

ISO/IEC JTC 1/SC 27 N11997

Date: 2012-11-10

ISO/IEC DIS 27036-3

ISO/IEC JTC 1/SC 27/WG 4

Secretariat: ANSI

Information technology — Security techniques — Information security for supplier relationships — Part 3: Guidelines for ICT supply chain security

Élément introductif — Élément central — Partie 3: Titre de la partie

Warning

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Document type: International Standard

Document subtype:

Document stage: (40) Enquiry

Document language: E

D:\Dokumente und Einstellungen\pas\Eigene Dateien\PROJECT_admin\27036-3\04_00_27036-3_20121114\N11997_Text_f_DIS_27036-3_20121114\N11997_Text_f_DIS_27036-3_by_editor_20121110_ITTF.doc STD Version 2.1c2

Copyright notice

This ISO document is a Draft International Standard and is copyright-protected by ISO. Except as permitted under the applicable laws of the user's country, neither this ISO draft nor any extract from it may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, photocopying, recording or otherwise, without prior written permission being secured.

Requests for permission to reproduce should be addressed to either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Reproduction may be subject to royalty payments or a licensing agreement.

Violators may be prosecuted.

Contents

Page

Foreword	v
Introduction.....	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	2
4 Structure of this Standard	3
5 Key concepts	3
5.1 Overview.....	3
5.1.1 Business case for ICT supply chain security	3
5.1.2 ICT supply chain risks and associated threats	3
5.1.3 Acquirer and supplier relationship types	4
5.2 Establishing organizational capability	4
5.3 Using system lifecycle processes	5
5.4 Using ISMS processes in relation to system lifecycle processes	5
5.5 Using ISMS information security controls in relation to ICT supply chain security	6
5.6 ICT supply chain security practices	6
6 ICT supply chain security in Lifecycle Processes	7
6.1 Agreement Processes.....	7
6.1.1 Acquisition Process	8
6.1.2 Supply Process.....	10
6.2 Organizational Project-Enabling Processes.....	11
6.2.1 Life Cycle Model Management Process	11
6.2.2 Infrastructure Management Process	11
6.2.3 Project Portfolio Management Process	12
6.2.4 Human Resource Management Process.....	12
6.2.5 Quality Management Process	13
6.3 Project Processes	13
6.3.1 Project Planning Process	13
6.3.2 Project Assessment and Control Process.....	13
6.3.3 Decision Management Process	14
6.3.4 Risk Management Process	14
6.3.5 Configuration Management Process.....	14
6.3.6 Information Management Process.....	15
6.3.7 Measurement Process	15
6.4 Technical Processes	15
6.4.1 Stakeholder Requirements Definition Process	15
6.4.2 Requirements Analysis Process.....	16
6.4.3 Architectural Design Process	17
6.4.4 Implementation Process	18
6.4.5 Integration Process	18
6.4.6 Verification Process	19
6.4.7 Transition Process	20
6.4.8 Validation Process	21
6.4.9 Operation Process.....	21
6.4.10 Maintenance Process.....	22
6.4.11 Disposal Process.....	22
Annex A (informative) Summary of Supply and Acquisition Processes from ISO/IEC 15288 and ISO/IEC 12207	24

Annex B (informative) Clause 6 Mapping to ISO/IEC 27002.....40

Bibliography.....43

Foreword

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

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

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

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

ISO/IEC 27036-3 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques*.

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

- *Part 1: Overview and concepts*
- *Part 2: Requirements*
- *Part 3: Guidelines for Information and Communication Technology (ICT) supply chain security*
- *Part 4: Guidelines for security of cloud services.*

Introduction

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

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

- Increased ICT supply chain visibility and traceability to enhance information security ability;
- Increased understanding by the acquirers of where their products are coming from, and of the practices used to develop or integrate these products, to enhance the implementation of information security requirements;
- In case of an information security compromise, the availability of information about what may have been compromised and who the involved actors may be.

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

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

Information technology — Security techniques — Information security for supplier relationships — Part 3: Guidelines for ICT supply chain security

1 Scope

This international standard which is Part 3 of ISO/IEC 27036, provides product and service acquirers and suppliers in ICT supply chain with guidance on:

- a) gaining visibility into and managing the information security risks caused by physically dispersed and multi-layered ICT supply chains;
- b) responding to risks stemming from the global ICT supply chain to ICT products and services that can have an information security impact on the organizations using these products and services. These risks may be related to organizational as well as technical aspects (e.g., insertion of malicious code or presence of the counterfeit information technology (IT) products);
- c) integrating information security processes and practices into the system and software lifecycle processes, described in ISO/IEC 15288 and ISO/IEC 12207 while supporting information security controls, described in ISO/IEC 27002.

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

2 Normative references

The following referenced documents are indispensable for the application 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 27001, *Information Technology – Security Techniques – Information Security Management System*

ISO/IEC 27002, *Information technology -- Security techniques -- Code of practice for information security controls*

ISO/IEC 15288, *Systems and software engineering -- System life cycle processes*

ISO/IEC 12207, *Systems and software engineering -- Software life cycle processes*

ISO/IEC 27036-1, *Information technology — Security techniques — Supplier relationships –Overview and Concepts*

ISO/IEC 27036-2, *Information technology — Security techniques — Supplier relationships –Common Requirements*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000, in ISO/IEC 27036 Part 1, in ISO/IEC 27036 Part 2 and the following apply.

3.1

auditability

property of a process that enables it to be verified for conformance to certain standard

3.2

authenticity

property that an entity is what it claims to be [ISO/IEC 27000]

3.3

defense-in-breadth

series of protection methods and mechanisms deployed throughout the lifecycle

3.4

integrity

property of protecting the accuracy and completeness of assets [ISO/IEC 27000]

3.5

global supply chain

supply chain that crosses multiple international or economic borders [adapted from ISO 28001]

3.6

reliability

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

3.7

repeatability

property of a process conducted to get the same test results on the same testing environment (same computer, hard drive, mode of operation, etc.)

3.8

scalability

property of a system or process to change, either increasing or decreasing in size

3.9

system element

member of a set of elements that constitutes a system

NOTE: A system element is a discrete part of a system that can be implemented to fulfill specified requirements. A system element can be hardware, software, data, humans, processes (e.g., processes for providing required functionality to users), procedures (e.g., operator instructions), facilities, materials, and naturally occurring entities (e.g., water, organisms, minerals), or any combination. [ISO/IEC 15288]

3.10

transparency

property of a system or process to imply openness and accountability

3.11

traceability

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

3.12**validation**

confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled [ISO 9000:2005]

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

3.13**verification**

confirmation, through the provision of objective evidence, that specified requirements have been fulfilled [ISO 9000:2005]

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

4 Structure of this Standard

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

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

5 Key concepts**5.1 Overview****5.1.1 Business case for ICT supply chain security**

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

For example, increased visibility into the ICT supply chain is obtained by defining adequate information security and quality requirements, and ongoing monitoring of suppliers and their products and services once a supplier relationship is in operation. Identifying and tracking individuals accountable for quality and security for critical elements provides greater traceability. Establishing contractual requirements and expectations, as well as reviewing processes and practices provides much needed transparency.

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

5.1.2 ICT supply chain risks and associated threats

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

Acquiring ICT products and services presents special risks to acquirers in terms of managing information security. The acquirers' concerns are the risk of limited (if any) visibility into and transparency of the processes and practices used by various suppliers within the ICT supply chain. Those concerns associated with ICT supply chain risk management include information security weaknesses, failure to protect information and intellectual property, data leakage, malicious code insertion, counterfeit component insertion, reduced functionality of resulting products and services, loss of confidentiality, availability, and integrity which can all result in the acquirers information security risks 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.

As global ICT supply chains get more physically dispersed and traverse multiple international and organizational boundaries, specific manufacturing and operation practices applied to individual ICT elements (products, services, and their components) become more difficult to trace including identifying individuals accountable for quality and security of those elements. This creates a general lack of traceability throughout the ICT supply chain which in turn results in higher risk of compromise to acquirers' information security and therefore to business operations through intentional events such as malicious code insertion and presence of counterfeit products in the ICT supply chain. It also increases the risk of unintentional events, such as sloppy software development practices which may lead to insecure applications potentially resulting in compromise to acquirer's data and operations.

5.1.3 Acquirer and supplier relationship types

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

- a) ICT system management support where systems are owned by acquirer and managed by supplier;
- b) ICT systems or services providers where systems or resources are owned and managed by the supplier;
- c) Product development, design, engineering and build where supplier provides all or parts of the service associated with creating ICT products;
- d) Commercial-off-the-shelf product suppliers;
- e) Open source product suppliers and distributors.

Acquirers' level of risk and need for trust in supplier relationships increases when granting a supplier a greater level of access to the acquirers' information and information systems and acquirers' dependency on the supplied ICT products and services. For example, acquiring IT 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 supplier reputation and trust with the specific acquirer whose information and information systems have been compromised.

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

5.2 Establishing organizational capability

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

- a) Identify and document specific information security risks related to ICT supply chain that need to be addressed (see clause 6.3.4).
- b) Establish and adhere to baseline information security controls for both acquirers and suppliers as a prerequisite to robust supplier relationships (see Annex B for a mapping of Clause 6 to ISO/IEC 27002).

- c) Establish and adhere to baseline system and software lifecycle processes and practices for establishing robust supplier relationships in regards to ICT supply chain information security risk management concerns (see Clause 6).
- d) Define, select, and implement the strategy for management of information security risks caused by ICT supply chain vulnerabilities:
 - 1) Establish and maintain a plan for identifying potential ICT supply chain-related vulnerabilities before they are exploited; in addition, have a plan for mitigating adverse impacts.
 - 2) Identify and document information security risks associated with the ICT supply chain-related threats, vulnerabilities, and consequences.
- e) Have a set of baseline information security requirements that apply to all supplier relationships and tailor them for specific suppliers as needed.
- f) 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.
- g) Establish change management processes to ensure changes that potentially affect information security are approved and applied in a timely manner.
- h) Define methods for identifying and managing incidents related to or caused by ICT supply chain and for sharing information about the incidents with suppliers and acquirers.

5.3 Using system lifecycle processes

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

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

Clause 5.6 provides a summary of specific ICT supply chain security practices. Clause 6 provides a mapping of these ICT supply chain security activities for each lifecycle process. Acquirers 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 described in Clause 5.2.

5.4 Using ISMS processes in relation to system lifecycle processes

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

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

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

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

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

- a) scope of the ISMS;
- b) statement of applicability;
- c) risk assessment procedures,
- d) audit plan;
- e) awareness programs;
- f) incident management;
- g) measurement programs;
- h) information classification scheme;
- i) change management;
- j) other relevant specific controls applied.

5.5 Using ISMS information security controls in relation to ICT supply chain security

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

Annex B maps specific ISO/IEC 27002 controls to individual lifecycle processes and provides additional specific ICT supply chain security activities for those lifecycle process- information security controls combinations.

5.6 ICT supply chain security practices

Some of the ICT supply chain risks can be addressed by applying the standards providing lifecycle processes (ISO/IEC 15288 and ISO/IEC 12207), requirements for establishing ISMS (ISO/IEC 27001), and information security controls (ISO/IEC 27002). More detailed practices are required to fully address these risks, such as:

- a) Chain of custody: the acquirer and supplier have the confidence that each change and handoff made during the element's lifetime is authorized, transparent and verifiable;
- b) Least privilege access: personnel can access critical information and information systems with only the privileges needed to do their jobs;

- c) Separation of duties: control the process of creation, modification, or deletion of data or the process of development, operation, or removal of hardware and software;
- d) Tamper resistance and evidence: attempts to tamper are obstructed, and when they occur they are evident and reversible;
- e) Persistent protection: critical data and information are protected in ways that remain effective even if the data or information are transferred from the location where it was created or modified;
- f) Compliance management: the success of the protections within the agreement can be continually and independently confirmed;
- g) Code assessment and verification: methods for code inspection are applied and suspicious code is detected;
- h) ICT supply chain security training: organization's ability to effectively train relevant personnel on information security practices. This should include secure development practices, recognition of tampering, etc., as appropriate;
- i) Vulnerability assessment and response: a formal understanding by acquirer of how well their suppliers are equipped with the capability to collect input on vulnerabilities from researchers, customers, or sources, and produce a meaningful impact analysis and appropriate remedies in the short timeframe involved. This should include acquirer and supplier agreement on systematic repeatable vulnerability response processes;
- j) Defined expectations: clear language regarding the requirements to be met by the element and design/development environment is set forth in the agreement. This should include commitment to provide information security testing, code fixes and warranties about the development, integration, and delivery processes used;
- k) Ownership and responsibilities: acquirer's and supplier's ownership of intellectual property rights and the other party's responsibilities for protecting the intellectual property rights are identified in the agreement;
- l) Avoid gray-market components: many ICT supply chain risks can be avoided by requiring verification of authenticity for system components;
- m) When appropriate and feasible, practice anonymous acquisition: when acquirer identity is sensitive, obscure the connection between the ICT supply chain and the acquirer;
- n) All-at-once acquisition: components for long-life systems (durable automatic controls) can become obsolete and increase ICT supply chain risk, acquiring all spare parts within a specified time-frame reduces these risks;
- o) Recursive requirements for suppliers: contracts can establish that suppliers place and validate ICT supply chain requirements on their upstream suppliers.

6 ICT supply chain security in Lifecycle Processes

6.1 Agreement Processes

Supplier relationships between acquirers and suppliers are achieved using agreements. Organizations can act simultaneously or successively as both acquirers and suppliers of ICT products and services. For those occasions when acquirer and supplier are within the same organization it is recommended to still use

Agreement Processes but with less formality. Agreement Processes include Acquisition Process and Supply Process.¹

ISO/IEC 27002 provides additional specific guidance regarding setting expectations during the agreement processes. Mapping of ISO/IEC 27036 Part 3 Clause 6 to ISO/IEC 27002 controls is provided in Annex B.

6.1.1 Acquisition Process

ISO/IEC 15288 provides guidance regarding implementing an Acquisition Process. Acquirers should include the following activities as a part of the Acquisition Process to ensure they are appropriately managing ICT supply chain risks:

- a) Prepare for the acquisition.
 - 1) Establish a strategy for how the acquisition will be conducted.
 - Establish sourcing strategies based on information security risk tolerance regarding ICT supply chain risks.
 - 2) Prepare a request for the supply of a product or service that includes the definition of requirements.
 - Establish information security requirements for suppliers including ICT-related regulatory requirements (i.e., telecommunications or IT), technical requirements, chain of custody, transparency and visibility, sharing information on information security incidents throughout the supply chain, rules for disposal or retention of elements such as components, data, or intellectual property, and other relevant requirements.
 - Establish requirements for the suppliers managing their suppliers in the ICT supply chain when appropriate.
 - Define requirements for suppliers in the ICT supply chain to provide credible evidence that they have fulfilled information security requirements.
 - Define requirements for suppliers of critical elements in the ICT supply chain to demonstrate a capability to remediate emerging vulnerabilities based on information gathered from acquirers and other sources.
 - 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 requirements for suppliers to identify the expected life span of the element to help acquirer plan for any migration that can be required in support of continued system and mission operations.
 - Define requirements for auditing of suppliers' information systems where applicable.
 - Define requirements for monitoring suppliers' work processes and work products where applicable.
 - To share acquirer's requirements of acquirer throughout the supply chain, define requirements for communicating to and requiring them from the upstream suppliers.
- b) Advertise the acquisition and select the supplier.

¹ Paraphrased from ISO/IEC 15288.

- 1) Communicate the request for the supply of a product or service to identified suppliers.
 - No activity specific to ICT supply chain is required.
- 2) Select one or more suppliers.
 - Select suppliers based on an evaluation of their ability to meet specified requirements including those for ICT supply chain.
 - Use established evaluation methods and results for ICT products, services, components or their suppliers (e.g., ISO/IEC 15408 repositories for components or information security management system (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 ICT 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.
- 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' work processes 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 ICT products or services provided through the supply chain.
 - 3) Evaluate suppliers for their ability to meet specified ICT supply chain requirements.
- e) Accept the product or service.
 - 1) Confirm that the delivered product or service complies with the agreement.
 - No activity specific to ICT supply chain is required.
 - 2) Make payment or provide other agreed consideration to the supplier for the product or service rendered that is required for closure of the agreement.
 - No activity specific to ICT supply chain is required.

6.1.2 Supply Process

Suppliers in the ICT supply chain should include the following activities as a part of the Supply Process to ensure and demonstrate they are appropriately managing ICT 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.

- No activity specific to ICT supply chain is required.

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 acquirer's information security requirements including ICT-related regulatory requirements (i.e., telecommunications or IT), technical requirements, chain of custody, transparency and visibility, 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 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.

- No activity specific to ICT supply chain is required.

- 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) Execute the agreement according to the Supplier's established project plans and in accordance with the agreement.

- No activity specific to ICT supply chain is required.

- 2) Assess the execution of the agreement.

- No activity specific to ICT supply chain is required.

- e) Deliver and support the product or service.
 - 1) Deliver the product or service in accordance with the agreement criteria.
 - No activity specific to ICT supply chain is required.
 - 2) Provide assistance to the acquirer in support of the delivered system or service in accordance with the agreement criteria.
 - No activity specific to ICT supply chain is required.
- f) Close the agreement.
 - 1) Accept and acknowledge payment or other agreed consideration.
 - No activity specific to ICT supply chain is required.
 - 2) Transfer the responsibility for the product or service to the acquirer, or other party, as directed by the agreement to obtain closure of the agreement.
 - No activity specific to ICT supply chain is required.

6.2 Organizational Project-Enabling Processes

The Organizational Project-Enabling Processes are concerned with ensuring that the resources needed to enable the project to meet the needs and expectations of the organization's interested parties are met.

The Organizational Project-Enabling Processes establish the environment in which projects are conducted². Unless specifically stated, these processes may be applicable to both acquirers and suppliers.

ISO/IEC 27002 provides additional specific guidance regarding setting expectations during the organizational project-enabling processes. Mapping of ISO/IEC 27036 Part 3 Clause 6 to ISO/IEC 27002 controls is provided in Annex B.

6.2.1 Life Cycle Model Management Process

The purpose of the Life Cycle Model Management Process is to define, maintain, and assure availability of policies, life cycle processes, life cycle models, and procedures for use by the organization. ICT supply chain security should be considered in this process but there is no specific guidance in addition to what is provided in ISO/IEC 15288 and ISO/IEC 27036 Part 2.

6.2.2 Infrastructure Management Process

Acquirers and suppliers should include the following, where appropriate, as a part of Infrastructure Management process to address information security risks in the ICT supply chain:

- a) Establish and maintain visibility into their processes, environment 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 all assets in the environment.
- c) Establish physical security processes and capability for hardware components, and media, including delivery, removal and maintenance.

² ISO/IEC 15288.

- 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 an active malware scanning program for both the code under development and for the environment, at least to the level described in ISO/IEC 27002.
- g) Establish secure storage for software elements source code with need-to-know access controls.
- h) Implement code exchange processes using digitally signed packages or verifiable checksums or hashes to ensure that received code is complete and authentic.

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 International Standard. (source ISO/IEC 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. Acquirers and suppliers should consider ICT supply chain security in this process but there is no specific guidance in addition to what is provided in ISO/IEC 15288 and ISO/IEC 27036 Part 2.

6.2.4 Human Resource Management Process

In addition to implementing Human Resource Management Process in ISO/IEC 15288 and human resource security control in ISO/IEC 27002, acquirers and suppliers should educate staff on specific ICT 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 ICT supply chain:

- a) Establish organizational policy and general contractual requirements to address awareness and training on ICT supply chain risk management throughout the organization.
- b) Define, design, specify, and require roles throughout the supply chain and system/element life cycle to limit opportunities and means available to individuals performing these roles that could result in adverse consequences.
- c) Develop a comprehensive awareness and training program that promotes the organization's ICT supply chain security policy and procedures.
- d) Train quality assurance and information security personnel on ICT 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 may 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 ICT 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 could result in compromise or loss.

- h) Define processes by which general ICT supply chain information is collected, lessons learned extracted, and shared between acquirers and suppliers 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 ICT supply chain and within the supported operating environment.
- j) Establish and enforce requirements for the assignment of unique identities to all individuals (e.g. logon account, user ID, etc) including requirements under what circumstances such items can be reused (e.g. employee termination, name change, etc).

6.2.5 Quality Management Process

Acquirers and suppliers should include the following as a part of Quality Management process to address information security risks in ICT supply chain:

- a) Active vulnerability management program at a minimum comparable to what is described in ISO/IEC 27002;

NOTE: General vulnerability management activities are addressed under clause 6.3.4, Risk Management Process.

- b) Integration of testing for weaknesses and vulnerabilities into quality management activities throughout the lifecycle including design and architecture reviews, documentation reviews, and a variety of testing that software and hardware undergo before delivery and installation.

NOTE: Integration of testing for reliability and resilience into quality management activities should be considered if appropriate.

6.3 Project Processes

Project processes are concerned with rigorous project management and project support for system and software engineering projects, including the ones that span across ICT supply chain or multiple ICT supply chains. Unless specifically stated, these processes may be applicable to both acquirers and suppliers.

6.3.1 Project Planning Process

For projects involving ICT products and services created and delivered across geographically dispersed supply chains controlled by multiple entities, acquirers and suppliers should consider and integrate into the project plans the following during project planning process:

- a) How the need for securing acquirer and supplier information will impact project plans and schedules;
- b) Any aspects of ICT supply chain information security risk management that need to be integrated in project roles, responsibilities, accountabilities, and authorities;
- c) Different legal requirements of multiple jurisdictions relevant to the ICT supply chain;
- d) Resources that are required to ensure protection of acquirer and supplier information across ICT supply chain(s) including staffing requirements.

6.3.2 Project Assessment and Control Process

In addition to implementing Project Assessment and Control Process in ISO/IEC 15288 and ISO/IEC 27036 Part 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 requirements. Document results of these audits in compliance reports. Periodicity of compliance audits should be determined based on the identified ICT 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 select the most beneficial course of project action where alternatives exist. Acquirers and suppliers should consider ICT supply chain security in this process but there is no specific guidance in addition to what is provided in ISO/IEC 15288 and ISO/IEC 27036 Part 2.

6.3.4 Risk Management Process

In addition to implementing Risk Management Process in ISO/IEC 15288, ISO/IEC 27036 Part 2 and information security risk management approach described in ISO/IEC 27005, acquirers and suppliers should implement the following activities to address information security risks in ICT supply chain including:

- a) Identify threats, vulnerabilities, and consequences related to ICT products and services.
- b) Identify and document ICT supply chain risks associated with the identified threats and vulnerabilities.
- c) Identify different legal requirements of multiple jurisdictions relevant to the ICT supply chain.
- d) Define and select strategy for management of ICT supply chain risks due to unintentional and intentional weaknesses and vulnerabilities at all stages of the lifecycle, including transition from a supplier to a new supplier or back to the acquirer, disposal of elements, and retention of elements by a supplier.
- e) Demarcate responsibilities in mitigating ICT 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 and sources suppliers in other products or services and apply to future activities.
- h) Determine root causes of weaknesses and vulnerabilities that are identified during development, delivery, and operations. Implement corrective actions, as appropriate.
- i) Monitor ICT supply chain for potential concerns, identify and analyse resulting information security risks, and update risk assessment and risk treatment strategies accordingly.

6.3.5 Configuration Management Process

Configuration management 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 ICT supply chain concerns are appropriately addressed, acquirers and suppliers should include the following as a part of Configuration Management process to address specific information security risks in ICT supply chain:

- a) Control access and changes to all hardware and hardware elements throughout the lifecycle, including design, manufacturing, testing, operations, maintenance, and disposal.
- b) Control access and changes to documentation associated with ICT products 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 related assets in source code repositories (also known as configuration management systems or source code control systems) to enable additional attention to information security and to access control.
- f) The servers that host the source code repositories should be housed securely, be configured to be secure by default (e.g., with least necessary privileges, disabled services that are not widely needed), and be protected appropriate to the sensitivity of code that they house.
- g) Access to source code repositories should be controlled 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.
- h) Within the repositories, access to branches, work areas or code sets must be understood by development management, and access privileges should be granted based on least privilege and need-to-know.
- i) Changes to the code repository, including review and approval, should be understood and preserved for future analysis.
- j) Change logs should provide file names, account name of a person checking in the file, check-in time stamp, and the line that was changed.
- k) A manifest of all code assets contributing to a product, including those developed in house and by suppliers should be maintained and managed, similar to a Bill of Materials.
- l) Chain of custody for each element should be established and preserved through code signing, time stamping, and other appropriate techniques.

ISO/IEC 27002 provides additional specific guidance regarding setting expectations during the Configuration Management process. Mapping of ISO/IEC 27036 Part 3 Clause 6 to ISO/IEC 27002 controls is provided in Annex B.

6.3.6 Information Management Process

In addition to implementing ISO/IEC 15288 Information Management process, a number of ISO/IEC 27002 controls provide additional guidance. Mapping of ISO/IEC 27036 Part 3 Clause 6 to ISO/IEC 27002 controls is provided in Annex B.

6.3.7 Measurement Process

The purpose of the Measurement Process is to collect, analyze, and report data relating to the products developed and processes implemented within the organization, to support effective management of the processes, and to objectively demonstrate the quality of the products. There are no ICT 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 ICT supply chain.

6.4 Technical Processes

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

6.4.1 Stakeholder Requirements Definition Process

The purpose of the Stakeholder Requirements Definition Process is to define the requirements for an ICT product or service that can provide the services needed by users and other stakeholders in a defined

environment³. Acquirers and suppliers should include the following as a part of Stakeholder Requirements Definition process to address specific ICT 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.
- d) Define and document system integrity requirements for ICT products and services suppliers.
- e) Define and document data and system availability requirements for ICT products and services suppliers.
- f) Define and document information confidentiality requirements for ICT products and services suppliers.
- g) Define and document information security aspects of ICT product and service delivery requirements.
- h) Define and document consequences of violations of information security requirements for ICT product and service delivery.

ISO/IEC 27002 provides additional specific guidance regarding setting expectations during the Stakeholder Requirements Definition process. Mapping of ISO/IEC 27036 Part 3 Clause 6 to ISO/IEC 27002 controls is provided in Annex B.

6.4.2 Requirements Analysis Process

The purpose of the Requirements Analysis Process is to transform the stakeholder, requirement-driven view of desired services into a technical view of a required product that could deliver those services⁴. Acquirers and suppliers should include the following as a part of Requirements Analysis process to address specific information security risks in ICT supply chain:

- a) Ensure that elements are assigned varying degrees of criticality depending on the purpose and use of each element.
- b) Incorporate ICT supply chain risk considerations and assessments in all management, operational and technical requirements and business processes to protect elements, processes, requirements, and business practices against compromise of confidentiality, integrity, or availability.
- c) Incorporate defensive design criteria in all technical requirements to result in design options for elements, systems, and/or processes that protect mission capabilities, system performance, or element confidentiality, integrity, and availability.
- d) Protect requirements and supporting documentation from exposure or access that could result in the loss of the confidentiality, integrity, or availability of the elements and systems through an ICT 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 intended and unintended use in requirements.

³ ISO/IEC 15288

⁴ ISO/IEC 15288

ISO/IEC 27002 provides additional specific guidance that can be used during the Requirements analysis process. Mapping of ISO/IEC 27036 Part 3 Clause 6 to ISO/IEC 27002 controls is provided in Annex B.

6.4.3 Architectural Design Process

The purpose of the Architectural Design Process is to synthesize a solution that satisfies system requirements⁵. Acquirers and suppliers should include the following as a part of Architectural Design process to address specific information security risks in ICT supply chain:

- a) Use defensive design techniques to anticipate maximum possible ways the ICT product 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 to reduce opportunities to exploit ICT 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 ICT. Design elements to include but not be limited to programming techniques or configurations.
- g) 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).
- h) Design elements to withstand out-of-bounds inputs (e.g., excessive voltages, numbers out of range, and so on).
- i) 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.
- j) Design delivery mechanisms to avoid exposure or access to the system and element delivery processes, and use of the element during the delivery process.
- k) Include fail-over/redundant or alternative systems or system elements where appropriate and ensure that the fail-over and redundant mechanisms are not subject to common mode failures.
- l) 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.
- m) Design relevant validation controls to be used during implementation and operation.

⁵ ISO/IEC 15288

6.4.4 Implementation Process

The purpose of the Implementation Process is to realize a specified system element⁶. Suppliers should include the following as a part of Implementation Process to address information security risks in ICT supply chain:

- a) Implement architecture and design that address ICT supply chain-related requirements for products and services.
- b) Identify deviations from ICT supply chain-related requirements and implement appropriate mitigations.
- c) 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.
- d) Protect access to test cases and results and ensure that they are signed to demonstrate absence of tampering. Store test cases and results in a source control system and protect similarly to how source code and build scripts are protected.
- e) 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 ICT supply chain-related compromise.
- f) Identify and implement interface standards wherever practical to promote system and element sustainability and element reusability.
- 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 the turning off of any unnecessary functions, prevalent in commercial-off-the-shelf products implementations which may be designed to support multiple applications or purposes. These functions if left active may permit unauthorized access or exposure of the system or perform a function that reduces the availability of other functions.
- i) 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. Mapping of ISO/IEC 27036 Part 3 Clause 6 to ISO/IEC 27002 controls is provided in Annex B.

