Date: 2023-01-25

ISO/IEC ~~JTC 1/SC 27 N~~

~~Date:~~ FDIS 27036-3:2022-~~07-19~~(E)

ISO/IEC ~~DIS 27036-3~~

~~ISO/IEC~~ JTC 1/SC 27/WG 4

Secretariat: DIN

Cybersecurity — Supplier relationships — Part 3: Guidelines for hardware, software, and services supply chain security

Style Definition: Emphasis

Formatted: English (United Kingdom)

Formatted: English (United Kingdom)

Formatted: English (United Kingdom)

Formatted: English (United Kingdom)

Formatted: English (United Kingdom)

Formatted: English (United Kingdom)

Formatted: English (United Kingdom)

~~**Copyright notice**~~

~~This~~

Formatted: Font: Cambria
Formatted: Font: Cambria
Formatted: Font: Cambria
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: Indent: Left: 14.2 pt, Right: 14.2 pt, Space After: 12 pt, Line spacing: At least 12 pt, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: Font: Cambria
Formatted: Font: Cambria
Formatted: Font: Cambria

Formatted: Font: Cambria, English (South Africa)
Formatted: Font: Cambria, English (South Africa)
Formatted: Font: Cambria, English (South Africa)
Formatted: Font: Cambria

Contents

Page

Formatted: English (United Kingdom)

Formatted: Highlight
Formatted: Font: Cambria, Not Bold
Formatted: Font: Cambria, Not Bold
Formatted: Font: Cambria
Formatted: Font: Cambria

Formatted: Font: Cambria
Formatted: Font: Cambria
Formatted: Font: Cambria
Formatted: Font: Cambria
Formatted: Font: Cambria
Formatted: Font: Cambria

Formatted: Font: Cambria, English (South Africa)
Formatted: Font: Cambria, English (South Africa)
Formatted: Font: Cambria, English (South Africa)
Formatted: Font: Cambria
Formatted: Font: Cambria, Not Bold
Formatted: Font: Cambria, Not Bold
Formatted: Font: Cambria
Formatted: Font: Cambria

Formatted: Font: Cambria
Formatted: Font: Cambria
Formatted: Font: Cambria

Formatted: Font: Cambria
Formatted: Font: Cambria
Formatted: Font: Cambria

Foreword

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

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

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see https://patents.iec.ch).

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

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

ISO/IEC 27036~~-~~-3 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity, and privacy protection*.

This second edition cancels and replaces the first edition (ISO/IEC 27036-3:2013), which has been technically revised.

The main changes are as follows:

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

— ~~—~~ former Annex ~~–~~ A~~, (informative) — Summary of Supply and Acquisition Processes from ISO/IEC/IEEE 15288 and ISO/IEC 12207~~ has been removed;

— ~~Informative Annex B, Essential elements of a software bill of materials (SBoM)~~ — 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 ~~boundariesThey~~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 ~~for~~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.

Formatted: Font: Cambria
Formatted: Font: Cambria
Formatted: Font: Cambria
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: std_docPartNumber, English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: Font: Cambria
Formatted: Font: Cambria
Formatted: Font: Cambria

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, and 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

Formatted: Font: Cambria
Formatted ...
Formatted ...
Formatted ...
Formatted ...
Formatted ...
Formatted ...
Formatted: Adjust space between Latin and Asian text, Adjust space between Asian text and numbers
Formatted ...
Formatted ...
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted ...
Formatted: Font: Cambria, 11 pt, English (United Kingdom)
Formatted: No underline, Font color: Auto, English (United Kingdom)
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers, Tab stops: 19.85 pt, Left + 39.7 pt, Left + 59.55 pt, Left + 79.4 pt, Left + 99.25 pt, Left + 119.05 pt, Left + 138.9 pt, Left + 158.75 pt, Left + 178.6 pt, Left + 198.45 pt, Left
Formatted: English (United Kingdom)
Formatted: Default Paragraph Font, English (United Kingdom)
Formatted ...
Formatted: Default Paragraph Font, English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: Font: Cambria, Not Bold
Formatted ...

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 ~~fulfill~~fulfil specified requirements.

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

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

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

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

Note 1 to entry: A system is able to accomplish its intended use, goals and objectives (i.e. meet stakeholder requirements) in the intended operational environment. The right system was built.

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

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

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

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

4 Structure

This structure of this document ~~has been structured to be~~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.

Formatted: Font: Cambria, English (South Africa)
Formatted: English (United Kingdom)
Formatted ...
Formatted ...
Formatted ...
Formatted: Source
Formatted ...
Formatted ...
Formatted: Source
Formatted ...
Formatted ...
Formatted: Source
Formatted ...
Formatted: English (United Kingdom)
Formatted ...
Formatted ...
Formatted: Font: Cambria

~~The document titles listed in Clause 6 of this document are generic and do not need to be elaborate or separate deliverables. Organizations should use existing documents to integrate hardware, software, and services supply chain security.~~

~~6~~5 Key concepts

~~6.1~~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.

~~6.2~~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.

~~6.3~~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: