure agreements	6.2.6	Knowledge management process
5.8	Information security in project management	6.3	Technical management processes
5.8	Information security in project management	6.3.1	Project planning process
5.8	Information security in project management	6.3.2	Project assessment and control process
5.8	Information security in project management	6.3.3	Decision management process
N/A	Not addressed in ISO/IEC 27002. See ISO/IEC 27005	6.3.4	Risk management process
8.32	Change management	6.3.5	Configuration management process
8.9	Configuration management	6.3.5	Configuration management process
5.12	Classification of information	6.3.6	Information management process
5.15	Access control	6.3.6	Information management process
8.24	Use of cryptography	6.3.6	Information management process
8.13	Information backup	6.3.6	Information management process
5.14	Information transfer	6.3.6	Information management process
6.6	Confidentiality and non-disclosure agreements	6.3.6	Information management process
N/A	ISO/IEC 27004	6.3.7	Measurement process
8.25	Secure development life cycle	6.3.8	Quality assurance process
8	Technological controls	6.4	Technical processes
5.1	Policies for information security	6.4.1	Business or mission analysis process
5.4	Management responsibilities	6.4.1	Business or mission analysis process
5.12	Classification of information	6.4.1	Business or mission analysis process
8.26	Application security requirements	6.4.2	Stakeholder needs and requirements definition process
8.26	Application security requirements	6.4.3	System requirements definition process
8.25	Secure development life cycle	6.4.4	Architectural design process
8.27	Secure system architecture and engineering principles	6.4.4	Architectural design process
8.27	Secure system architecture and engineering principles	6.4.5	Design definition process
8.27	Secure system architecture and engineering principles	6.4.6	System analysis process
8.28	Secure coding	6.4.7	Implementation process
8.31	Separation of development, test and production environments	6.4.7	Implementation process

Table A.1 *(continued)*

ISO/IEC 27002:2022 subclause number	ISO/IEC 27002:2022 controls	Subclause number from this document	ISO/IEC 27036-2 subclause heading
8.29	Security testing in development and acceptance	6.4.8	Integration process
8.29	Security testing in development and acceptance	6.4.9	Verification process
8.33	Test information	6.4.9	Verification process
8.29	Security testing in development and acceptance	6.4.10	Transition process
8.29	Security testing in development and acceptance	6.4.11	Validation process
8.33	Test information	6.4.9	Verification process
5	Organizational controls	6.4.12	Operation process
6	People controls	6.4.12	Operation process
7	Physical controls	6.4.12	Operation process
8	Technological controls	6.4.12	Operation process
7.10	Storage media	6.4.13	Maintenance process
7.13	Equipment maintenance	6.4.13	Maintenance process
7.14	Secure disposal or re-use of equipment	6.4.14	Disposal process

Annex B
(informative)

Essential elements of a software bill of materials

B.1 General

B.1.1 Overview

5.8 recommends and enumerates activities that ensure an up-to-date inventory of assets used within the supply of the product or service. Inventory can be further refined to include parts or components of software and software systems. This level of inventory detail can help organizations manage risk and compliance requirements in areas such as intellectual property and licence management (ISO/IEC 27002:2022, 5.32) and technical vulnerabilities (ISO/IEC 27002:2022, 8.8) among others. This annex describes elements that support the creation, maintenance, and exchange of software component inventories. These inventories are sometimes referred to as software bill of materials (SBoM) or software component inventory (SCI). Throughout this annex, these concepts are referred to as SBoM. An organization producing or requesting SBoM should consult this annex to help determine the quality of information contained with a provided or published SBoM.

The SBoM concept was developed to provide consumers with information on specific software components in their products to enable consumers ability to identify and manage vulnerabilities. This concept was developed for off-the-shelf and on-premise products, not managed services. An on-premise download and its associated download SBoM is immutable, allowing unambiguous and consistent component relationships over time. Such SBoMs do not fit the model of managed services involving multiple servers managed by multiple suppliers with software that is frequently updated. This is as a result of the fact that two identical transactions entered a minute apart can be processed by two different sets of components on possibly different servers, whose contents can be updated independently of each other in time. Given that, the managed services analogue of the on-premise SBoM should accommodate a continuously evolving component list associated with each supported transaction. Thus, for managed services, a transactional model rather than a product model is needed.

The SBoM is not itself a risk management tool or activity. The SBoM is intended to be a highly scalable mechanism to produce and maintain accurate software component inventories. These inventories then support a number of risk management and risk assurance activities.

In order to scale, SBoM data and processes should be machine readable and processable. Several well-defined and established SBoM document and data formats exist.

SBoM and software component inventory are in active use, however this use varies widely across software ecosystems and different types of products and services. Broadly speaking, SBoM is under active development and this annex is intended to provide basic and introductory information about SBoM to suppliers and SBoM consumers.

B.1.2 Audience

This annex is primarily intended for use by software suppliers and SBoM authors. A software supplier is an entity that creates, wholly or in part, modifies, or distributes software for the purpose of its intent to be used by other parties.

Consumers of SBoM information include end users, customers, auditors, regulators, policy makers, and suppliers. Many software suppliers are users or consumers of upstream software components.

There are differences between on-premises, product-oriented software components and cloud services. The accurate inventory and supply chain knowledge are important to both models, but the rapid development of cloud solutions can necessitate variances in the information and processes required for each individual model.

B.2 Essential SBoM elements

B.2.1 Overview

The following elements are necessary to convey SBoM information. SBoM elements are broken into three core areas: metadata, identifiers, and association.

Metadata elements provide information about the SBoM itself and should not be used as identifiers of the SBoM subject or components. Minimum metadata elements include Author, Timestamp, and Life cycle.

Identifier elements provide information concerning the SBoM subject and its components. It is possible that singular identifying elements are not sufficient to uniquely identify a given component and should be used in conjunction with additional identifiers to accurately describe and identify the component. Organizations can use identifiers as a value for determining policy-as-code conformance and vulnerability discovery, however this is out of the scope of this annex. Identifier elements include Supplier, Component, Version, Hash, and UID.

Association elements provide information about a given component in relation to the subject or other components where known. It is possible that association elements will not reveal the construct of a given software subject and are discouraged from use as a means of reverse engineering as this can result in licensing or contract violations. Association elements include Relationship and Source.

B.2.2 Author

The author is the entity who creates the SBoM. The author is often, but not necessarily, the supplier of the primary component or subject of the SBoM. For example, if an organization uses binary software composition analysis to develop an SBoM, that organization is the author of the SBoM, but not the supplier of the analysed component.

B.2.3 Timestamp

The timestamp is the date and time the SBoM was last modified. Timestamps should be represented according to the ISO 8601 series.

B.2.4 Life cycle

The life cycle phases assume the following definition of a build: the conversion of files and other assets into a final or consumable software product or service. A build can include compiling source code files, testing, packaging compiled files into compressed formats, and making components available to users.

The life cycle phases are:

— pre-build: the SBoM was produced prior to the build of the software;

— build: the SBoM is a byproduct and artefact of the build or continuous integration (CI) process;

— post-build: the SBoM was produced after the software was built, possibly through reverse engineering or black-box analysis.

B.2.5 Supplier name

The supplier is the entity who provides (e.g. owns, produces, or maintains) the primary component or subject of an SBoM. The supplier is often, but not necessarily, the author of the SBoM. Suppliers often have the most direct and readily available knowledge about their components, therefore it is preferable for suppliers to create SBoMs as opposed to non-supplier authors.

B.2.6 Component name

These are the name or names given to the component. Common names alone are typically insufficient to uniquely identify components. SBoM authors can use a namespace:name construct, for example using the supplier or author name as the “namespace” and the component name (and other identifiers) as the “name.”

For components retrieved from a package manager or package distribution the component name can be represented through the use of the Package URL specification[1].