6.4.5 Integration Process

The purpose of the Integration Process is to assemble a system (including services) that is consistent with the architectural design⁷. Acquirers and suppliers should include the following as art of Integration process to address information security risks in ICT supply chain:

⁶ ISO/IEC 15288

- a) Integration with existing systems should include activities of 6.4.4 pending on the characteristics of the integration;
- b) Documentation should be made on how the activities in 6.4.4 are applied during integration and the integrated existing systems that were in place prior to the implementation.

6.4.6 Verification Process

The purpose of the Verification Process is to confirm that the specified design requirements are fulfilled by the System (including services)⁸. This should include verifying the pre-acquisition information shared between the supplier and acquirer and developing verification requirements based on clauses 6.2, 6.3 and 6.4.

Suppliers should include the following as a part of Verification process to address specific information security risks in ICT supply chain:

- a) Verify and validate that ICT supply chain security requirements have been addressed.
- b) Verify that supplier support activities align with acquirer 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 supplier product documentation links product features to architecture, design, requirements, code, tests, and test results.
- e) Verify that the supplier implements verification and validation activities to ensure controls are in place and working as intended and meet acquirer requirements.
- f) Verify that chain of custody is maintained between organizations.
- g) 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.
- h) Conduct network and web application vulnerability scanning.
- i) Conduct malware scanning.
- j) Run compliance validation tools.
- k) Conduct stress testing.
- l) 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. Mapping of ISO/IEC 27036 Part 3 Clause 6 to ISO/IEC 27002 controls is provided in Annex B.

⁷ ISO/IEC 15288

⁸ ISO/IEC 15288

6.4.7 Transition Process

The purpose of the Transition Process is to establish a capability to provide products and services specified by stakeholder requirements in the operational environment⁹. Acquirers should include the following as a part of Transition process to address specific information security risks in ICT 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 (to know who the inventory should go to, 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 delivery mechanisms to avoid exposure or access to the system and element delivery processes, and use of the element 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) Use non-destructive techniques or mechanisms to determine if there is any unauthorized access throughout the delivery process.
- f) Stipulate assurance levels and monitor logical delivery of products and services, requiring downloading from approved, verification-enhanced sites. Consider requiring encryption of elements (software, software patches, etc.) in transit (motion) and at rest throughout delivery.
- g) Scan software products for malware using the most recent signatures.
- h) Verify marks such as digital signatures and hologram tags for all critical elements.

Suppliers should include the following as a part of Transition process to address specific information security risks in ICT supply chain:

- a) Scan software products for malware using the most recent signatures.
- b) Consider encrypting elements (software, software patches, etc.) in transit (motion) and at rest throughout delivery.
- c) 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 all critical elements, digital markings that include software vendor's identity, cryptographically signing software components and using digital hashes.
- d) Deploy specific delivery processes for both on line and off line software delivery. Provide information on code signing and checksums to the acquirer.
- e) Deliver products in such a way that the acquirer can confirm that the product is coming from the specific supplier.
- f) Use anti-tamper mechanisms for prevention and discovery, including tamper-resistant and tamper-evident packaging (e.g., tamper tape or seals). These must not be easy to remove and replace without leaving evidence of such activity.

⁹ ISO/IEC 15288

ISO/IEC 27002 provides additional specific guidance regarding setting expectations during the Transition process. Mapping of ISO/IEC 27036 Part 3 Clause 6 to ISO/IEC 27002 controls is provided in Annex B.

6.4.8 Validation Process

The purpose of the Validation Process is to provide objective evidence that the services comply with stakeholders' requirements, achieving its intended use in its intended operational environment¹⁰. This should include determining whether the product received is genuine, and unaltered based on the supplier's product description or requirements, and agreement between 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 ICT supply chain:

- a) Verify and validate that ICT 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 could 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.

6.4.9 Operation Process

Acquirers and suppliers should include the following as a part of Operation process to address specific ICT supply chain- risks:

- a) Suppliers should ship elements "secured by default" at a level appropriate to acquirer's requirements.
- b) Include applicable system integration and custom code extension activities as part of the upgrade and maintenance efforts in system operational requirements.
- c) Perform all applicable information security activities and implement applicable information security requirements in operations.

ISO/IEC 27002 provides additional specific guidance regarding setting expectations during the Operation process. Mapping of ISO/IEC 27036 Part 3 Clause 6 to ISO/IEC 27002 controls is provided in Annex B.

¹⁰ ISO/IEC 15288

6.4.10 Maintenance Process

The purpose of the Maintenance Process is to sustain the capability of the system and its ICT components to provide a service¹¹. Acquirers and suppliers should include the following as a part of Maintenance process to address specific information security risks in ICT supply chain:

- a) Use procurement clauses to reduce ICT supply chain risk in formal service and maintenance agreements with suppliers.
- b) When acquiring OEM original equipment manufacturer(s) 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 may not be available, especially late in the element's life.
- e) Consider ICT supply chain risks when acquiring replacement components or field additions/modifications/upgrades, particularly if they do not go through traditional acquisition processes that examine SC 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.
- i) Develop and implement an approach for handling and processing reported ICT supply chain anomalies while in operation.
- j) Monitor 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.

ISO/IEC 27002 provides additional specific guidance regarding setting expectations during the Maintenance process. Mapping of ISO/IEC 27036 Part 3 Clause 6 to ISO/IEC 27002 controls is provided in Annex B.

6.4.11 Disposal Process

The purpose of the Disposal Process is to end the existence of a system entity.¹² Disposal can happen at any point in the system or element lifecycle and includes both electronic and non-electronic media. Acquirers and

¹¹ ISO/IEC 15288

¹² ISO/IEC 15288

suppliers should include the following as a part of Disposal process to address information security risks in ICT supply chain, specifically the risk of counterfeit products contaminating the supply chain:

- a) Preserve 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 chain of custody.
- e) Implement procedures for the secure and permanent destruction of elements.
- 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 processes. Mapping of ISO/IEC 27036 Part 3 Clause 6 to ISO/IEC 27002 controls is provided in Annex B.

Annex A (informative)

Summary of Supply and Acquisition Processes from ISO/IEC 15288 and ISO/IEC 12207

ISO/IEC 15288 and ISO/IEC 12207 Acquisition and Supply processes are complimentary, in other words, each activity of acquisition has a corresponding activity in supply.

Note that ISO/IEC 15288 and ISO/IEC 12207 are written in slightly different formats. ISO/IEC 15288 makes use of nested lists, while ISO/IEC 12207 uses deep numbering of sub-clauses.

The table below presents the processes in a side-by-side format that is intended to illustrate the complimentary relationship between acquisition and supply as well as the fact that ISO/IEC 12207 represents a specialization of ISO/IEC 15288

Systems (15288) Acquisition process	Systems (15288) Supply process	Software (12207) Acquisition process	Software (12207) Supply process
6.1.1 Acquisition Process 6.1.1.1 Purpose The purpose of the Acquisition Process is to obtain a product or service in accordance with the acquirer's requirements.	6.1.2 Supply Process 6.1.2.1 Purpose The purpose of the Supply Process is to provide an acquirer with a product or service that meets agreed requirements.	6.1.1 Acquisition Process 6.1.1.1 Purpose The purpose of the Acquisition Process is to obtain the product and/or service that satisfies the need expressed by the acquirer. The process begins with the identification of customer needs and ends with the acceptance of the product and/or service needed by the acquirer.	6.1.2 Supply Process 6.1.2.1 Purpose The purpose of the Supply Process is to provide a product or service to the acquirer that meets the agreed requirements.
6.1.1.2 Outcomes As a result of the successful implementation of the Acquisition Process: a) A strategy for the acquisition is established. b) One or more suppliers are selected. c) Communication with the supplier is maintained.	6.1.2.2 Outcomes As a result of the successful implementation of the Supply Process: a) An acquirer for a product or service is identified. b) A response to the acquirer's request is made. c) An agreement to supply a product or service according to	6.1.1.2 Outcomes As a result of successful implementation of the Acquisition Process: a) acquisition needs, goals, product and/or service acceptance criteria and acquisition strategies are defined; b) an agreement is developed that clearly expresses the expectation, responsibilities and liabilities of both the	6.1.2.2 Outcomes As a result of successful implementation of the Supply Process: a) an acquirer for a product or service is identified; b) a response to an acquirer's request is produced; c) an agreement is established between the acquirer and the supplier for developing,

Systems (15288) Acquisition process	Systems (15288) Supply process	Software (12207) Acquisition process	Software (12207) Supply process
<p>d) An agreement to acquire a product or service according to defined acceptance criteria is established.</p> <p>e) A product or service complying with the agreement is accepted.</p> <p>f) Payment or other consideration is rendered.</p>	<p>defined acceptance criteria is established.</p> <p>d) Communication with the acquirer is maintained.</p> <p>e) A product or service conforming to the agreement is supplied according to agreed delivery procedures and conditions.</p> <p>f) Responsibility for the acquired product or service, as directed by the agreement, is transferred.</p> <p>g) Payment or other agreed consideration is received.</p>	<p>acquirer and the supplier;</p> <p>c) one or more suppliers is selected;</p> <p>d) a product and/or service is acquired that satisfies the acquirer's stated need;</p> <p>e) the acquisition is monitored so that specified constraints such as cost, schedule and quality are met;</p> <p>f) supplier deliverables are accepted; and</p> <p>g) any identified open items have a satisfactory conclusion as agreed to by the acquirer and the supplier.</p>	<p>maintaining, operating, packaging, delivering, and installing the product and/or service;</p> <p>d) a product and/or service that meets the agreed requirements are developed by the supplier;</p> <p>e) the product and/or service is delivered to the acquirer in accordance with the agreed requirements; and</p> <p>f) the product is installed in accordance with the agreed requirements.</p>
<p>6.1.1.3 Activities and tasks</p> <p>The acquirer shall implement the following activities and tasks in accordance with applicable organizational policies and procedures with respect to the Acquisition Process.</p> <p>NOTE The activities and tasks in this process can apply to one or more suppliers.</p>	<p>6.1.2.3 Activities and tasks</p> <p>The supplier shall implement the following activities and tasks in accordance with applicable organizational policies and procedures with respect to the Supply Process.</p>	<p>6.1.1.3 Activities and tasks</p> <p>The acquirer shall implement the following activities in accordance with applicable organizational policies and procedures with respect to the Acquisition Process.</p> <p>NOTE The activities and tasks in this process can apply to one or more suppliers.</p>	<p>6.1.2.3 Activities and tasks</p> <p>The supplier shall implement the following activities in accordance with applicable organizational policies and procedures with respect to the Supply Process.</p>
<p>a) Prepare for the acquisition. This activity consists of the following tasks:</p> <p>1) Establish a strategy for how the acquisition will be conducted.</p> <p>NOTE This strategy includes reference to the life cycle model, a schedule</p>	<p>a) Identify opportunities. This activity consists of the following task:</p> <p>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</p>	<p>6.1.1.3.1 Acquisition preparation. This activity consists of the following tasks:</p> <p>6.1.1.3.1.1 The acquirer begins the acquisition process by describing a concept or a need to acquire, develop, or enhance a system, software product or</p>	<p>6.1.2.3.1 Opportunity identification. This activity consists of the following task:</p> <p>6.1.2.3.1.1 The supplier should determine the existence and identity of an acquirer who has, or who represents an organization or organizations having, a</p>

Systems (15288) Acquisition process	Systems (15288) Supply process	Software (12207) Acquisition process	Software (12207) Supply process
<p>of milestones and selection criteria if the supplier is external to the acquiring organization.</p> <p>2) Prepare a request for the supply of a product or service that includes the definition of requirements.</p> <p>NOTE Provide a definition of requirements to one or more suppliers. If a supplier is external to organization, then the request can include the business practices with which a supplier is expected to comply and the criteria for selecting a supplier.</p>	<p>service.</p> <p>NOTE For a product or service developed for consumers, an agent, e.g., a marketing function within the supplier organization, may represent the acquirer.</p>	<p>software service.</p> <p>6.1.1.3.1.2 The acquirer shall define and analyze the system requirements. The system requirements should include business, organizational and user as well as safety, security, and other criticality requirements along with related design, testing, and compliance standards and procedures.</p> <p>6.1.1.3.1.3 The acquirer may perform the definition and analysis of software requirements by itself or may retain a supplier to perform this task.</p> <p>6.1.1.3.1.4 If the acquirer retains a supplier to perform system or software requirements analysis, the acquirer shall retain approval authority for the analyzed requirements.</p> <p>6.1.1.3.1.5 The Technical Processes (subclause 6.4) should be used to perform the tasks in subclauses 6.1.1.3.1.2 and 6.1.1.3.1.4. The acquirer may use the Stakeholder Requirements Definition Process to establish the customer requirements.</p> <p>6.1.1.3.1.6 The acquirer shall consider options for acquisition against analysis of appropriate criteria to include risk, cost and benefits for each option. Options include:</p> <p>a) Purchase an off-the-shelf software product</p>	<p>need for a product or service.</p> <p>NOTE For a product or service developed for consumers, an agent, e.g., a marketing function within the supplier organization, may represent the acquirer.</p>

Systems (15288) Acquisition process	Systems (15288) Supply process	Software (12207) Acquisition process	Software (12207) Supply process
		<p>that satisfies the requirements.</p> <p>b) Develop the software product or obtain the software service internally.</p> <p>c) Develop the software product or obtain the software service through contract.</p> <p>d) A combination of a, b, and c above.</p> <p>e) Enhance an existing software product or service.</p> <p>6.1.1.3.1.7 When an off-the-shelf software product is to be acquired, the acquirer shall ensure the following conditions are satisfied:</p> <p>a) The requirements for the software product are satisfied.</p> <p>b) The required documentation is available.</p> <p>c) Proprietary, usage, ownership, warranty and licensing rights are satisfied.</p> <p>d) Future support for the software product is planned.</p> <p>6.1.1.3.1.8 The acquirer should prepare, document and execute an acquisition plan. The plan should contain the following:</p> <p>a) Requirements for the system.</p> <p>b) Planned employment</p>	

Systems (15288) Acquisition process	Systems (15288) Supply process	Software (12207) Acquisition process	Software (12207) Supply process
		<p>of the system.</p> <p>c) Type of contract to be employed.</p> <p>d) Responsibilities of the organizations involved.</p> <p>e) Support concept to be used.</p> <p>f) Risks considered as well as methods to manage the risks.</p> <p>6.1.1.3.1.9 The acquirer shall define and document the acceptance strategy and conditions (criteria).</p> <p>6.1.1.3.1.10 The acquirer should document the acquisition requirements (e.g., request for proposal), the content of which depends upon the acquisition option selected in subclause 6.1.1.3.1.6. The acquisition documentation should include, as appropriate:</p> <p>a) System requirements.</p> <p>b) Scope statement.</p> <p>c) Instructions for bidders.</p> <p>d) List of software products.</p> <p>e) Terms and conditions.</p> <p>f) Control of subcontracts.</p> <p>g) Technical constraints (e.g., target environment).</p> <p>6.1.1.3.1.11 The acquirer should determine which processes of this</p>	

Systems (15288) Acquisition process	Systems (15288) Supply process	Software (12207) Acquisition process	Software (12207) Supply process
		<p>International Standard are appropriate for the acquisition and specify any acquirer requirements for tailoring those processes. The acquirer should specify if any of the processes are to be performed by parties other than the supplier, so that suppliers may, in their proposals, define their approach to supporting the work of other parties. The acquirer shall define the scope of those tasks that reference the contract.</p> <p>6.1.1.3.1.12 The acquisition documentation shall also define the contract milestones at which the supplier's progress shall be reviewed and audited as part of monitoring the acquisition (see subclauses 7.2.6 and 7.2.7).</p> <p>6.1.1.3.1.13 The acquisition requirements should be given to the organization selected for performing the acquisition activities.</p>	
<p>b) Advertise the acquisition and select the supplier. This activity consists of the following tasks:</p> <p>1) Communicate the request for the supply of a product or service to identified suppliers.</p> <p>NOTE This may include supply chain management partnering which exchanges information with related suppliers and acquirers to achieve a harmonized or collective approach to</p>	<p>b) Respond to a tender. This activity consists of the following tasks:</p> <p>1) Evaluate a request for the supply of a product or service to determine feasibility and how to respond.</p> <p>2) Prepare a response that satisfies the solicitation.</p>	<p>6.1.1.3.2 Acquisition advertisement. This activity consists of the following task:</p> <p>6.1.1.3.2.1 The acquirer shall communicate the request for the supply of a product or service to identified suppliers.</p> <p>NOTE This may include supply chain management partnering which exchanges information with related suppliers and acquirers to achieve a harmonized or collective approach to</p>	<p>6.1.2.3.2 Supplier tendering. This activity consists of the following tasks:</p> <p>6.1.2.3.2.1 The supplier should conduct a review of requirements in the request for proposal taking into account organizational policies and other regulations.</p> <p>6.1.2.3.2.2 The supplier should make a decision to bid or accept the contract.</p> <p>6.1.2.3.2.3 The supplier</p>

Systems (15288) Acquisition process	Systems (15288) Supply process	Software (12207) Acquisition process	Software (12207) Supply process
common technical and commercial issues.		common technical and commercial issues.	shall prepare a proposal in response to the request for proposal.
<p>2) Select one or more suppliers.</p> <p>NOTE To obtain competitive solicitations, proposals to supply are evaluated and compared against the selection criteria. Where proposals include offerings that are not covered by the criteria, then the proposals are compared with each other to determine their order of suitability and thus supplier preference. The justification for rating each proposal is declared and suppliers may be informed why they were or were not selected.</p>		<p>6.1.1.3.3 Supplier selection. This activity consists of the following tasks:</p> <p>6.1.1.3.3.1 The acquirer should establish a procedure for supplier selection including proposal evaluation criteria and requirements compliance weighting.</p> <p>6.1.1.3.3.2 The acquirer should select a supplier based upon the evaluation of the suppliers' proposals, capabilities, and in accordance with the acquirer's acceptance strategy and conditions.</p>	
<p>c) Initiate an agreement. This activity consists of the following tasks:</p> <p>1) Negotiate an agreement with the supplier.</p> <p>NOTE This agreement may range in formality from a written contract to a verbal understanding. Appropriate to the level of formality, the agreement establishes requirements, development and delivery milestones, verification, validation and acceptance conditions, exception-handling procedures, change control procedures and payment schedules, so that both parties of the agreement understand the basis for executing the agreement. Rights and restrictions associated with technical</p>	<p>c) Initiate an agreement. This activity consists of the following tasks:</p> <p>1) Negotiate an agreement with the acquirer.</p> <p>NOTE This agreement may range in formality from a written contract to a verbal understanding. Negotiate the differences, where applicable, between the acquisition request or tasking statement and the capability expressed in the response. The Supplier confirms that the requirements, delivery milestones and acceptance conditions are achievable, that exception handling and change control procedures and payment schedules are acceptable, and that they establish a basis for</p>	<p>6.1.1.3.4 Contract agreement. This activity consists of the following tasks:</p> <p>6.1.1.3.4.1 The acquirer may involve other parties, including potential suppliers or any necessary third parties (such as regulators), before contract award, in determining the acquirer's requirements for tailoring of this International Standard for the project. In making this determination, the acquirer shall consider the effect of the tailoring requirements upon the supplier's organizationally-adopted processes. The acquirer shall include or reference the tailoring requirements in the contract.</p>	<p>6.1.2.3.3 Contract agreement. This activity consists of the following tasks:</p> <p>6.1.2.3.3.1 The supplier shall negotiate and enter into a contract with the acquirer to provide the software product or service.</p> <p>6.1.2.3.3.2 The supplier may request modification to the contract as part of the change control mechanism.</p>

Systems (15288) Acquisition process	Systems (15288) Supply process	Software (12207) Acquisition process	Software (12207) Supply process
<p>data and intellectual property are noted in the agreement. The negotiation is complete when the acquirer accepts the terms of an agreement offered by the supplier.</p> <p>2) Commence the agreement with the supplier.</p>	<p>executing the agreement without unnecessary risks. In the agreement or project plans, the supplier should define or select a life cycle model appropriate to the scope, magnitude, and complexity of the project. Ideally, this is performed by using an organizationally-defined life cycle model.</p> <p>2) Commence the agreement with acquirer.</p>	<p>6.1.1.3.4.2 The acquirer shall then prepare and negotiate a contract with the supplier that addresses the acquisition requirements, including the cost and schedule, of the software product or service to be delivered. The contract shall address proprietary, usage, ownership, warranty and licensing rights associated with the reusable off-the-shelf software products.</p> <p>6.1.1.3.4.3 Once the contract is underway, the acquirer shall control changes to the contract through negotiation with the supplier as part of a change control mechanism. Changes to the contract shall be investigated for impact on project plans, costs, benefits, quality, and schedule.</p> <p>NOTE 1 The acquirer determines whether the term "contract" or "agreement" is to be used in the application of this International Standard.</p> <p>NOTE 2 The agreement between the acquirer and the supplier should clearly express the expectation, responsibilities and liabilities of both.</p> <p>NOTE 3 The contract change control mechanism should address the change management roles and responsibilities, level of formality of the proposed change requests and contract renegotiation, and communication to the affected stakeholders. An informative Annex F</p>	

Systems (15288) Acquisition process	Systems (15288) Supply process	Software (12207) Acquisition process	Software (12207) Supply process
		contains a sample contract change management process that may be utilized to support this.	
<p>d) Monitor the agreement. This activity consists of the following tasks:</p> <p>1) Assess the execution of the agreement.</p> <p>NOTE This includes confirmation that all parties are meeting their responsibilities according to the agreement. Projected cost, performance and schedule risks are monitored, and the impact of undesirable outcomes on the organization is evaluated regularly. Variations to the terms of the agreement are negotiated as necessary.</p> <p>2) Provide data needed by the supplier and resolve issues in a timely manner.</p>	<p>d) Execute the agreement. This activity consists of the following tasks:</p> <p>1) Execute the agreement according to the Supplier's established project plans and in accordance with the agreement.</p> <p>NOTE 1 A supplier may adopt, or agree to use, acquirer processes.</p> <p>NOTE 2 Communication with the acquirer is maintained throughout the execution of the agreement.</p> <p>2) Assess the execution of the agreement.</p> <p>NOTE Projected cost, performance and schedule risks are monitored and communicated to the acquirer as appropriate. The impact of undesirable outcomes on the organization is evaluated.</p>	<p>6.1.1.3.5 Agreement monitoring. This activity consists of the following tasks:</p> <p>6.1.1.3.5.1 The acquirer shall monitor the supplier's activities in accordance with the Software Review Process (subclause 7.2.6) and the Software Audit Process (subclause 7.2.7). The acquirer should supplement the monitoring with the Software Verification Process (subclause 7.2.4) and the Software Validation Process (subclause 7.2.5) as needed.</p> <p>6.1.1.3.5.2 The acquirer shall cooperate with the supplier to provide all necessary information in a timely manner and resolve all pending items.</p>	<p>6.1.2.3.4 Contract execution. This activity consists of the following tasks:</p> <p>6.1.2.3.4.1 The supplier shall conduct a review of the acquisition requirements to define the framework for managing and assuring the project and for assuring the quality of the deliverable software product or service.</p> <p>6.1.2.3.4.2 If not stipulated in the contract, the supplier shall define or select a life cycle model appropriate to the scope, magnitude, and complexity of the project. The life cycle model shall be comprised of stages and the purpose and outcomes of each stage. The processes, activities, and tasks of this International Standard shall be selected and mapped onto the life cycle model.</p> <p>NOTE Ideally, this is performed by using an organizationally-defined life cycle model.</p> <p>6.1.2.3.4.3 The supplier shall establish requirements for the plans for managing and assuring the project and for assuring the quality of the deliverable software product or service. Requirements for the plans should include resource needs and</p>

Systems (15288) Acquisition process	Systems (15288) Supply process	Software (12207) Acquisition process	Software (12207) Supply process
			<p>acquirer involvement.</p> <p>6.1.2.3.4.4 Once the planning requirements are established, the supplier shall consider the options for developing the software product or providing the software service against an analysis of risks associated with each option. Options include:</p> <p>a) Develop the software product or provide the software service using internal resources.</p> <p>b) Develop the software product or provide the software service by subcontracting.</p> <p>c) Obtain off-the-shelf software products from internal or external sources.</p> <p>d) A combination of a, b, and c above.</p> <p>6.1.2.3.4.5 The supplier shall develop and document project management plan(s) based upon the planning requirements and options selected in subclause 6.1.2.3.4.4.</p> <p>NOTE Items to be considered in the plan include but are not limited to the following:</p> <p>a) Project organizational structure and authority and responsibility of each organizational unit, including external organizations.</p> <p>b) Engineering environment (for development, operation,</p>

Systems (15288) Acquisition process	Systems (15288) Supply process	Software (12207) Acquisition process	Software (12207) Supply process
			<p>or maintenance, as applicable), including test environment, library, equipment, facilities, standards, procedures, and tools.</p> <p>c) Work breakdown structure of the life cycle processes and activities, including the software products, software services and non-deliverable items, to be performed together with budgets, staffing, physical resources, software size, and schedules associated with the tasks.</p> <p>d) Management of the quality characteristics of the software products or services. Separate plans for quality may be developed.</p> <p>e) Management of the safety, security, and other critical requirements of the software products or services. Separate plans for safety and security may be developed.</p> <p>f) Subcontractor management, including subcontractor selection and involvement between the subcontractor and the acquirer, if any.</p> <p>g) Quality assurance (see subclause 7.2.3).</p> <p>h) Verification (see subclause 7.2.4) and validation (see subclause 7.2.5), including the approach for interfacing with the verification and validation agent, if specified.</p> <p>i) Acquirer involvement; that is, by such means as</p>

Systems (15288) Acquisition process	Systems (15288) Supply process	Software (12207) Acquisition process	Software (12207) Supply process
			<p>reviews (see subclause 7.2.6), audits (see subclause 7.2.7), informal meetings, reporting, modification and change; implementation, approval, acceptance, and access to facilities.</p> <p>j) User involvement; by such means as requirements setting exercises, prototype demonstrations and evaluations.</p> <p>k) Risk management; that is, management of the areas of the project that involve potential technical, cost, or schedule risks.</p> <p>l) Security policy; that is, the rules for need-to-know and access-to-information at each project organization level.</p> <p>m) Approval required by such means as regulations, required certifications, proprietary, usage, ownership, warranty and licensing rights.</p> <p>n) Means for scheduling, tracking, and reporting.</p> <p>o) Training of personnel (see subclause 6.2.4).</p> <p>6.1.2.3.4.6 The supplier shall implement and execute the project management plan(s) developed under subclause 6.1.2.3.4.5.</p> <p>6.1.2.3.4.7 The supplier shall:</p> <p>a) Develop the software</p>

Systems (15288) Acquisition process	Systems (15288) Supply process	Software (12207) Acquisition process	Software (12207) Supply process
			<p>product in accordance with the Technical Processes (subclause 6.4).</p> <p>b) Operate the software product in accordance with the Software Operation Process (subclause 6.4.9).</p> <p>c) Maintain the software product in accordance with the Software Maintenance Process (subclause 6.4.10).</p> <p>6.1.2.3.4.8 The supplier shall monitor and control the progress and the quality of the software products or services of the project throughout the contracted life cycle. This shall be an ongoing, iterative task, which shall provide for:</p> <p>a) Monitoring progress of technical performance, costs, and schedules and reporting of project status.</p> <p>b) Problem identification, recording, analysis, and resolution.</p> <p>6.1.2.3.4.9 The supplier shall manage and control the subcontractors in accordance with the Acquisition Process (subclause 6.1.1). The supplier shall pass down all contractual requirements necessary to ensure that the software product or service delivered to the acquirer is developed or performed in accordance with the prime-contract requirements.</p> <p>6.1.2.3.4.10 The supplier shall interface with the</p>

Systems (15288) Acquisition process	Systems (15288) Supply process	Software (12207) Acquisition process	Software (12207) Supply process
			<p>independent verification, validation, or test agent as specified in the contract and project plans.</p> <p>6.1.2.3.4.11 The supplier shall interface with other parties as specified in the contract and project plans.</p> <p>6.1.2.3.4.12 The supplier should coordinate contract review activities, interfaces, and communication with the acquirer's organization.</p> <p>6.1.2.3.4.13 The supplier shall conduct or support the informal meetings, acceptance review, acceptance testing, joint reviews, and audits with the acquirer as specified in the contract and project plans. The joint reviews shall be conducted in accordance with subclause 7.2.6, audits in accordance with subclause 7.2.7.</p> <p>6.1.2.3.4.14 The supplier should perform verification and validation in accordance with subclauses 7.2.4 and 7.2.5 respectively to demonstrate that the software products or services and processes fully satisfy their respective requirements.</p> <p>6.1.2.3.4.15 The supplier shall make available to the acquirer the reports of evaluation, reviews, audits, testing, and problem resolutions as specified in the contract.</p> <p>6.1.2.3.4.16 The supplier shall provide the acquirer</p>

Systems (15288) Acquisition process	Systems (15288) Supply process	Software (12207) Acquisition process	Software (12207) Supply process
			<p>access to the supplier's and subcontractors' facilities for review of software products or services as specified in the contract and project plans.</p> <p>6.1.2.3.4.17 The supplier shall perform quality assurance activities in accordance with subclause 7.2.3.</p>
<p>e) Accept the product or service. This activity consists of the following tasks:</p> <p>1) Confirm that the delivered product or service complies with the agreement.</p> <p>NOTE Exceptions that arise during the conduct of the agreement or with the delivered product or service are resolved according to the procedures established in the agreement.</p>	<p>e) Deliver and support the product or service. This activity consists of the following tasks:</p> <p>1) Deliver the product or service in accordance with the agreement criteria.</p> <p>2) Provide assistance to the acquirer in support of the delivered system or service in accordance with the agreement criteria.</p>	<p>6.1.1.3.6 Acquirer acceptance. This activity consists of the following tasks:</p> <p>6.1.1.3.6.1 The acquirer should prepare for acceptance based on the defined acceptance strategy and criteria. The preparation of test cases, test data, test procedures, and test environment should be included. The extent of supplier involvement should be defined.</p> <p>6.1.1.3.6.2 The acquirer shall conduct acceptance review and acceptance testing of the deliverable software product or service and shall accept it from the supplier when all acceptance conditions are satisfied. The acceptance procedure should comply with the provisions of subclause 6.1.1.3.1.9.</p> <p>6.1.1.3.6.3 After acceptance, the acquirer should take the responsibility for the configuration management of the delivered software product (see subclause 7.2.2).</p>	<p>6.1.2.3.5 Product/service delivery and support. This activity consists of the following tasks:</p> <p>6.1.2.3.5.1 The supplier shall deliver the software product or service as specified in the contract.</p> <p>NOTE When required by the agreement, the supplier should install the product in accordance with established requirements.</p> <p>6.1.2.3.5.2 The supplier shall provide assistance to the acquirer in support of the delivered software product or service as specified in the contract.</p>

Systems (15288) Acquisition process	Systems (15288) Supply process	Software (12207) Acquisition process	Software (12207) Supply process
		NOTE The acquirer may install the software product or perform the software service in accordance with instructions defined by the supplier.	
2) Make payment or provide other agreed consideration to the supplier for the product or service rendered that is required for closure of the agreement.	<p>f) Close the agreement. This activity consists of the following tasks:</p> <p>1) Accept and acknowledge payment or other agreed consideration.</p> <p>2) Transfer the responsibility for the product or service to the acquirer, or other party, as directed by the agreement to obtain closure of the agreement.</p>	<p>6.1.1.3.7 Closure. This activity consists of the following tasks:</p> <p>6.1.1.3.7.1 The acquirer shall make payment or provide other agreed consideration to the supplier for the product or service rendered.</p> <p>NOTE 1 When the supplied product or service has satisfied the conditions of the agreement and identified open items have been satisfactorily closed, the acquirer concludes the agreement by rendering payment or other agreed consideration and notification of conclusion of the agreement.</p> <p>NOTE 2 A product or service may be supplied incrementally and payment or other agreed consideration may be provided in increments.</p>	<p>6.1.2.3.6 Closure. This activity consists of the following tasks:</p> <p>6.1.2.3.6.1 The supplier shall accept and acknowledge payment or other agreed consideration.</p> <p>6.1.2.3.6.2 The supplier shall transfer the responsibility for the product or service to the acquirer, or other party, as directed by the agreement.</p> <p>NOTE The agreement should address terms and authorization for initiating closure of the project.</p>

Annex B (informative)

Clause 6 Mapping to ISO/IEC 27002

ISO/IEC 27036 Clause/Subclause	ISO/IEC 27002 Clause/Subclause
6 ICT supply chain security in Lifecycle Processes	See individual processes for specific mapping
6.1 Agreement Processes	5. Security Policies 6. Organization of Information Security 15. Supplier Relationships 18. Compliance
6.1.1 Acquisition Processes	See 6.1 mapping
6.1.2 Supply Process	See 6.1 mapping
6.2 Organization Project-Enabling Processes	See individual processes for specific mapping
6.2.1 Lifecycle Model Management Process	None
6.2.2 Infrastructure Management Process	8. Asset Management 9. Access Control 10. Cryptography 11. Physical and Environmental Security 12. Operations Security 13. Communications Security 16. Information Security Incident Management 17. Information Security aspects of Business Continuity Management
6.2.3 Project Portfolio Management Process	None
6.2.4 Human Resource Management Process	7. Human Resources Security
6.2.5 Quality Management Process	14.2 Security in development and support processes 14.3 Test data
6.3 Project Processes	See individual processes for specific mapping

ISO/IEC 27036 Clause/Subclause	ISO/IEC 27002 Clause/Subclause
6.3.1 Project Planning Processes	None
6.3.2 Project Assessment and Control Process	None
6.3.3 Decision Management Process	None
6.3.4 Risk Management Process	ISO/IEC 27005
6.3.5 Configuration Management Process	12.1.2 Change management
6.3.6 Information Management Process	12.1.1 Documented operating procedures 13.2.1 Information transfer 18. Compliance
6.3.7 Measurement Process	ISO/IEC 27004
6.4 Technical Processes	See individual processes for specific mapping
6.4.1 Stakeholder Requirements Definition Process	14.1 Security requirements of information systems
6.4.2 Requirements Analysis Processes	14.1 Security requirements of information systems
6.4.3 Architectural Design Processes	None
6.4.4 Implementation Processes	14.2 Security in development and support processes
6.4.5 Integration Process	14.2 Security in development and support processes
6.4.6 Verification Process	14.2 Security in development and support processes 14.3 Test data
6.4.7 Transition Process	15. Supplier Relationships
6.4.8 Validation Process	14.2 Security in development and support processes 14.3 Test data
6.4.9 Operation Process	8. Asset Management 9. Access Control 10. Cryptography 12. Operations Security

ISO/IEC 27036 Clause/Subclause	ISO/IEC 27002 Clause/Subclause
	<p>13. Communications Security</p> <p>16. Information Security Incident Management</p> <p>17. Information Security aspects of Business Continuity Management</p> <p>18. Compliance</p>
6.4.10 Maintenance Process	<p>8.3. Media Handling</p> <p>13. Communications Security</p> <p>17. Information Security aspects of Business Continuity Management</p>
6.4.11 Disposal Process	<p>8. Asset Management</p> <p>13.2. Information Transfer</p>

Bibliography

- [1] ISO/IEC 15288, *Systems and software engineering — System life cycle processes*
- [2] ISO/IEC 12207, *Systems and software engineering — Software life cycle processes*
- [3] ISO/IEC 15026, *Systems and software engineering — Systems and Software Assurance*
- [4] ISO/IEC 27004, *Information security management systems – Information security management measurement*
- [5] ISO/IEC 27005, *Information security management systems – Information security risk management*
- [6] ISO/IEC 27007, *Information security management systems – Information security management – Guidelines for information security management systems auditing*
- [7] ISO/IEC 28001, *Security management systems for the supply chain -- Best practices for implementing supply chain security, assessments and plans -- Requirements and guidance*
- [8] ISO/IEC 20000-1, *Information technology -- Service management -- Part 1: Service management system requirements*
- [9] 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
- [10] SAFECode, *Software Integrity Controls, An Assurance-Based Approach to Minimizing Risks in the Software Supply Chain*, June 14, 2010
- [11] National Institute of Standards and Technology Interagency Report 7622, *Piloting Information Supply Chain Risk Management for Federal Information*, June 2010


**EXPLANATORY REPORT
RAPPORT EXPLICATIF**
ISO/IEC DIS 27036-3
ISO/IEC JTC 1/SC 27

 Secretariat **DIN**

This form should be sent to the ISO Central Secretariat, together with the English and French versions of the committee draft, by the secretariat of the technical committee or subcommittee concerned.

Ce formulaire doit être envoyé au Secrétariat central de l'ISO en même temps que les versions anglaise et française du projet de comité, par le secrétariat du comité technique ou du sous-comité concerné.

The accompanying document is submitted for circulation to member body vote as a DIS, following consensus obtained from the P-members of the committee.

Le document ci-joint est soumis, pour diffusion comme DIS, au vote comité membre, suite au consensus des membres (P) du comité obtenu.

 on **2012-10-26**

☒ at the meeting of **TC 1 / SC 27 / WG 4**
à la réunion du

see resolution No. **35** in document **N11941**
voir résolution n° dans le

☐ by postal ballot initiated on
par un vote par correspondance démarré le

P-members in favour: Membres (P) approuvant le projet:	Number 18	Countries Belgium, China, Czech Republic, Denmark, Ireland, Italy, Kenya, Korea, Republic of, Luxembourg, Mexico, Norway, Romania, Russian Federation, Slovenia, Sweden, Thailand, Ukraine, United States
P-members voting against: Membres (P) désapprouvant:	3	Japan, Netherlands, United United Kingdom*
P-members abstaining: Membres (P) s'abstenant:	16	Australia, Brazil, Canada**, Finland**, Germany**, India**, Kazakhstan, Malaysia**, Morocco, New Zealand, Poland, South Africa**, Spain, Switzerland, Uruguay
P-members who did not vote: Membres (P) n'ayant pas voté:	11	Algeria, Austria, Côte d'Ivoire, Cyprus, Estonia, France, Mauritius, Singapore, Slovakia, Sri Lanka, United Arab Emirates

Remarks/Remarques

The 1st CD document was circulated as SC 27 N11016. The summary of voting is presented in SC 27 N11527. Additional National Body comments were circulated as SC 27 N11538 and SC 27 N11656. The disposition of comments is shown in SC 27 N11996. The text for a 3-month DIS balloting is contained in N11997.