EXAMPLE 1 pkg:deb/debian/curl@7.50.3–1?arch = i386&distro = jessie

EXAMPLE 2 pkg:docker/cassandra@sha256:244fd47e07d1004f0aed9c

EXAMPLE 3 pkg:gem/jruby-launcher@1.1.2?platform = java

EXAMPLE 4 pkg:maven/org.apache.xmlgraphics/batik-anim@1.9.1?packaging = sources

EXAMPLE 5 pkg:npm/%40angular/animation@12.3.1

EXAMPLE 6 pkg:nuget/EnterpriseLibrary.Common@6.0.1304

EXAMPLE 7 pkg:pypi/django@1.11.1

EXAMPLE 8 pkg:rpm/fedora/curl@7.50.3–1.fc25?arch = i386&distro = fedora-25

B.2.7 Version

The version of a component should be expressed as semantic versioning when available.

B.2.8 Cryptographic hash

A cryptographic hash of a component (as defined by the SBoM author or supplier) is an intrinsic identifier of the component. Authors should provide sufficient information about how hashes are created so that SBoM consumers can correctly verify values. Digital signatures can be used in place of hashes, at the increased costs associated with identity and key management. If a component has been modified from its original source, authors should include both the hash of the source component and the modified component.

B.2.9 Unique identifier

A unique identifier is a string generated by the SBoM author or supplier to uniquely identify the component referenced. SBoM authors can consult ISO/IEC 9834-8 on the generation of universally unique identifiers.

B.2.10 Relationship

Relationships between components are necessary to determine path traversal, complexity in mitigation, and general architecture. Supply chain relationships and dependencies are fundamental to understanding the overall health of a software ecosystem prior to its deployment. For example, a software library can be a component of an application, the application a component of an operating system, and the operating system a component of an Internet of Things (IoT) product.

The minimum necessary relationship is one of dependency or inclusion, for example: component A includes component B. Variations or other types of relationships can be useful or necessary. The process of compiling and building software changes the software but still maintains heritage. An example of this type of relationship can be: component B (binary) was generated from component A (source).

[1] https://github.com/package-url

B.2.11 Source

Source is the location that the component was retrieved from. It can also relay additional details regarding when and where the retrieval from source occurred depending on the manner in which it was retrieved. Timestamps should be represented according to the ISO 8601 series.

For components retrieved through git or a browser the branch (if applicable) and URL should be listed. The examples follow SPDX format.

EXAMPLE 1

SourceInfo: <text>uses glibc-2_11-branch from git://sourceware.org/git/glibc.git at 2021–08–03T17:43:41+00:00</text>

For components retrieved through a package manager or package distribution, the package manager or distribution and its version should be listed.

EXAMPLE 2

SourceInfo: <text>cassandra@sha256:244fd47e07d1004f0aed9c from docker@20.10.7 at 2021–08–03T17:43:41+00:00</text>

For components provided through a second-party or contracted for development, the party should be defined as the source or if the relationship is deemed sensitive, can be cited as "protected" in accordance with Clause 5.8 m) of ISO/IEC 27036-3 regarding anonymous acquisition.

EXAMPLE 3

SourceInfo: <text>jruby-launcher from protected at 2021–08–03</text>

For components provided by the supplier themselves as internal, non-public components and created wholly unto themselves — are not built from 3rd or 2nd party source or modified from 3rd or 2nd party source — the source should reflect the supplier. If additional concerns are present, such as proprietary components, suppliers are encouraged to refer to B.3.4 concerning availability and cryptographic protection.

EXAMPLE 4

SourceInfo: <text>bom-verify@0.11.2 from supplier at 2021–08–03T17:43:41+00:00</text>

B.3 Essential SBoM processes

B.3.1 Overview

The general process model using these attributes is based on:

a) suppliers defining their components and documenting direct upstream dependencies;

b) consumers assembling dependency graphs of components and their relationships to each other.

Non-supplier authors can also define components and create SBoMs, but it is preferred that suppliers provide authoritative information about their components, products, systems, and services.

Suppliers should provide SBoMs to their users as part of the delivery of software products and systems. Suppliers can also provide SBoMs to potential users and customers as part of procurement. SBoMs can be published or distributed privately. It is suggested that organizations, where reasonable and appropriate, leverage public ledger technology to publish SBoM content, or encrypt the protected components of the SBoM prior to publishing to the public ledger with a mechanism for consumers to retrieve the corresponding key.

B.3.2 Frequency

A SBoM should be produced for each release or build of the software. The author of the SBoM should produce as complete a SBoM as possible, the manner in which they chose to generate the updated or newer SBoM is their prerogative.

B.3.3 Depth and extent

Components within a software's SBoM should include direct and transitive dependencies to the fullest extent possible. Where all dependencies are identified, the content should indicate no further dependencies. Where not all dependencies are capable of being listed and identified, the content should indicate incomplete coverage of dependencies.

B.3.4 Availability

The SBoM for software should be made available at the time the software itself is made available. It is not recommended to produce a SBoM after the software has been made available. The SBoM should be made available to the consumer of the software either through publication, packaging, or another agreed upon means of delivery.

The SBoM, its contents, or a portion thereof can be cryptographically protected, however the supplier is expected to provide a means by which a defined, authorized entity can securely retrieve the decryption key to make use of the SBoM in its totality.

B.3.5 Errors in SBoMs

Should the supplier discover an error in the SBoM provided, it is recommended a correction be issued within two weeks of discovery and be annotated to note the discrepancy.

Should a software consumer discover an error in the SBoM provided, the consumer should notify the supplier upon discovery. It is recommended the supplier issue a correction within two weeks of notification that annotates the discrepancy.

B.3.6 Non-repudiation

The SBoM, once produced, should be signed by the author in order to allow consumers to validate the authenticity of the SBoM. Where reasonable and appropriate, authors can record signed SBoMs to an immutable public transparency ledger in order to assist in independent attestation. Other parties can then query said metadata, enabling them to make informed decisions on trust and non-repudiation of a software's life cycle.

Bibliography

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

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

[3] ISO/IEC/IEEE 15026-1, *Systems and software engineering — Systems and software assurance — Part 1: Concepts and vocabulary*

[4] ISO/IEC 27001, *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*

[5] ISO/IEC 27002, *Information security, cybersecurity and privacy protection — Information security controls*

[6] ISO/IEC 27004, *Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation*

[7] ISO/IEC 27005, *Information security, cybersecurity and privacy protection — Guidance on managing information security risks*

[8] ISO/IEC 27007, *Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing*

[9] ISO/IEC 27036-2, *Cybersecurity — Supplier relationships — Part 2: Requirements*

[10] ISO/IEC 27031, *Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity*

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

[12] ISO/IEC 20000-1, *Information technology — Service management — Part 1: Service management system requirements*

[13] ISO/IEC 20243-1:2018, *Information technology — Open Trusted Technology ProviderTM Standard (O-TTPS) — Mitigating maliciously tainted and counterfeit products — Part 1: Requirements and recommendations*

[14] Software Assurance Forum for Excellence in Code (SAFECode) *The Software Supply Chain Integrity Framework, Defining Risks and Responsibilities for Securing Software in the Global Supply Chain, July 21,* 2009

[15] SAFECode, Software Integrity Controls, *An Assurance-Based Approach to Minimizing Risks in the Software Supply Chain, June 14,* 2010

[16] National Institute of Standards and Technology Interagency Report 7622, *Notional Supply Chain Risk Management Practices for Federal Information Systems, October* 2012

[17] National Institute of Standards and Technology Special Publication 800-161 Revision1, *Cyber Supply Chain Risk Management Practices for Systems and Organizations, April* 2021

[18] Package URL https://github.com/package-url

[19] ISO 8601 (all parts), *Date and time — Representations for information interchange*

[20] Software Package Data Exchange (SPDX) https://spdx.dev/specifications/

[21] ISO/IEC 9834-8, *Information technology — Procedures for the operation of object identifier registration authorities — Part 8: Generation of universally unique identifiers (UUIDs) and their use in object identifiers*

[22] IEC 62443-4-1, *Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements*

ICS 35.030

Price based on 35 pages