* Negative votes of the National Bodies indicated have been satisfactorily resolved and changed to APPROVAL.

** National Bodies indicated changed their votes to APPROVAL.

I hereby confirm that this draft meets the requirements of part 2 of the ISO/IEC Directives
Je confirme que ce projet satisfait aux prescriptions de la partie 2 des Directives ISO/CEI

Date

Name and signature of the secretary
Nom et signature du secrétaire

2012-11-14
Krystyna Passia

Result of voting

Ballot Information

Ballot reference	ISO/IEC CD 27036-3
Ballot type	CD
Ballot title	Information technology -- Security techniques -- Information security for supplier relationships -- Part 3: Guidelines for ICT supply chain security
Opening date	2012-06-01
Closing date	2012-09-01
Note	<p>1st CD Registration and Consideration</p> <p>In accordance with resolution 6 (see SC 27 N11330) of the 24</p> <p>th SC 27 Plenary meeting held in Stockholm, Sweden (14th and 15th May 2012) the attached document has been registered with the ISO Central Secretariat (ITTF) as a 1st Committee Draft (CD) and is hereby circulated for a 1st CD letter ballot closing by</p> <p>2012-09-01</p>

Member responses:

Votes cast (35)	<p>Australia (SA)</p> <p>Belgium (NBN)</p> <p>Brazil (ABNT)</p> <p>Canada (SCC)</p> <p>China (SAC)</p> <p>Czech Republic (UNMZ)</p> <p>Denmark (DS)</p> <p>Finland (SFS)</p> <p>India (BIS)</p> <p>Ireland (NSAI)</p> <p>Italy (UNI)</p> <p>Japan (JISC)</p> <p>Kazakhstan (KAZMEMST)</p> <p>Kenya (KEBS)</p> <p>Korea, Republic of (KATS)</p> <p>Luxembourg (ILNAS)</p> <p>Malaysia (DSM)</p> <p>Mexico (DGN)</p>
------------------------	--

	Morocco (IMANOR) Netherlands (NEN) New Zealand (SNZ) Norway (SN) Poland (PKN) Romania (ASRO) Russian Federation (GOST R) Slovenia (SIST) South Africa (SABS) Spain (AENOR) Sweden (SIS) Switzerland (SNV) Thailand (TISI) Ukraine (DSSU) United Kingdom (BSI) United States (ANSI) Uruguay (UNIT)
Comments submitted (0)	
Votes not cast (12)	Algeria (IANOR) Austria (ASI) Côte d'Ivoire (CODINORM) Cyprus (CYS) Estonia (EVS) France (AFNOR) Germany (DIN) Mauritius (MSB) Singapore (SPRING SG) Slovakia (SUTN) Sri Lanka (SLSI) United Arab Emirates (ESMA)

Questions:	
Q.1	"Do you agree with approval of the CD text?"
Q.2	"If you approve the CD text with comments, would you please indicate which type ? (General, Technical or Editorial)"
Q.3	"If you disapprove the draft, would you please indicate if you accept to change your vote to Approval if the reasons and appropriate changes will be accepted?"

Votes by members	Q.1	Q.2	Q.3
Australia (SA)	Abstention	Ignore	Ignore
Belgium (NBN)	Approval as presented	Ignore	Ignore
Brazil (ABNT)	Abstention	Ignore	Ignore
Canada (SCC)	Abstention	Ignore	Ignore
China (SAC)	Approval with comments	All	Ignore
Czech Republic (UNMZ)	Approval as presented	Ignore	Ignore
Denmark (DS)	Approval as	Ignore	Ignore

	presented		
Finland (SFS)	Abstention	Ignore	Ignore
India (BIS)	Abstention	Ignore	Ignore
Ireland (NSAI)	Approval as presented	Ignore	Ignore
Italy (UNI)	Approval as presented	Ignore	Ignore
Japan (JISC)	Disapproval of the draft	Ignore	No
Kazakhstan (KAZMEMST)	Abstention	Ignore	Ignore
Kenya (KEBS)	Approval as presented	Ignore	Ignore
Korea, Republic of (KATS)	Approval as presented	Ignore	Ignore
Luxembourg (ILNAS)	Approval as presented	Ignore	Ignore
Malaysia (DSM)	Abstention	Ignore	Ignore
Mexico (DGN)	Approval as presented	Ignore	Ignore
Morocco (IMANOR)	Abstention	Ignore	Ignore
Netherlands (NEN)	Disapproval of the draft	General	No
New Zealand (SNZ)	Abstention	Ignore	Ignore
Norway (SN)	Approval as presented	Ignore	Ignore
Poland (PKN)	Abstention	Ignore	Ignore
Romania (ASRO)	Approval as presented	Ignore	Ignore
Russian Federation (GOST R)	Approval as presented	Ignore	Ignore
Slovenia (SIST)	Approval as presented	Ignore	Ignore
South Africa (SABS)	Abstention	Ignore	Ignore
Spain (AENOR)	Abstention	Ignore	Ignore
Sweden (SIS)	Approval as presented	Ignore	Ignore
Switzerland (SNV)	Abstention	Ignore	Ignore
Thailand (TISI)	Approval as presented	Ignore	Ignore
Ukraine (DSSU)	Approval as presented	Ignore	Ignore
United Kingdom (BSI)	Disapproval of the draft	All	No
United States (ANSI)	Approval with	All	Ignore

	comments		
Uruguay (UNIT)	Abstention	Ignore	Ignore

Answers to Q.1: "Do you agree with approval of the CD text?"

16 x	Approval as presented	Belgium (NBN) Czech Republic (UNMZ) Denmark (DS) Ireland (NSAI) Italy (UNI) Kenya (KEBS) Korea, Republic of (KATS) Luxembourg (ILNAS) Mexico (DGN) Norway (SN) Romania (ASRO) Russian Federation (GOST R) Slovenia (SIST) Sweden (SIS) Thailand (TISI) Ukraine (DSSU)
2 x	Approval with comments	China (SAC) United States (ANSI)
3 x	Disapproval of the draft	Japan (JISC) Netherlands (NEN) United Kingdom (BSI)
14 x	Abstention	Australia (SA) Brazil (ABNT) Canada (SCC) Finland (SFS) India (BIS) Kazakhstan (KAZMEMST) Malaysia (DSM) Morocco (IMANOR) New Zealand (SNZ) Poland (PKN) South Africa (SABS) Spain (AENOR) Switzerland (SNV) Uruguay (UNIT)

Answers to Q.2: "If you approve the CD text with comments, would you please indicate which type ? (General, Technical or Editorial)"

1 x	General	Netherlands (NEN)
0 x	Technical	
0 x	Editorial	
3 x	All	China (SAC) United Kingdom (BSI) United States (ANSI)
31 x	Ignore	Australia (SA) Belgium (NBN)

		Brazil (ABNT) Canada (SCC) Czech Republic (UNMZ) Denmark (DS) Finland (SFS) India (BIS) Ireland (NSAI) Italy (UNI) Japan (JISC) Kazakhstan (KAZMEMST) Kenya (KEBS) Korea, Republic of (KATS) Luxembourg (ILNAS) Malaysia (DSM) Mexico (DGN) Morocco (IMANOR) New Zealand (SNZ) Norway (SN) Poland (PKN) Romania (ASRO) Russian Federation (GOST R) Slovenia (SIST) South Africa (SABS) Spain (AENOR) Sweden (SIS) Switzerland (SNV) Thailand (TISI) Ukraine (DSSU) Uruguay (UNIT)
--	--	--

Answers to Q.3: "If you disapprove the draft, would you please indicate if you accept to change your vote to Approval if the reasons and appropriate changes will be accepted?"

0 x	Yes	
3 x	No	Japan (JISC) Netherlands (NEN) United Kingdom (BSI)
32 x	Ignore	Australia (SA) Belgium (NBN) Brazil (ABNT) Canada (SCC) China (SAC) Czech Republic (UNMZ) Denmark (DS) Finland (SFS) India (BIS) Ireland (NSAI) Italy (UNI) Kazakhstan (KAZMEMST) Kenya (KEBS) Korea, Republic of (KATS) Luxembourg (ILNAS) Malaysia (DSM) Mexico (DGN) Morocco (IMANOR) New Zealand (SNZ) Norway (SN)

Poland (PKN) Romania (ASRO) Russian Federation (GOST R) Slovenia (SIST) South Africa (SABS) Spain (AENOR) Sweden (SIS) Switzerland (SNV) Thailand (TISI) Ukraine (DSSU) United States (ANSI) Uruguay (UNIT)
--

Comments from Voters		
Member:	Comment:	Date:
China (SAC)	<i>Comment File</i>	2012-08-27 10:01:23
CommentFiles/ISO_IEC_CD_27036-3_SAC.doc		
Japan (JISC)	<i>Comment File</i>	2012-08-29 04:42:29
CommentFiles/ISO_IEC_CD_27036-3_JISC.doc		
Netherlands (NEN)	<i>Comment File</i>	2012-08-16 14:11:33
CommentFiles/ISO_IEC_CD_27036-3_NEN.doc		
United Kingdom (BSI)	<i>Comment File</i>	2012-08-28 13:21:09
CommentFiles/ISO_IEC_CD_27036-3_BSI.doc		
United States (ANSI)	<i>Comment File</i>	2012-08-31 16:50:58
CommentFiles/ISO_IEC_CD_27036-3_ANSI.doc		

Comments from Commenters		
Member:	Comment:	Date: