Technical Report

ISO/IEC TR 33022

First edition
2024-10

Information technology — Process assessment — Application of ISO/IEC/IEEE 12207 processes to the ISO/IEC 33020 process capability measurement scale

Technologies de l'information — Évaluation du processus — Application des processus ISO/IEC/IEEE 12207 à l'échelle de la mesure de la capacité de procesus de l'ISO/IEC 33020

Reference number
ISO/IEC TR 33022:2024(en)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

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

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

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

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

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

This document was prepared by Technical Committee ISO/IEC JTC1, *Information technology*, Subcommittee SC 7, *Software and systems engineering*.

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

Introduction

This document provides a specification for mapping the ISO/IEC/IEEE 12207 life cycle processes to the ISO/IEC 33020 process attributes with the intent of demonstrating support for the levels 1 to 3 of the ISO/IEC 33020 process capability measurement framework.

This document is primarily addressed to developers of process assessment models for the process quality characteristic of process capability. It is also addressed to the lead assessor and other stakeholders, such as the sponsor of the assessment, who need to be assured that the requirements of the ISO/IEC 33020 process measurement framework have been met.

Within this document:

— Clause 4 provides a summary description of the relationship between the ISO/IEC 33020 process attribute outcomes and the ISO/IEC/IEEE 12207 life cycle processes.

— Annex A extends the summary mapping in Clause 4 by providing details of the relationship between the process attribute outcomes and the life cycle process outcomes. Links to the information items listed in Annex C are identified. These details are provided for validating by inspection the relationships between the process attribute outcomes of ISO/IEC 33020 and the ISO/IEC/IEEE 12207 life cycle process outcomes.

— Annex B focuses on the relationships between the generic practices associated with ISO/IEC 33020 and the task descriptions of ISO/IEC/IEEE 12207. These model elements are linked via the information item characteristics listed in Annex C.

— Annex C provides a listing of the applicable information items and their characteristics.

— Annex D provides an overview of the key concerns arising from the application of ISO/IEC/IEEE 24774 when attempting to demonstrate objective relationships between process model elements.

Information technology — Process assessment — Application of ISO/IEC/IEEE 12207 processes to the ISO/IEC 33020 process capability measurement scale

1 Scope

This document provides a specification for associating the life cycle processes of ISO/IEC/IEEE 12207 with the process attribute outcomes of ISO/IEC 33020 with the intent of demonstrating support for levels 1 to 3 of the process capability measurement scale defined in ISO/IEC 33020.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 33001, *Information technology — Process assessment — Concepts and terminology*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 33001 apply.

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

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

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

4 Content of the process capability measurement framework

4.1 General

In ISO/IEC 33020:2019, Clause 5, the relationship between process attributes and process capability levels is described.

Process capability is defined in ISO/IEC 33020:2019, Clause 5 on a six-point ordinal scale that enables process capability to be assessed from the bottom of the scale, 'incomplete', through to the top end of the scale, 'innovating'. The scale represents increasing capability of an implemented process, from failing to achieve the process purpose through to continually improving and able to respond to process change.

The relationship between the process capability levels and the process attributes is shown in Table 1. In addition, a summary view is presented of the relationship of the process attributes to the life cycle processes associated with ISO/IEC/IEEE 12207.

Two processes from ISO/IEC/IEEE 12207 do not appear in the list in Table 1, namely, the acquisition and decision management processes. These outcomes of these processes do not have any discernible relationships to the process attribute outcomes of ISO/IEC 33020.

Certain ISO/IEC/IEEE 12207 processes have been partitioned into sub processes, namely life cycle model management, infrastructure management, human resource management, knowledge management, quality management, measurement and quality assurance. This action has been taken to address outcomes in the basic processes that deal with firstly, establishment concerns, and secondly, performance (or operational)

concerns. The 'establishment' outcomes of these sub processes are mapped to ISO/IEC 33020:2019 PA 3.1 concerns. The 'performance' concerns of the sub processes are mapped to either PA 3.2 or PA 3.3, as appropriate.

As an example, with reference to ISO/IEC/IEEE 12207:2017, 6.2.1, life cycle model management, the basic and sub process outcomes are presented in Table 1.

Table 1 — ISO/IEC/IEEE 12207:2017, 6.2.1, life cycle model management

Basic process outcomes	Sub process: Establish	Sub process: Perform
a) Organizational policies and procedures for the management and deployment of life cycle models and processes are established.	a) Organizational policies and procedures for the management and deployment of life cycle models and processes are established.	
b) Responsibility, accountability, and authority within life cycle policies, processes, models, and procedures are defined.	b) Responsibility, accountability, and authority within life cycle policies, processes, models, and procedures are defined.	
c) Life cycle models and processes for use by the organization are assessed.		c) Life cycle models and processes for use by the organization are assessed.
d) Prioritized process, model, and procedure improvements are implemented.		d) Prioritized process, model, and procedure improvements are implemented.

The list of ISO/IEC/IEEE 12207 processes that have been mapped as sub processes is presented in Table 2.

Table 2 — ISO/IEC/IEEE 12207 processes mapped as sub processes

Basic process reference in ISO/IEC/IEEE 12207:2017	Basic processes	Sub process reference in ISO/IEC/IEEE 12207:2017	Sub processes
6.2.1	Life cycle model management	6.2.1.1	Life cycle model management: Establish
		6.2.1.2	Life cycle model management: Assess and improve
6.2.2	Infrastructure management	6.2.2.1	Infrastructure management: Establish
		6.2.2.2	Infrastructure management: Maintain
6.2.4	Human resource management	6.2.4.1	Human resource management: Establish
		6.2.4.2	Human resource management: Perform
6.2.5	Quality management	6.2.5.1	Quality management: Establish
		6.2.5.2	Quality management: Perform
6.2.6	Knowledge management	6.2.6.1	Knowledge management: Establish
		6.2.6.2	Knowledge management: Share and manage
6.3.7	Measurement	6.3.7.1	Measurement: Establish
		6.3.7.2	Measurement: Perform
6.3.8	Quality assurance	6.3.8.1	Quality assurance: Establish
		6.3.8.2	Quality assurance: Perform

The summary relationship between the ISO/IEC/IEEE 12207 processes and the ISO/IEC 33020 process capability levels is presented in Table 3.

Table 3 — Relationship between the ISO/IEC 33020 process capability levels and process attributes, and the ISO/IEC/IEEE 12207 life cycle processes

Process Capability Level	ISO/IEC 33020:2019 process attribute outcomes	Reference in ISO/IEC/IEEE 12207:2017	ISO/IEC/IEEE 12207:2017 life cycle processes
1	5.2.3.2 PA 1.1 Process performance process attribute	6.4	The processes in this group are typically identified in the assessment scope. The processes ISO/IEC/IEEE 12207:2017, 6.4 are likely candidates.
2	5.2.4.2 PA 2.1 Performance management process attribute	6.3.1	Project planning
		6.3.2	Project assessment and control
		6.3.4	Risk management
2	5.2.4.3 PA 2.2 Documented information management process attribute	6.3.5	Configuration management
		6.3.6	Information management
3	5.2.5.2 PA 3.1 Process definition process attribute	6.2.1.1	Life cycle model management: Establish
		6.2.2.1	Infrastructure management: Establish
		6.2.4.1	Human resource management: Establish
		6.2.5.1	Quality management: Establish
		6.2.6.1	Knowledge management: Establish
		6.3.7.1	Measurement: Establish
		6.3.8.1	Quality assurance: Establish
3	5.2.5.3 PA 3.2 Process deployment process attribute	6.2.1.2	Life cycle model management: Assess and improve
		6.2.2.2	Infrastructure management: Maintain
		6.2.3	Portfolio management
		6.2.4.2	Human resource management: Perform
		6.2.6.2	Knowledge management: Share and manage
3	5.2.5.4 PA 3.3 Process assurance process attribute	6.2.5.2	Quality management: Perform
		6.3.7.2	Measurement: Perform
		6.3.8.2	Quality assurance: Perform

4.2 Relationships between model elements

The rationale for the selection of the ISO/IEC/IEEE 12207 life cycle processes and their associations with the ISO/IEC 33020 process attribute outcomes can be found in Annexes A and B.

Annex A elaborates the summary mapping in Clause 4 by providing extended details of the relationship between the ISO/IEC 33020 process attribute outcomes and the ISO/IEC/IEEE 12207 life cycle process outcomes. Links to the information items described in Annex C are provided in a summary format. The level of detail provides the basis for validation by inspecting the relationships between the ISO/IEC 33020 process attribute outcomes and the ISO/IEC/IEEE 12207 life cycle process outcomes.

Annex B focuses on the relationships between the ISO/IEC 33020 generic practices and the ISO/IEC/IEEE 12207 activity/task descriptions. These model elements are linked via the information item characteristics, as listed in Annex C.

Annex A
(informative)

Associations between the ISO/IEC 33020 process attribute outcomes, ISO/IEC/IEEE 12207 life cycle process outcomes and information items

A.1 General

This annex describes the relationships between the ISO/IEC 33020 process attribute outcomes and the ISO/IEC/IEEE 12207 life cycle process outcomes. The model outcomes are linked by applicable information item characteristics, as described in Annex D.

A.2 Associations between the ISO/IEC 33020 process attribute outcomes, ISO/IEC/IEEE 12207 life cycle processes and information items

Information item characteristics provide the link between the ISO/IEC 33020 process attribute outcomes and the ISO/IEC/IEEE 12207 life cycle process outcomes. Each linked information item in Table A.1 is indicated by its reference label and name, and the reference number of the characteristic.

Table A.1 provides the basis for a detailed validation by inspection of the associations between the ISO/IEC 33020 process attribute outcomes and ISO/IEC/IEEE 12207 life cycle process outcomes in accordance with ISO/IEC/IEEE 24774:2021, Annex B model mapping considerations.

Table A.1 — Associations between the ISO/IEC 33020 process attribute outcomes, ISO/IEC/IEEE 12207 life cycle process outcomes and information item characteristics

ISO/IEC 33020:2019 process attribute outcomes	Description	ISO/IEC/IEEE 12207:2017	Description	ISO/IEC/IEEE 12207:2017
5.2.3.2	**PA 1.1 Process performance process attribute** 1) the process achieves its defined process outcomes.	6.1.2	**Supply** 1) An acquirer for a product or service is identified.	03-23 Request for proposal (RFP) 3) 04-28 Supply strategy 3)
		6.1.2	**Supply** 2) A response to the acquirer's request is produced.	03-24 Response to RFP 2) 08-65 RFP acquisition requirements review record 2)
		6.1.2	**Supply** 3) An agreement is established between the acquirer and supplier.	01-2 Supply agreement 5), 6)
		6.1.2	**Supply** 4) A product or service is provided.	08-07 Agreement performance review record 6) 08-75 Supply Delivery Records (for system, software, product or service) 3)

Table A.1 *(continued)*

ISO/IEC 33020:2019 process attribute outcomes	Description	ISO/IEC/IEEE 12207:2017	Description	ISO/IEC/IEEE 12207:2017
		6.1.2	**Supply** 5) Supplier obligations defined in the agreement are satisfied.	08-52 Product acceptance record 8) 08-73 Supplier payment receipt record 2) 11-6 Request for Supply (e.g., Request for Proposal, Request for Tender) 1)
		6.1.2	**Supply** 6) Responsibility for the acquired product or service, as directed by the agreement, is transferred.	08-52 Product acceptance record 6)
		6.4.1	**Business or mission analysis** 1) The problem or opportunity space is defined.	03-08 Identify business opportunities 6) 04-02 Business strategy 3) 08-10 Business opportunities review record 3)
		6.4.1	**Business or mission analysis** 2) The solution space is characterized.	03-08 Identify business opportunities 7)
		6.4.1	**Business or mission analysis** 3) Preliminary operational concepts and other concepts in the life cycle stages are defined.	03-07 Business opportunity space 7)
		6.4.1	**Business or mission analysis** 4) Candidate alternative solution classes are identified and analysed.	03-07 Business opportunity space 8)
		6.4.1	**Business or mission analysis** 5) The preferred candidate alternative solution class(es) are selected.	08-09 Business opportunities evaluation record 6), 7)
		6.4.1	**Business or mission analysis** 6) Any enabling systems or services needed for business or mission analysis are available.	08-20 Enabling system records: Business or Mission Analysis. 1), 2)
		6.4.2	**Stakeholder needs and requirements definition** 1) Stakeholders of the system are identified.	02-2 Stakeholders 3) 04-29 System requirements definition strategy 3)
		6.4.2	**Stakeholder needs and requirements definition** 2) Required characteristics and context of use of capabilities and concepts in the life cycle stages, including operational concepts, are defined.	03-31 Stakeholder Needs 11) 03-32 System operational concept 7), 8)
		6.4.2	**Stakeholder needs and requirements definition** 3) Constraints on a system are identified.	12-11 System stakeholder requirements 13)
		6.4.2	**Stakeholder needs and requirements definition** 4) Stakeholder needs are defined.	03-31 Stakeholder Needs 12), 14)
		6.4.2	**Stakeholder needs and requirements definition** 5) Stakeholder needs are prioritized and transformed into clearly defined stakeholder requirements.	03-02 Analyse stakeholder requirements 8), 9), 11) 03-31 Stakeholder Needs 13)
		6.4.2	**Stakeholder needs and requirements definition** 6) Critical performance measures are defined.	12-11 System stakeholder requirements 14), 15)

Table A.1 *(continued)*

ISO/IEC 33020:2019 process attribute outcomes	Description	ISO/IEC/IEEE 12207:2017	Description	ISO/IEC/IEEE 12207:2017
		6.4.2	**Stakeholder needs and requirements definition** 7) Stakeholder agreement that their needs and expectations are reflected adequately in the requirements is achieved.	03-02 Analyse stakeholder requirements 10) 08-44 Manage stakeholder requirements 3)
		6.4.2	**Stakeholder needs and requirements definition** 8) Any enabling systems or services needed for stakeholder needs and requirements are available.	08-27 Enabling system records: Stakeholder needs and requirements 1), 2)
		6.4.3	**System/software requirements definition** 1) The system or element description, including interfaces, functions and boundaries, for a system solution is defined.	03-34 System requirements definition 5), 6) 12-10 System requirements 16)
		6.4.3	**System/software requirements definition** 2) System/software requirements (functional, performance, process, non-functional, and interface) and design constraints are defined.	12-10 System requirements 18), 19), 20)
		6.4.3	**System/software requirements definition** 3) Critical performance measures are defined.	12-10 System requirements 17)
		6.4.3	**System/software requirements definition** 4) The system/software requirements are analysed.	03-33 System requirements analysis 11), 12), 13), 14)
		6.4.3	**System/software requirements definition** 5) Any enabling systems or services needed for system/software requirements definition are available.	08-29 Enabling system records: System/software requirements 1), 2)
		6.4.3	**System/software requirements definition** 6) Traceability of system/software requirements to stakeholder requirements is developed.	08-45 Manage system requirements 3)
		6.4.4	**Architecture definition** 1) Identified stakeholder concerns are addressed by the architecture.	03-03 Architecture definition 10), 11), 12), 13)
		6.4.4	**Architecture definition** 2) Architecture viewpoints are developed.	03-05 Architecture viewpoints 7), 8), 9), 10)
		6.4.4	**Architecture definition** 3) Context, boundaries, and external interfaces of the system are defined.	03-06 Architecture views 11)
		6.4.4	**Architecture definition** 4) Architecture views and models of the system are developed.	03-06 Architecture views 12), 13), 14), 15), 16)
		6.4.4	**Architecture definition** 5) Concepts, properties, characteristics, behaviours, functions, or constraints that are significant to architecture decisions of the system are allocated to architectural entities.	08-66 Requirements allocation 9), 12), 13)
		6.4.4	**Architecture definition** 6) System elements and their interfaces are identified.	08-66 Requirements allocation 10)

Table A.1 *(continued)*

ISO/IEC 33020:2019 process attribute outcomes	Description	ISO/IEC/IEEE 12207:2017	Description	ISO/IEC/IEEE 12207:2017
		6.4.4	**Architecture definition** 7) Architecture candidates are assessed.	08-08 Architecture assessment result 8), 9), 10)
		6.4.4	**Architecture definition** 8) An architectural basis for processes throughout the life cycle is achieved.	08-08 Architecture assessment result 11)
		6.4.4	**Architecture definition** 9) Alignment of the architecture with requirements and design characteristics is achieved.	08-41 Manage architecture 8), 9), 10), 11), 12) 08-66 Requirements allocation 11)
		6.4.4	**Architecture definition** 10) Any enabling systems or services needed for architecture definition are available.	08-19 Enabling system records: Architecture definition 1), 2)
		6.4.5	**Design definition** 1) Design characteristics of each system element are defined.	03-28 Software system design definition 5), 6) 03-29 Software system element design 12) 03-30 Software system element evaluation 9)
		6.4.5	**Design definition** 3) Design enablers necessary for design definition are selected or defined.	03-29 Software system element design 13)
		6.4.5	**Design definition** 4) Interfaces between system elements composing the system are defined or refined.	03-29 Software system element design 15)
		6.4.5	**Design definition** 5) Design alternatives for system elements are assessed.	03-29 Software system element design 14) 03-30 Software system element evaluation 10), 11), 12)
		6.4.5	**Design definition** 6) Design artifacts are developed.	03-29 Software system element design 16) 08-43 Manage software system element design 6)
		6.4.5	**Design definition** 7) Any enabling systems or services needed for design definition are available.	08-21 Enabling system records: Design definition 1), 2)
		6.4.5	**Design definition** 8) Traceability of the design characteristics to the architectural entities of the system architecture is established.	08-43 Manage software system element design 7)
		6.4.6	**System analysis** 1) System analyses needed are identified.	04-30 Systems analysis strategy 9), 10), 11), 12), 13)
		6.4.6	**System analysis** 2) System analysis assumptions and results are validated.	08-48 Perform systems analysis 8), 9), 10)
		6.4.6	**System analysis** 3) System analysis results are provided for decisions.	08-48 Perform systems analysis 11), 12)
		6.4.6	**System analysis** 4) Any enabling systems or services needed for system analysis are available.	08-28 Enabling system records: System analysis 1), 2)

Table A.1 *(continued)*

ISO/IEC 33020:2019 process attribute outcomes	Description	ISO/IEC/IEEE 12207:2017	Description	ISO/IEC/IEEE 12207:2017
		6.4.7	**Implementation** 1) Implementation constraints that influence the requirements, architecture, or design are identified.	04-07 Implementation Plan 6), 7)
		6.4.7	**Implementation** 2) A system element is realized.	07-8 Software element 9), 10), 11) 08-69 Software code & test evaluation record 5), 6)
		6.4.7	**Implementation** 3) A system element is packaged or stored.	08-42 Manage software elements 5), 6)
		6.4.7	**Implementation** 4) Any enabling systems or services needed for implementation are available.	08-23 Enabling system records: Implementation 1), 2)
		6.4.8	**Integration** 1) Integration constraints that influence system requirements, architecture, or design, including interfaces, are identified.	04-26 Software integration plan 11), 13)
		6.4.8	**Integration** 2) Approach and checkpoints for the correct operation of the assembled interfaces and system functions are defined.	04-26 Software integration plan 12)
		6.4.8	**Integration** 3) Any enabling systems or services needed for integration are available.	08-24 Enabling system records: Integration 1), 2)
		6.4.8	**Integration** 4) A system composed of implemented system elements is integrated.	07-6 Integrated system 9), 10)
		6.4.8	**Integration** 7) Integration results and anomalies are identified.	08-71 Software integration test results 3)
		6.4.9	**Verification** 1) Constraints of verification that influence the requirements, architecture, or design are identified.	04-32 Verification strategy 14), 15), 16), 17) 06-3 Verification Procedures 5)
		6.4.9	**Verification** 2) Any enabling systems or services needed for verification are available.	08-32 Enabling system records: Verification 1), 2)
		6.4.9	**Verification** 6) Verification results and anomalies are identified.	08-93 Verification problems and non-conformances 6), 7)
		6.4.10	**Transition** 1) Transition constraints that influence system/software requirements, architecture, or design are identified.	04-27 Software release plan 12), 13), 14), 15), 16)
		6.4.10	**Transition** 2) Any enabling systems or services needed for transition are available.	08-30 Enabling system records: Transition 1), 2)
		6.4.10	**Transition** 3) The site is prepared.	08-76 System/ software installation record 17), 18)
		6.4.10	**Transition** 4) The system, as installed in its operational location, is capable of delivering its specified functions.	08-76 System/ software installation record 19)
		6.4.10	**Transition** 5) Operators, users and other stakeholders necessary to the system utilization and support are trained.	08-76 System/ software installation record 20)

Table A.1 *(continued)*

ISO/IEC 33020:2019 process attribute outcomes	Description	ISO/IEC/IEEE 12207:2017	Description	ISO/IEC/IEEE 12207:2017
		6.4.10	**Transition** 6) Transition results and anomalies are identified.	08-72 Software operation release test results 5), 6)
		6.4.10	**Transition** 7) The installed system is activated and ready for operation.	08-76 System/ software installation record 21)
		6.4.11	**Validation** 1) Validation criteria for stakeholder requirements are defined.	04-31 Validation plan 14), 16), 17) 06-2 Validation Procedures 5)
		6.4.11	**Validation** 2) The availability of services required by stakeholders is confirmed.	08-90 Validation Records 2)
		6.4.11	**Validation** 3) Constraints of validation that influence the requirements, architecture, or design are identified.	04-31 Validation plan 15)
		6.4.11	**Validation** 4) The system or system element is validated.	06-2 Validation Procedures 6)
		6.4.11	**Validation** 5) Any enabling systems or services needed for validation are available.	08-31 Enabling system records: Validation 1), 2)
		6.4.11	**Validation** 6) Validation results and anomalies are identified.	08-90 Validation Records 4) 08-91 Validation problems and non-conformances 3)
		6.4.11	**Validation** 7) Objective evidence that the realized system or system element satisfies stakeholder needs is provided.	08-92 Validation test suite confirmation record 2)
		6.4.12	**Operation** 1) Operation constraints that influence system/software requirements, architecture, or design are identified.	04-15 Operation plan 8), 9), 10)
		6.4.12	**Operation** 2) Any enabling systems, services, and material needed for operation are available.	08-26 Enabling system records: Operation 1), 2)
		6.4.12	**Operation** 3) Trained, qualified operators are available.	04-15 Operation plan 11)
		6.4.12	**Operation** 4) System product services that meet stakeholder requirements are delivered.	08-46 Operation actions 13), 14), 16), 18)
		6.4.12	**Operation** 5) System product performance during operation is monitored.	08-46 Operation actions 15), 17) 11-4 Operation requests 9)
		6.4.12	**Operation** 6) Support to the customer is provided.	08-47 Operation records 7), 8) 11-4 Operation requests 7), 8)
		6.4.13	**Maintenance** 1) Maintenance constraints that influence system requirements, architecture, or design are identified.	04-14 Maintenance Plan 8), 9), 10), 11)
		6.4.13	**Maintenance** 2) Any enabling systems or services needed for maintenance are available.	08-25 Enabling system records: Maintenance 1), 2)

Table A.1 *(continued)*

ISO/IEC 33020:2019 process attribute outcomes	Description	ISO/IEC/IEEE 12207:2017	Description	ISO/IEC/IEEE 12207:2017
		6.4.13	**Maintenance** 3) Replacement, repaired, or revised system elements are made available.	09-07 Maintenance (Logistics) Report 10), 11), 12), 13) 11-3 Maintenance Requests 14), 15), 16), 17)
		6.4.13	**Maintenance** 4) The need for changes to address corrective, perfective, or adaptive maintenance is reported.	08-40 Maintenance (Logistics) Records 8) 11-3 Maintenance Requests 18), 19)
		6.4.13	**Maintenance** 5) Failure and lifetime data, including associated costs, is determined.	08-40 Maintenance (Logistics) Records 9), 10)
		6.4.14	**Disposal** 1) Disposal constraints are provided as inputs to requirements, architecture, design, and implementation.	04-06 Disposal strategy 6), 7), 8), 9)
		6.4.14	**Disposal** 2) Any enabling systems or services needed for disposal are available.	08-22 Enabling system records: Disposal 1), 2)
		6.4.14	**Disposal** 3) The system elements or waste products are destroyed, stored, reclaimed or recycled in accordance with requirements, e.g. , safety and security requirements.	08-17 Disposal Records 14), 15), 16), 17), 18), 19)
		6.4.14	**Disposal** 4) The environment is returned to its original or an agreed state.	08-17 Disposal Records 20)
		6.4.14	**Disposal** 5) Records of disposal actions and analysis are available.	08-17 Disposal Records 21)
5.2.4.2	**PA 2.1 Performance management process attribute** 1) results to be achieved are determined and communicated;	6.3.1	**Project planning** 1) Objectives and plans are defined.	03-17 Project goals 6), 7)
5.2.4.2	**PA 2.1 Performance management process attribute** 2) risks that can affect performance of the process are determined and addressed;	6.3.1	**Project planning** 1) Objectives and plans are defined.	04-25 Risk Management Plan 6), 7)
		6.3.4	**Risk management** 1) Risks are identified.	03-26 Risk identification 3) 03-27 Risk management profile 5), 6), 7)
		6.3.4	**Risk management** 2) Risks are analysed.	03-25 Risk analysis 6), 7), 8)
		6.3.4	**Risk management** 3) Risk treatment options are identified, prioritized, and selected.	08-67 Risk treatment evaluation 6), 7), 8)
		6.3.4	**Risk management** 4) Appropriate treatment is implemented.	08-67 Risk treatment evaluation 9)
		6.3.4	**Risk management** 5) Risks are evaluated to assess changes in status and progress in treatment.	09-16 Risk monitoring report 4), 5), 6)

Table A.1 *(continued)*

ISO/IEC 33020:2019 process attribute outcomes	Description	ISO/IEC/IEEE 12207:2017	Description	ISO/IEC/IEEE 12207:2017
5.2.4.2	**PA 2.1 Performance management process attribute** 3) performance of the process is planned, monitored, measured, evaluated and adjusted (as needed);	6.3.1	**Project planning** 1) Objectives and plans are defined.	04-03 Configuration Management Plan 8), 9) 04-08 Information management plan 11), 13) 04-20 Project budget 3) 04-21 Project plan 14) 04-22 Project schedule 3) 04-33 Work breakdown structure 4)
		6.3.2	**Project assessment and control** 1) Performance measures or assessment results are available.	04-19 Project assessment strategy 3) 09-13 Project status report 20), 27), 30)
		6.3.2	**Project assessment and control** 3) Adequacy of resources is assessed.	09-13 Project status report 24)
		6.3.2	**Project assessment and control** 4) Technical progress reviews are performed.	09-13 Project status report 22), 26)
		6.3.2	**Project assessment and control** 5) Deviations in project performance from plans are investigated and analysed.	09-13 Project status report 21), 25), 28)
		6.3.2	**Project assessment and control** 7) Corrective action is defined and directed, when project achievement is not meeting targets.	11-5 Project change request 9), 11)
		6.3.2	**Project assessment and control** 8) Project replanning is initiated, as necessary.	11-5 Project change request 10)
		6.3.2	**Project assessment and control** 9) Project action to progress (or not) from one scheduled milestone or event to the next is authorized.	08-55 Project continuation authorization record 1)
5.2.4.2	**PA 2.1 Performance management process attribute** 4) responsibilities and authorities for performing the process are determined, assigned and communicated;	6.3.1	**Project planning** 1) Objectives and plans are defined.	04-08 Information management plan 12)
		6.3.1	**Project planning** 2) Roles, responsibilities, accountabilities, and authorities are defined.	04-21 Project plan 11)
5.2.4.2	**PA 2.1 Performance management process attribute** 5) resources necessary for performing the process are determined, provided and maintained (as needed);	6.3.1	**Project planning** 1) Objectives and plans are defined.	04-21 Project plan 12)
		6.3.1	**Project planning** 3) Resources and services necessary to achieve the objectives are formally requested and committed.	04-21 Project plan 13) 08-59 Project resource request record 3)
		6.3.1	**Project planning** 4) Plans for the execution of the project are activated.	08-56 Project initiation authorization record 9), 10)
5.2.4.2	**PA 2.1 Performance management process attribute** 6) person(s) performing the process are competent on the basis of appropriate education, training, or experience;	6.3.2	**Project assessment and control** 2) Adequacy of roles, responsibilities, accountabilities, and authorities is assessed.	09-13 Project status report 23)

Table A.1 *(continued)*

ISO/IEC 33020:2019 process attribute outcomes	Description	ISO/IEC/IEEE 12207:2017	Description	ISO/IEC/IEEE 12207:2017
5.2.4.2	**PA 2.1 Performance management process attribute** 7) interfaces between the involved parties are managed to ensure both effective communication and the level of control expected.	6.3.1	**Project planning** 1) Objectives and plans are defined.	04-21 Project plan 15)
		6.3.2	**Project assessment and control** 6) Affected stakeholders are informed of project status.	09-13 Project status report 29)
5.2.4.3	**PA 2.2 Documented information management process attribute** 1) requirements for the documented information of the process are determined;	6.3.6	**Information management** 1) Information to be managed is identified.	04-10 Information management plan: item identification 1)
		6.3.6	**Information management** 2) Information representations are defined.	04-09 Information management plan: Presentation 1)
5.2.4.3	**PA 2.2 Documented information management process attribute** 3) documented information is appropriately identified, and controlled according to requirements;	6.3.5	**Configuration management** 1) Items requiring configuration management are identified and managed.	08-13 Configuration management identification records 10), 11)
		6.3.5	**Configuration management** 2) Configuration baselines are established.	12-03 Configuration Baseline 6), 7)
		6.3.5	**Configuration management** 3) Changes to items under configuration management are controlled.	08-06 Agreement impact evaluation record 3)
		6.3.5	**Configuration management** 4) Configuration status information is available.	09-02 Configuration Status Report 5), 6)
		6.3.6	**Information management** 1) Information to be managed is identified.	07-1 Information item 10), 11), 12), 13), 14), 15), 16), 18), 19), 20), 21), 22)
		6.3.6	**Information management** 5) Information is available to designated stakeholders.	07-3 Information item: Publish 1)
5.2.4.3	**PA 2.2 Documented information management process attribute** 4) documented information is reviewed and approved for suitability and adequacy in accordance with planned arrangements and adjusted as necessary to meet requirements;	6.3.5	**Configuration management** 3) Changes to items under configuration management are controlled.	08-11 Configuration Management Change Requests 9), 10), 11) 11-1 Agreement Change Request 5), 6)
5.2.4.3	**PA 2.2 Documented information management process attribute** 5) documented information is determined, maintained and retained to the extent necessary to have confidence that the process has been performed as planned and to demonstrate the conformity of products and/or services to their requirements.	6.3.6	**Information management** 3) Information is obtained, developed, transformed, stored, validated, presented, [and disposed of].	07-1 Information item 9), 17) 08-04 Agreement amendment record 3), 4) 08-61 Quality Assurance Records 4) 10-1 Information Item Archive 3)
		6.3.6	**Information management** 4) The status of information is identified.	07-2 Information item: Item status 1)
		6.3.6	**Information management** 5) Information is available to designated stakeholders.	08-61 Quality Assurance Records 5)
		6.3.6	**Information management** 6) Information is archived, or disposed of, as required.	08-33 Information item disposal record 3)

Table A.1 *(continued)*

ISO/IEC 33020:2019 process attribute outcomes	Description	ISO/IEC/IEEE 12207:2017	Description	ISO/IEC/IEEE 12207:2017
5.2.5.2	**PA 3.1 Process definition process attribute** 1) a standard process, including appropriate tailoring guidelines, is established and maintained that describes the fundamental elements that must be incorporated into a defined process;	6.2.1.1	**Life cycle model management: Establish** 1) Organizational policies and procedures for the management and deployment of life cycle models and processes are established.	03-10 Life cycle model 22), 23), 24), 25), 26), 27), 28)
		6.2.5.1	**Quality management: Establish** 1) Organizational quality management policies, objectives, and procedures are defined and implemented.	03-22 Quality management authorities and responsibilities 3) 04-23 Quality Management Plan 4)
		6.2.5.1	**Quality management: Establish** 2) Quality evaluation criteria and methods are established.	12-09 Quality evaluation criteria and methods 2)
		6.3.7.1	**Measurement: Establish** 1) Information needs are identified.	03-13 Organizational characteristics 2) 03-14 Organizational information needs 3) 04-11 Information measurement strategy 3), 4)
		6.3.7.1	**Measurement: Establish** 2) An appropriate set of measures, based on the information needs, is identified or developed.	03-09 Information measures 2)
		6.3.8.1	**Quality assurance: Establish** 1) Project quality assurance procedures are defined and implemented.	04-24 Quality assurance strategy 6)
		6.3.8.1	**Quality assurance: Establish** 2) Criteria and methods for quality assurance evaluations are defined.	04-24 Quality assurance strategy 7)
5.2.5.2	**PA 3.1 Process definition process attribute** 4) roles, competences, responsibilities and authorities for performing the standard process are determined;	6.2.1.1	**Life cycle model management: Establish** 2) Responsibility, accountability, and authority within life cycle policies, processes, models, and procedures are defined.	03-11 Life cycle model: Responsibilities 1)
		6.2.4.1	**Human resource management: Establish** 1) Skills required by projects are identified.	03-12 Organization skills identification 2) 03-15 Organizational skill needs 2)
5.2.5.2	**PA 3.1 Process definition process attribute** 5) resources for performing the standard process are determined;	6.2.2.1	**Infrastructure management: Establish** 1) The requirements for infrastructure are defined.	12-05 Infrastructure Requirements 5)
		6.2.2.1	**Infrastructure management: Establish** 2) The infrastructure elements are identified and specified.	04-12 Infrastructure plan 3)
5.2.5.2	**PA 3.1 Process definition process attribute** 6) knowledge necessary for the operation of the standard process is determined [and maintained].	6.2.1.1	**Life cycle model management: Establish** 1) Organizational policies and procedures for the management and deployment of life cycle models and processes are established.	04-13 Knowledge Management: Establish 6), 7), 8)
		6.2.6.1	**Knowledge management: Establish** 1) A taxonomy for the application of knowledge assets is identified.	12-06 Knowledge Management: Taxonomy 6), 7)

Table A.1 *(continued)*

ISO/IEC 33020:2019 process attribute outcomes	Description	ISO/IEC/IEEE 12207:2017	Description	ISO/IEC/IEEE 12207:2017
5.2.5.3	**PA 3.2 Process deployment process attribute** 1) a defined process is deployed based upon an appropriately tailored standard process;	6.2.1.2	**Life cycle model management: Assess and improve** 1) Life cycle models and processes for use by the organization are assessed.	04-17 Process Improvement Opportunity 3) 08-51 Process review result 4), 5)
		6.2.1.2	**Life cycle model management: Assess and improve** 2) Prioritized process, model, and procedure improvements are implemented.	04-18 Process Improvement plan 4)
		6.2.3	**Portfolio management** 2) Projects are identified.	03-19 Project portfolio goals 1)
5.2.5.3	**PA 3.2 Process deployment process attribute** 2) required roles, responsibilities and authorities necessary for performing the defined process are assigned and communicated;	6.2.3	**Portfolio management** 4) Project management responsibilities, accountability, and authorities are defined.	03-16 Project accountabilities and authorities 2)
5.2.5.3	**PA 3.2 Process deployment process attribute** 3) required person(s) necessary for performing the defined process are competent on the basis of defined education, training and experience;	6.2.4.2	**Human resource management: Perform** 1) Necessary human resources are provided to projects.	04-16 Organizational skills development plan 3) 12-08 Project skill needs and provision 6), 7), 8), 9)
		6.2.4.2	**Human resource management: Perform** 2) Skills of personnel are developed, maintained or enhanced.	07-7 Skills development resources 3) 08-68 Skill development records 3), 4)
		6.2.4.2	**Human resource management: Perform** 3) Conflicts in multi-project resource demands are resolved.	08-60 Project team interface conflict resolution 3)
5.2.5.3	**PA 3.2 Process deployment process attribute** 4) required resources necessary for performing the defined process are made available, monitored and measured;	6.2.2.2	**Infrastructure management: Maintain** 1) Infrastructure elements are developed or acquired.	08-36 Infrastructure provision record 3)
		6.2.2.2	**Infrastructure management: Maintain** 2) The infrastructure is available.	08-35 Infrastructure evaluation record 2) 11-2 Infrastructure Change Request 2)
		6.2.3	**Portfolio management** 3) Resources and budgets for each project are allocated.	03-20 Project resource allocation 2)
5.2.5.3	**PA 3.2 Process deployment process attribute** 5) knowledge necessary for the operation of the standard process is [determined and] maintained.	6.2.6.2	**Knowledge management: Share and manage** 1) The organizational knowledge, skills, and knowledge assets are developed or acquired.	08-37 Knowledge Asset Records 6), 7), 8)
		6.2.6.2	**Knowledge management: Share and manage** 2) The organizational knowledge, skills, and knowledge assets are available.	08-38 Knowledge Asset application 4), 5)
		6.2.6.2	**Knowledge management: Share and manage** 3) Knowledge management usage data is gathered and analysed.	08-39 Knowledge asset review record 3)

Table A.1 *(continued)*

ISO/IEC 33020:2019 process attribute outcomes	Description	ISO/IEC/IEEE 12207:2017	Description	ISO/IEC/IEEE 12207:2017
5.2.5.4	**PA 3.3 Process assurance process attribute** 1) appropriate data and information are collected and analysed from monitoring and measurement of the process to evaluate the effectiveness and risks of the process, and to identify needs and opportunities for improvement;	6.2.5.2	**Quality management: Perform** 2) Quality assurance evaluation results are gathered and analysed.	09-04 Corrective and preventive actions status report 4)
		6.3.7.2	**Measurement: Perform** 1) Required data is collected, verified, and stored.	07-4 Information measurement data item 2)
		6.3.7.2	**Measurement: Perform** 2) The data is analysed and the results interpreted.	07-5 Information product 2)
		6.3.8.2	**Quality assurance: Perform** 1) Evaluations of the project's products, services, and processes are performed, consistent with quality management policies, procedures, and requirements.	09-06 Incident Report 4)
		6.3.8.2	**Quality assurance: Perform** 3) Incidents are resolved.	09-06 Incident Report 5)
5.2.5.4	**PA 3.3 Process assurance process attribute** 3) conformity of the defined process (and associated activities, outputs and documented information) is objectively assured;	6.2.5.2	**Quality management: Perform** 2) Quality assurance evaluation results are gathered and analysed.	09-05 Customer satisfaction analysis report 3) 09-14 Quality assurance evaluation results 2)
		6.3.8.2	**Quality assurance: Perform** 1) Evaluations of the project's products, services, and processes are performed, consistent with quality management policies, procedures, and requirements.	08-70 Software code & test evaluation: Evaluation 1)
		6.3.8.2	**Quality assurance: Perform** 2) Results of evaluations are provided to relevant stakeholders.	08-70 Software code & test evaluation: Evaluation 2)
5.2.5.4	**PA 3.3 Process assurance process attribute** 4) action is taken on any nonconformity, based on its nature and effect, and tracked to closure;	6.2.5.2	**Quality management: Perform** 2) Quality assurance evaluation results are gathered and analysed.	09-15 Quality improvements status report 2)
		6.3.8.2	**Quality assurance: Perform** 2) Results of evaluations are provided to relevant stakeholders.	08-50 Problem status communication record 2)
5.2.5.4	**PA 3.3 Process assurance process attribute** 5) the standard process is continually improved based on identified needs and opportunities.	6.2.5.2	**Quality management: Perform** 1) Resources and information are provided to projects to support the operation and monitoring of project quality assurance activities.	08-63 Quality management resources 2)
		6.2.5.2	**Quality management: Perform** 3) Quality management policies and procedures are improved based upon project and organizational results.	04-04 Corrective and preventive actions plan 3), 4) 08-62 Quality assurance review records 3)

A.3 Generic information items – exceptions list

There are no exceptions in the mapping between process attribute outcomes and the selected life cycle process outcomes.

Annex B
(informative)

Associations between the ISO/IEC 33020 generic practices, ISO/IEC/IEEE 12207 life cycle process activities, tasks and information item characteristics

B.1 General

This clause presents a detailed perspective of the relationship between the ISO/IEC 33020 generic practices, the ISO/IEC/IEEE 12207 life cycle process activities and tasks, and the information item characteristics. See Table B.1.

Table B.1 — Associations between the ISO/IEC 33020 generic practices, ISO/IEC/IEEE 12207 activities and tasks and associated information item characteristics

ISO/IEC 33020:2019 Annex B Generic Practices	Description	ISO/IEC/IEEE 12207:2017	Description	ISO/IEC/IEEE 12207:2017
B3.1 PA.1.1.GP1	**Achieve the process outcomes** 2) Relevant information items to evidence achievement of the process outcomes are identified.	6.1.2.3 a)	**Prepare for the supply** 1) Determine the existence and identity of an acquirer who has a need for a product or service.	03-23 Request for proposal (RFP) 3)
		6.1.2.3 a)	**Prepare for the supply** 2) Define a supply strategy.	04-28 Supply strategy 3)
		6.1.2.3 b)	**Respond to a request for supply of products or services** 1) Evaluate a request for the supply of a product or service to determine feasibility and how to respond.	08-65 RFP acquisition requirements review record 2)
		6.1.2.3 b)	**Respond to a request for supply of products or services** 2) Prepare a response that satisfies the solicitation.	03-24 Response to RFP 2)
		6.1.2.3 c)	**Establish and maintain an agreement** 1) Negotiate an agreement with the acquirer that includes acceptance criteria.	01-2 Supply agreement 5)
		6.1.2.3 c)	**Establish and maintain an agreement** 2) Identify necessary changes to the agreement.	11-7 Supply agreement change request 3)
		6.1.2.3 c)	**Establish and maintain an agreement** 3) Evaluate impact of changes on the agreement.	08-06 Agreement impact evaluation record 3)
		6.1.2.3 c)	**Establish and maintain an agreement** 4) Negotiate the agreement with the acquirer, as necessary.	01-2 Supply agreement 6)
		6.1.2.3 c)	**Establish and maintain an agreement** 5) Update the agreement with the acquirer, as necessary.	08-04 Agreement amendment record 4)
		6.1.2.3 d)	**Execute the agreement** 1) Execute the agreement according to the established project plans.	08-07 Agreement performance review record 6)

Table B.1 *(continued)*

ISO/IEC 33020:2019 Annex B Generic Practices	Description	ISO/IEC/IEEE 12207:2017	Description	ISO/IEC/IEEE 12207:2017
		6.1.2.3 d)	**Execute the agreement** 2) Assess the execution of the agreement.	08-07 Agreement performance review record 7)
		6.1.2.3 e)	**Deliver and support the product or service** 1) Deliver the product or service in accordance with the agreement criteria.	08-75 Supply Delivery Records (for system, software, product or service) 3)
		6.1.2.3 e)	**Deliver and support the product or service** 3) Accept and acknowledge payment or other agreed consideration.	08-73 Supplier payment receipt record 2)
		6.1.2.3 e)	**Deliver and support the product or service** 4) Transfer the product or service to the acquirer, or other party, as directed by the agreement.	08-52 Product acceptance record 6)
		6.1.2.3 e)	**Deliver and support the product or service** 5) Close the agreement.	08-52 Product acceptance record 7)
		6.4.1.3 a)	**Prepare for Business or Mission Analysis** 1) Review identified problems and opportunities in the organization strategy with respect to desired organization goals or objectives.	08-10 Business opportunities review record 3)
		6.4.1.3 a)	**Prepare for Business or Mission Analysis** 2) Define the business or mission analysis strategy.	04-02 Business strategy 3)
		6.4.1.3 a)	**Prepare for Business or Mission Analysis** 3) Identify and plan for the necessary enabling systems or services needed to support business or mission analysis.	08-20 Enabling system records: Business or Mission Analysis. 1)
		6.4.1.3 a)	**Prepare for Business or Mission Analysis** 4) Obtain or acquire access to the enabling systems or services to be used.	08-20 Enabling system records: Business or Mission Analysis. 2)
		6.4.1.3 b)	**Define the problem or opportunity space** 1) Analyse customer complaints, problems and opportunities in the context of relevant trade-space factors.	03-08 Identify business opportunities 6)
		6.4.1.3 b)	**Define the problem or opportunity space** 2) Define the mission, business, or operational problem or opportunity.	03-08 Identify business opportunities 7)
		6.4.1.3 c)	**Characterize the solution space** 1) Define preliminary operational concepts and other concepts in life cycle stages.	03-07 Business opportunity space 7)
		6.4.1.3 c)	**Characterize the solution space** 2) Identify candidate alternative solution classes that span the potential solution space.	03-07 Business opportunity space 8)
		6.4.1.3 d)	**Evaluate alternative solution classes** 1) Assess each alternative solution class.	08-09 Business opportunities evaluation record 6)
		6.4.1.3 d)	**Evaluate alternative solution classes** 2) Select the preferred alternative solution class(es).	08-09 Business opportunities evaluation record 7)

Table B.1 *(continued)*

ISO/IEC 33020:2019 Annex B Generic Practices	Description	ISO/IEC/IEEE 12207:2017	Description	ISO/IEC/IEEE 12207:2017
		6.4.1.3 e)	**Manage the business or mission analysis** 2) Provide key artifacts and information items that have been selected for baselines.	07-1 Information item 10)
		6.4.2.3 a)	**Prepare for Stakeholder Needs and Requirements Definition** 1) Identify the stakeholders who have an interest in the software system throughout its life cycle.	02-2 Stakeholders 3)
		6.4.2.3 a)	**Prepare for Stakeholder Needs and Requirements Definition** 2) Define the stakeholder needs and requirements definition strategy.	04-29 System requirements definition strategy 3)
		6.4.2.3 a)	**Prepare for Stakeholder Needs and Requirements Definition** 3) Identify and plan for the necessary enabling systems or services needed to support stakeholder needs and requirements definition.	08-27 Enabling system records: Stakeholder needs and requirements 1)
		6.4.2.3 a)	**Prepare for Stakeholder Needs and Requirements Definition** 4) Obtain or acquire access to the enabling systems or services to be used.	08-27 Enabling system records: Stakeholder needs and requirements 2)
		6.4.2.3 b)	**Define stakeholder needs** 1) Define context of use within the concept of operations and the preliminary life cycle concepts.	03-31 Stakeholder Needs 11)
		6.4.2.3 b)	**Define stakeholder needs** 2) Identify stakeholder needs.	03-31 Stakeholder Needs 12)
		6.4.2.3 b)	**Define stakeholder needs** 3) Prioritize and down-select needs.	03-31 Stakeholder Needs 13)
		6.4.2.3 b)	**Define stakeholder needs** 4) Define the stakeholder needs and rationale.	03-31 Stakeholder Needs 14)
		6.4.2.3 c)	**Develop the operational concept and other life cycle concepts** 1) Define a representative set of scenarios to identify the required capabilities that correspond to anticipated operational and other life cycle concepts.	03-32 System operational concept 7)
		6.4.2.3 c)	**Develop the operational concept and other life cycle concepts** 2) Identify the factors affecting interactions between users and the system. i) Anticipated physical, mental, and learned capabilities of the users; ii) Workplace, environment and facilities, including other equipment in the context of use; iii) Normal, unusual, and emergency conditions; and iv) Operator and user recruitment, training and culture.	03-32 System operational concept 8)
		6.4.2.3 d)	**Transform stakeholder needs into stakeholder requirements** 1) Identify the constraints on a system solution.	12-11 System stakeholder requirements 13)
		6.4.2.3 d)	**Transform stakeholder needs into stakeholder requirements** 2) Identify the stakeholder requirements and functions that relate to critical quality characteristics, such as assurance, safety, security, environment, or health.	12-11 System stakeholder requirements 14)

Table B.1 *(continued)*

ISO/IEC 33020:2019 Annex B Generic Practices	Description	ISO/IEC/IEEE 12207:2017	Description	ISO/IEC/IEEE 12207:2017
		6.4.2.3 d)	**Transform stakeholder needs into stakeholder requirements** 3) Define stakeholder requirements, consistent with life cycle concepts, scenarios, interactions, constraints, and critical quality characteristics.	12-11 System stakeholder requirements 15)
		6.4.2.3 e)	**Analyse stakeholder requirements** 1) Analyse the complete set of stakeholder requirements.	03-02 Analyse stakeholder requirements 8)
		6.4.2.3 e)	**Analyse stakeholder requirements** 2) Define critical performance measures that enable the assessment of technical achievement.	03-02 Analyse stakeholder requirements 9)
		6.4.2.3 e)	**Analyse stakeholder requirements** 3) Feed back the analysed requirements to applicable stakeholders to validate that their needs and expectations have been adequately captured and expressed.	03-02 Analyse stakeholder requirements 10)
		6.4.2.3 e)	**Analyse stakeholder requirements** 4) Resolve stakeholder requirements issues.	03-02 Analyse stakeholder requirements 11)
		6.4.2.3 f)	**Manage the stakeholder needs and requirements definition** 1) Obtain explicit agreement with designated stakeholders on the stakeholder requirements.	08-44 Manage stakeholder requirements 3)
		6.4.3.3 a)	**Prepare for System/Software Requirements Definition** 1) Define the functional boundary of the software system or element in terms of the behavior and properties provided.	03-34 System requirements definition 5)
		6.4.3.3 a)	**Prepare for System/Software Requirements Definition** 2) Define the system/software requirements definition strategy.	03-34 System requirements definition 6)
		6.4.3.3 a)	**Prepare for System/Software Requirements Definition** 3) Identify and plan for the necessary enabling systems or services needed to support system/software requirements definition.	08-29 Enabling system records: System/software requirements 1)
		6.4.3.3 a)	**Prepare for System/Software Requirements Definition** 4) Obtain or acquire access to the enabling systems or services to be used.	08-29 Enabling system records: System/software requirements 2)
		6.4.3.3 b)	**Define system/software requirements** 1) Define each function that the software system or element is required to perform.	12-10 System requirements 16)
		6.4.3.3 b)	**Define system/software requirements** 2) Identify required states or modes of operation of the software system.	12-10 System requirements 17)
		6.4.3.3 b)	**Define system/software requirements** 3) Define necessary implementation constraints.	12-10 System requirements 18)
		6.4.3.3 b)	**Define system/software requirements** 4) Identify requirements that relate to risks, criticality of the software system, or critical quality characteristics.	12-10 System requirements 19)

Table B.1 *(continued)*

ISO/IEC 33020:2019 Annex B Generic Practices	Description	ISO/IEC/IEEE 12207:2017	Description	ISO/IEC/IEEE 12207:2017
		6.4.3.3 b)	**Define system/software requirements** 5) Define system/software requirements and requirements attributes, including the following: i) Data elements, data structures and formats, and database or data retention requirements; ii) User interfaces and user documentation (information for users) and user training; iii) Interfaces with other systems and services; iv) Functions and non-functional characteristics, including critical quality characteristics and cost targets; v) Transition of operational processes and data from existing automated and manual systems, migration approach and schedule, software installation and acceptance of the product; and vi) Requirement attributes, such as rationale; priority; traceability to software system elements, test cases, and information items; methods of verification; inclusion in approved baselines; and evaluated risk.	12-10 System requirements 20)
		6.4.3.3 c)	**Analyse system/software requirements** 1) Analyse the complete set of system/software requirements.	03-33 System requirements analysis 11)
		6.4.3.3 c)	**Analyse system/software requirements** 2) Define critical performance measures that enable the assessment of technical achievement.	03-33 System requirements analysis 12)
		6.4.3.3 c)	**Analyse system/software requirements** 3) Feed back the analysed requirements to applicable stakeholders for review.	03-33 System requirements analysis 13)
		6.4.3.3 c)	**Analyse system/software requirements** 4) Identify and resolve issues, deficiencies, conflicts, and weaknesses within the complete set of requirements.	03-33 System requirements analysis 14)
		6.4.3.3 d)	**Manage system/software requirements** 1) Obtain explicit agreement on the system/software requirements.	08-45 Manage system requirements 3)
		6.4.3.3 d)	**Manage system/software requirements** 3) Provide key artifacts and information items that have been selected for baselines.	07-1 Information item 12)
		6.4.4.3 a)	**Prepare for architecture definition** 1) Review pertinent information and identify key drivers of the architecture.	03-03 Architecture definition 10)
		6.4.4.3 a)	**Prepare for architecture definition** 2) Identify stakeholder concerns.	03-03 Architecture definition 11)
		6.4.4.3 a)	**Prepare for architecture definition** 3) Define the Architecture Definition roadmap, approach, and strategy.	03-03 Architecture definition 12)
		6.4.4.3 a)	**Prepare for architecture definition** 4) Define architecture evaluation criteria based on stakeholder concerns and key requirements.	03-03 Architecture definition 13)

Table B.1 *(continued)*

ISO/IEC 33020:2019 Annex B Generic Practices	Description	ISO/IEC/IEEE 12207:2017	Description	ISO/IEC/IEEE 12207:2017
		6.4.4.3 a)	**Prepare for architecture definition** 5) Identify and plan for the necessary enabling systems or services needed to support the Architecture Definition process.	08-19 Enabling system records: Architecture definition 1)
		6.4.4.3 a)	**Prepare for architecture definition** 6) Obtain or acquire access to the enabling systems or services to be used.	08-19 Enabling system records: Architecture definition 2)
		6.4.4.3 b)	**Develop architecture viewpoints** 1) Select, adapt, or develop viewpoints and model kinds based on stakeholder concerns.	03-05 Architecture viewpoints 7)
		6.4.4.3 b)	**Develop architecture viewpoints** 2) stablish or identify potential architecture framework(s) to be used in developing models and views.	03-05 Architecture viewpoints 8)
		6.4.4.3 b)	**Develop architecture viewpoints** 3) Capture rationale for selection of framework(s), viewpoints and model kinds.	03-05 Architecture viewpoints 9)
		6.4.4.3 b)	**Develop architecture viewpoints** 4) Select or develop supporting modelling techniques and tools.	03-05 Architecture viewpoints 10)
		6.4.4.3 c)	**Develop models and views of candidate architectures** 1) Define the software system context and boundaries in terms of interfaces and interactions with external entities.	03-06 Architecture views 11)
		6.4.4.3 c)	**Develop models and views of candidate architectures** 2) Identify architectural entities and relationships between entities that address key stakeholder concerns and critical software system requirements.	03-06 Architecture views 12)
		6.4.4.3 c)	**Develop models and views of candidate architectures** 3) Allocate concepts, properties, characteristics, behaviors, functions, or constraints that are significant to architecture decisions of the software system to architectural entities.	03-06 Architecture views 13)
		6.4.4.3 c)	**Develop models and views of candidate architectures** 4) Select, adapt, or develop models of the candidate architectures of the software system.	03-06 Architecture views 14)
		6.4.4.3 c)	**Develop models and views of candidate architectures** 5) Compose views from the models in accordance with identified viewpoints to express how the architecture addresses stakeholder concerns and meets stakeholder and system/software requirements.	03-06 Architecture views 15)
		6.4.4.3 c)	**Develop models and views of candidate architectures** 6) Harmonize the architecture models and views with each other.	03-06 Architecture views 16)
		6.4.4.3 d)	**Relate the architecture to design** 1) Identify software system elements that relate to architectural entities and the nature of these relationships.	08-66 Requirements allocation 9)

Table B.1 *(continued)*

ISO/IEC 33020:2019 Annex B Generic Practices	Description	ISO/IEC/IEEE 12207:2017	Description	ISO/IEC/IEEE 12207:2017
		6.4.4.3 d)	**Relate the architecture to design** 2) Define the interfaces and interactions among the software system elements and external entities.	08-66 Requirements allocation 10)
		6.4.4.3 d)	**Relate the architecture to design** 3) Partition, align and allocate requirements to architectural entities and system elements.	08-66 Requirements allocation 11)
		6.4.4.3 d)	**Relate the architecture to design** 4) Map software system elements and architectural entities to design characteristics.	08-66 Requirements allocation 12)
		6.4.4.3 d)	**Relate the architecture to design** 5) Define principles for the software system design and evolution.	08-66 Requirements allocation 13)
		6.4.4.3 e)	**Assess architecture candidates** 1) Assess each candidate architecture against constraints and requirements.	08-08 Architecture assessment result 8)
		6.4.4.3 e)	**Assess architecture candidates** 2) Assess each candidate architecture against stakeholder concerns using evaluation criteria.	08-08 Architecture assessment result 9)
		6.4.4.3 e)	**Assess architecture candidates** 3) Select the preferred architecture(s) and capture key decisions and rationale.	08-08 Architecture assessment result 10)
		6.4.4.3 e)	**Assess architecture candidates** 4) Establish the architecture baseline of the selected architecture.	08-08 Architecture assessment result 11)
		6.4.4.3 f)	**Manage the selected architecture** 1) Formalize the architecture governance approach and specify governance-related roles and responsibilities, accountabilities, and authorities related to design, quality, security, and safety.	08-41 Manage architecture 8)
		6.4.4.3 f)	**Manage the selected architecture** 2) Obtain explicit acceptance of the architecture by stakeholders.	08-41 Manage architecture 9)
		6.4.4.3 f)	**Manage the selected architecture** 3) Maintain concordance and completeness of the architectural entities and their architectural characteristics.	08-41 Manage architecture 10)
		6.4.4.3 f)	**Manage the selected architecture** 4) Organize, assess and control evolution of the architecture models and views to help ensure that the architectural intent is met and the architectural vision and key concepts are correctly implemented.	08-41 Manage architecture 11)
		6.4.4.3 f)	**Manage the selected architecture** 5) Maintain the architecture definition and evaluation strategy.	08-41 Manage architecture 12)
		6.4.4.3 f)	**Manage the selected architecture** 7) Provide key artifacts and information items that have been selected for baselines.	07-1 Information item 13)
		6.4.5.3 a)	**Prepare for software system design definition** 1) Define the design definition strategy, consistent with the selected life cycle model and anticipated design artifacts.	03-28 Software system design definition 5)

Table B.1 *(continued)*

ISO/IEC 33020:2019 Annex B Generic Practices	Description	ISO/IEC/IEEE 12207:2017	Description	ISO/IEC/IEEE 12207:2017
		6.4.5.3 a)	**Prepare for software system design definition** 2) Select and prioritize design principles and design characteristics.	03-28 Software system design definition 6)
		6.4.5.3 a)	**Prepare for software system design definition** 3) Identify and plan for the necessary enabling systems or services needed to support design definition.	08-21 Enabling system records: Design definition 1)
		6.4.5.3 a)	**Prepare for software system design definition** 4) Obtain or acquire access to the enabling systems or services to be used.	08-21 Enabling system records: Design definition 2)
		6.4.5.3 b)	**Establish designs related to each software system element** 1) Transform architectural and design characteristics into the design of software system elements.	03-29 Software system element design 12)
		6.4.5.3 b)	**Establish designs related to each software system element** 2) Define and prepare or obtain the necessary design enablers.	03-29 Software system element design 13)
		6.4.5.3 b)	**Establish designs related to each software system element** 3) Examine design alternatives and feasibility of implementation.	03-29 Software system element design 14)
		6.4.5.3 b)	**Establish designs related to each software system element** 4) Refine or define the interfaces among the software system elements and with external entities.	03-29 Software system element design 15)
		6.4.5.3 b)	**Establish designs related to each software system element** 5) Establish the design artifacts.	03-29 Software system element design 16)
		6.4.5.3 c)	**Assess alternatives for obtaining software system elements** 1) Determine technologies required for each element composing the software system.	03-30 Software system element evaluation 9)
		6.4.5.3 c)	**Assess alternatives for obtaining software system elements** 2) Identify candidate alternatives for the software system elements.	03-30 Software system element evaluation 10)
		6.4.5.3 c)	**Assess alternatives for obtaining software system elements** 3) Assess each candidate alternative against criteria developed from expected design characteristics and element requirements to determine suitability for the intended application.	03-30 Software system element evaluation 11)
		6.4.5.3 c)	**Assess alternatives for obtaining software system elements** 4) Choose the preferred alternatives among candidate design solutions for the software system elements.	03-30 Software system element evaluation 12)
		6.4.5.3 d)	**Manage the design** 1) Capture the design and rationale.	08-43 Manage software system element design 6)
		6.4.5.3 d)	**Manage the design** 3) Determine the status of the software system and element design.	08-43 Manage software system element design 7)
		6.4.5.3 d)	**Manage the design** 4) Provide key artifacts and information items that have been selected for baselines.	07-1 Information item 14)

Table B.1 *(continued)*

ISO/IEC 33020:2019 Annex B Generic Practices	Description	ISO/IEC/IEEE 12207:2017	Description	ISO/IEC/IEEE 12207:2017
		6.4.6.3 a)	**Define the system analysis strategy and prepare for system analysis** 1) Identify the problem or question that requires analysis.	04-30 Systems analysis strategy 9)
		6.4.6.3 a)	**Define the system analysis strategy and prepare for system analysis** 2) Identify the stakeholders of the analysis.	04-30 Systems analysis strategy 10)
		6.4.6.3 a)	**Define the system analysis strategy and prepare for system analysis** 3) Define the scope, objectives, and level of fidelity of the analysis.	04-30 Systems analysis strategy 11)
		6.4.6.3 a)	**Define the system analysis strategy and prepare for system analysis** 4) Select the methods to support the analysis.	04-30 Systems analysis strategy 12)
		6.4.6.3 a)	**Define the system analysis strategy and prepare for system analysis** 5) Identify and plan for the necessary enabling systems or services needed to support the analysis.	08-28 Enabling system records: System analysis 1)
		6.4.6.3 a)	**Define the system analysis strategy and prepare for system analysis** 6) Obtain or acquire access to the enabling systems or services to be used.	08-28 Enabling system records: System analysis 2)
		6.4.6.3 a)	**Define the system analysis strategy and prepare for system analysis** 7) Collect the data and inputs needed for the analysis.	04-30 Systems analysis strategy 13)
		6.4.6.3 b)	**Perform system analysis** 1) Identify and validate contexts and assumptions.	08-48 Perform systems analysis 8)
		6.4.6.3 b)	**Perform system analysis** 2) Apply the selected analysis methods to perform the required analysis.	08-48 Perform systems analysis 9)
		6.4.6.3 b)	**Perform system analysis** 3) Review the analysis results for quality and validity.	08-48 Perform systems analysis 10)
		6.4.6.3 b)	**Perform system analysis** 4) Establish conclusions and recommendations.	08-48 Perform systems analysis 11)
		6.4.6.3 b)	**Perform system analysis** 5) Record the results of the system analysis,	08-48 Perform systems analysis 12)
		6.4.6.3 c)	**Manage the system analysis** 2) Provide key artifacts and information items that have been selected for baselines.	07-1 Information item 15)

Table B.1 *(continued)*

ISO/IEC 33020:2019 Annex B Generic Practices	Description	ISO/IEC/IEEE 12207:2017	Description	ISO/IEC/IEEE 12207:2017
		6.4.7.3 a)	**Prepare for implementation** 1) Refine an implementation strategy, with consideration of the following: i) development policies and standards, including standards that govern applicable safety, security, privacy and environmental practices; programming or coding standards; unit test policies; and language-specific standards for implementing security features; ii) For reused or adapted software, methods to determine the level, source, and suitability of the reused system elements and security of the supply chain; iii) procedures and methods for software development (construction) and development of unit tests; and the use of peer reviews, unit tests, and walkthroughs during implementation; iv) use of CM control during software construction; v) change management considerations for manual processes; vi) implementation priorities to support data and software migration and transition, along with retirement of legacy systems; vii) creation of manual or automated test procedures to verify that a software unit meets its requirements before creation of the software unit (test-driven development); and viii) comprehensive or specialized life cycle development and support environments for realizing and managing requirements, models and prototypes, deliverable system or software elements, and test specifications and test cases.	04-07 Implementation Plan 6)
		6.4.7.3 a)	**Prepare for implementation** 2) Identify constraints from the implementation strategy and implementation technology on the system/software requirements, architecture characteristics, design characteristics, or implementation techniques.	04-07 Implementation Plan 7)
		6.4.7.3 b)	**Perform implementation.** 1) Realize or adapt software elements, according to the strategy, constraints, and defined implementation procedures.	07-8 Software element 9)
		6.4.7.3 b)	**Perform implementation.** 2) Realize or adapt hardware elements of software systems.	07-8 Software element 10)
		6.4.7.3 b)	**Perform implementation.** 3) Realize or adapt service elements of software systems.	07-8 Software element 11)
		6.4.7.3 b)	**Perform implementation.** 4) Evaluate software unit and affiliated data or other information according to the implementation strategy and criteria.	08-69 Software code & test evaluation record 5)
		6.4.7.3 b)	**Perform implementation.** 5) Package and store the software system element.	08-42 Manage software elements 5)
		6.4.7.3 b)	**Perform implementation.** 6) Record objective evidence that the software system element meets requirements.	08-42 Manage software elements 6)

Table B.1 *(continued)*

ISO/IEC 33020:2019 Annex B Generic Practices	Description	ISO/IEC/IEEE 12207:2017	Description	ISO/IEC/IEEE 12207:2017
		6.4.7.3 c)	**Manage results of implementation** 3) Provide key artifacts and information items that have been selected for baselines.	07-1 Information item 16)
		6.4.8.3 a)	**Prepare for integration** 1) Define the integration strategy.	04-26 Software integration plan 11)
		6.4.8.3 a)	**Prepare for integration** 2) Identify and define criteria for integration and points at which the correct operation and integrity of the interfaces and the selected software system functions will be verified.	04-26 Software integration plan 12)
		6.4.8.3 a)	**Prepare for integration** 3) Identify and plan for the necessary enabling systems or services needed to support integration.	08-24 Enabling system records: Integration 1)
		6.4.8.3 a)	**Prepare for integration** 4) Obtain or acquire access to the enabling systems or services to be used to support integration.	08-24 Enabling system records: Integration 2)
		6.4.8.3 a)	**Prepare for integration** 5) Identify constraints for integration to be incorporated in the system/ software requirements, architecture or design.	04-26 Software integration plan 13)
		6.4.8.3 b)	**Perform integration** 1) Obtain implemented software system elements in accordance with agreed schedules.	07-6 Integrated system 9)
		6.4.8.3 b)	**Perform integration** 2) Integrate the implemented elements.	07-6 Integrated system 10)
		6.4.8.3 b)	**Perform integration** 3) Check that the integrated software interfaces or functions run from initiation to an expected termination within an expected range of data values.	07-6 Integrated system 11)
		6.4.8.3 c)	**Manage results of integration** 1) Record integration results and anomalies encountered.	08-71 Software integration test results 3)
		6.4.8.3 c)	**Manage results of integration** 3) Provide key artifacts and information items that have been selected for baselines.	07-1 Information item 17)
		6.4.9.3 a)	**Prepare for verification** 1) Refine the verification strategy, which includes the following: i) Identify the verification scope, including the software system, element, or artifact, the properties to be verified, and the expected results. ii) Identify the constraints that potentially limit the feasibility of verification actions. iii) Identify verification priorities.	04-32 Verification strategy 14)
		6.4.9.3 a)	**Prepare for verification** 2) Identify constraints from the verification strategy to be incorporated in the system/software requirements, architecture, or design.	04-32 Verification strategy 15)
		6.4.9.3 a)	**Prepare for verification** 3) Define the purpose, conditions and conformance criteria for each verification action.	04-32 Verification strategy 16)

Table B.1 *(continued)*

ISO/IEC 33020:2019 Annex B Generic Practices	Description	ISO/IEC/IEEE 12207:2017	Description	ISO/IEC/IEEE 12207:2017
		6.4.9.3 a)	**Prepare for verification** 4) Select appropriate verification methods or techniques and associated criteria for verification actions, such as inspection, analysis, demonstration, or testing.	04-32 Verification strategy 17)
		6.4.9.3 a)	**Prepare for verification** 5) Identify and plan for the necessary enabling systems or services needed to support verification.	08-32 Enabling system records: Verification 1)
		6.4.9.3 a)	**Prepare for verification** 6) Obtain or acquire access to the enabling systems or services to be used to support verification.	08-32 Enabling system records: Verification 2)
		6.4.9.3 b)	**Perform verification** 1) Define the verification procedures, each supporting one or a set of verification actions.	06-3 Verification Procedures 5)
		6.4.9.3 b)	**Perform verification** 2) Perform the verification procedures.	06-3 Verification Procedures 6)
		6.4.9.3 c)	**Manage results of verification** 1) Review verification results and anomalies encountered and identify follow-up actions.	08-93 Verification problems and non-conformances 6)
		6.4.9.3 c)	**Manage results of verification** 2) Record incidents and problems during verification and track their resolution.	08-93 Verification problems and non-conformances 7)
		6.4.9.3 c)	**Manage results of verification** 3) Obtain stakeholder agreement that the software system or element meets the specified requirements.	08-52 Product acceptance record 8)
		6.4.9.3 c)	**Manage results of verification** 5) Provide key artifacts and information items that have been selected for baselines.	07-1 Information item 18)
		6.4.10.3 a)	**Prepare for the software system transition** 1) Refine a strategy for managing software releases and other software system transitions, including the following considerations: i) establishing the type of transition and transition success criteria; ii) determining the frequency of recurring transitions, such as updates and upgrades to development, test, and operational software systems; iii) minimizing security risks, disruption, and downtime during transition; iv) archiving, destroying, or converting and validating data from previous systems to the new system; including data received through external interfaces; v) contingency planning for problem resolution, backup and return to the last working system version; vi) scheduling transitions consistent with ongoing business processing, with phased or synchronized transition of systems vii) change management for stakeholders, including interface partners, human operators, system administrators, and software system or service users;	04-27 Software release plan 12)

Table B.1 *(continued)*

ISO/IEC 33020:2019 Annex B Generic Practices	Description	ISO/IEC/IEEE 12207:2017	Description	ISO/IEC/IEEE 12207:2017
		6.4.10.3 a)	**Prepare for the software system transition** 2) Identify and define facility, site, communications network, or target environment changes needed for software system installation or transition.	04-27 Software release plan 13)
		6.4.10.3 a)	**Prepare for the software system transition** 3) Identify information needs and arrange for user documentation and training of operators, users, and other stakeholders necessary for system utilization and support.	04-27 Software release plan 14)
		6.4.10.3 a)	**Prepare for the software system transition** 4) Prepare detailed transition information, such as plans, schedules, and procedures.	04-27 Software release plan 15)
		6.4.10.3 a)	**Prepare for the software system transition** 5) Identify system constraints from transition to be incorporated in the software system requirements, architecture or design.	04-27 Software release plan 16)
		6.4.10.3 a)	**Prepare for the software system transition** 6) Identify and plan for the necessary enabling systems or services needed to support transition.	08-30 Enabling system records: Transition 1)
		6.4.10.3 a)	**Prepare for the software system transition** 7) Obtain or acquire access to the enabling systems or services to be used.	08-30 Enabling system records: Transition 2)
		6.4.10.3 b)	**Perform the transition** 1) Prepare the site of operation or virtual environment in accordance with installation requirements.	08-76 System/ software installation record 17)
		6.4.10.3 b)	**Perform the transition** 2) Deliver the software system or element for installation at the correct location and time.	08-76 System/ software installation record 18)
		6.4.10.3 b)	**Perform the transition** 3) Install the product in its physical or virtual operational location and interface to its environment.	08-76 System/ software installation record 19)
		6.4.10.3 b)	**Perform the transition** 4) Provide user documentation and training for the operators, users, and other stakeholders necessary for product utilization and support.	08-76 System/ software installation record 20)
		6.4.10.3 b)	**Perform the transition** 5) Perform activation and check-out, including the following as agreed: i) Demonstrate proper installation of the software system. ii) Demonstrate the installed or transitioned product is capable of delivering its required functions. iii) Demonstrate the functions provided by the system are sustainable by the enabling systems. iv) Review the software system for operational readiness. v) Commission the software system for operations.	08-76 System/ software installation record 21)
		6.4.10.3 c)	**Manage results of transition** 1) Record transition results and anomalies encountered.	08-72 Software operation release test results 5)

Table B.1 *(continued)*

ISO/IEC 33020:2019 Annex B Generic Practices	Description	ISO/IEC/IEEE 12207:2017	Description	ISO/IEC/IEEE 12207:2017
		6.4.10.3 c)	**Manage results of transition** 2) Record transition incidents and problems and track their resolution.	08-72 Software operation release test results 6)
		6.4.10.3 c)	**Manage results of transition** 4) Provide key artifacts and information items that have been selected for baselines.	07-1 Information item 19)
		6.4.11.3 a)	**Prepare for validation** 1) Refine the validation strategy, which includes the following: i) Identify the validation scope, including the characteristics of the software system, element, or artifact to be validated, and the expected results of validation. ii) Identify the constraints that potentially limit the feasibility of validation actions. iii) Identify validation priorities.	04-31 Validation plan 14)
		6.4.11.3 a)	**Prepare for validation** 2) Identify system constraints from the validation strategy to be incorporated in the stakeholder requirements.	04-31 Validation plan 15)
		6.4.11.3 a)	**Prepare for validation** 3) Define the purpose, conditions and conformance criteria for each validation action.	04-31 Validation plan 16)
		6.4.11.3 a)	**Prepare for validation** 4) Select appropriate validation methods or techniques and associated criteria for each validation action.	04-31 Validation plan 17)
		6.4.11.3 a)	**Prepare for validation** 5) Identify and plan for the necessary enabling systems or services needed to support validation.	08-31 Enabling system records: Validation 1)
		6.4.11.3 a)	**Prepare for validation** 6) Obtain or acquire access to the enabling systems or services to be used to support validation.	08-31 Enabling system records: Validation 2)
		6.4.11.3 b)	**Perform validation** 1) Define the validation procedures, each supporting one or a set of validation actions.	06-2 Validation Procedures 5)
		6.4.11.3 b)	**Perform validation** 2) Perform the validation procedures in the defined environment.	06-2 Validation Procedures 6)
		6.4.11.3 c)	**Manage results of validation** 1) Review validation results and anomalies encountered and identify follow-up actions.	08-90 Validation Records 2)
		6.4.11.3 c)	**Manage results of validation** 2) Record incidents and problems during validation and track their resolution.	08-91 Validation problems and non-conformances 3)
		6.4.11.3 c)	**Manage results of validation** 3) Obtain stakeholder agreement that the software system or element meets the stakeholder needs.	08-92 Validation test suite confirmation record 2)
		6.4.11.3 c)	**Manage results of validation** 5) Provide key artifacts and information items that have been selected for baselines.	07-1 Information item 20)

Table B.1 *(continued)*

ISO/IEC 33020:2019 Annex B Generic Practices	Description	ISO/IEC/IEEE 12207:2017	Description	ISO/IEC/IEEE 12207:2017
		6.4.12.3 a)	**Prepare for operation** 1) Refine an operation strategy, including the following considerations: i) The expected or agreed capacity, availability, response time, and security of services as they are introduced, routinely operated and withdrawn from service; ii) The human resources strategy, depending on the need to define training and qualification requirements, train or obtain personnel to control and monitor software system operations, administer system access, and support customer service requests and user assistance; iii) The release criteria and schedules of the software system to permit modifications that sustain existing or enhanced services; iv) The approach to implement the operational modes in the Operational Concept, including normal operations and preparations for, and testing of, envisioned types of contingency operations; v) Measures for operation that will provide insight into performance levels; vi) The operational and occupational safety strategy for operators and others using or in contact with the software system during operation, accounting for safety regulations; and vii) The environmental protection and sustainability strategy for operating the software system.	04-15 Operation plan 8)
		6.4.12.3 a)	**Prepare for operation** 2) Identify system constraints from operation to be incorporated in changes to the system/software requirements, architecture, design, implementation, or transition.	04-15 Operation plan 9)
		6.4.12.3 a)	**Prepare for operation** 3) Identify and plan for the necessary enabling systems or services needed to support operation.	08-26 Enabling system records: Operation 1)
		6.4.12.3 a)	**Prepare for operation** 4) Obtain or acquire access to the enabling systems or services to be used.	08-26 Enabling system records: Operation 2)
		6.4.12.3 a)	**Prepare for operation** 5) Identify or define training and qualification requirements for personnel needed for software system operation.	04-15 Operation plan 10)
		6.4.12.3 a)	**Prepare for operation** 6) Depending on the need for human intervention and control of operations, assign trained, qualified personnel to be operators.	04-15 Operation plan 11)
		6.4.12.3 b)	**Perform operation** 1) Use the software system in its intended operational environment.	08-46 Operation actions 13)
		6.4.12.3 b)	**Perform operation** 2) Apply materials and other resources, as required, to operate the software system and sustain its services.	08-46 Operation actions 14)

Table B.1 *(continued)*

ISO/IEC 33020:2019 Annex B Generic Practices	Description	ISO/IEC/IEEE 12207:2017	Description	ISO/IEC/IEEE 12207:2017
		6.4.12.3 b)	**Perform operation** 3) Monitor software system operation, including consideration of the following: i) Managing adherence to the operation strategy (e.g. , operational procedures); ii) Recording and reporting significant events, such as possible breaches of software and data confidentiality and integrity; iii) Operating the software system in a safe manner and compliant with legislated guidelines e.g. , those concerning occupational safety and environmental protection; and iv) Recording when software system or service performance is not within acceptable parameters.	08-46 Operation actions 15)
		6.4.12.3 b)	**Perform operation** 4) Consistent with the operational strategy, develop and, where feasible, automate operational procedures to minimize the risk of operational anomalies.	08-46 Operation actions 16)
		6.4.12.3 b)	**Perform operation** 5) Consistent with the operational strategy, analyse measurements to confirm that: i) Service performance is within acceptable parameters or agreed service levels for the agreed workload; ii) System and service availability and response times are acceptable; iii) Cost of operation is consistent with objectives and constraints; and iv) Potential improvements are identified and prioritized.	08-46 Operation actions 17)
		6.4.12.3 b)	**Perform operation** 6) Perform contingency operations, if necessary.	08-46 Operation actions 18)
		6.4.12.3 c)	**Manage results of operation** 1) Record results of operation and anomalies encountered.	08-47 Operation records 7)
		6.4.12.3 c)	**Manage results of operation** 2) Record operational incidents and problems and track their resolution.	08-47 Operation records 8)
		6.4.12.3 c)	**Manage results of operation** 4) Provide key artifacts and information items that have been selected for baselines.	07-1 Information item 21)
		6.4.12.3 d)	**Support the customer** 1) Provide assistance and consultation to the customers and users to resolve complaints, incidents, problems, and service requests.	11-4 Operation requests 7)
		6.4.12.3 d)	**Support the customer** 2) Record and monitor requests and subsequent actions for support.	11-4 Operation requests 8)
		6.4.12.3 d)	**Support the customer** 3) Determine the degree to which the delivered software system or services satisfy the needs of the customers and users.	11-4 Operation requests 9)

Table B.1 *(continued)*

ISO/IEC 33020:2019 Annex B Generic Practices	Description	ISO/IEC/IEEE 12207:2017	Description	ISO/IEC/IEEE 12207:2017
		6.4.13.3 a)	**Prepare for maintenance** 1) Refine a maintenance strategy, including consideration of the following: i) Establishing priorities, typical schedules, and procedures for performing, verifying, distributing, and installing software maintenance changes in conformance with operational availability requirements; ii) Establishing techniques and methods for becoming aware of the need for corrective, adaptive, and perfective maintenance; iii) Periodic assessment of the design characteristics in case of evolution of the software system and of its architecture; iv) Forecasting potential obsolescence of components and technologies using information on technical changes in related systems; v) Establishing priorities and resources to obtain access to the correct versions of the product and product information needed for performing maintenance (e.g. , scheduled or phased installation, maintenance patches or software upgrades); vi) Measures for maintenance that will provide insight into performance levels, effectiveness, and efficiency, including access to historical fault and failure; vii) Agreed rights to data and the impact on data in the system during problem resolution and maintenance activity; viii) Approach to assure that counterfeit or unauthorized system elements are not introduced into the system; ix) Impact of the maintenance change on other software systems elements versus the risk of leaving a reported software anomaly in place; and x) The skill and personnel levels required to effect system or software repairs or replacements, fixes, patches, updates, and upgrades, considering legal and regulatory requirements regarding health and safety, security, and the environment.	04-14 Maintenance Plan 8)
		6.4.13.3 a)	**Prepare for maintenance** 2) For non-software elements, define a logistics strategy throughout the life cycle, including acquisition and operational considerations: the number and type of replacement elements to be stored, their storage locations and conditions, their anticipated replacement rate, and their storage life and renewal frequency.	04-14 Maintenance Plan 9)
		6.4.13.3 a)	**Prepare for maintenance** 3) Identify constraints from maintenance to be incorporated in the system/software requirements, architecture, or design.	04-14 Maintenance Plan 10)
		6.4.13.3 a)	**Prepare for maintenance** 4) Identify trades such that the system and associated maintenance and logistics actions result in a solution that is affordable, operable, supportable, and sustainable.	04-14 Maintenance Plan 11)

Table B.1 *(continued)*

ISO/IEC 33020:2019 Annex B Generic Practices	Description	ISO/IEC/IEEE 12207:2017	Description	ISO/IEC/IEEE 12207:2017
		6.4.13.3 a)	**Prepare for maintenance** 5) Identify and plan for the necessary enabling systems or services needed to support maintenance.	08-25 Enabling system records: Maintenance 1)
		6.4.13.3 a)	**Prepare for maintenance** 6) Obtain or acquire access to the enabling systems or services to be used.	08-25 Enabling system records: Maintenance 2)
		6.4.13.3 b)	**Perform maintenance** 1) Review stakeholder requirements, complaints, events, incident and problem reports to identify corrective, adaptive, perfective and preventive maintenance needs.	11-3 Maintenance Requests 14)
		6.4.13.3 b)	**Perform maintenance** 2) Analyse the impact of maintenance changes on data structures, data, and related software functions, user documentation, and interfaces.	11-3 Maintenance Requests 15)
		6.4.13.3 b)	**Perform maintenance** 3) Upon encountering unexpected faults that cause a software system failure, restore the system to operational status.	11-3 Maintenance Requests 16)
		6.4.13.3 b)	**Perform maintenance** 4) implement the procedures for correction of flaws (defects) and errors, or for replacement or upgrade of system elements.	11-3 Maintenance Requests 17)
		6.4.13.3 b)	**Perform maintenance** 5) Perform preventive maintenance by replacing, patching, augmenting, or upgrading software system elements, to improve the performance of a software system that is projected to reach unacceptable service levels, e.g., lack of capacity due to increases in demand or stored data, or to avoid unacceptable operating conditions, e.g., running with outdated security software.	11-3 Maintenance Requests 18)
		6.4.13.3 b)	**Perform maintenance** 6) Identify when adaptive or perfective maintenance is required.	11-3 Maintenance Requests 19)
		6.4.13.3 c)	**Perform logistics support** 1) Obtain resources to support the software system through its life cycle or the project's life (acquisition logistics).	09-07 Maintenance (Logistics) Report 10)
		6.4.13.3 c)	**Perform logistics support** 2) Monitor the quality and availability of replacement elements and enabling systems, their delivery mechanisms and their continued integrity during storage.	09-07 Maintenance (Logistics) Report 11)
		6.4.13.3 c)	**Perform logistics support** 3) Implement mechanisms for software system or element distribution, including packaging, handling, storage and communications or transportation needed for items during the life cycle.	09-07 Maintenance (Logistics) Report 12)
		6.4.13.3 c)	**Perform logistics support** 4) Confirm that logistics actions to fulfill software system or element supportability requirements or achieve operational readiness are planned and implemented.	09-07 Maintenance (Logistics) Report 13)

Table B.1 *(continued)*

ISO/IEC 33020:2019 Annex B Generic Practices	Description	ISO/IEC/IEEE 12207:2017	Description	ISO/IEC/IEEE 12207:2017
		6.4.13.3 d)	**Manage results of maintenance and logistics** 1) Record incidents and problems, including their resolutions, and significant maintenance and logistics results.	08-40 Maintenance (Logistics) Records 8)
		6.4.13.3 d)	**Manage results of maintenance and logistics** 2) Identify and record trends of incidents, problems, and maintenance and logistics actions.	08-40 Maintenance (Logistics) Records 9)
		6.4.13.3 d)	**Manage results of maintenance and logistics** 4) Provide key artifacts and information items that have been selected for baselines.	07-1 Information item 22)
		6.4.13.3 d)	**Manage results of maintenance and logistics** 5) Monitor and measure customer satisfaction with system and maintenance support.	08-40 Maintenance (Logistics) Records 10)
		6.4.14.3 a)	**Prepare for disposal** 1) Refine a disposal strategy for the software system, to include each system element and to identify and address critical disposal needs, including the following considerations: i) Permanent termination of the system's functions and delivery of services, e.g. physical destruction of data storage devices, or transition of the software system elements for future reuse in modified or adapted form; ii) Identification of ownership and responsibility for retention or destruction of data and intellectual property in the software system; iii) Transformation of the product into, or retention in a socially and physically acceptable state, thereby avoiding subsequent adverse effects on stakeholders, society and the environment; iv) The health, safety, security and privacy concerns applicable to disposal actions and to the long-term condition of resulting physical material and information; v) Notification to relevant stakeholders of significant disposal activities, e.g. , retirement or replacement of a system, software products or services, retirement schedule, or replacement options; and vi) Identification of schedules, actions, responsibilities, and resources for disposal activities.	04-06 Disposal strategy 6)
		6.4.14.3 a)	**Prepare for disposal** 2) Identify constraints on disposal for the system/software requirements, architecture and design characteristics, or implementation techniques.	04-06 Disposal strategy 7)
		6.4.14.3 a)	**Prepare for disposal** 3) Identify and plan for the necessary enabling systems or services needed to support disposal.	08-22 Enabling system records: Disposal 1)
		6.4.14.3 a)	**Prepare for disposal** 4) Obtain or acquire access to the enabling systems or services to be used.	08-22 Enabling system records: Disposal 2)

Table B.1 *(continued)*

ISO/IEC 33020:2019 Annex B Generic Practices	Description	ISO/IEC/IEEE 12207:2017	Description	ISO/IEC/IEEE 12207:2017
		6.4.14.3 a)	**Prepare for disposal** 5) Specify containment facilities, storage locations, inspection criteria and storage periods, if the software system or data is to be stored, consistent with security and environmental considerations.	04-06 Disposal strategy 8)
		6.4.14.3 a)	**Prepare for disposal** 6) Define preventive methods to preclude disposed elements and materials that should not be repurposed, reclaimed or reused from re-entering the supply chain.	04-06 Disposal strategy 9)
		6.4.14.3 b)	**Perform disposal** 1) Deactivate the software system or element to prepare it for removal.	08-17 Disposal Records 14)
		6.4.14.3 b)	**Perform disposal** 2) Remove the software system, its elements, its data, and non-reusable material from use or production for appropriate disposition and action.	08-17 Disposal Records 15)
		6.4.14.3 b)	**Perform disposal** 3) Withdraw impacted operating staff from the software system or system element and record relevant operating knowledge.	08-17 Disposal Records 16)
		6.4.14.3 b)	**Perform disposal** 4) Reuse, recycle, recondition, overhaul, archive, or destroy designated software system elements.	08-17 Disposal Records 17)
		6.4.14.3 b)	**Perform disposal** 5) Conduct destruction of the system elements, as necessary, to reduce the amount of waste treatment or to make the waste easier to handle.	08-17 Disposal Records 18)
		6.4.14.3 c)	**Finalize the disposal** 1) Confirm that detrimental health, safety, security, and environmental conditions following disposal have been identified and treated.	08-17 Disposal Records 19)
		6.4.14.3 c)	**Finalize the disposal** 2) Return the environment to its original state or to a state that is specified by agreement.	08-17 Disposal Records 20)
		6.4.14.3 c)	**Finalize the disposal** 3) Archive information gathered through the lifetime of the product to permit audits and reviews in the event of long-term hazards to health, safety, security and the environment, and to permit future software system creators and users to build a knowledge base from experience.	08-17 Disposal Records 21)
B4.1 PA.2.1.GP1	**Determine results to be achieved for the performance of the process** 1) Results to be achieved are determined.	6.3.1.3 a)	**Define the project** 1) Identify the project objectives and constraints.	03-17 Project goals 6)
		6.3.1.3 b)	**Plan project and technical management** 4) Define roles, responsibilities, accountabilities, and authorities.	04-21 Project plan 11)
B4.1 PA.2.1.GP1	**Determine results to be achieved for the performance of the process** 2) Process performance goals are defined.	6.3.1.3 a)	**Define the project** 1) Identify the project objectives and constraints.	03-17 Project goals 6)

Table B.1 *(continued)*

ISO/IEC 33020:2019 Annex B Generic Practices	Description	ISO/IEC/IEEE 12207:2017	Description	ISO/IEC/IEEE 12207:2017
B4.1 PA.2.1.GP1	**Determine results to be achieved for the performance of the process** 3) Assumptions and constraints are considered when identifying the performance goals.	6.3.1.3 a)	**Define the project** 1) Identify the project objectives and constraints.	03-17 Project goals 6)
B4.1 PA.2.1.GP1	**Determine results to be achieved for the performance of the process** 4) Results to be achieved are communicated to involved parties.	6.3.1.3 b)	**Plan project and technical management** 8) 2 [Generate and] communicate a plan for project and technical management and execution, including reviews.	04-21 Project plan 15)
B4.1 PA.2.1.GP2	**Determine and address risks relevant to the performance of the process** 1) Risks that can affect performance of the process are identified and evaluated for effect and severity.	6.3.4.3 c)	**Analyse risks** 1) Identify risks in the categories described in the risk management context.	03-26 Risk identification 3)
B4.1 PA.2.1.GP2	**Determine and address risks relevant to the performance of the process** 2) Actions to mitigate the risks are planned and performed.	6.3.4.3 b)	**Manage the risk profile** 1) Define and record the risk thresholds and conditions under which a level of risk may be accepted.	03-27 Risk management profile 5)
		6.3.4.3 b)	**Manage the risk profile** 2) Establish and maintain a risk profile.	03-27 Risk management profile 6)
B4.1 PA.2.1.GP2	**Determine and address risks relevant to the performance of the process** 3) Monitor the risks and record the mitigation activities throughout the performance of the process.	6.3.4.3 b)	**Manage the risk profile** 3) Periodically provide the relevant risk profile to stakeholders based upon their needs.	03-27 Risk management profile 7)
B4.1 PA.2.1.GP3	**Plan the performance of the process to achieve the determined results.** 1) Plan(s) for the performance of the process are developed.	6.3.1.3 b)	**Plan project and technical management** 7) 1 Generate [and communicate] a plan for project and technical management and execution, including reviews.	04-21 Project plan 14)
B4.1 PA.2.1.GP3	**Plan the performance of the process to achieve the determined results.** 2) Process activities and tasks are defined.	6.3.1.3 a)	**Define the project** 3) Define and maintain a life cycle model that is comprised of stages using the defined life cycle models of the organization.	03-10 Life cycle model 26)
B4.1 PA.2.1.GP3	**Plan the performance of the process to achieve the determined results.** 3) Schedule and milestones are defined and aligned with the approach to performing the process.	6.3.1.3 b)	**Plan project and technical management** 1) Define and maintain a project schedule based on management and technical objectives and work estimates.	04-22 Project schedule 3)
B4.1 PA.2.1.GP3	**Plan the performance of the process to achieve the determined results.** 4) Documented information reviews are planned.	6.3.1.3 a)	**Define the project** 5) Define and maintain the processes that will be applied on the project.	03-10 Life cycle model 27)
B4.1 PA.2.1.GP4	**Control the performance of the process** 1) Process performance measures are established.	6.3.1.3 a)	**Define the project** 3) Define and maintain a life cycle model that is comprised of stages using the defined life cycle models of the organization.	03-10 Life cycle model 26)
B4.1 PA.2.1.GP4	**Control the performance of the process** 2) Process performance is monitored and the results are controlled.	6.3.2.3 b)	**Assess the project** 10) Record and provide status and findings from assessment tasks.	09-13 Project status report 29)
		6.3.2.3 b)	**Assess the project** 11) Monitor process execution within the project.	09-13 Project status report 30)

Table B.1 *(continued)*

ISO/IEC 33020:2019 Annex B Generic Practices	Description	ISO/IEC/IEEE 12207:2017	Description	ISO/IEC/IEEE 12207:2017
B4.1 PA.2.1.GP4	**Control the performance of the process** 3) Appropriate actions are taken when planned results are not achieved.	6.3.2.3 c)	**Control the project** 3) Initiate change actions when there is a contractual change to cost, time or quality due to the impact of an acquirer or supplier request.	11-5 Project change request 11)
B4.1 PA.2.1.GP4	**Control the performance of the process** 4) The plan(s) are adjusted and rescheduling is performed, as necessary.	6.3.2.3 c)	**Control the project** 2) Initiate necessary project replanning.	11-5 Project change request 10)
B4.1 PA.2.1.GP5	**Assign competent people with the relevant responsibilities and authorities for performing the process** 1) Responsibilities and authorities to perform the process are determined, assigned and communicated.	6.3.1.3 b)	**Plan project and technical management** 4) Define roles, responsibilities, accountabilities, and authorities.	04-21 Project plan 11)
		6.3.1.3 c)	**Activate the project** 2) Submit requests and obtain commitments for necessary resources to perform the project.	08-59 Project resource request record 3)
B4.1 PA.2.1.GP5	**Assign competent people with the relevant responsibilities and authorities for performing the process** 2) Required competencies are identified based on the responsibilities.	6.3.1.3 b)	**Plan project and technical management** 5) Define the infrastructure and services required.	04-21 Project plan 12)
B4.1 PA.2.1.GP5	**Assign competent people with the relevant responsibilities and authorities for performing the process** 3) Competencies for management and execution of the process are ensured by training or work-based learning.	6.3.2.3 b)	**Assess the project** 4) Assess the adequacy of roles, responsibilities, accountabilities, and authorities.	09-13 Project status report 23)
B4.1 PA.2.1.GP5	**Assign competent people with the relevant responsibilities and authorities for performing the process** 4) Person(s) performing the process are considered competent on the basis of appropriate education, training, or experience.	6.3.2.3 b)	**Assess the project** 4) Assess the adequacy of roles, responsibilities, accountabilities, and authorities.	09-13 Project status report 23)
B4.1 PA.2.1.GP5	**Assign competent people with the relevant responsibilities and authorities for performing the process** 5) Necessary competencies are acquired externally when needed.	6.3.1.3 c)	**Activate the project** 2) Submit requests and obtain commitments for necessary resources to perform the project.	08-59 Project resource request record 3)
B4.1 PA.2.1.GP6	**Allocate and maintain resources to perform the process according to plan** 1) The human and infrastructure resources needed for performing the process are determined, provided and maintained.	6.3.1.3 b)	**Plan project and technical management** 5) Define the infrastructure and services required.	04-21 Project plan 12)
B4.1 PA.2.1.GP6	**Allocate and maintain resources to perform the process according to plan** 2) The information necessary to perform the process is identified and made available.	6.3.1.3 c)	**Activate the project** 2) Submit requests and obtain commitments for necessary resources to perform the project.	08-59 Project resource request record 3)

Table B.1 *(continued)*

ISO/IEC 33020:2019 Annex B Generic Practices	Description	ISO/IEC/IEEE 12207:2017	Description	ISO/IEC/IEEE 12207:2017
B4.1 PA.2.1.GP6	**Allocate and maintain resources to perform the process according to plan** 3) The use of the resources is measured and monitored to identify possible deviations.	6.3.2.3 b)	**Assess the project** 5) Assess the adequacy and availability of resources.	09-13 Project status report 24)
B4.1 PA.2.1.GP7	**Manage the interfaces between the involved parties** 1) The individuals and groups involved in the process performance are identified.	6.3.1.3 b)	**Plan project and technical management** 4) Define roles, responsibilities, accountabilities, and authorities.	04-21 Project plan 11)
B4.1 PA.2.1.GP7	**Manage the interfaces between the involved parties** 2) Responsibilities of the involved parties are assigned.	6.3.1.3 c)	**Activate the project** 2) Submit requests and obtain commitments for necessary resources to perform the project.	08-59 Project resource request record 3)
B4.1 PA.2.1.GP7	**Manage the interfaces between the involved parties** 3) Communication is assured between the involved parties.	6.3.1.3 c)	**Activate the project** 2) Submit requests and obtain commitments for necessary resources to perform the project.	08-59 Project resource request record 3)
B4.2 PA.2.2.GP1	**Define the requirements for the documented information** 1) The requirements for the documented information to be produced are defined. Requirements may include defining contents and structure.	6.3.6.3 a)	**Prepare for information management** 2) Define the items of information that will be managed.	04-10 Information management plan: item identification 1)
		6.3.6.3 a)	**Prepare for information management** 4) Define the content, formats and structure of information items.	04-09 Information management plan: Presentation 1)
B4.2 PA.2.2.GP2	**Define the requirements for documentation and control of the documented information** 1) Requirements for the documentation and control of the documented information are defined. Such requirements may include requirements for (1) distribution, (2) identification of documented information and their components (3) traceability	6.3.6.3 a)	**Prepare for information management** 5) Define information maintenance actions.	04-08 Information management plan 13)
B4.2 PA.2.2.GP2	**Define the requirements for documentation and control of the documented information** 2) Dependencies between documented information are identified and understood.	6.3.5.3 a)	**Plan configuration management** 2) Define the storage, archive and retrieval procedures for configuration items, CM artifacts, and records.	04-03 Configuration Management Plan 9)
B4.2 PA.2.2.GP2	**Define the requirements for documentation and control of the documented information** 3) Requirements for the approval of documented information to be controlled are defined.	6.3.5.3 b)	**Perform configuration identification** 3) Define baselines through the life cycle.	12-03 Configuration Baseline 6)
B4.2 PA.2.2.GP3	**Identify and control the documented information in accordance with requirements** 1) Change control is established for documented information.	6.3.5.3 b)	**Perform configuration identification** 3) Define baselines through the life cycle.	12-03 Configuration Baseline 6)
B4.2 PA.2.2.GP3	**Identify and control the documented information in accordance with requirements** 2) The documented information is identified and controlled in accordance with requirements.	6.3.6.3 b)	**Perform information management** 1) Obtain, develop, or transform the identified items of information.	07-1 Information item 9)

Table B.1 *(continued)*

ISO/IEC 33020:2019 Annex B Generic Practices	Description	ISO/IEC/IEEE 12207:2017	Description	ISO/IEC/IEEE 12207:2017
B4.2 PA.2.2.GP3	**Identify and control the documented information in accordance with requirements** 3) Versions of documented information are assigned to product configurations as applicable.	6.3.5.3 c)	**Perform configuration change management** 3) Track and manage approved changes to the baseline, Requests for Change and Requests for Variance.	08-11 Configuration Management Change Requests 11)
B4.2 PA.2.2.GP3	**Identify and control the documented information in accordance with requirements** 4) The documented information is made available through appropriate access mechanisms.	6.3.6.3 b)	**Perform information management** 3) Publish, distribute or provide access to information and information items to designated stakeholders.	07-3 Information item: Publish 1)
B4.2 PA.2.2.GP3	**Identify and control the documented information in accordance with requirements** 5) The revision status of the documented information may readily be ascertained.	6.3.6.3 b)	**Perform information management** 2) Maintain information items and their storage records, and record the status of information.	07-2 Information item: Item status 1)
B4.2 PA.2.2.GP4	**Review and adjust documented information to meet the defined requirements** 1) Documented information is reviewed against the defined requirements in accordance with planned arrangements.	6.3.5.3 c)	**Perform configuration change management** 1) Identify and record Requests for Change and Requests for Variance.	08-11 Configuration Management Change Requests 9)
B4.2 PA.2.2.GP4	**Review and adjust documented information to meet the defined requirements** 2) Issues arising from documented information reviews are resolved.	6.3.5.3 c)	**Perform configuration change management** 2) Coordinate, evaluate, and disposition Requests for Change and Requests for Variance.	08-11 Configuration Management Change Requests 10)
B4.2 PA.2.2.GP5	**Maintain and retain information products to demonstrate that planned results are achieved** 1) Documented information needed to confirm the performance of the process is determined.	6.3.6.3 b)	**Perform information management** 4) Archive designated information.	10-1 Information Item Archive 3)
B4.2 PA.2.2.GP5	**Maintain and retain information products to demonstrate that planned results are achieved** 2) Documented information is used to demonstrate that the products and/or services satisfy their requirements.	6.3.6.3 b)	**Perform information management** 5) Dispose of unwanted, invalid or unvalidated information.	08-33 Information item disposal record 3)
B5.1 PA.3.1.GP1	**Establish and maintain a standard process that will support the deployment of the defined process.** 1) A standard process is developed that includes the fundamental process elements.	6.2.1.3 a)	**Establish the process** 2) Establish the processes that implement the requirements of this document and that are consistent with organizational strategies.	03-10 Life cycle model 23)
		6.2.1.3 a)	**Establish the process** 5) Establish standard life cycle models for the organization that are comprised of stages and define the purpose and outcomes for each stage.	03-10 Life cycle model 25)
B5.1 PA.3.1.GP1	**Establish and maintain a standard process that will support the deployment of the defined process.** 3) Guidance and/or procedures are provided to support implementation of the process as needed.	6.2.1.3 a)	**Establish the process** 1) Establish policies and procedures for process management and deployment that are consistent with organizational strategies.	03-10 Life cycle model 22)

Table B.1 *(continued)*

ISO/IEC 33020:2019 Annex B Generic Practices	Description	ISO/IEC/IEEE 12207:2017	Description	ISO/IEC/IEEE 12207:2017
B5.1 PA.3.1.GP2	**Determine the inputs and outputs of the standard process** 3) Start and stop criteria for the standard process are defined as needed.	6.2.1.3 a)	**Establish the process** 4) Define business criteria that control progression through the life cycle.	03-10 Life cycle model 24)
B5.1 PA.3.1.GP4	**Determine the roles, competencies, responsibilities and authorities for performing the standard process** 1) Roles and related competencies for performing the process are determined.	6.2.1.3 a)	**Establish the process** 3) Define the roles, responsibilities, accountabilities, and authorities to facilitate implementation of processes and the strategic management of life cycles.	03-11 Life cycle model: Responsibilities 1)
B5.1 PA.3.1.GP4	**Determine the roles, competencies, responsibilities and authorities for performing the standard process** 2) Authorities necessary for executing responsibilities are determined.	6.2.1.3 a)	**Establish the process** 3) Define the roles, responsibilities, accountabilities, and authorities to facilitate implementation of processes and the strategic management of life cycles.	03-11 Life cycle model: Responsibilities 1)
B5.1 PA.3.1.GP5	**Determine the resources for performing the standard process** 1) Appropriate resources are identified and determined.	6.2.2.3 a)	**Establish the infrastructure** 2) 1. Identify, [obtain and provide] infrastructure resources and services that are needed to implement and support projects.	04-12 Infrastructure plan 3)
B5.1 PA.3.1.GP5	**Determine the resources for performing the standard process** 3) Process infrastructure components are identified (facilities, tools, networks, methods, etc).	6.2.2.3 a)	**Establish the infrastructure** 2) 1. Identify, [obtain and provide] infrastructure resources and services that are needed to implement and support projects.	04-12 Infrastructure plan 3)
B5.1 PA.3.1.GP6	**Determine and maintain necessary knowledge for the operation of the standard process** 1) Information and understanding needed to perform the process is determined and maintained.	6.2.4.3 a)	**Identify skills** 1) Identify skill needs based on current and expected projects.	03-15 Organizational skill needs 2)
B5.2 PA.3.2.GP1	**Deploy a defined process that satisfies the context specific requirements of the use of the standard process** 1) The defined process is appropriately selected and/or tailored from the standard process.	6.2.1.3 a)	**Establish the process** 1) Establish policies and procedures for process management and deployment that are consistent with organizational strategies.	03-10 Life cycle model 22)
B5.2 PA.3.2.GP1	**Deploy a defined process that satisfies the context specific requirements of the use of the standard process** 2) Criteria to verify conformity of the defined process with the standard process are determined.	6.2.1.3 a)	**Establish the process** 1) Establish policies and procedures for process management and deployment that are consistent with organizational strategies.	03-10 Life cycle model 22)
B5.2 PA.3.2.GP1	**Deploy a defined process that satisfies the context specific requirements of the use of the standard process** 3) The defined process is used to achieve the process outcomes.	6.2.1.3 a)	**Establish the process** 2) Establish the processes that implement the requirements of this document and that are consistent with organizational strategies.	03-10 Life cycle model 23)
B5.2 PA.3.2.GP2	**Deploy competent people with defined responsibilities and authorities to support the performance of the defined process** 1) Competency criteria for the required roles are defined.	6.2.1.3 a)	**Establish the process** 3) Define the roles, responsibilities, accountabilities, and authorities to facilitate implementation of processes and the strategic management of life cycles.	03-11 Life cycle model: Responsibilities 1)

Table B.1 *(continued)*

ISO/IEC 33020:2019 Annex B Generic Practices	Description	ISO/IEC/IEEE 12207:2017	Description	ISO/IEC/IEEE 12207:2017
B5.2 PA.3.2.GP2	**Deploy competent people with defined responsibilities and authorities to support the performance of the defined process** 2) The roles for performing the defined process are assigned and communicated.	6.2.4.3 c)	**Acquire and provide skills** 3) Make project assignments based on project and staff-development needs.	12-08 Project skill needs and provision 8)
B5.2 PA.3.2.GP2	**Deploy competent people with defined responsibilities and authorities to support the performance of the defined process** 3) The responsibilities and authorities for performing the defined process are assigned and communicated.	6.2.4.3 c)	**Acquire and provide skills** 2) Maintain and manage the pool of skilled personnel necessary to staff ongoing projects.	12-08 Project skill needs and provision 7)
B5.2 PA.3.2.GP2	**Deploy competent people with defined responsibilities and authorities to support the performance of the defined process** 4) Competency of the required person(s) is monitored and maintained with appropriate education, training, or experience.	6.2.4.3 c)	**Acquire and provide skills** 4) Motivate personnel, e.g. through career development and reward mechanisms.	12-08 Project skill needs and provision 9)
B5.2 PA.3.2.GP3	**Provide resources and information to support the performance of the defined process** 3) Resources are measured and monitored to ensure their effective use.	6.2.2.3 b)	**Maintain the infrastructure** 1) Evaluate the degree to which delivered infrastructure resources satisfy project needs.	08-35 Infrastructure evaluation record 2)
		6.2.4.3 a)	**Identify skills** 2) Identify and record skills of personnel.	03-12 Organization skills identification 2)
B5.2 PA.3.2.GP4	**Maintain documented information as evidence of the process achieving expected results** 1) Documented information is maintained.	6.2.4.3 b)	**Develop skills** 4) Maintain records of skill development.	08-68 Skill development records 4)
B5.3 PA.3.3.GP1	**Collect and analyse data about performance of the process to identify needs for improvement** 1) Data required to understand the behaviour, suitability and effectiveness of the process are identified, collected and analysed.	6.3.8.3 d)	**Manage QA records and reports** 3) Identify incidents and problems associated with product, service, and process evaluations.	09-06 Incident Report 4)
		6.3.8.3 e)	**Treat incidents and problems** 1) Record, analyse and classify incidents.	09-06 Incident Report 5)
		6.3.8.3 e)	**Treat incidents and problems** 3) Record, analyse and classify problems.	09-09 Problem analysis report 6)
B5.3 PA.3.3.GP1	**Collect and analyse data about performance of the process to identify needs for improvement** 2) Results of the analysis are used to identify where continual improvement of the standard and/or defined process can be made.	6.3.8.3 e)	**Treat incidents and problems** 4) Identify root causes and treatment of problems where feasible.	09-09 Problem analysis report 7)
		6.3.8.3 e)	**Treat incidents and problems** 7) Identify improvements in processes and products that may prevent future incidents and problems.	08-49 Problem resolution improvement record 3)
B5.3 PA.3.3.GP2	**Determine suitable methods and measures to monitor and evaluate the process** 1) Methods and measures for monitoring the suitability, effectiveness and adequacy of the process are determined.	6.3.8.3 a)	**Prepare for quality assurance** 1) Define a Quality Assurance strategy.	04-24 Quality assurance strategy 6)

Table B.1 *(continued)*

ISO/IEC 33020:2019 Annex B Generic Practices	Description	ISO/IEC/IEEE 12207:2017	Description	ISO/IEC/IEEE 12207:2017
B5.3 PA.3.3.GP2	**Determine suitable methods and measures to monitor and evaluate the process** 2) Appropriate criteria and data needed to monitor the process are defined.	6.3.8.3 a)	**Prepare for quality assurance** 2) The strategy is consistent with the organizational Quality Management policies and objectives and includes: i) Priorities for applying Quality Assurance resources to processes and tasks that have the most significant impact on the quality of the delivered products and services; ii) Defined roles, responsibilities, accountabilities, and authorities; iii) Evaluation criteria and methods for processes, products, and services, including criteria for product or service acceptance; iv) Activities appropriate to each supplier (including subcontractors); v) Required verification, validation, monitoring, measurement, review, inspection, audit, and test activities specific to the products or services; and vi) Problem resolution and process and product improvement activities.	04-24 Quality assurance strategy 7)
B5.3 PA.3.3.GP2	**Determine suitable methods and measures to monitor and evaluate the process** 3) The need to conduct internal audit, process compliance audit/reviews and management review is established.	6.3.8.3 a)	**Prepare for quality assurance** 3) Establish independence of quality assurance from other life cycle processes.	04-24 Quality assurance strategy 8)
B5.3 PA.3.3.GP3	**Assure conformity of the defined process** 3) Any nonconformities are identified and documented.	6.3.8.3 d)	**Manage QA records and reports** 1) Create records and reports related to quality assurance activities.	08-61 Quality Assurance Records 4)
B5.3 PA.3.3.GP4	**Act on nonconformities to adjust the performance of the process** 1) The nature and effect of nonconformities are analysed to plan appropriate actions.	6.3.8.3 e)	**Treat incidents and problems** 2) Identify selected incidents to associate with known errors or problems.	09-06 Incident Report 6)
		6.3.8.3 e)	**Treat incidents and problems** 6) Analyse trends in incidents and problems.	09-11 Problem trend report 2)
B5.3 PA.3.3.GP4	**Act on nonconformities to adjust the performance of the process** 2) Any changes needed are implemented to ensure that the process achieves its intended results.	6.3.8.3 e)	**Treat incidents and problems** 5) Prioritize treatment of problems (problem resolution) and track corrective actions.	09-09 Problem analysis report 8)
B5.3 PA.3.3.GP4	**Act on nonconformities to adjust the performance of the process** 3) Actions are managed and tracked to closure.	6.3.8.3 e)	**Treat incidents and problems** 9) Track incidents and problems to closure.	09-10 Problem resolution tracking report 2)

B.2 Mapping exceptions

The exceptions in the mapping of the process attribute generic practices and the life cycle process tasks are listed in Table B.2.

Table B.2 — Exceptions list - Associations between the ISO/IEC 33020 generic practices, ISO/IEC/IEEE 12207 tasks and associated information item

ISO/IEC 33020:2019 Annex B Generic Practices	Name	Description
B3.1 PA.1.1.GP1	**Achieve the process outcomes**	1) Achieve the intent of the base practices.
B4.1 PA.2.1.GP7	**Manage the interfaces between the involved parties**	4) Communication between the involved parties is effective.
B4.2 PA.2.2.GP1	**Define the requirements for the documented information**	2) Quality criteria of the documented information are identified.
B4.2 PA.2.2.GP1	**Define the requirements for the documented information**	3) Appropriate review and approval criteria for the documented information are defined.
B5.1 PA.3.1.GP1	**Establish and maintain a standard process that will support the deployment of the defined process.**	2) The standard process identifies the deployment needs and deployment context.
B5.1 PA.3.1.GP1	**Establish and maintain a standard process that will support the deployment of the defined process.**	4) Appropriate tailoring guideline(s) are available as needed.
B5.1 PA.3.1.GP1	**Establish and maintain a standard process that will support the deployment of the defined process.**	5) The standard process is maintained to meet the improvement needs and opportunities.
B5.1 PA.3.1.GP2	**Determine the inputs and outputs of the standard process**	1) Required inputs are identified, including information needed.
B5.1 PA.3.1.GP2	**Determine the inputs and outputs of the standard process**	2) Expected outputs are identified.
B5.1 PA.3.1.GP3	**Determine the sequence and interaction of the process as an integrated system of processes**	1) The process's sequence and interaction with other processes are determined.
B5.1 PA.3.1.GP3	**Determine the sequence and interaction of the process as an integrated system of processes**	2) Deployment of the standard process as a defined process maintains integrity of processes.
B5.1 PA.3.1.GP5	**Determine the resources for performing the standard process**	2) Requirements for the quality of the resources are defined.
B5.1 PA.3.1.GP5	**Determine the resources for performing the standard process**	4) Work environment requirements are defined.
B5.2 PA.3.2.GP3	**Provide resources and information to support the performance of the defined process**	2) Required information to perform the process is made available, allocated and used.
B5.2 PA.3.2.GP4	**Maintain documented information as evidence of the process achieving expected results**	2) Documented information is available for review.
B5.2 PA.3.2.GP4	**Maintain documented information as evidence of the process achieving expected results**	3) Documented information can be verified by person(s) independent of those performing the process
B5.3 PA.3.3.GP2	**Determine suitable methods and measures to monitor and evaluate the process**	4) Suitability, adequacy and effectiveness of the process are measured and analysed continually using appropriate methods.
B5.3 PA.3.3.GP2	**Determine suitable methods and measures to monitor and evaluate the process**	5) Identified risks are evaluated and managed.
B5.3 PA.3.3.GP3	**Assure conformity of the defined process**	1) Associated activities, outputs and documented information are evaluated.
B5.3 PA.3.3.GP3	**Assure conformity of the defined process**	2) Conformity of the defined process with the standard process requirements is verified.
B5.3 PA.3.3.GP3	**Assure conformity of the defined process**	4) Assurance activities are performed independently of the process instance to ensure objectivity.
B5.3 PA.3.3.GP5	**Improve the process based on the monitoring of the process**	1) Suitability, adequacy and effectiveness of the process are measured and analysed continually using appropriate methods.
B5.3 PA.3.3.GP5	**Improve the process based on the monitoring of the process**	2) Internal audits, process capability audits/reviews and management reviews are performed when needed.
B5.3 PA.3.3.GP5	**Improve the process based on the monitoring of the process**	3) Process changes are implemented to maintain the standard process.
		Total: 24

Annex C
(informative)

Listing of the information items and their characteristics

Table C.1 presents a list of the applicable information items associated with ISO/IEC/IEEE 12207.

Table C.1 — Listing of the information items and their characteristics

Reference	Name	Category	Characteristics
01-2	Supply agreement	Contract	1) - An agreement is negotiated with the acquirer that includes acceptance criteria. 2) This agreement ranges in formality from a written contract to a verbal agreement. The Supplier confirms that the requirements, delivery milestones, and acceptance conditions are achievable, that exception handling and agreement change management procedures and payment schedules are acceptable, and that they establish a basis for executing the agreement without unnecessary risks. Issues are discussed and resolved during negotiation, after which the acquirer and supplier accept the terms of an agreement and the agreement commences. For a contract, this occurs when the contract is signed. 3) - The agreement is negotiated with the acquirer, as necessary. 4) Changes to agreement terms are negotiated between the supplier and acquirer. This includes changes due to changing market context. Negotiation occurs for the initial agreement, and as required for any changes. Changed agreements are based on the required change and identified impacts. [ISO/IEC/IEEE 12207:2017, 6.1.2.3 c) 1)] 5) Negotiate an agreement with the acquirer that includes acceptance criteria. [ISO/IEC/IEEE 12207:2017, 6.1.2.3 c) 4)] 6) Negotiate the agreement with the acquirer, as necessary.
02-1	Business opportunities portfolio	Data	1) - Potential new or modified capabilities or missions are identified. 2) The organization business strategy, concept of operations, or gap analysis or opportunity analysis is reviewed for current gaps, problems, or opportunities. A new capability or enterprise need is usually determined in the Business or Mission Analysis process, further defined in the Stakeholder Needs and Requirements Definition process, and managed through this process. 3) - New business opportunities, ventures or undertakings are identified, prioritized and selected. 4) These are usually consistent with the business strategy and action plans of the organization. The potential projects are prioritized, and thresholds established, to determine which projects will be executed. The characteristics of identified projects are often determined, including stakeholder value, risks and barriers to success, dependencies and interrelationships, constraints, resource needs and mutual contention for resources. Each potential project is then assessed with respect to likelihood of success and costbenefit. The Decision Management and System Analysis processes provide details on performing an analysis of alternatives. [ISO/IEC/IEEE 12207:2017, 6.2.3.3 a) 1)] 5) Identify potential new or modified capabilities or missions. [ISO/IEC/IEEE 12207:2017, 6.2.3.3 a) 2)] 6) Prioritize, select and establish new business opportunities, ventures or undertakings.
02-2	Stakeholders	Data	1) - The stakeholders are identified who have an interest in the software system throughout its life cycle. 2) This includes individuals and classes of stakeholders who are users, operators, supporters, developers, producers, trainers, maintainers, disposers, acquirer and supplier organizations, parties responsible for external interfacing entities, regulatory bodies, and others who have a legitimate interest in the system. Where direct communication is not practicable (e.g., for consumer products and services), representatives or designated proxy stakeholders are selected. [ISO/IEC/IEEE 12207:2017, 6.4.02.3 a) 1)] 3) Identify the stakeholders who have an interest in the software system throughout its life cycle.

Table C.1 *(continued)*

Reference	Name	Category	Characteristics
03-02	Analyse stakeholder requirements	Description	1) - The complete set of stakeholder requirements is analysed. 2) Stakeholder requirements are analysed for characteristics of individual requirements, as well as characteristics of the set of requirements. Potential analysis characteristics include that the requirements are necessary, implementation-free, unambiguous, consistent, complete, singular, feasible, traceable, verifiable, affordable, and bounded. ISO/IEC/IEEE 29148 provides additional information on characteristics of requirements. 3) The System Analysis process is used to assess feasibility and affordability. The Verification and Validation processes are used in the review of stakeholder requirements. 4) - Critical performance measures that enable the assessment of technical achievement are defined. 5) This includes defining technical and quality measures and critical performance parameters associated with each effectiveness measure identified in the stakeholder requirements. The critical performance measures (e.g., measures of effectiveness and measures of suitability) are defined, analysed and reviewed to help ensure stakeholder requirements are met and to help ensure identification of project cost, schedule or performance risk associated with any noncompliance. ISO/IEC 15939 provides a process to identify, define and use appropriate measures. INCOSE TP-2003-020-01, Technical Measurement, provides information on the selection, definition and implementation of critical performance measures. The ISO/IEC 25000 series of standards provides relevant quality measures. 6) - The analysed requirements are fed back to applicable stakeholders to validate that their needs and expectations have been adequately captured and expressed. 7) - Stakeholder requirements issues are resolved. [ISO/IEC/IEEE 12207:2017, 6.4.2.3 e) 1)] 8) Analyse the complete set of stakeholder requirements. [ISO/IEC/IEEE 12207:2017, 6.4.2.3 e) 2)] 9) Define critical performance measures that enable the assessment of technical achievement. [ISO/IEC/IEEE 12207:2017, 6.4.2.3 e) 3)] 10) Feed back the analysed requirements to applicable stakeholders to validate that their needs and expectations have been adequately captured and expressed. [ISO/IEC/IEEE 12207:2017, 6.4.2.3 e) 4)] 11) Resolve stakeholder requirements issues.
03-03	Architecture definition	Description	1) - Pertinent information is reviewed and key drivers of the architecture identified. 2) Key drivers are identified by reviewing: (a) market studies, industry projections, competitor product plans, and scientific findings; (b) organizational strategies, organizational level concept of operations, organizational policies and directives, regulatory and legal constraints, and stakeholder requirements; (c) mission or business concept of operations, system-of-interest and related system operational concept, operational environment, technology roadmaps, and system/software requirements, and (d) other factors that impact the suitability of the software system through its life cycle. This analysis of key drivers typically builds from the Business or Mission Analysis, Stakeholder Requirements Definition, and System/software Requirements Definition processes. 3) Key drivers of the architecture can include architecture styles and patterns, elements, principles such as replaceable components, feasibility of implementation and integration; availability of COTS and open source components; data sources for data-intensive systems; and performance implications. The effect of choosing various design elements can be lessened if the software system is properly architected. 4) - Stakeholder concerns are identified. 5) Stakeholders are initially identified in the Stakeholder Needs and Requirements process. Additional stakeholders are usually identified during the Architecture Definition process. Stakeholder concerns related to architecture include system integrity concerns that the software system will be compromised intentionally or unintentionally via a threat agent or cause accidents as a safety hazard. Stakeholder. expectations or constraints are often associated with the system's life cycle stages, such as utilization (e.g., availability, security, effectiveness, usability, interoperability with existing systems, availability or risks to data in the system), support (e.g., the supportability of the system over its projected life-span, obsolescence management), evolution of the software system and its environment (e.g., adaptability, scalability, survivability), production (e.g., distribution, testability), and retirement (e.g., sensitive data eradication or retention).

Table C.1 *(continued)*

Reference	Name	Category	Characteristics
			6) Concerns affecting software system architecture include data sources and performance implications for data-intensive systems, and constraints on the use of outsourced, existing, newly developed, proprietary, commercially available, or open source software elements, including software licensing. While software architecture is ideally design-agnostic, the feasibility of implementing the architecture in an affordable software system is a significant constraint for most systems. 7) - The Architecture Definition roadmap, approach, and strategy is defined. 8) This includes the identification of opportunities to communicate with designated stakeholders, the definition of architecture review activities, evaluation approach and criteria, measurement approach, and measurement methods (refer to the Measurement process). The roadmap shows how the architecture will evolve to an envisioned end state and often has a longer timeframe than for the current system-of-interest. The approach is the manner in which the work will be accomplished, such as how to engage with stakeholders, how to vet the results, or where to do the work. The strategy deals with the systematic plan of action for implementing the approach consistent with the roadmap. 9) - Architecture evaluation criteria based on stakeholder concerns and key requirements are defined. [ISO/IEC/IEEE 12207:2017, 6.4.4.3 a) 1)] 10) Review pertinent information and identify key drivers of the architecture. [ISO/IEC/IEEE 12207:2017, 6.4.4.3 a) 2)] 11) Identify stakeholder concerns. [ISO/IEC/IEEE 12207:2017, 6.4.4.3 a) 3)] 12) Define the Architecture Definition roadmap, approach, and strategy. [ISO/IEC/IEEE 12207:2017, 6.4.4.3 a) 4)] 13) Define architecture evaluation criteria based on stakeholder concerns and key requirements.
03-05	Architecture viewpoints	Description	1) - Viewpoints and model kinds based on stakeholder concerns are selected, adapted, or developed. 2) - Potential architecture framework(s) to be used in developing models and views are established or identified. 3) Some architecture frameworks identify stakeholders and their concerns, and relevant viewpoints that address those concerns, while other architecture frameworks are more general in their guidance. Viewpoints specify the kinds of models to be used and how the resulting models can be used to generate architecture views. Refer to ISO/IEC/IEEE 42010 for more information on architecture framework and architecture description practices. 4) - The rationale for selection of framework(s), viewpoints and model kinds is captured. 5) - Supporting modelling techniques and tools are selected or developed. 6) Both the SWEBOK and ISO/IEC TR 24748-3 describe modeling techniques that support Architecture Definition and Design Definition of software elements. [ISO/IEC/IEEE 12207:2017, 6.4.4.3 b) 1)] 7) Select, adapt, or develop viewpoints and model kinds based on stakeholder concerns. [ISO/IEC/IEEE 12207:2017, 6.4.4.3 b) 2)] 8) Establish or identify potential architecture framework(s) to be used in developing models and views. [ISO/IEC/IEEE 12207:2017, 6.4.4.3 b) 3)] 9) Capture rationale for selection of framework(s), viewpoints and model kinds. [ISO/IEC/IEEE 12207:2017, 6.4.4.3 b) 4)] 10) Select or develop supporting modelling techniques and tools.

Table C.1 *(continued)*

Reference	Name	Category	Characteristics
03-06	Architecture views	Description	1) - The software system context and boundaries in terms of interfaces and interactions with external entities is defined. 2) This task is mainly based on the outcomes of the Business or Mission Analysis process, and is performed concurrently with the Stakeholder Needs and Requirements Definition process. It consists of identifying the entities external to the software system (i.e., existing and projected systems, products, and services that constitute the system context) and defining the boundaries of the software system (i.e., interactions with these external entities through the interfaces that cross the boundaries). The external entities include the necessary enabling systems. The Architecture Definition process defines interfaces to the extent needed to support essential architectural decisions and understanding. These interface definitions are then refined by the Design Definition process. 3) - Architectural entities and relationships between entities are identified that address key stakeholder concerns and critical software system requirements. 4) Architecture is not necessarily concerned with all requirements, but rather only with those system/software requirements that drive the architecture. On the other hand, the Design Definition process addresses and takes into account all the requirements. Sometimes, through the Architecture Definition process there will be requirements that are deemed to be inappropriate, unaffordable, or unsuitable. These are requirements issues that are resolved through iteration of the System/Software Requirements Definition process. It is also important that the architecture addresses key stakeholder concerns since not all of these will be captured in requirements. 5) - Concepts, properties, characteristics, behaviors, functions, or constraints that are significant to architecture decisions of the software system to architectural entities are allocated. 6) The items being allocated can be physical, logical, or conceptual. 7) - Models of the candidate architectures of the software system are selected, adapted or developed. 8) It is common to use models in architecture definition. The models used are those that best address key stakeholder concerns. Refer to ISO/IEC/IEEE 42010 for how this can be done. Historically, it has been common to use logical and physical models in architecture definition. Information on logical and other models is provided in Annex F. 9) - Views are composed from the models in accordance with identified viewpoints to express how the architecture addresses stakeholder concerns and meets stakeholder and system/software requirements. 10) - The architecture models and views are harmonised with each other. [ISO/IEC/IEEE 12207:2017, 6.4.4.3 c) 1)] 11) Define the software system context and boundaries in terms of interfaces and interactions with external entities. [ISO/IEC/IEEE 12207:2017, 6.4.4.3 c) 2)] 12) Identify architectural entities and relationships between entities that address key stakeholder concerns and critical software system requirements. [ISO/IEC/IEEE 12207:2017, 6.4.4.3 c) 3)] 13) Allocate concepts, properties, characteristics, behaviors, functions, or constraints that are significant to architecture decisions of the software system to architectural entities. [ISO/IEC/IEEE 12207:2017, 6.4.4.3 c) 4)] 14) Select, adapt, or develop models of the candidate architectures of the software system. [ISO/IEC/IEEE 12207:2017, 6.4.4.3 c) 5)] 15) Compose views from the models in accordance with identified viewpoints to express how the architecture addresses stakeholder concerns and meets stakeholder and system/software requirements. [ISO/IEC/IEEE 12207:2017, 6.4.4.3 c) 6)] 16) Harmonize the architecture models and views with each other.

Table C.1 *(continued)*

Reference	Name	Category	Characteristics
03-07	Business opportunity space	Description	1) - Preliminary operational concepts and other concepts in life cycle stages are defined. 2) This involves the identification of major stakeholder groups, such as customers, users, administrations, regulators, and system owners, that are defined in the Stakeholder Needs and Requirements Definition process. 3) Preliminary life cycle concepts include preliminary acquisition concepts, preliminary deployment concepts, preliminary operational concepts, preliminary support concepts, and preliminary retirement concepts. Operational concepts include high level operational modes or states, operational scenarios, potential use cases, or usage within a proposed business strategy. These concepts enable feasibility analysis and evaluation of alternatives. These concepts are further refined within the Stakeholder Needs and Requirements Definition process. 4) The operating environment can have known vulnerabilities associated with specific security threats and safety hazards. These vulnerabilities need to be understood in association with the product under development. The system and human interfaces are an element of the system assurance context and related vulnerabilities are examined in the context of mission-critical threats. 5) - Candidate alternative solution classes that span the potential solution space are identified. 6) These classes can range from simple operational changes to various software system developments or modifications. This solution space can include the identification of existing assets, systems, and software products suitable for reuse, and changes in services that can address the need for operational or functional modifications. This includes deducing what potential expected services will be needed. The solution space characterization often invokes the Architecture Definition process for a user architecture viewpoint, resulting in architecture views (e.g., capability views, program views and operational views) as proposed by ISO/IEC/IEEE 42010. [ISO/IEC/IEEE 12207:2017, 6.4.1.3 c) 1)] 7) Define preliminary operational concepts and other concepts in life cycle stages. [ISO/IEC/IEEE 12207:2017, 6.4.1.3 c) 2)] 8) Identify candidate alternative solution classes that span the potential solution space.
03-08	Identify business opportunities	Description	1) - Customer complaints, problems and opportunities are analysed in the context of relevant trade-space factors. 2) This analysis is focused on understanding the scope, basis, or drivers of the problems or opportunities, as opposed to the synthesis that is the focus of system analysis and decision management needed for trade studies. The focus here includes changes in mission requirements, business opportunities, capabilities, performance improvement, or lack of existing systems, security and safety improvement, factors such as cost and effectiveness, regulation changes, user dissatisfaction, and PESTEL factors (Political, Economic, Social, Technological, Environmental, and Legal). Relevant factors can be identified through external, internal, or SWOT (Strengths, Weaknesses, Opportunities and Threats) analysis. 3) The outputs of the analysis are considered as part of the portfolio management decisions. 4) - The mission, business, or operational problem or opportunity is defined. 5) This definition includes the context and any key parameters, without regard to a specific solution, since the solution can be an operational change, a change to an existing product or service, or a new system. [ISO/IEC/IEEE 12207:2017, 6.4.1.3 b) 1)] 6) Analyse customer complaints, problems and opportunities in the context of relevant trade-space factors. [ISO/IEC/IEEE 12207:2017, 6.4.1.3 b) 2)] 7) Define the mission, business, or operational problem or opportunity.
03-09	Information measures	Description	1) - Measures that satisfy the information needs are selected and specified. [ISO/IEC/IEEE 12207:2017, 6.3.7.3 a) 4)] 2) Select and specify measures that satisfy the information needs.

Table C.1 *(continued)*

Reference	Name	Category	Characteristics
03-10	Life cycle model	Description	1) - Policies and procedures are established for process management and deployment that are consistent with organizational strategies. 2) - The processes are established that implement the requirements of this document and that are consistent with organizational strategies. 3) - The roles, responsibilities, accountabilities, and authorities to facilitate implementation of processes and the strategic management of life cycles are defined. 4) - Business criteria are defined that control progression through the life cycle. 5) The decision-making criteria regarding entering and exiting each life cycle stage and key milestones are established. These are sometimes expressed in terms of business achievement. 6) - Standard life cycle models are established for the organization that are comprised of stages and define the purpose and outcomes for each stage. 7) The life cycle model comprises one or more stage models, as needed. It is assembled as a sequence of stages that can overlap or iterate, as appropriate for the system-of-interest's scope, magnitude, complexity, changing needs and opportunities. Stages are illustrated in ISO/IEC TS 24748-1 using a commonly encountered example of life cycle stages. Specific examples for systems and software are provided in ISO/IEC TR 24748-2 and ISO/IEC TR 24748-3. The life cycle processes and activities are selected, tailored as appropriate and employed in a stage to fulfill the purpose and outcomes of that stage. 8) - A life cycle model that is comprised of stages using the defined life cycle models of the organization is defined and maintained. 9) ISO/IEC TS 24748-1 provides detailed information regarding life cycle stages and the definition of an appropriate life cycle model. It defines a general set of exemplar system life cycle stages, including Concept, Development, Production, Utilization, Support and Retirement. It also identifies a generic exemplar set of software life cycle stages, including Needs determination, Concept exploration and definition, Demonstration and evaluation, Engineering/development, Production/manufacturing, Deployment/sales, Operations, Maintenance and support, and Retirement. 10) - The processes that will be applied on the project are defined and maintained. 11) These processes are based on the defined processes of the organization (see Life Cycle Model Management process). Annex A contains information on tailoring that can be used to address project-specific needs. The definition of the processes includes the entry and exit criteria, inputs, process sequence constraints (predecessor/successor relationships), process concurrency requirements (what processes and tasks are to be worked concurrently with other process area tasks or activities), Measures of Effectiveness/Measures of Performance attributes, and scope and cost parameters (for critically important cost estimation). 12) Identifying interfaces with other projects or organizational units is addressed through the Portfolio Management process. 13) - Achievement criteria are defined for the life cycle stage decision gates, delivery dates and major dependencies on external inputs or outputs.

Table C.1 *(continued)*

Reference	Name	Category	Characteristics
			14) The time intervals between internal reviews are defined in accordance with organizational policy on issues such as business and system criticality, schedule and technical risks. 15) - A life cycle model that is comprised of stages using the defined life cycle models of the organization is defined and maintained. 16) ISO/IEC TS 24748-1 provides detailed information regarding life cycle stages and the definition of an appropriate life cycle model. It defines a general set of exemplar system life cycle stages, including Concept, Development, Production, Utilization, Support and Retirement. It also identifies a generic exemplar set of software life cycle stages, including Needs determination, Concept exploration and definition, Demonstration and evaluation, Engineering/development, Production/manufacturing, Deployment/sales, Operations, Maintenance and support, and Retirement. 17) - The processes that will be applied on the project are defined and maintained. 18) These processes are based on the defined processes of the organization (see Life Cycle Model Management process). Annex A contains information on tailoring that can be used to address project-specific needs. The definition of the processes includes the entry and exit criteria, inputs, process sequence constraints (predecessor/successor relationships), process concurrency requirements (what processes and tasks are to be worked concurrently with other process area tasks or activities), Measures of Effectiveness/Measures of Performance attributes, and scope and cost parameters (for critically important cost estimation). 19) Identifying interfaces with other projects or organizational units is addressed through the Portfolio Management process. 20) - Achievement criteria are defined for the life cycle stage decision gates, delivery dates and major dependencies on external inputs or outputs. 21) The time intervals between internal reviews are defined in accordance with organizational policy on issues such as business and system criticality, schedule and technical risks. [ISO/IEC/IEEE 12207:2017, 6.2.1.3 a) 1)] 22) Establish policies and procedures for process management and deployment that are consistent with organizational strategies. [ISO/IEC/IEEE 12207:2017, 6.2.1.3 a) 2)] 23) Establish the processes that implement the requirements of this document and that are consistent with organizational strategies. [ISO/IEC/IEEE 12207:2017, 6.2.1.3 a) 4)] 24) Define business criteria that control progression through the life cycle. [ISO/IEC/IEEE 12207:2017, 6.2.1.3 a) 5)] 25) Establish standard life cycle models for the organization that are comprised of stages and define the purpose and outcomes for each stage. [ISO/IEC/IEEE 12207:2017, 6.2.1.3 a) 3)] 26) Define and maintain a life cycle model that is comprised of stages using the defined life cycle models of the organization. [ISO/IEC/IEEE 12207:2017, 6.2.1.3 a) 5)] 27) Define and maintain the processes that will be applied on the project. [ISO/IEC/IEEE 12207:2017, 6.2.1.3 b) 2)] 28) Define achievement criteria for the life cycle stage decision gates, delivery dates and major dependencies on external inputs or outputs.
03-11	Life cycle model: Responsibilities	Description	[ISO/IEC/IEEE 12207:2017, 6.2.1.3 a) 3)] 1) Define the roles, responsibilities, accountabilities, and authorities to facilitate implementation of processes and the strategic management of life cycles.
03-12	Organization skills identification	Description	1) - Skills of personnel are identified and recorded. [ISO/IEC/IEEE 12207:2017, 6.2.4.3 a) 2)] 2) Identify and record skills of personnel.
03-13	Organizational characteristics	Description	1) - The characteristics of the organization that are relevant to measurement, such as business and technical objectives are described. [ISO/IEC/IEEE 12207:2017, 6.3.7.3 a) 2)] 2) Describe the characteristics of the organization that are relevant to measurement, such as business and technical objectives.

Table C.1 *(continued)*

Reference	Name	Category	Characteristics
03-14	Organizational information needs	Description	1) - The information needs are identified and prioritized. 2) The information needs are based on the organization's business objectives, the project objectives, identified risks, and other items related to project decisions. Measurements can relate to projects, processes, products, or decisions. [ISO/IEC/IEEE 12207:2017, 6.3.7.3 a) 3)] 3) Identify and prioritize the information needs.
03-15	Organizational skill needs	Description	1) - Skill needs based on current and expected projects are identified. [ISO/IEC/IEEE 12207:2017, 6.2.4.3 a) 1)] 2) Identify skill needs based on current and expected projects.
03-16	Project accountabilities and authorities	Description	1) - [Projects,] accountabilities and authorities are defined. [ISO/IEC/IEEE 12207:2017, 6.2.3.3 a) 3)] 2) Define projects, accountabilities and authorities.
03-17	Project goals	Description	1) - The project objectives and constraints are identified. 2) Objectives and constraints include performance and other quality aspects, cost, time and customer and user satisfaction. Each objective is identified with a level of detail that permits selection, tailoring and implementation of the appropriate processes and activities. 3) ISO/IEC 15026 Systems and software assurance, ISO/IEC 27001 Information Security Management System and ISO/IEC 27036, Information Security for Supplier Relationships, provide additional guidance on objectives and constraints related to assurance and security. 4) - The project scope is identified as established in the agreement. 5) This includes the relevant activities required to satisfy business decision criteria and complete the project successfully. A project can have responsibility for one or more stages in the complete software system life cycle. Project Planning includes defining appropriate actions for maintaining project plans, performing assessments and controlling the project. [ISO/IEC/IEEE 12207:2017, 6.3.1.3 a) 1)] 6) Identify the project objectives and constraints. [ISO/IEC/IEEE 12207:2017, 6.3.1.3 a) 2)] 7) Define the project scope as established in the agreement.
03-18	Project interface description	Description	1) - Multi-project interfaces and dependencies to be managed or supported by each project are identified. 2) This includes the use or reuse of enabling systems used by more than one project and the use or reuse of common system elements, including software elements, by more than one project. 3) Understanding each project in the context of the enterprise architecture helps to ensure interfaces and constraints are identified. [ISO/IEC/IEEE 12207:2017, 6.2.3.3 a) 6)] 4) Identify multi-project interfaces and dependencies to be managed or supported by each project.
03-19	Project portfolio goals	Description	[ISO/IEC/IEEE 12207:2017, 6.2.3.3 a) 4)] 1) Identify the expected goals, objectives, and outcomes of each project.
03-20	Project resource allocation	Description	1) - Resources are identified and allocated for the achievement of project goals and objectives. [ISO/IEC/IEEE 12207:2017, 6.2.3.3 a) 5)] 2) Identify and allocate resources for the achievement of project goals and objectives.
03-21	Projects portfolio	Description	1) - Projects, [accountabilities and authorities] are defined. [ISO/IEC/IEEE 12207:2017, 6.2.3.3 a) 3)] 2) Define projects, accountabilities and authorities.
03-22	Quality management authorities and responsibilities	Description	1) - Responsibilities and authority for implementation of quality management are defined. 2) Resources for quality management are often assigned from distinct organizations for independence from project management. [ISO/IEC/IEEE 12207:2017, 6.2.5.3 a) 2)] 3) Define responsibilities and authority for implementation of quality management.
03-23	Request for proposal (RFP)	Description	1) - The existence and identity is determined of an acquirer who has a need for a product or service. 2) This is often generated through the Business or Mission Analysis process. For a product or service developed for consumers, an agent, e.g., a marketing function within the supplier organization, often represents the acquirer. [ISO/IEC/IEEE 12207:2017, 6.1.2.3 a) 1)] 3) Determine the existence and identity of an acquirer who has a need for a product or service.

Table C.1 *(continued)*

Reference	Name	Category	Characteristics
03-24	Response to RFP	Description	1) - A response is prepared that satisfies the solicitation. [ISO/IEC/IEEE 12207:2017, 6.1.2.3 b) 2)] 2) Prepare a response that satisfies the solicitation.
03-25	Risk analysis	Description	1) - The likelihood of occurrence and consequences of each identified risk is estimated. 2) Consequences of a risk typically involve technical, schedule, cost, or quality impacts. 3) - Each risk is evaluated against its risk thresholds. 4) - For each risk that does not meet its risk threshold, recommended treatment strategies and measures are defined and recorded. 5) Risk treatment strategies include, but are not limited to, eliminating the risk, reducing its likelihood of occurrence or severity of consequence, or accepting the risk. Treatments also include taking or increasing risk in order to pursue an opportunity. Measures provide information about the effectiveness of the treatment alternatives. [ISO/IEC/IEEE 12207:2017, 6.3.4.3 c) 2)] 6) Estimate the likelihood of occurrence and consequences of each identified risk. [ISO/IEC/IEEE 12207:2017, 6.3.4.3 c) 3)] 7) Evaluate each risk against its risk thresholds. [ISO/IEC/IEEE 12207:2017, 6.3.4.3 c) 4)] 8) For each risk that does not meet its risk threshold, define and record recommended treatment strategies and measures.
03-26	Risk identification	Description	1) - Risks are identified in the categories described in the risk management context. 2) Risks are commonly identified through various analyses, such as safety, reliability, security, and performance analyses; technology, architecture, and readiness assessments; and trade studies. These risks are often identified early in the life cycle and continue into the utilization, support, and retirement of the software system. Additionally, risks are often identified through the analysis of measurements of the evolving software system. [ISO/IEC/IEEE 12207:2017, 6.3.4.3 c) 1)] 3) Identify risks in the categories described in the risk management context.
03-27	Risk management profile	Description	1) - A risk profile is established and maintained. 2) - A risk profile is established and maintained. 3) The risk profile records: the risk management context; a record of each risk's state including its likelihood of occurrence, consequences, and risk thresholds; the priority of each risk based on risk criteria supplied by the stakeholders; and the risk action requests along with the status of their treatment. The risk profile is updated when there are changes in an individual risk's state. The priority in the risk profile is used to determine the application of resources for treatment. 4) - The relevant risk profile is periodically provided to stakeholders based upon their needs. [ISO/IEC/IEEE 12207:2017, 6.3.4.3 b) 1)] 5) Define and record the risk thresholds and conditions under which a level of risk may be accepted. [ISO/IEC/IEEE 12207:2017, 6.3.4.3 b) 2)] 6) Establish and maintain a risk profile. [ISO/IEC/IEEE 12207:2017, 6.3.4.3 b) 3)] 7) Periodically provide the relevant risk profile to stakeholders based upon their needs.

Table C.1 *(continued)*

Reference	Name	Category	Characteristics
03-28	Software system design definition	Description	1) - The design definition strategy is defined, consistent with the selected life cycle model and anticipated design artifacts. 2) The software design strategy can include initial or incremental decomposition into system elements; creation of various views of automated procedures, data structures and control systems; selection of design patterns, or progressively more detailed definition of objects and their relationships. 3) - Design principles and design characteristics are selected and prioritized. 4) Design principles include controlling ideas such as abstraction, modularization and encapsulation, separation of interface and implementation, concurrency, and persistence of data. Security considerations include the principle of least privilege, layered defences, restricted access to system services, and other considerations to minimize and defend the system attack surface. Design characteristics include, for example, availability, fault tolerance and resilience, scalability, usability, capacity and performance, testability, portability, and affordability. [ISO/IEC/IEEE 12207:2017, 6.4.5.3 a) 1)] 5) Define the design definition strategy, consistent with the selected life cycle model and anticipated design artifacts. [ISO/IEC/IEEE 12207:2017, 6.4.5.3 a) 2)] 6) Select and prioritize design principles and design characteristics.
03-29	Software system element design	Description	1) - Architectural and design characteristics are transformed into the design of software system elements. 2) Characteristics apply to physical and logical system elements, such as database structures, provisions for memory and storage, software processes and controls, external interfaces such as user interfaces, or services. ISO 9241-210 provides human centred design/ergonomic design guidelines. 3) - The necessary design enablers are defined, prepared or obtained. 4) Design enablers include models, equations, algorithms, calculations, formal expressions and values of parameters, patterns, and heuristics, which are associated with design characteristics using adequate representation such as drawings, logical diagrams, flowcharts, coding conventions, logic patterns, information models, business rules, user profiles, scenarios, use cases or user stories, and tables of metrics and their values, e.g., function points or user story points. 5) - Design alternatives are examined and feasibility of implementation. 6) For the software system and software elements, typically reuse, adaptation, outsourced service, or new development are examined. 7) Assess the feasibility of realizing design characteristics. If warranted by assessment results, examine other alternative design options or perform trade-offs in the architecture or requirements when design characteristics are impractical to implement. 8) - The interfaces among the software system elements and with external entities are refined or defined.

Table C.1 *(continued)*

Reference	Name	Category	Characteristics
			9) Interfaces are identified and defined in the Architecture Definition process (see 6.4.4) to the level or extent needed for the architecture intent and understanding. These are refined in the Design Definition process based on the design characteristics, interfaces, and interactions of software elements with other elements composing the software system and with external entities. Additional interfaces are sometimes identified and defined that were not addressed in the architecture definition. 10) - The design artifacts are established. 11) This task formalizes the design characteristics of the software system elements through dedicated artifacts, depending on the implementation technology. Examples of artifacts include prototypes, data models, pseudocode, entity relationship diagrams, use cases, user role and privilege matrixes, interface specifications, service descriptions, and procedures. Design artifacts are developed, obtained, or modified for selected alternatives. The data is associated with detailed acceptable margins for implementation (if relevant at this process or task iteration). [ISO/IEC/IEEE 12207:2017, 6.4.5.3 b) 1)] 12) Transform architectural and design characteristics into the design of software system elements. [ISO/IEC/IEEE 12207:2017, 6.4.5.3 b) 2)] 13) Define and prepare or obtain the necessary design enablers. [ISO/IEC/IEEE 12207:2017, 6.4.5.3 b) 3)] 14) Examine design alternatives and feasibility of implementation. [ISO/IEC/IEEE 12207:2017, 6.4.5.3 b) 4)] 15) Refine or define the interfaces among the software system elements and with external entities. [ISO/IEC/IEEE 12207:2017, 6.4.5.3 b) 5)] 16) Establish the design artifacts.
03-30	Software system element evaluation	Description	1) - Technologies required for each element composing the software system are determined. 2) Several technologies are sometimes used for a given software system element, e.g. internet presence, embedded systems, adaptation of open source software, human operator roles. 3) - Candidate alternatives are identified for the software system elements. 4) Alternatives include newly designed and constructed items; adaptations of existing product lines, components, objects, or services; or acquisition or reuse of Non-Developed Items (NDI). NDI include COTS (Commercial-Off-The-Shelf) or FOSS (Free and Open Source Software) packages or elements, reuse of a previous design, or existing assets, including acquirer provided items. 5) - Each candidate is assessed alternative against criteria developed from expected design characteristics and element requirements to determine suitability for the intended application. 6) A make-or-buy decision and resulting implementation and integration approach typically involve trade-offs of the design criteria, including cost. Design choices commonly consider enabling systems required to test the candidate alternative (test-driven design and development) and sustainability over the system life, including maintenance costs. The Maintenance process can be used to determine the suitability of the design for long-term maintenance and sustainability. 7) - The preferred alternatives among candidate design solutions for the software system elements are chosen. 8) The System Analysis process can be used for analyses and assessments to support the Decision Management process in performing the selection. Design reviews are conducted using the Validation process. [ISO/IEC/IEEE 12207:2017, 6.4.5.3 c) 1)] 9) Determine technologies required for each element composing the software system. [ISO/IEC/IEEE 12207:2017, 6.4.5.3 c) 2)] 10) Identify candidate alternatives for the software system elements. [ISO/IEC/IEEE 12207:2017, 6.4.5.3 c) 3)] 11) Assess each candidate alternative against criteria developed from expected design characteristics and element requirements to determine suitability for the intended application. [ISO/IEC/IEEE 12207:2017, 6.4.5.3 c) 4)] 12) Choose the preferred alternatives among candidate design solutions for the software system elements.

Table C.1 *(continued)*

Reference	Name	Category	Characteristics
03-31	Stakeholder Needs	Description	1) - Context of use is defined within the concept of operations and the preliminary life cycle concepts. 2) Context of use is often captured using a Context of Use Description [ISO/IEC 25063]. Preliminary life cycle concepts are developed by the Business or Mission Analysis process. 3) - Stakeholder needs are identified. 4) Identification of stakeholder needs includes elicitation of needs directly from the stakeholders, identification of implicit stakeholder needs based on domain knowledge and context understanding, and documented gaps from previous activities. Needs often include measures of effectiveness. Functional analysis is often used to aid the elicitation of needs. Also quality characteristics of the quality model in ISO/IEC 25010 and quality model application to requirements analysis in ISO/IEC 25030 are useful to elicit and identify quality requirements of non-functional requirements, which are often implicit stakeholder needs. 5) The SWEBOK, Guide to the Software Engineering Body of Knowledge, Software Requirements knowledge area discusses some additional techniques for eliciting and clarifying software requirements, such as, prototyping, observation, user stories to determine required functionality, data mining, and analyzing competitor's products. 6) Stakeholder needs describe the needs, wants, desires, expectations and perceived constraints of identified stakeholders. Understanding stakeholder needs for the minimum security and privacy requirements necessary for the operational environment minimizes the potential for disruption in plans, schedules, and performance. If significant issues are likely to arise relating to users and other stakeholders and their involvement in or interaction with a software system, recommendations for identifying and treating human-system issues can be found in ISO TS 18152. 7) - Needs are prioritized and down-selected. 8) The Decision Management process is typically used to support prioritization. The System Analysis process is used to analyse needs for feasibility or other factors. 9) - The stakeholder needs and rationale are defined. 10) Needs concentrate on system purpose and behavior, and are described in the context of the operational environment and conditions. It is useful to trace needs to their sources and rationale. [ISO/IEC/IEEE 12207:2017, 6.4.2.3 b) 1)] 11) Define context of use within the concept of operations and the preliminary life cycle concepts. [ISO/IEC/IEEE 12207:2017, 6.4.2.3 b) 2)] 12) Identify stakeholder needs. [ISO/IEC/IEEE 12207:2017, 6.4.2.3 b) 3)] 13) Prioritize and down-select needs. [ISO/IEC/IEEE 12207:2017, 6.4.2.3 b) 4)] 14) Define the stakeholder needs and rationale.
03-32	System operational concept	Description	1) - A representative set of scenarios are defined to identify the required capabilities that correspond to anticipated operational and other life cycle concepts. 2) Scenarios are used to analyse the operation of the system in its intended environment in order to identify additional needs or requirements that perhaps have not been explicitly identified by any of the stakeholders, e.g., legal, regulatory and social obligations The context of use of the system is identified and analysed, including the activities that users perform to achieve system objectives, the relevant characteristics of the users (e.g., expected training and knowledge, frequency of system use, responsibilities, accessibility concerns), the physical environment (e.g., available light, temperature) and any equipment to be used (e.g., protective or communication equipment). The social and organizational influences on users that affect system use or constrain its design are analysed when applicable. Scenarios centered on attackers, their environments, tools, techniques, and capabilities are key considerations for operational concept development. Scenarios are prioritized in order to reflect the weighted importance of the various operational needs. 3) These scenarios often motivate updates to the operational or other life cycle concepts. Abuse and failure scenarios highlight the need for additional functional requirements (or more specific derived requirements) to mitigate risks that are identified in the abuse or failure scenarios. 4) - The factors affecting interactions between users and the system are identified.

Table C.1 *(continued)*

Reference	Name	Category	Characteristics
			5) Usability requirements take into account human capabilities and skills limitations. Where possible, applicable standards, e.g., ISO 9241, and accepted professional practices are used. 6) If usability is important, usability requirements are planned, specified, and implemented through the life cycle processes. Refer to ISO TS 18152 for information on human-system issues and ISO/IEC 25060:2010 for information on usability. [ISO/IEC/IEEE 12207:2017, 6.4.2.3 c) 1)] 7) Define a representative set of scenarios to identify the required capabilities that correspond to anticipated operational and other life cycle concepts. [ISO/IEC/IEEE 12207:2017, 6.4.2.3 c) 2)] 8) Identify the factors affecting interactions between users and the system. i) Anticipated physical, mental, and learned capabilities of the users; ii) Workplace, environment and facilities, including other equipment in the context of use; iii) Normal, unusual, and emergency conditions; and iv) Operator and user recruitment, training and culture.
03-33	System requirements analysis	Description	1) - The complete set of system/software requirements is analysed. 2) Requirements are analysed for characteristics of individual requirements, as well as characteristics of the set of requirements. Potential analysis characteristics include that the requirements are necessary, implementation-free, unambiguous, consistent, complete, singular, feasible, traceable, verifiable, affordable, and bounded. The Verification process is used to determine if requirements meet the attributes and characteristics of good requirements. In some cases, the technical and economic feasibility of validating and verifying alternative formulations of requirements is evaluated. ISO/IEC/IEEE 29148 provides additional information on characteristics of requirements. 3) The System Analysis process can be used to assess feasibility, affordability, balance and other requirements characteristics. The System Analysis process is used to determine appropriate values for requirement parameters, considering the estimated cost, schedule, and technical performance of the software system. 4) Anticipating that some requirements can be achieved incrementally or even deferred or waived, requirements can be prioritized. 5) - Critical performance measures that enable the assessment of technical achievement are defined. 6) This includes defining technical and quality measures and critical performance parameters associated with each effectiveness measure identified in the software system element requirements. The critical performance measures (e.g., measures of performance and technical performance measures) are analysed and reviewed to help ensure system/software requirements are met and to help ensure identification of project cost, schedule or performance risk associated with any non-compliance. ISO/IEC 15939 provides a process to identify, define and use appropriate measures. INCOSE TP-2003-020-01, Technical Measurement, provides information on the selection, definition and implementation of critical performance measures. The ISO/IEC 25000 series of standards provides relevant quality measures. 7) - The analysed requirements are fed back to applicable stakeholders for review. 8) Feedback helps validate that the specified requirements have been adequately captured and expressed. Confirmation is made that they are a necessary and sufficient response to stakeholder requirements and a necessary and sufficient input to other processes, in particular software architecture, design, and verification. The Validation process is used to determine if the system/software requirements address the users' needs. 9) - Issues, deficiencies, conflicts, and weaknesses within the complete set of requirements are identified and resolved. 10) This includes requirements that are not verifiable, ambiguous, violate the characteristics for individual requirements, or are inconsistent with others in the set of requirements. Resolution of issues with requirements can be iterative within certain life cycle models. [ISO/IEC/IEEE 12207:2017, 6.4.3.3 c) 1)] 11) Analyse the complete set of system/software requirements. [ISO/IEC/IEEE 12207:2017, 6.4.3.3 c) 2)] 12) Define critical performance measures that enable the assessment of technical achievement. [ISO/IEC/IEEE 12207:2017, 6.4.3.3 c) 3)] 13) Feed back the analysed requirements to applicable stakeholders for review. [ISO/IEC/IEEE 12207:2017, 6.4.3.3 c) 4)] 14) Identify and resolve issues, deficiencies, conflicts, and weaknesses within the complete set of requirements.

Table C.1 *(continued)*

Reference	Name	Category	Characteristics
03-34	System requirements definition	Description	1) - The functional boundary of the software system or element is defined in terms of the behavior and properties provided. 2) The functional boundary definition is partly based on the context of use and operational scenarios defined in the frame of the Stakeholder Needs and Requirements Definition process. This includes the software system's stimuli (input) and its responses to users and external systems, and an analysis and description of the required interactions between the software system and its operational environment in terms of interface properties and constraints, such as procedural flows, calling orders, data formats and flows, throughput, and timing. This establishes the expected software system behavior, expressed in quantitative terms, at its boundary. For software, boundaries are commonly expressed in Application Program Interfaces (API) and a graphical user interface (GUI) or interface files or services, including data formats. Annex E (E.5) provides an interface management view of the life cycle processes. 3) - The system/software requirements definition strategy is defined. 4) This includes the approach to be used to identify and define, and manage the system/software requirements with the selected life cycle model, e.g., evolutionary, incremental or iterative. Many factors can influence the strategy, e.g., complexity of the software system and information and functions to be managed; need for ready access and common understanding by multiple team members; degree of collaborative involvement by the acquirer or user representatives throughout the development stage; whether the project involves a new development, a modification, re-use or integration of existing systems; and process documentation requirements including period of retention. The life cycle model will influence when and how often the system/software requirements definition will be done ISO/IEC/IEEE 12207:2017, Annex H describes the progressive development of requirements in projects using agile methods. [ISO/IEC/IEEE 12207:2017, 6.4.3.3 a) 1)] 5) Define the functional boundary of the software system or element in terms of the behavior and properties provided. [ISO/IEC/IEEE 12207:2017, 6.4.3.3 a) 2)] 6) Define the system/software requirements definition strategy.
04-02	Business strategy	Plan	1) - The business or mission analysis strategy is defined. 2) This includes the approach to be used to identify and define the problem space, characterize the solution space and select a solution class. [ISO/IEC/IEEE 12207:2017, 6.4.1.3 a) 2)] 3) Define the business or mission analysis strategy.
04-03	Configuration Management Plan	Plan	1) - A configuration management strategy is defined, including approaches for the following: i) Governance of CM, including roles, responsibilities, accountabilities, and authorities, and use of configuration control (change control) boards; and ii) Consideration of the level of risk and impact in approval of configuration baselines and regular and emergency change requests. iii) Coordination of CM across the set of acquirer, supplier, and supply chain organizations for the life of the software system, or the extent of the agreement or project, as appropriate. iv) Control of access and changes to and disposition of configuration items. v) The necessary baselines to be established, including criteria or events for commencing configuration control and maintaining baselines of evolving configurations. vi) Control of software licenses, data rights, and other intellectual property assets. vii) Frequency, priorities, and content of software versions and releases. viii) The audit strategy and the responsibilities for validating continuous integrity and security of the configuration definition information. ix) Change management, including preparing stakeholders and especially users for changes in operational software systems and services. 2) Regularly scheduled changes to apply software patches using approved procedures or check-in and check-out of unit-tested software elements under development are typically performed automatically, or reviewed and approved daily as a matter of routine. In comparison, significant changes to the software system design with major impact on project cost and schedule can involve extensive analyses, consultations with suppliers, stakeholder reviews, and approvals at the highest levels of the organization. 3) For complex software systems, trade-off studies are performed, e.g., to select an appropriate automated tool to support SCM needs and scope as identified in the strategy.

Table C.1 *(continued)*

Reference	Name	Category	Characteristics
			4) Additional guidance regarding configuration management activities can be found in ISO 10007, IEEE Std 828, and SAE NSI/EIA-649-B. 5) The SWEBOK, Guide to the Software Engineering Body of knowledge, provides detailed discussion on SCM. This knowledge area addresses SCM in the context of a system, SCM project and process planning, SCM plan and outline, tool selection, subcontractor control, surveillance and other audits, software configuration items and relationships, software libraries, and Configuration Management process activities. 6) The SCM strategy is commonly documented in a plan, e.g., a configuration management plan, or sometimes in a project's SEMP, SDP, or Project Management Plan (PMP). The strategy planning for Configuration Management is coordinated through the Project Planning process. In establishing points to establish baselines and conduct audits, CM planning is aligned with the software life cycle. The frequency of recurring SCM activities aligns with the iteration of technical processes and stages. SCM planning typically includes deciding when to review Configuration Management planning, what conditions require updating the CM plan, and who is authorized to change the CM plans and items held in configuration control. 7) - The storage, archive and retrieval procedures are defined for configuration items, CM artifacts, and records. [ISO/IEC/IEEE 12207:2017, 6.3.5.3 a) 1)] 8) Define a configuration management strategy, including approaches for the following: i) Governance of CM, including roles, responsibilities, accountabilities, and authorities, and use of configuration control (change control) boards; and ii) Consideration of the level of risk and impact in approval of configuration baselines and regular and emergency change requests. iii) Coordination of CM across the set of acquirer, supplier, and supply chain organizations for the life of the software system, or the extent of the agreement or project, as appropriate. iv) Control of access and changes to and disposition of configuration items. v) The necessary baselines to be established, including criteria or events for commencing configuration control and maintaining baselines of evolving configurations. vi) Control of software licenses, data rights, and other intellectual property assets. [ISO/IEC/IEEE 12207:2017, 6.3.5.3 a) 2)] 9) Define the storage, archive and retrieval procedures for configuration items, CM artifacts, and records.
04-04	Corrective and preventive actions plan	Plan	1) - Corrective actions are planned when quality management objectives are not achieved. 2) - Preventive actions are planned when there is a sufficient risk that quality management objectives will not be achieved. [ISO/IEC/IEEE 12207:2017, 6.2.5.3 c) 1)] 3) Plan corrective actions when quality management objectives are not achieved. [ISO/IEC/IEEE 12207:2017, 6.2.5.3 c) 2)] 4) Plan preventive actions when there is a sufficient risk that quality management objectives will not be achieved.

Table C.1 *(continued)*

Reference	Name	Category	Characteristics
04-06	Disposal strategy	Plan	1) - A disposal strategy is defined for the software system, to include each system element and to identify and address critical disposal needs, including the following considerations: i) Permanent termination of the system's functions and delivery of services, e.g., physical destruction of data storage devices, or transition of the software system elements for future reuse in modified or adapted form; ii) Identification of ownership and responsibility for retention or destruction of data and intellectual property in the software system; iii) Transformation of the product into, or retention in a socially and physically acceptable state, thereby avoiding subsequent adverse effects on stakeholders, society and the environment; iv) The health, safety, security and privacy concerns applicable to disposal actions and to the long-term condition of resulting physical material and information; v) Notification to relevant stakeholders of significant disposal activities, e.g., retirement or replacement of a system, software products or services, retirement schedule, or replacement options; and vi) Identification of schedules, actions, responsibilities, and resources for disposal activities. 2) - Constraints on disposal are identified for the system/software requirements, architecture and design characteristics, or implementation techniques. 3) This includes access to and availability of archives or longterm storage locations and available skilled resources for system deactivation and communication with stakeholders and interface partners. 4) - Containment facilities, storage locations, inspection criteria and storage periods, are specified, if the software system or data is to be stored, consistent with security and environmental considerations. 5) - Preventive methods are defined to preclude disposed elements and materials that should not be repurposed, reclaimed or reused from re-entering the supply chain. [ISO/IEC/IEEE 12207:2017, 6.4.14.3 a) 1)] 6) Define a disposal strategy for the software system, to include each system element and to identify and address critical disposal needs, including the following considerations: i) Permanent termination of the system's functions and delivery of services, e.g., physical destruction of data storage devices, or transition of the software system elements for future reuse in modified or adapted form; ii) Identification of ownership and responsibility for retention or destruction of data and intellectual property in the software system; iii) Transformation of the product into, or retention in a socially and physically acceptable state, thereby avoiding subsequent adverse effects on stakeholders, society and the environment; iv) The health, safety, security and privacy concerns applicable to disposal actions and to the long-term condition of resulting physical material and information; v) Notification to relevant stakeholders of significant disposal activities, e.g., retirement or replacement of a system, software products or services, retirement schedule, or replacement options; and vi) Identification of schedules, actions, responsibilities, and resources for disposal activities. [ISO/IEC/IEEE 12207:2017, 6.4.14.3 a) 2)] 7) Identify constraints on disposal for the system/software requirements, architecture and design characteristics, or implementation techniques. [ISO/IEC/IEEE 12207:2017, 6.4.14.3 a) 5)] 8) Specify containment facilities, storage locations, inspection criteria and storage periods, if the software system or data is to be stored, consistent with security and environmental considerations. [ISO/IEC/IEEE 12207:2017, 6.4.14.3 a) 6)] 9) Define preventive methods to preclude disposed elements and materials that should not be repurposed, reclaimed or reused from re-entering the supply chain.

Table C.1 *(continued)*

Reference	Name	Category	Characteristics
04-07	Implementation Plan	Plan	1) - An implementation strategy is defined, with consideration of the following: i) development policies and standards, including standards that govern applicable safety, security, privacy and environmental practices; programming or coding standards; unit test policies; and language-specific standards for implementing security features; ii) For reused or adapted software, methods to determine the level, source, and suitability of the reused system elements and security of the supply chain; iii) procedures and methods for software development (construction) and development of unit tests; and the use of peer reviews, unit tests, and walkthroughs during implementation; iv) use of CM control during software construction; v) change management considerations for manual processes; vi) implementation priorities to support data and software migration and transition, along with retirement of legacy systems; 2) The implementation strategy is commonly recorded in a project's SDP or SEMP, or sometimes in a PMP. 3) - Constraints are identified from the implementation strategy and implementation technology on the system/software requirements, architecture characteristics, design characteristics, or implementation techniques. 4) Constraints include current or anticipated limitations of the chosen implementation technology (e.g., for software, the operating system, database management system, web services), acquirer furnished materials or system elements for adaptation, and limitations resulting from the use of required implementation-enabling systems. 5) The implementation strategy for software typically identifies and allocates 'implement-to' criteria, e.g., software architecture and design characteristics, system/software requirements including software assurance, usability considerations, configuration management, traceability, or other conditions to be satisfied. These criteria can clarify appropriate unit aggregation levels, specifications, and constraints. [ISO/IEC/IEEE 12207:2017, 6.4.7.3 a) 1)] 6) Define an implementation strategy, with consideration of the following: i) development policies and standards, including standards that govern applicable safety, security, privacy and environmental practices; programming or coding standards; unit test policies; and language-specific standards for implementing security features; ii) For reused or adapted software, methods to determine the level, source, and suitability of the reused system elements and security of the supply chain; iii) procedures and methods for software development (construction) and development of unit tests; and the use of peer reviews, unit tests, and walkthroughs during implementation; iv) use of CM control during software construction; v) change management considerations for manual processes; vi) implementation priorities to support data and software migration and transition, along with retirement of legacy systems; [ISO/IEC/IEEE 12207:2017, 6.4.7.3 a) 2)] 7) Identify constraints from the implementation strategy and implementation technology on the system/software requirements, architecture characteristics, design characteristics, or implementation techniques.
04-08	Information management plan	Plan	1) - The strategy for information management is defined. 2) Information about the same topic can be developed in different ways at different points in the life cycle and for different audiences. 3) - The items of information that will be managed are defined. 4) This includes the information that will be managed during the software life cycle and possibly maintained for a defined period beyond. This is done according to organizational policy, agreements, or legislation. 5) - Authorities and responsibilities for information management are designated. 6) Due regard is paid to information and data legislation, security and privacy, e.g., ownership, agreement restrictions, rights of access to data and ownership of data, intellectual property and patents. Where restrictions or constraints apply, information is identified accordingly. Staff members with knowledge of such items of information are informed of their obligations and responsibilities.

Table C.1 *(continued)*

Reference	Name	Category	Characteristics
			7) - The content, formats and structure of information items is defined. 8) The information originates and terminates in many forms (e.g., audio-visual, textual, graphical, numerical) and mediums (e.g., electronic, printed, magnetic, optical). Organization constraints, e.g., infrastructure, interorganizational communications, and distributed project workings, are taken into account. Relevant information item standards and conventions are used according to policy, agreements and legislation constraints. 9) - Information maintenance actions are defined. 10) Information maintenance includes status reviews of stored information for integrity, validity and availability. It also includes any needs for replication or transformation to an alternative medium, as necessary, either to retain infrastructure as technology changes so that archived media can be read or to migrate archived media to newer technology. [ISO/IEC/IEEE 12207:2017, 6.3.6.3 a) 1)] 11) Define the strategy for information management. [ISO/IEC/IEEE 12207:2017, 6.3.6.3 a) 3)] 12) Designate authorities and responsibilities for information management. [ISO/IEC/IEEE 12207:2017, 6.3.6.3 a) 5)] 13) Define information maintenance actions.
04-09	Information management plan: Presentation	Plan	[ISO/IEC/IEEE 12207:2017, 6.3.6.3 a) 4)] 1) Define the content, formats and structure of information items.
04-10	Information management plan: item identification	Plan	[ISO/IEC/IEEE 12207:2017, 3ED 6.3.6.3 a) 2)] 1) Define the items of information that will be managed.
04-11	Information measurement strategy	Plan	1) - The measurement strategy is defined. 2) - Data collection, analysis, access and reporting procedures are defined. [ISO/IEC/IEEE 12207:2017, 6.3.7.3 a) 1)] 3) Define the measurement strategy. [ISO/IEC/IEEE 12207:2017, 6.3.7.3 a) 5)] 4) Define data collection, analysis, access and reporting procedures.
04-12	Infrastructure plan	Plan	1) - Infrastructure resources and services that are needed to implement and support projects are identified, obtained and provided. 2) An inventory asset registry is often established to track infrastructure elements and support reuse of infrastructure assets. [ISO/IEC/IEEE 12207:2017, 6.2.2.3 a) 2)] 3) Identify, [obtain and provide] infrastructure resources and services that are needed to implement and support projects. [ISO/IEC/IEEE 12207:2017, 6.2.2.3 a) 2)] 4) [Identify,] obtain and provide infrastructure resources and services that are needed to implement and support projects.
04-13	Knowledge Management: Establish	Plan	1) - Knowledge management strategy is defined. 2) This knowledge management strategy generally includes: i) Identifying domains and their potential for the reapplication of knowledge. ii) Plans for obtaining and maintaining knowledge, skills, and knowledge assets for their useful life. iii) Characterization of the types of knowledge, skills, and knowledge assets to be collected and maintained. iv) Criteria for accepting, qualifying, and retiring knowledge, skills, and knowledge assets. v) Procedures for controlling changes to the knowledge, skills, and knowledge assets. vi) Plans, mechanisms, and procedures for protection, control, and access to classified or sensitive data and information. vii) Mechanisms for storage and retrieval. 3) Knowledge management includes knowledge shared both internally within the organization and knowledge that is shared outside the organization with designated stakeholders, acquirers, and business partners, subject to intellectual property and non-disclosure agreements. 4) - The knowledge, skills, and knowledge assets to be managed are identified. 5) - Projects are identified that can benefit from the application of the knowledge, skills, and knowledge assets. [ISO/IEC/IEEE 12207:2017, 6.2.6.3 a) 1)] 6) Define the knowledge management strategy. [ISO/IEC/IEEE 12207:2017, 6.2.6.3 a) 2)] 7) Identify the knowledge, skills, and knowledge assets to be managed. [ISO/IEC/IEEE 12207:2017, 6.2.6.3 a) 3)] 8) Identify projects that can benefit from the application of the knowledge, skills, and knowledge assets.

Table C.1 *(continued)*

Reference	Name	Category	Characteristics
04-14	Maintenance Plan	Plan	1) - A maintenance strategy is defined, including consideration of the following: i) Establishing priorities, typical schedules, and procedures for performing, verifying, distributing, and installing software maintenance changes in conformance with operational availability requirements; ii) Establishing techniques and methods for becoming aware of the need for corrective, adaptive, and perfective maintenance; iii) Periodic assessment of the design characteristics in case of evolution of the software system and of its architecture; iv) Forecasting potential obsolescence of components and technologies using information on technical changes in related systems; v) Establishing priorities and resources to obtain access to the correct versions of the product and product information needed for performing maintenance (e.g., scheduled or phased installation, maintenance patches or software upgrades); 2) - For non-software elements, a logistics strategy is defined throughout the life cycle, including acquisition and operational considerations: the number and type of replacement elements to be stored, their storage locations and conditions, their anticipated replacement rate, and their storage life and renewal frequency. 3) Supportability implications are considered early during concept exploration or development stages. Logistics helps to ensure that the necessary material and resources, in the right quantity and quality, are available at the right place and time throughout deployment and sustainment stages. 4) - Constraints are identified from maintenance to be incorporated in the system/software requirements, architecture, or design. 5) These often result from the need to 1) re-use existing maintenance and verification enabling systems; 2) re-use existing holdings of replaceable system element and accommodate re-supply limitations; 3) conduct maintenance in specific locations or environments. For example, software architectures and designs that emphasize encapsulation, modularity, and scalability can be simpler to maintain. Requirements to document the system design and construction can reduce the effort needed to reverse engineer systems and elements when maintenance is needed. The system architecture and design reflect the need to roll back, back up, and recover data during problem resolution. Functions to make the system available for remote diagnostics and maintenance can be incorporated in the architecture and design. 6) - Trades such that the system and associated maintenance and logistics actions result in a solution that is affordable, operable, supportable, and sustainable, are identified. 7) The System Analysis and Decision Management processes are used to perform the assessments and trade decisions. [ISO/IEC/IEEE 12207:2017, 6.4.13.3 a) 1)] 8) Define a maintenance strategy, including consideration of the following: i) Establishing priorities, typical schedules, and procedures for performing, verifying, distributing, and installing software maintenance changes in conformance with operational availability requirements; ii) Establishing techniques and methods for becoming aware of the need for corrective, adaptive, and perfective maintenance; iii) Periodic assessment of the design characteristics in case of evolution of the software system and of its architecture; iv) Forecasting potential obsolescence of components and technologies using information on technical changes in related systems; v) Establishing priorities and resources to obtain access to the correct versions of the product and product information needed for performing maintenance (e.g. , scheduled or phased installation, maintenance patches or software upgrades); [ISO/IEC/IEEE 12207:2017, 6.4.13.3 a) 2)] 9) For non-software elements, define a logistics strategy throughout the life cycle, including acquisition and operational considerations: the number and type of replacement elements to be stored, their storage locations and conditions, their anticipated replacement rate, and their storage life and renewal frequency. [ISO/IEC/IEEE 12207:2017, 6.4.13.3 a) 3)] 10) Identify constraints from maintenance to be incorporated in the system/software requirements, architecture, or design. [ISO/IEC/IEEE 12207:2017, 6.4.13.3 a) 4)] 11) Identify trades such that the system and associated maintenance and logistics actions result in a solution that is affordable, operable, supportable, and sustainable.

Table C.1 *(continued)*

Reference	Name	Category	Characteristics
04-15	Operation plan	Plan	1) - An operation strategy is defined, including the following considerations: i) The expected or agreed capacity, availability, response time, and security of services as they are introduced, routinely operated and withdrawn from service; ii) The human resources strategy, depending on the need to define training and qualification requirements, train or obtain personnel to control and monitor software system operations, administer system access, and support customer service requests and user assistance; iii) The release criteria and schedules of the software system to permit modifications that sustain existing or enhanced services; iv) The approach to implement the operational modes in the Operational Concept, including normal operations and preparations for, and testing of, envisioned types of contingency operations; v) Measures for operation that will provide insight into performance levels; 2) ISO/IEC 16350 Information technology - Systems and software engineering - Application management, provides guidance for operational aspects. 3) - System constraints are identified from operation to be incorporated in changes to the system/software requirements, architecture, design, implementation, or transition. 4) - Training and qualification requirements are identified or defined for personnel needed for software system operation. 5) The training and qualification includes awareness of the software system in its operational environment and a defined program of familiarization, with appropriate failure detection and isolation instruction. Operator knowledge, skill and experience requirements guide the personnel selection criteria, and where relevant, their authorization to operate is confirmed. The scope of qualification depends on the system-of-interest and its environment. For example, in some environments regulatory requirements include certification of operators, whereas in others there is no certification requirement. 6) - Trained, qualified personnel are assigned to be operators, depending on the need for human intervention and control of operations. 7) With due regard for separation of duties, such as for administrative control of system access and investigation of security issues, many modern software products minimize the need for operators as distinct from end users, Operators commonly support enabling systems, such as cloud services, database and system software, security monitors, data storage, and help desk. [ISO/IEC/IEEE 12207:2017, 6.4.12.3 a) 1)] 8) Define an operation strategy, including the following considerations: i) The expected or agreed capacity, availability, response time, and security of services as they are introduced, routinely operated and withdrawn from service; ii) The human resources strategy, depending on the need to define training and qualification requirements, train or obtain personnel to control and monitor software system operations, administer system access, and support customer service requests and user assistance; iii) The release criteria and schedules of the software system to permit modifications that sustain existing or enhanced services; iv) The approach to implement the operational modes in the Operational Concept, including normal operations and preparations for, and testing of, envisioned types of contingency operations; v) Measures for operation that will provide insight into performance levels; [ISO/IEC/IEEE 12207:2017, 6.4.12.3 a) 2)] 9) Identify system constraints from operation to be incorporated in changes to the system/software requirements, architecture, design, implementation, or transition. [ISO/IEC/IEEE 12207:2017, 6.4.12.3 a) 5)] 10) Identify or define training and qualification requirements for personnel needed for software system operation. [ISO/IEC/IEEE 12207:2017, 6.4.12.3 a) 6)] 11) Depending on the need for human intervention and control of operations, assign trained, qualified personnel to be operators.
04-16	Organizational skills development plan	Plan	1) - Skills development strategy is established. 2) This plan includes types and levels of training, categories of personnel, schedules, personnel resource requirements, and training needs. [ISO/IEC/IEEE 12207:2017, 6.2.4.3 b) 1)] 3) Establish skills development strategy.
04-17	Process Improvement Opportunity	Plan	1) - Improvement opportunities are identified from assessment results. 2) Improvements can affect the stages, processes, and achievement criteria that control progression through the life cycle. [ISO/IEC/IEEE 12207:2017, 6.2.1.3 b) 3)] 3) Identify improvement opportunities from assessment results.

Table C.1 *(continued)*

Reference	Name	Category	Characteristics
04-18	Process Improvement plan	Plan	1) - Improvement opportunities are prioritized and planned. 2) Implement improvement opportunities and inform relevant stakeholders. 3) Process Improvement includes improvements to any of the processes in the organization. Lessons learned are captured and available. [ISO/IEC/IEEE 12207:2017, 6.2.1.3 c) 1)] 4) Prioritize and plan improvement opportunities. [ISO/IEC/IEEE 12207:2017, 6.2.1.3 c) 2)] 5) Implement improvement opportunities [and inform relevant stakeholders.]
04-19	Project assessment strategy	Plan	1) - The project assessment and control strategy is defined. 2) The strategy identifies the expected Project Assessment and Control activities, including planned assessment methods and timeframes, and necessary management and technical reviews. [ISO/IEC/IEEE 12207:2017, 6.3.2.3 a) 1)] 3) Define the project assessment and control strategy.
04-20	Project budget	Plan	1) - The costs are defined and a budget is planned. 2) Budgeted costs are based on the schedule, software size and complexity estimates, labor estimates, infrastructure costs, procurement items, acquired service and enabling system estimates, and budget reserves for risk management. [ISO/IEC/IEEE 12207:2017, 6.3.1.3 b) 3)] 3) Define the costs and plan a budget.
04-21	Project plan	Plan	1) - Roles, responsibilities, accountabilities, and authorities are defined. 2) This includes defining the project organization, staff acquisitions, and the development of staff skills. Authorities include, as appropriate, the legally responsible roles and individuals, e.g., design authorization, safety authorization, and those responsible for applicable certifications or accreditations. 3) - The infrastructure and services required are defined. 4) This includes defining the capacity needed, its availability and its allocation to project tasks. Infrastructure includes facilities, services, tools, communications, and information technology assets. The requirements for enabling systems and services for each life cycle stage are also specified. 5) - The acquisition of materials and enabling systems and services supplied from outside the project is planned. 6) This includes, as necessary, plans for solicitation, supplier selection, acceptance, contract administration and contract closure. The agreement processes are used for the planned acquisitions. 7) ISO/IEC 27036, Information security for supplier relationships, provides guidance for acquisition of infrastructure and services. 8) - A plan is generated and communicated for project and technical management and execution, including reviews. 9) Technical planning for the software system is often captured in a Systems Engineering Management Plan (SEMP) or a Software Engineering Management Plan or a Software Development Plan (SDP). ISO/IEC/IEEE 247485 provides more detail on software engineering technical management planning and includes an annotated outline for an SDP. Planning for the project is often captured in a Project Management Plan. ISO/IEC/IEEE 16326 provides more detail on project planning. 10) The strategy activities and tasks from each of the other processes provide inputs and are integrated in the Project Planning process. The Project Assessment and Control process is used to help ensure that the plans are integrated, aligned, and feasible. [ISO/IEC/IEEE 12207:2017, 6.3.1.3 b) 4)] 11) Define roles, responsibilities, accountabilities, and authorities. [ISO/IEC/IEEE 12207:2017, 6.3.1.3 b) 5)] 12) Define the infrastructure and services required. [ISO/IEC/IEEE 12207:2017, 6.3.1.3 b) 6)] 13) Plan the acquisition of materials and enabling systems and services supplied from outside the project. [ISO/IEC/IEEE 12207:2017, 6.3.1.3 b) 7)] 14) Generate [and communicate] a plan for project and technical management and execution, including reviews. [ISO/IEC/IEEE 12207:2017, 6.3.1.3 b) 7)] 15) [Generate and] communicate a plan for project and technical management and execution, including reviews.

Table C.1 *(continued)*

Reference	Name	Category	Characteristics
04-22	Project schedule	Plan	1) - A project schedule based on management and technical objectives and work estimates is defined and maintained. 2) This includes definition of the duration, relationship, dependencies and sequence of activities, achievement milestones, resources employed and the reviews and schedule reserves for risk management necessary to achieve timely completion of the project. [ISO/IEC/IEEE 12207:2017, 6.3.1.3 b) 1)] 3) Define and maintain a project schedule based on management and technical objectives and work estimates.
04-23	Quality Management Plan	Plan	1) - Quality management policies, objectives, and procedures are established. 2) ISO 9004:2009 contains guidelines for performance improvements. 3) The policies, objectives, and procedures are based on the business strategy for customer satisfaction and risk management considerations. [ISO/IEC/IEEE 12207:2017, 6.2.5.3 a) 1)] 4) Establish quality management policies, objectives, and procedures.
04-24	Quality assurance strategy	Plan	1) - A Quality Assurance strategy is defined. 2) - The strategy is consistent with the organizational Quality Management policies and objectives and includes: i) Priorities for applying Quality Assurance resources to processes and tasks that have the most significant impact on the quality of the delivered products and services; ii) Defined roles, responsibilities, accountabilities, and authorities; iii) Evaluation criteria and methods for processes, products, and services, including criteria for product or service acceptance; iv) Activities appropriate to each supplier (including subcontractors); v) Required verification, validation, monitoring, measurement, review, inspection, audit, and test activities specific to the products or services; and vi) Problem resolution and process and product improvement activities. 3) In software projects, activities and tasks that have significant impact on product quality include obtaining agreement on new and changed requirements, performance of peer reviews and unit testing, analysis of problem reports and feedback from users; validating completion of corrective actions assigned at project milestone reviews, and root cause analysis of defects. 4) - The independence of quality assurance from other life cycle processes is established. 5) Resources for quality assurance are often assigned from distinct organizations for independence from project management. [ISO/IEC/IEEE 12207:2017, 6.3.8.3 a) 1)] 6) 1. Define a Quality Assurance strategy. [ISO/IEC/IEEE 12207:2017, 6.3.8.3 a) 1)] 7) 2. The strategy is consistent with the organizational Quality Management policies and objectives and includes: i) Priorities for applying Quality Assurance resources to processes and tasks that have the most significant impact on the quality of the delivered products and services; ii) Defined roles, responsibilities, accountabilities, and authorities; iii) Evaluation criteria and methods for processes, products, and services, including criteria for product or service acceptance; iv) Activities appropriate to each supplier (including subcontractors); v) Required verification, validation, monitoring, measurement, review, inspection, audit, and test activities specific to the products or services; and vi) Problem resolution and process and product improvement activities. [ISO/IEC/IEEE 12207:2017, 6.3.8.3 a) 2)] 8) Establish independence of quality assurance from other life cycle processes.

Table C.1 *(continued)*

Reference	Name	Category	Characteristics
04-25	Risk Management Plan	Plan	1) - The risk management strategy is defined. 2) This includes the risk management process of supply chain suppliers and describes how risks from suppliers will be raised to the next level(s) for incorporation in the project risk process. 3) - The context of the Risk Management process is defined and recorded. 4) This includes a description of stakeholders? perspectives, risk categories, and a description (perhaps by reference) of the technical and managerial objectives, assumptions and constraints. The risk categories include the relevant technical areas of the software system and facilitate identification of risks across the product life cycle. As noted in ISO 31000, the aim of this step is to generate a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate, or delay the achievement of objectives. 5) Opportunities, which are one type of risk, provide potential benefits for the software system or project. Each of the opportunities pursued has associated risks that detract from the expected benefit. This includes the risks associated with not pursuing an opportunity, as well as the risk of not achieving the effects of the opportunity. [ISO/IEC/IEEE 12207:2017, 6.3.4.3 a) 1)] 6) Define the risk management strategy. [ISO/IEC/IEEE 12207:2017, 6.3.4.3 a) 2)] 7) Define and record the context of the Risk Management process.
04-26	Software integration plan	Plan	1) - The integration strategy is defined. 2) Integration builds sequences of progressively more complete software system element or software item configurations. It is dependent on applicable software system element availability and is consistent with a fault isolation and diagnosis strategy. Successive applications of the Integration process and the Verification process, and when appropriate the Validation process, are repeated for elements in the system structure until the system-of-interest has been realized. Simulators or prototypes are typically utilized for system elements that are not yet implemented, e.g., receiving data from interfacing systems. Integrating the implemented software system elements is based on the priorities of the related requirements and architecture definition, typically focusing on the interfaces, while minimizing integration time, cost, and risks. Software system integration commonly maintains version control through the Configuration Management process for selection of configuration items to be integrated. 3) For software integration, the integration strategy typically is consistent with a regression strategy which is applied for re-verifying software elements when related software units (and potentially associated requirements, design and user documentation) are changed. 4) Defining a strategy for software unit and element integration commonly accompanies defining the strategy for other processes that occur concurrently, such as: i) The Implementation process to help ensure timely coordination of Implementation and Integration process tasks and enabling systems, e.g., combined software development and test environments to support automated or continuous implementation and integration of software units and elements. ii) The Verification process to provide objective evidence that the integrated software fulfils its specified requirements and to identify anomalies (errors, defects, faults) in integration-related information items, (e.g., system/software requirements, architecture, design, test, or other descriptions), processes, software elements, items, units. iii) The Validation process to confirm that a work product fulfils requirements for a specific intended use of an integrated software function. iv) The Quality Assurance process to support integration process and work product audits and inspections and to address problem, nonconformance, or incident reporting and handling. 5) The integration strategy is commonly recorded in a plan, e.g., an integration plan, or a project's SDP or SEMP. 6) - Criteria for integration and points at which the correct operation and integrity of the interfaces and the selected software system functions will be verified are identified and defined.

Table C.1 *(continued)*

Reference	Name	Category	Characteristics
			7) Detailed verification of the interfaces is performed using the Verification process. Software integration typically involves combining software elements, resulting in a set of integrated software elements, that is consistent with the software design, and that satisfies the functional and non-functional system/ software requirements on an equivalent of the operational environment. 8) For projects involving multiple suppliers or development teams, the availability of software system elements for integration is typically part of the project schedule with milestones under the Project Assessment and Control process. Integration proceeds as the software is verified in its functionality, performance, and suitability for site-specific or platform-specific environments. At major integration points, e.g., completion of a stage, element, or version, check points for reviews and validation with stakeholders are typically held. The frequency of these reviews is related to the selected life cycle model and development method. 9) - Constraints for integration to be incorporated in the system/software requirements, architecture or design are identified. 10) This includes requirements such as accessibility, supply chain security, safety for integrators, required interconnections for sets of implemented software system elements and/or enablers, and interface constraints. [ISO/IEC/IEEE 12207:2017, 6.4.8.3 a) 1)] 11) Define the integration strategy. [ISO/IEC/IEEE 12207:2017, 6.4.8.3 a) 2)] 12) Identify and define criteria for integration and points at which the correct operation and integrity of the interfaces and the selected software system functions will be verified. [ISO/IEC/IEEE 12207:2017, 6.4.8.3 a) 5)] 13) Identify constraints for integration to be incorporated in the system/software requirements, architecture or design.
04-27	Software release plan	Plan	1) - A strategy is defined for managing software releases and other software system transitions, including the following considerations: i) establishing the type of transition and transition success criteria; ii) determining the frequency of recurring transitions, such as updates and upgrades to development, test, and operational software systems; iii) minimizing security risks, disruption, and downtime during transition; iv) archiving, destroying, or converting and validating data from previous systems to the new system; including data received through external interfaces; v) contingency planning for problem resolution, backup and return to the last working system version; vi) scheduling transitions consistent with ongoing business processing, with phased or synchronized transition of systems vii) change management for stakeholders, including interface partners, human operators, system administrators, and software system or service users; 2) Change management activities are often conducted to design changes in business processes associated with the new system, plan the transition in business processes, and gain user commitment to productive use of the new system. 3) The strategy includes roles and responsibilities, approval authority, use of readiness reviews and training. 4) - Facility, site, communications network, or target environment changes needed for software system installation or transition are identified and defined. 5) For each transition, identify and define any needed changes in infrastructure or enabling systems. A site survey can be performed to identify needed changes in the physical environment to install or use the software system, such as changes to maintain the physical and information security of the system.

Table C.1 *(continued)*

Reference	Name	Category	Characteristics
			6) - Information needs and arrange for user documentation and training of operators, users, and other stakeholders necessary for system utilization and support are identified. 7) Transition includes migration or activation of user access to the software system. User roles are established and user accounts and access controls are implemented. 8) - Detailed transition information, such as plans, schedules, and procedures are prepared. 9) The transition strategy is commonly recorded in a plan, e.g., a transition plan, or a project's SDP or SEMP. Transition schedules help validate that sufficient resources and infrastructure are available to support the transition, so that activities can be executed within a reasonable timeframe to minimize disruption. Schedules can include rehearsals for complex transitions, in which procedures, such as database and system backup and restore and software installation, are tested to verify durations and correct results. 10) During a specified period of changeover or concurrent operation, the transfer of services is managed so that continuing conformance to persistent stakeholder needs or an agreed level of service is achieved. If a period of parallel operations for both the old and new systems is needed, special procedures are identified and developed for receiving and utilizing data from interface partners. 11) - System constraints from transition to be incorporated in the software system requirements, architecture or design are identified. [ISO/IEC/IEEE 12207:2017, 6.4.10.3 a) 1)] 12) Define a strategy for managing software releases and other software system transitions, including the following considerations: i) establishing the type of transition and transition success criteria; ii) determining the frequency of recurring transitions, such as updates and upgrades to development, test, and operational software systems; iii) minimizing security risks, disruption, and downtime during transition; iv) archiving, destroying, or converting and validating data from previous systems to the new system; including data received through external interfaces; v) contingency planning for problem resolution, backup and return to the last working system version; vi) scheduling transitions consistent with ongoing business processing, with phased or synchronized transition of systems vii) change management for stakeholders, including interface partners, human operators, system administrators, and software system or service users; [ISO/IEC/IEEE 12207:2017, 6.4.10.3 a) 2)] 13) Identify and define facility, site, communications network, or target environment changes needed for software system installation or transition. [ISO/IEC/IEEE 12207:2017, 6.4.10.3 a) 3)] 14) Identify information needs and arrange for user documentation and training of operators, users, and other stakeholders necessary for system utilization and support. [ISO/IEC/IEEE 12207:2017, 6.4.10.3 a) 4)] 15) Prepare detailed transition information, such as plans, schedules, and procedures. [ISO/IEC/IEEE 12207:2017, 6.4.10.3 a) 5)] 16) Identify system constraints from transition to be incorporated in the software system requirements, architecture or design.
04-28	Supply strategy	Plan	1) - A supply strategy is determined. 2) This strategy describes or references the life cycle model, risks and issues mitigation, and a schedule of milestones. It also includes key drivers and characteristics of the acquisition, such as responsibilities and liabilities; specific models, methods, or processes; level of criticality; formality; and priority of relevant trade factors. [ISO/IEC/IEEE 12207:2017, 6.1.2.3 a) 2)] 3) Define a supply strategy.

Table C.1 *(continued)*

Reference	Name	Category	Characteristics
04-29	System requirements definition strategy	Plan	1) - The stakeholder needs and requirements definition strategy is defined. 2) Some stakeholders have interests that oppose the acquirer's interests (e.g., market competitors, hackers, terrorists) or oppose each other. When the stakeholder interests oppose each other, but do not oppose the software system, this process is intended to gain consensus among the stakeholder classes to establish a common set of acceptable requirements. The intent or desires of those that oppose the acquirers, or detractors of the system, are addressed through the Risk Management process, threat analyses of the System Analysis process, or the system/software requirements for security, adaptability, or resilience. In this case, the stakeholder needs are not satisfied, but rather addressed in a manner to help ensure system assurance and integrity if actions from the detractors are encountered. [ISO/IEC/IEEE 12207:2017, 6.4.2.3 a) 2)] 3) Define the stakeholder needs and requirements definition strategy.
04-30	Systems analysis strategy	Plan	1) - The problem or question that requires analysis is identified. 2) This includes technical, functional, and non-functional objectives of the analysis. Non-functional objectives include critical quality characteristics, various properties, technology maturity, and technical risks. The problem statement or question to be answered by the analysis is essential to establish the objectives of the analysis and the expectations and utility of the results. 3) - The stakeholders of the analysis are identified. 4) - The scope, objectives, and level of fidelity of the analysis are defined. 5) The necessary level of fidelity (accuracy or precision) is a factor in determining the appropriate level of rigor. 6) - The methods to support the analysis are selected. 7) The methods are chosen based on time, cost, fidelity, technical drivers, and criticality of analysis. Analysis methods have a wide range of levels of rigor and include expert judgment, worksheet computations, parametric estimates and calculations, historical data and trend analysis, engineering models, simulation, visualization, and prototyping. Due to cost and schedule constraints, most projects typically perform system analysis only for critical characteristics. 8) - The data and inputs needed for the analysis are collected. [ISO/IEC/IEEE 12207:2017, 6.4.6.3 a) 1)] 9) Identify the problem or question that requires analysis. [ISO/IEC/IEEE 12207:2017, 6.4.6.3 a) 2)] 10) Identify the stakeholders of the analysis. [ISO/IEC/IEEE 12207:2017, 6.4.6.3 a) 3)] 11) Define the scope, objectives, and level of fidelity of the analysis. [ISO/IEC/IEEE 12207:2017, 6.4.6.3 a) 4)] 12) Select the methods to support the analysis. [ISO/IEC/IEEE 12207:2017, 6.4.6.3 a) 7)] 13) Collect the data and inputs needed for the analysis.

Table C.1 *(continued)*

Reference	Name	Category	Characteristics
04-31	Validation plan	Plan	1) - The validation strategy is defined, which includes the following: i) Identify the validation scope, including the characteristics of the software system, element, or artifact to be validated, and the expected results of validation. ii) Identify the constraints that potentially limit the feasibility of validation actions.iii) Identify validation priorities. 2) A validation strategy generally focuses on minimizing cost, schedule, or risk by progressively building confidence in the quality and suitability of the software system for the stakeholders. 3) The validation strategy reflects the life cycle model, and often involves repeated validation for iterative, incremental, or evolutionary life cycles. 4) The validation strategy can be documented in a plan, e.g., an acceptance plan, or a project's SDP or SEMP. 5) Software system validation is typically performed both in distinct controlled environments that do not interfere with operational software or ongoing development, as well as in operational environments, typically before full operational use (e.g., beta testing or acceptance testing for a specified duration with agreed criteria). Scope includes stakeholder requirements, including related views of the system (e.g., scenarios or concept of operation) to be evaluated. The scope depends on what is appropriate for the systems life cycle stage: the system-of-interest or a system element or engineering artifact, such as a concept description or document, an operational scenario, a model, a mock-up, or prototype. The scope also includes evaluating that the software product or service is usable in its intended environment for the principal or critical functions. Additional characteristics to be validated can include usability of the documentation; fault tolerance, resilience, and recovery features of the software. 6) Constraints include practical limitations of accuracy, uncertainty, repeatability that are imposed by the validation enablers, the associated measurement methods, and the availability, accessibility and interconnection with enablers. The validation strategy is constrained by the progress of the project; in particular, planned validation actions are redefined or rescheduled when unexpected events or system evolutions occur. Validation can be extended to include ongoing measurements of user satisfaction and customer complaints. 7) To make effective use of stakeholders' time and expertise, validation typically focuses on stakeholder priorities, while verification is used for non-functional requirements. Potential validation actions that are candidates for deletion are evaluated for the risks their withdrawal imposes 8) The supplier, the acquirer, or an agent of the acquirer participates in or performs validation. The responsibility is often designated in the agreement. 9) - Identify system constraints from the validation strategy to be incorporated in the stakeholder requirements. 10) - Training and qualification requirements for personnel needed for software system operation are identified and defined. 11) The training and qualification includes awareness of the software system in its operational environment and a defined program of familiarization, with appropriate failure detection and isolation instruction. Operator knowledge, skill and experience requirements guide the personnel selection criteria, and where relevant, their authorization to operate is confirmed. The scope of qualification depends on the system-of-interest and its environment. For example, in some environments regulatory requirements include certification of operators, whereas in others there is no certification requirement.

Table C.1 *(continued)*

Reference	Name	Category	Characteristics
			12) - Trained, qualified personnel to be operators are assigned, depending on the need for human intervention and control of operations. 13) With due regard for separation of duties, such as for administrative control of system access and investigation of security issues, many modern software products minimize the need for operators as distinct from end users, Operators commonly support enabling systems, such as cloud services, database and system software, security monitors, data storage, and help desk. [ISO/IEC/IEEE 12207:2017, 6.4.11.3 a) 1)] 14) Define the validation strategy, which includes the following: [ISO/IEC/IEEE 12207:2017, 6.4.11.3 a) 2)] 15) Identify system constraints from the validation strategy to be incorporated in the stakeholder requirements. [ISO/IEC/IEEE 12207:2017, 6.4.11.3 a) 3)] 16) Define the purpose, conditions and conformance criteria for each validation action. [ISO/IEC/IEEE 12207:2017, 6.4.11.3 a) 4)] 17) Select appropriate validation methods or techniques and associated criteria for each validation action.
04-32	Verification strategy	Plan	1) - The verification strategy is defined, which includes the following: i) Identify the verification scope, including the software system, element, or artifact, the properties to be verified, and the expected results. ii) Identify the constraints that potentially limit the feasibility of verification actions. iii) Identify verification priorities. 2) A verification strategy generally focuses on minimizing cost, schedule, or risk, providing a balanced approach for confirming that the software system or element has been 'built right'. 3) The verification strategy and schedule account for dynamic changes when anomalous results (events, incidents, or problems) occur. According to the progress of the project, planned verification actions are redefined or rescheduled when unexpected events or system evolutions occur. 4) The verification strategy can be documented in a plan, e.g., a verification plan or a project's SDP or SEMP. 5) Overall verification scope includes the software system-of-interest or system elements, including interfaces. For each verification action, the scope identifies the software system, element, or artifact to be verified (e.g., the actual system, or a model, a mock-up, a prototype, code, a procedure, a plan or other document) and the expected results, such as conformance, or performance, fault tolerance, and recovery after service interruption. The properties to be verified can include requirements, architecture and design characteristics, integration, and accuracy of documentation. Design characteristics can include security implications of the design in the context of the planned operational environment and the achievement of critical quality characteristics as stated in the requirements. 6) Constraints include technical feasibility, cost, time, availability of verification enablers or qualified personnel, contractual constraints, and characteristics such as criticality of the mission. Such constraints often factor into verification strategy determination, e.g., whether an organizationally independent verification effort is necessary or justified. 7) In software systems, verification of every possible scenario (100 % code coverage) is typically infeasible. The verification strategy typically includes trading off what will be verified (scope) against the constraints or limits, and deducing what verification actions to perform and how many iterations of verification actions and rework are needed to reduce risk. A model-based testing approach can enable the generation and management of multiple scenarios. Potential verification actions that are candidates for deletion are evaluated for the risks their withdrawal imposes. 8) - Constraints are identified from the verification strategy to be incorporated in the system/software requirements, architecture, or design. 9) This includes practical limitations of accuracy, uncertainty, repeatability that are imposed by the verification enablers, the associated measurement methods, the need for software system integration, and the availability, accessibility and interconnection with enablers. 10) - The purpose, conditions and conformance criteria for each verification action is defined. 11) - Appropriate verification methods or techniques and associated criteria for verification actions, such as inspection, analysis, demonstration, or testing are selected.

Table C.1 *(continued)*

Reference	Name	Category	Characteristics
			12) The selection of verification methods or techniques is made according to the type of system, the purpose of the verification, the objectives of the project, and the acceptable risks. Verification methods or techniques include inspection (including code walkthroughs and peer review), analysis (including modelling and simulation, and analogy/similarity), demonstration, and dynamic and static testing. 13) The selected verification approach, methods, and techniques can be coordinated with relevant stakeholders to help ensure the verification approach is acceptable. [ISO/IEC/IEEE 12207:2017, 6.4.9.3 a) 1)] 14) Define the verification strategy, which includes the following: [ISO/IEC/IEEE 12207:2017, 6.4.9.3 a) 2)] 15) Identify constraints from the verification strategy to be incorporated in the system/software requirements, architecture, or design. [ISO/IEC/IEEE 12207:2017, 6.4.9.3 a) 3)] 16) Define the purpose, conditions and conformance criteria for each verification action. [ISO/IEC/IEEE 12207:2017, 6.4.9.3 a) 4)] 17) Select appropriate verification methods or techniques and associated criteria for verification actions, such as inspection, analysis, demonstration, or testing.
04-33	Work breakdown structure	Plan	1) - A work breakdown structure (WBS) based on the deliverable products or the evolving architecture of the software system is established. 2) Each element of the software system architecture, and appropriate processes and activities, are described with a level of detail that is consistent with identified risks. Related tasks in the work breakdown structure are grouped for performance. Project tasks identify work items being developed or produced. The Practice Management Standard for Work Breakdown Structures of the Project Management Institute (PMI) contains additional details on WBSs. 3) For projects with agile or iterative methods, a WBS element can correspond to the primary features, from a user perspective, to be produced during iterations. [ISO/IEC/IEEE 12207:2017, 6.3.1.3 a) 4)] 4) Establish a work breakdown structure (WBS) based on the deliverable products or the evolving architecture of the software system.
06-1	Information Management Procedures	Procedure	1) - Manual or automated procedures for data generation, collection, analysis and reporting into the relevant processes are integrated. 2) This task can involve change impacts to other life cycle processes to accomplish procedural integration. [ISO/IEC/IEEE 12207:2017, 6.3.7.3 b) 1)] 3) Integrate manual or automated procedures for data generation, collection, analysis and reporting into the relevant processes.
06-2	Validation Procedures	Procedure	1) - The validation procedures, each supporting one or a set of validation actions are defined. 2) Validation procedures identify stakeholder requirements to be validated, the associated software system artifact (e.g., the actual system, or a model, a mock-up, a prototype, code, a set of instructions or other information item), and the expected results (success criteria), such as completed and timely performance of a function. The procedures identify the purpose of the validation with success criteria (expected results), the validation technique to be applied, the necessary enabling systems (facilities, equipment), and the environmental conditions to perform each validation procedure (resources, qualified personnel, participating stakeholders, and specialized procedural set-up or work instructions). Validation strategy includes how the validation procedure results will be recorded, analysed, stored, and reported. 3) - The validation procedures are performed in the defined environment. 4) Validation occurs, in accordance with the validation strategy, at the appropriate time in the schedule, in a defined environment (such as the operational environment, a similar test environment, or other representative environment), with defined enablers and resources. The performance of a validation action typically consists of capturing execution results, comparing the obtained result with the success criteria, and deducing a degree of compliance or stakeholder satisfaction with the software system, element, service, or engineering artifact. [ISO/IEC/IEEE 12207:2017, 6.4.11.3 b) 1)] 5) Define the validation procedures, each supporting one or a set of validation actions. [ISO/IEC/IEEE 12207:2017, 6.4.11.3 b) 2)] 6) Perform the validation procedures in the defined environment.

Table C.1 *(continued)*

Reference	Name	Category	Characteristics
06-3	Verification Procedures	Procedure	1) - The verification procedures, each supporting one or a set of verification actions are defined. 2) Verification procedures, which can be performed by automated scripts, include the requirements to be verified, the type of software system element or artifact to be verified (e.g., the actual system, or a model, a mock-up, a prototype, code, a procedure, a plan, or other information item), and the expected results (success criteria), such as conformance, or performance of a function or capacity in terms of response time or throughput. The procedures identify the purpose of the verification with success criteria (expected results), the verification technique to be applied, the necessary enabling systems (facilities, equipment), and the environmental conditions to perform each verification procedure (resources, qualified personnel, specialized procedural setup or work instructions). Verification procedures include how the verification procedure results will be recorded, analysed, stored, and reported. 3) - The verification procedures are performed. 4) Verification occurs, in accordance with the verification strategy, at the appropriate time in the schedule, in the defined environment, with defined enabling systems and resources. The performance of a verification action consists of capturing a result from the execution of the verification procedure; comparing the obtained and recorded result with the expected result; and deducing a degree of correctness (or success/failure) of the submitted element. [ISO/IEC/IEEE 12207:2017, 6.4.9.3 b) 1)] 5) Define the verification procedures, each supporting one or a set of verification actions. [ISO/IEC/IEEE 12207:2017, 6.4.9.3 b) 2)] 6) Perform the verification procedures.
07-1	Information item	Product	1) - The identified items of information are obtained, developed or transformed. 2) This includes collecting the data, information, or information items from appropriate sources (e.g., resulting from any life cycle process), and writing, illustrating, or transforming it into usable information for stakeholders. It includes reviewing, validating, and editing information per information standards. 3) - Information items and their storage records are maintained. 4) Information items are maintained according to their integrity, security and privacy requirements. The status of information items is maintained, (e.g., version description, date of issue or validity date, record of distribution, security classification). Legible information is stored and retained in such a way that it is readily retrievable. 5) The source data and tools used to transform information, along with the resulting documentation is placed under configuration control in accordance with the Configuration Management process. ISO/IEC/IEEE 26531 provides requirements for content management systems useful for life cycle information and documentation. 6) - Information and information items are published and distributed, and access provided to designated stakeholders. 7) Information is provided to designated stakeholders in an appropriate form, as required by agreed schedules or defined circumstances. Information items include documentation used for certification, accreditation, license or assessment ratings, as required.

Table C.1 *(continued)*

Reference	Name	Category	Characteristics
			8) - Key artifacts and information items are provided that have been selected for baselines. [ISO/IEC/IEEE 12207:2017, 6.3.6.3 b) 1)] 9) Obtain, develop, or transform the identified items of information. [ISO/IEC/IEEE 12207:2017, 6.4.1.3 e) 2)] 10) Provide key artifacts and information items that have been selected for baselines. [ISO/IEC/IEEE 12207:2017, 6.4.2.3 f) 3)] 11) Provide key artifacts and information items that have been selected for baselines. [ISO/IEC/IEEE 12207:2017, 6.4.3.3 d) 3)] 12) Provide key artifacts and information items that have been selected for baselines. [ISO/IEC/IEEE 12207:2017, 6.4.4.3 f) 7)] 13) Provide key artifacts and information items that have been selected for baselines. [ISO/IEC/IEEE 12207:2017, 6.4.5.3 d) 4)] 14) Provide key artifacts and information items that have been selected for baselines. [ISO/IEC/IEEE 12207:2017, 6.4.6.3 c) 2)] 15) Provide key artifacts and information items that have been selected for baselines. [ISO/IEC/IEEE 12207:2017, 6.4.7.3 c) 3)] 16) Provide key artifacts and information items that have been selected for baselines. [ISO/IEC/IEEE 12207:2017, 6.4.8.3 c) 3)] 17) Provide key artifacts and information items that have been selected for baselines. [ISO/IEC/IEEE 12207:2017, 6.4.9.3 c) 5)] 18) Provide key artifacts and information items that have been selected for baselines. [ISO/IEC/IEEE 12207:2017, 6.4.10.3 c) 4)] 19) Provide key artifacts and information items that have been selected for baselines. [ISO/IEC/IEEE 12207:2017, 6.4.11.3 c) 5)] 20) Provide key artifacts and information items that have been selected for baselines. [ISO/IEC/IEEE 12207:2017, 6.4.12.3 c) 4)] 21) Provide key artifacts and information items that have been selected for baselines. [ISO/IEC/IEEE 12207:2017, 6.4.13.3 d) 4)] 22) Provide key artifacts and information items that have been selected for baselines.
07-2	Information item: Item status	Product	[ISO/IEC/IEEE 12207:2017, 6.3.6.3 b) 2)] 1) Maintain information items and their storage records, and record the status of information.
07-3	Information item: Publish	Product	[ISO/IEC/IEEE 12207:2017, 6.3.6.3 b) 3)] 1) Publish, distribute or provide access to information and information items to designated stakeholders.
07-4	Information measurement data item	Product	1) - Data are collected, stored, and verified. [ISO/IEC/IEEE 12207:2017, 6.3.7.3 b) 2)] 2) Collect, store, and verify data.
07-5	Information product	Product	1) - Data is analysed and information items are developed. [ISO/IEC/IEEE 12207:2017, 6.3.7.3 b) 3)] 2) Analyse data and develop information items.
07-6	Integrated system	Product	1) - Implemented software system elements in accordance with agreed schedules are obtained. 2) The implemented software system elements are provided from the developers or received from suppliers, the acquirer, or other resources and typically placed under CM control. The elements are handled in accordance with relevant health, safety, security and privacy considerations. 3) - The implemented elements are integrated. 4) This task is performed to achieve software system element configuration (complete or partial) connecting the implemented elements as prescribed in the integration strategy, using the defined procedures, interface control descriptions, and the related integration enabling systems. 5) In terms of software, integrating the implemented elements can involve linking together pieces of object code or simply bringing together the implemented elements that are part of the software configuration in a methodical piece by piece approach. Software elements are typically compiled into a 'build' so that branched units are properly linked or merged in the assembled element. Firmware elements are fabricated, often as prototypes, and installed in hardware elements. If software functions are not yet available for integration, emulated functionality (stubs or scaffolding) can be used to temporarily support integration of software elements or represent input from external interfaces. Successful aggregations result in an integrated software element, that is stored and available for further processing, i.e., additional software system element integration, verification, or validation.

Table C.1 *(continued)*

Reference	Name	Category	Characteristics
			6) Anti-counterfeit, anti-tamper, system and software assurance and interoperability concerns can arise when performing integration and identifying and defining checkpoints. Integration and Verification processes often use fictitious data for security or privacy considerations. ISO/IEC/IEEE 15026 and the ISO/IEC 27000 series include information on assurance, integrity, and security considerations affecting integration. 7) - The integrated software interfaces or functions run from initiation to an expected termination within an expected range of data values are checked. 8) As part of the acceptance of the implemented software system elements, selected elements are checked to help ensure they meet acceptance criteria as specified in the integration strategy and applicable agreements. Checking can include conformance to the agreed configuration, compatibility of interfaces, and the presence of mandatory information items. The Project Assessment and Control process can be used in accordance with the integration strategy to plan and conduct technical reviews of the integrated software system elements, e.g., a test readiness review to help ensure the integrated element or system with its affiliated data and information items is ready for qualification testing. [ISO/IEC/IEEE 12207:2017, 6.4.8.3 b) 1)] 9) Obtain implemented software system elements in accordance with agreed schedules. [ISO/IEC/IEEE 12207:2017, 6.4.8.3 b) 2)] 10) Integrate the implemented elements. [ISO/IEC/IEEE 12207:2017, 6.4.8.3 b) 3)] 11) Check that the integrated software interfaces or functions run from initiation to an expected termination within an expected range of data values.
07-7	Skills development resources	Product	1) - Training, education or mentoring resources are obtained or developed. 2) These resources include training materials that are developed by the organization or external parties, training courses that are available from external suppliers, computer based instruction. [ISO/IEC/IEEE 12207:2017, 6.2.4.3 b) 2)] 3) Obtain or develop training, education or mentoring resources.
07-8	Software element	Product	1) - Software elements, according to the strategy, constraints, and defined implementation procedures are realized or adapted. 2) Software elements are acquired, identified for reuse from organizational assets, or developed (constructed). Software elements that are acquired can range from a simple product purchase in accordance with organizational or project purchasing rules to a complex acquisition of a software system that involves the Acquisition and Supply processes. Adaptation includes configuration of software elements that are reused or modified. Construction can involve software coding, adaptive reuse and integration of existing units, refactoring, database development, and construction of manual or automated test procedures for each unit. 3) For software elements that are developed, at the lowest level of implementation executable software units are constructed (often with associated data structures, application programming interfaces, service descriptions, user documentation, test cases, or other elements), controlled, made available to authorized roles, and stored according to the CM procedures for development artifacts. 4) The SWEBOK, Guide to the Software Engineering Body of Knowledge provides detailed discussion on Software Construction. This knowledge area addresses fundamentals, management, measurement, practical considerations (e.g., construction design, languages, testing, reuse and integration), construction technologies (e.g., object oriented, error and exception handling, executable models, distributed software), and tools and environments. 5) - Hardware elements of software systems are realized or adapted.

Table C.1 *(continued)*

Reference	Name	Category	Characteristics
			6) Hardware elements are acquired or fabricated using applicable techniques relevant to the physical implementation technology and materials selected. As appropriate, hardware elements are verified for conformance to specified system requirements and critical quality characteristics. In the case of repeated system element implementation (e.g., mass production, replacement system elements) the implementation procedures and fabrication processes are defined and can be automated to achieve consistent and repeatable producibility. Some common hardware elements in software systems include integrations of acquired COTS systems, special modifications, e.g., for test or operational environments, and hardware controls with embedded software. 7) - Service elements of software systems are realized or adapted. 8) Service elements include a set of services to be provided. ISO/IEC 20000 (IEEE Std 20000) applies to management of system elements realized in services, including strategy, design, and transition. As appropriate, service elements are verified for conformance to the system requirements and service criteria. For example, operational resource elements are verified for conformance to the system requirements and operational concept. Service elements can include network communications, training, software packaging and distribution services, software customization services for customer-specific needs, operational and security monitoring, and user assistance. [ISO/IEC/IEEE 12207:2017, 6.4.7.3 b) 1)] 9) Realize or adapt software elements, according to the strategy, constraints, and defined implementation procedures. [ISO/IEC/IEEE 12207:2017, 6.4.7.3 b) 2)] 10) Realize or adapt hardware elements of software systems. [ISO/IEC/IEEE 12207:2017, 6.4.7.3 b) 3)] 11) Realize or adapt service elements of software systems.
08-04	Agreement amendment record	Record	1) - The agreement with the acquirer is updated, as necessary. 2) The result of the agreement modification is incorporated into the project plans and communicated to all affected parties. [ISO/IEC/IEEE 12207:2017, 6.1.1.3 c) 5)] 3) Update the agreement with the supplier, as necessary. [ISO/IEC/IEEE 12207:2017, 6.1.2.3 c) 5)] 4) Update the agreement with the acquirer, as necessary.
08-05	Agreement closure record	Record	1) - The agreement is closed. 2) The project is closed by the Portfolio Management process. [ISO/IEC/IEEE 12207:2017, 6.1.1.3 e) 4)] 3) Close the agreement.
08-06	Agreement impact evaluation record	Record	1) - The impact of changes is evaluated on the agreement. 2) Any change is investigated for impacts to project plans, schedule, cost, technical capability, or quality. A change can be handled within the existing agreement, can require a modification to the agreement, or can require a new agreement. [ISO/IEC/IEEE 12207:2017, 6.1.2.3 c) 3)] 3) Evaluate impact of changes on the agreement.
08-07	Agreement performance review record	Record	1) - The agreement is executed according to the established project plans. 2) A supplier sometimes adopts, or agrees to use, acquirer processes. 3) - The execution of the agreement is assessed. 4) This includes confirmation that all parties are meeting their responsibilities according to the agreement. The Project Assessment and Control process is used to evaluate projected cost, schedule, performance, and the impact of undesirable outcomes on the organization. The change management activity of the Configuration Management process is used to control changes to the system elements. This information is combined with other assessments of the execution of the terms of the agreement. If execution of the agreement does not result in an acceptable product or service, the acquirer or supplier can terminate the agreement as allowed in its terms. [ISO/IEC/IEEE 12207:2017, 6.1.1.3 d) 1)] 5) Assess the execution of the agreement. [ISO/IEC/IEEE 12207:2017, 6.1.2.3 d) 1)] 6) Execute the agreement according to the established project plans. [ISO/IEC/IEEE 12207:2017, 6.1.2.3 d) 2)] 7) Assess the execution of the agreement.

Table C.1 *(continued)*

Reference	Name	Category	Characteristics
08-08	Architecture assessment result	Record	1) - Each candidate architecture is assessed against constraints and requirements. 2) - Each candidate architecture is assessed against stakeholder concerns using evaluation criteria. 3) The System Analysis process and the Risk Management process can be used to support this task. 4) - The preferred architecture(s) selected and key decisions and rationale are captured. 5) The Decision Management process can be used to support this task. 6) - The architecture baseline of the selected architecture is established. 7) The architecture baseline is composed of models, views and other relevant architecture descriptions. [ISO/IEC/IEEE 12207:2017, 6.4.4.3 e) 1)] 8) Assess each candidate architecture against constraints and requirements. [ISO/IEC/IEEE 12207:2017, 6.4.4.3 e) 2)] 9) Assess each candidate architecture against stakeholder concerns using evaluation criteria. [ISO/IEC/IEEE 12207:2017, 6.4.4.3 e) 3)] 10) Select the preferred architecture(s) and capture key decisions and rationale. [ISO/IEC/IEEE 12207:2017, 6.4.4.3 e) 4)] 11) Establish the architecture baseline of the selected architecture.
08-09	Business opportunities evaluation record	Record	1) - Each alternative solution class is assessed. 2) Each alternative solution class is assessed against defined criteria that are established based on the organization's strategy. Feasibility of the solution class is one key decision criteria. The Portfolio Management process provides some criteria to be considered. 3) The System Analysis process is used to assess the value of each criterion for each alternative solution class. Structured affordability trade-offs are recommended. Including cost as a criterion will aid affordability decisions. The assessment of alternatives can include modeling, simulation, analytical techniques, or expert judgment to understand the risks, feasibility and value of the alternative candidate solution classes. 4) - The preferred alternative solution class(es) is selected. 5) The Decision Management process is used to evaluate alternatives and to guide selection. Selected alternatives are validated in the context of the organization's strategy. Feedback on risks, feasibility, market factors, and alternatives is provided for use in updating the organization's strategy. [ISO/IEC/IEEE 12207:2017, 6.4.1.3 d) 1)] 6) Assess each alternative solution class. [ISO/IEC/IEEE 12207:2017, 6.4.1.3 d) 2)] 7) Select the preferred alternative solution class(es).
08-10	Business opportunities review record	Record	1) - Identified problems and opportunities are reviewed in the organization strategy with respect to desired organization goals or objectives. 2) This includes problems or opportunities with respect to the organization business or mission, vision, Concept of Operations, and other organization strategic goals and objectives. This includes identified deficiencies or gaps in existing capabilities, systems, products, or services. [ISO/IEC/IEEE 12207:2017, 6.4.1.3 a) 1)] 3) Review identified problems and opportunities in the organization strategy with respect to desired organization goals or objectives.
08-11	Configuration Management Change Requests	Record	1) - Requests for Change and Requests for Variance are identified and recorded. 2) A request for variance is often referred to as a deviation, waiver, or concession. 3) - Requests for Change and Requests for Variance are coordinated, evaluated and dispositioned. 4) Evaluation commonly includes analysis of rationale and need versus impact on the software and interoperating systems, considering risks and opportunities, quality, users, schedule, and cost. A decision is made on whether to implement or deny the change request. 5) Requests for Change and Requests for Variance are often under the formal control of a Configuration Control Board (CCB). 6) - Approved changes to the baseline, Requests for Change and Requests for Variance are tracked and managed.

Table C.1 *(continued)*

Reference	Name	Category	Characteristics
			7) This task involves prioritization, tracking, scheduling, and closing changes. Changes are then made through the Technical Processes. These changes are verified or validated through the Verification and Validation processes, to help ensure that the approved changes have been correctly applied. 8) Changes and rationales are typically recorded when approved and when completed. [ISO/IEC/IEEE 12207:2017, 6.3.5.3 c) 1)] 9) Identify and record Requests for Change and Requests for Variance. [ISO/IEC/IEEE 12207:2017, 6.3.5.3 c) 2)] 10) Coordinate, evaluate, and disposition Requests for Change and Requests for Variance. [ISO/IEC/IEEE 12207:2017, 6.3.5.3 c) 3)] 11) Track and manage approved changes to the baseline, Requests for Change and Requests for Variance.
08-12	Configuration Management Release Records	Record	1) - Release requests, identifying the software system elements in a release are identified and recorded. 2) The life cycle model helps determine the frequency of iterative or incremental software releases. The Integration process is used to select and configure a release package, software version, update or patch. These changes are verified or validated through the Verification or Validation processes. Changes are made through the Technical processes, particularly Transition. 3) Releases for a software test, for software or system qualification or other formal tests, or for trial (beta) or operational use. 4) - Software system releases and deliveries are approved. 5) Releases often involve prioritization, tracking, scheduling, and closing changes. Approval of a release for operational use can include acceptance of the verified and validated changes. Criteria for approval of a release often includes rollback plans or contingency plans in the event of an unsuccessful release. 6) For software systems, automated version control tools can help ensure that only the correct source code versions are accessed, updated, tested and documented for approved changes by appropriate personnel, and released. 7) - Distribution of software system releases to specified environments or software deliveries is tracked and managed. 8) Master copies or copies of incremental changes to released software versions can be maintained for the life of the system or project in a controlled environment. Software suppliers often track delivered copies of licensed software to the acquirer in order to provide agreed software maintenance. The software system release is stored and distributed in accordance with agreement and with the policies of the organizations involved. [ISO/IEC/IEEE 12207:2017, 6.3.5.3 d) 1)] 9) Identify and record release requests, identifying the software system elements in a release. [ISO/IEC/IEEE 12207:2017, 6.3.5.3 d) 2)] 10) Approve software system releases and deliveries. [ISO/IEC/IEEE 12207:2017, 6.3.5.3 d) 3)] 11) Track and manage distribution of software system releases to specified environments or software deliveries.

Table C.1 *(continued)*

Reference	Name	Category	Characteristics
08-13	Configuration management identification records	Record	1) - The software system elements to be uniquely identified as configuration items subject to configuration control are selected. 2) Configuration items subject to configuration control in software systems usually include system/software requirements specifications, interface specifications; product and system elements (e.g., software objects, hardware, and services) while under development, baseline configurations or software versions established for transition between stages and as released for operational use; master ('gold') copies of source code or executable software for different platforms or versions; site-specific configurations in operational use; and information items, such as agreements, architecture models, service descriptions and operational procedures; and items in enabling systems. 3) Unique identification can be applied to software components, versions, or to individually licensed copies. The identifiers are in accordance with relevant standards and product sector conventions, such that the items under configuration control are unambiguously traceable to their supplier and to their specifications or equivalent recorded descriptions. Information items are often identified and managed separately from other configuration items. 4) Software configuration identifiers facilitate traceability when more than one developer or maintenance programmer is working on the same software function, so that various branches of code can be successfully reassembled and tested. 5) The ISO/IEC 19770 standard (multiple parts) provides an IT Asset management system for tracking software licenses. 6) - The attributes of configuration items are identified. 7) Attributes refers to item status, or physical or logical features useful for managing or maintaining the software system. Appropriate attributes can differ for hardware and software configuration items. 8) Configuration attributes and identifiers can reflect a decomposition of the software system, so that configuration items are tracked at the level at which change needs to be controlled. 9) Software from external suppliers can be tracked by its license and maintenance agreement, which can involve tracking to the location, number or size of systems where it is used or the number of concurrent users allowed. Software versions can be traced to the stakeholder requirements which they implement. [ISO/IEC/IEEE 12207:2017, 6.3.5.3 b) 1)] 10) Select the software system elements to be uniquely identified as configuration items subject to configuration control. [ISO/IEC/IEEE 12207:2017, 6.3.5.3 b) 2)] 11) Identify the attributes of configuration items.
08-17	Disposal Records	Record	1) - The software system or element is deactivated to prepare it for removal. 2) Interfaces to other systems are considered, in accordance with special procedures or instructions, and relevant health, safety, security and privacy constraints. 3) - The software system, its elements, its data, and non-reusable material from use or production for appropriate disposition and action is removed. 4) The disposition includes reuse, recycling, reconditioning, overhaul, or destruction. The disposition and subsequent actions are conducted in accordance with relevant safety, security, privacy and environmental standards, directives and laws. Elements of the software system that have useful life remaining, either in their current condition or following modification, are transferred to other systems-of-interest or organizations. Where appropriate, consider refurbishing system elements to extend their useful life. 5) - Impacted operating staff are withdrawn from the software system or system element and record relevant operating knowledge. 6) Reallocate, redeploy or retire operators. This is conducted in accordance with relevant safety, security, privacy and environmental standards, directives and laws. Act to safeguard and secure operator's knowledge and skills, using the Knowledge Management process.

Table C.1 *(continued)*

Reference	Name	Category	Characteristics
			7) - Designated software system elements are reused, recycled, reconditioned, overhauled, archived, or destroyed. 8) Handle system elements and their parts that are not intended for reuse in a manner that will assure they do not get back into the supply chain. 9) - Destruction is conduced of the system elements, as necessary, to reduce the amount of waste treatment or to make the waste easier to handle. 10) When the element is non-maintainable or non-recyclable, it is necessary to prevent the elements from getting back into the supply chain, e.g., complete erasure of all software from all system storage media and removal of license keys, data, and interfaces. This activity includes obtaining the destruction services to melt, crush, incinerate, demolish or eradicate the system or its elements as necessary. 11) - Confirm that detrimental health, safety, security, and environmental conditions following disposal have been identified and treated. 12) - The environment is returned to its original state or to a state that is specified by agreement. 13) - Information gathered through the lifetime of the product to permit audits and reviews in the event of long-term hazards to health, safety, security and the environment, and to permit future software system creators and users to build a knowledge base from experience is archived. [ISO/IEC/IEEE 12207:2017, 6.4.14.3 b) 1)] 14) Deactivate the software system or element to prepare it for removal. [ISO/IEC/IEEE 12207:2017, 6.4.14.3 b) 2)] 15) Remove the software system, its elements, its data, and non-reusable material from use or production for appropriate disposition and action. [ISO/IEC/IEEE 12207:2017, 6.4.14.3 b) 3)] 16) Withdraw impacted operating staff from the software system or system element and record relevant operating knowledge. [ISO/IEC/IEEE 12207:2017, 6.4.14.3 b) 4)] 17) Reuse, recycle, recondition, overhaul, archive, or destroy designated software system elements. [ISO/IEC/IEEE 12207:2017, 6.4.14.3 b) 5)] 18) Conduct destruction of the system elements, as necessary, to reduce the amount of waste treatment or to make the waste easier to handle. [ISO/IEC/IEEE 12207:2017, 6.4.14.3 c) 1)] 19) Confirm that detrimental health, safety, security, and environmental conditions following disposal have been identified and treated. [ISO/IEC/IEEE 12207:2017, 6.4.14.3 c) 2)] 20) Return the environment to its original state or to a state that is specified by agreement. [ISO/IEC/IEEE 12207:2017, 6.4.14.3 c) 3)] 21) Archive information gathered through the lifetime of the product to permit audits and reviews in the event of long-term hazards to health, safety, security and the environment, and to permit future software system creators and users to build a knowledge base from experience.
08-18	Enabling system records: Measurement	Record	[ISO/IEC/IEEE 12207:2017, 6.3.7.3 a) 7)] 1) Identify and plan for the necessary enabling systems or services to be used.
08-19	Enabling system records: Architecture definition	Record	[ISO/IEC/IEEE 12207:2017, 6.4.4.3 a) 5)] 1) Identify and plan for the necessary enabling systems or services needed to support the Architecture Definition process. [ISO/IEC/IEEE 12207:2017, 6.4.4.3 a) 6)] 2) Obtain or acquire access to the enabling systems or services to be used.
08-20	Enabling system records: Business or Mission Analysis.	Record	[ISO/IEC/IEEE 12207:2017, 6.4.1.3 a) 3)] 1) Identify and plan for the necessary enabling systems or services needed to support business or mission analysis. [ISO/IEC/IEEE 12207:2017, 6.4.1.3 a) 4)] 2) Obtain or acquire access to the enabling systems or services to be used.
08-21	Enabling system records: Design definition	Record	[ISO/IEC/IEEE 12207:2017, 6.4.5.3 a) 3)] 1) Identify and plan for the necessary enabling systems or services needed to support design definition. [ISO/IEC/IEEE 12207:2017, 6.4.5.3 a) 4)] 2) Obtain or acquire access to the enabling systems or services to be used.
08-22	Enabling system records: Disposal	Record	[ISO/IEC/IEEE 12207:2017, 6.4.14.3 a) 3)] 1) Identify and plan for the necessary enabling systems or services needed to support disposal. [ISO/IEC/IEEE 12207:2017, 6.4.14.3 a) 4)] 2) Obtain or acquire access to the enabling systems or services to be used.

Table C.1 *(continued)*

Reference	Name	Category	Characteristics
08-23	Enabling system records: Implementation	Record	[ISO/IEC/IEEE 12207:2017, 6.4.7.3 a) 3)] 1) Identify and plan for the necessary and distinct software environments, including enabling systems or services needed to support development and testing. [ISO/IEC/IEEE 12207:2017, 6.4.7.3 a) 4)] 2) Obtain or acquire access to the software environments and other enabling systems or services.
08-24	Enabling system records: Integration	Record	[ISO/IEC/IEEE 12207:2017, 6.4.8.3 a) 3)] 1) Identify and plan for the necessary enabling systems or services needed to support integration. [ISO/IEC/IEEE 12207:2017, 6.4.8.3 a) 4)] 2) Obtain or acquire access to the enabling systems or services to be used to support integration.
08-25	Enabling system records: Maintenance	Record	[ISO/IEC/IEEE 12207:2017, 6.4.13.3 a) 5)] 1) Identify and plan for the necessary enabling systems or services needed to support maintenance. [ISO/IEC/IEEE 12207:2017, 6.4.13.3 a) 6)] 2) Obtain or acquire access to the enabling systems or services to be used.
08-26	Enabling system records: Operation	Record	[ISO/IEC/IEEE 12207:2017, 6.4.12.3 a) 3)] 1) Identify and plan for the necessary enabling systems or services needed to support operation. [ISO/IEC/IEEE 12207:2017, 6.4.12.3 a) 4)] 2) Obtain or acquire access to the enabling systems or services to be used.
08-27	Enabling system records: Stakeholder needs and requirements	Record	[ISO/IEC/IEEE 12207:2017, 6.4.2.3 a) 3)] 1) Identify and plan for the necessary enabling systems or services needed to support stakeholder needs and requirements definition. [ISO/IEC/IEEE 12207:2017, 6.4.2.3 a) 4)] 2) Obtain or acquire access to the enabling systems or services to be used.
08-28	Enabling system records: System analysis	Record	[ISO/IEC/IEEE 12207:2017, 6.4.6.3 a) 5)] 1) Identify and plan for the necessary enabling systems or services needed to support the analysis. [ISO/IEC/IEEE 12207:2017, 6.4.6.3 a) 6)] 2) Obtain or acquire access to the enabling systems or services to be used.
08-29	Enabling system records: System/software requirements	Record	[ISO/IEC/IEEE 12207:2017, 6.4.3.3 a) 3)] 1) Identify and plan for the necessary enabling systems or services needed to support system/software requirements definition. [ISO/IEC/IEEE 12207:2017, 6.4.3.3 a) 4)] 2) Obtain or acquire access to the enabling systems or services to be used.
08-30	Enabling system records: Transition	Record	[ISO/IEC/IEEE 12207:2017, 6.4.10.3 a) 6)] 1) Identify and plan for the necessary enabling systems or services needed to support transition. [ISO/IEC/IEEE 12207:2017, 6.4.10.3 a) 7)] 2) Obtain or acquire access to the enabling systems or services to be used.
08-31	Enabling system records: Validation	Record	[ISO/IEC/IEEE 12207:2017, 6.4.11.3 a) 5)] 1) Identify and plan for the necessary enabling systems or services needed to support validation. [ISO/IEC/IEEE 12207:2017, 6.4.11.3 a) 6)] 2) Obtain or acquire access to the enabling systems or services to be used to support validation.
08-32	Enabling system records: Verification	Record	[ISO/IEC/IEEE 12207:2017, 6.4.9.3 a) 5)] 1) Identify and plan for the necessary enabling systems or services needed to support verification. [ISO/IEC/IEEE 12207:2017, 6.4.9.3 a) 6)] 2) Obtain or acquire access to the enabling systems or services to be used to support verification.
08-33	Information item disposal record	Record	1) - Unwanted, invalid or unvalidated information is disposed. 2) This is done according to organization policy, and security and privacy requirements. [ISO/IEC/IEEE 12207:2017, 6.3.6.3 b) 5)] 3) Dispose of unwanted, invalid or unvalidated information.
08-34	Information measurement communication record	Record	1) - Measurement users are informed. 2) - Results are recorded. 3) The measurement analyses results are reported to relevant stakeholders in a timely, usable fashion to support decision making and assist in corrective actions, risk management, and improvements. Results are reported to decision process participants, technical and management review participants, and product and process improvement process owners. [ISO/IEC/IEEE 12207:2017, 6.3.7.3 b) 4)] 4) Record results [and inform the measurement users.] [ISO/IEC/IEEE 12207:2017, 6.3.7.3 b) 4)] 5) [Record results and] inform the measurement users.
08-35	Infrastructure evaluation record	Record	1) - The degree to which delivered infrastructure resources satisfy project needs is evaluated. [ISO/IEC/IEEE 12207:2017, 6.2.2.3 b) 1)] 2) Evaluate the degree to which delivered infrastructure resources satisfy project needs.

Table C.1 *(continued)*

Reference	Name	Category	Characteristics
08-36	Infrastructure provision record	Record	1) - Infrastructure resources and services that are needed to implement and support projects are identified,] obtained and provided. 2) An inventory asset registry is often established to track infrastructure elements and support reuse of infrastructure assets. [ISO/IEC/IEEE 12207:2017, 6.2.2.3 a) 2)] 3) [Identify,] obtain and provide infrastructure resources and services that are needed to implement and support projects.
08-37	Knowledge Asset Records	Record	1) - Knowledge and skills are captured or acquired. 2) - Knowledge assets are developed or acquired. 3) Knowledge assets include system elements or their representations (e.g., reusable code libraries, reference architectures) architecture or design elements (e.g., architecture or design patterns), processes, criteria, or other technical information (e.g., training materials) related to domain knowledge, and lessons learned. 4) - Knowledge, skills, and knowledge assets are maintained. 5) - The reuse of knowledge, skills, and knowledge assets is recorded and monitored. [ISO/IEC/IEEE 12207:2017, 6.2.6.3 b) 2)] 6) Capture or acquire knowledge and skills. [ISO/IEC/IEEE 12207:2017, 6.2.6.3 c) 2)] 7) Develop or acquire knowledge assets. [ISO/IEC/IEEE 12207:2017, 6.2.6.3 d) 1)] 8) Maintain knowledge, skills, and knowledge assets. [ISO/IEC/IEEE 12207:2017, 6.2.6.3 d) 2)] 9) Monitor and record the reuse of knowledge, skills, and knowledge assets.
08-38	Knowledge Asset application	Record	1) - Knowledge and skills are shared across the organization. 2) - Knowledge assets are shared across the organization. 3) Automated search capabilities improve access to knowledge assets. [ISO/IEC/IEEE 12207:2017, 6.2.6.3 b) 3)] 4) Share knowledge and skills across the organization. [ISO/IEC/IEEE 12207:2017, 6.2.6.3 c) 3)] 5) Share knowledge assets across the organization.
08-39	Knowledge asset review record	Record	1) - The currency of technology and market needs for the knowledge assets are periodically reassessed. 2) Assess the business benefits which the organization gained through the use of knowledge management practices. [ISO/IEC/IEEE 12207:2017, 6.2.6.3 d) 3)] 3) Periodically reassess the currency of technology and market needs for the knowledge assets.
08-40	Maintenance (Logistics) Records	Record	1) - Incidents and problems are recorded, including their resolutions, and significant maintenance and logistics results. 2) This includes anomalies due to the maintenance strategy, the maintenance enabling systems, execution of the maintenance and logistics, or incorrect system definition. The Project Assessment and Control and Quality Assurance processes are used to perform maintenance problem identification and resolution, e.g., analyse the data to identify the root cause, enable corrective or improvement actions, and record lessons learned. This activity can include changes to logistics or software distribution procedures. Changes to the software system requirements, architecture, or design are done within other Technical processes. 3) - Trends of incidents, problems, and maintenance and logistics actions are identified and recorded. 4) Trend data and problem resolution reports are used to inform operations and maintenance personnel, customers, and other stakeholders and projects that are creating or utilizing similar system entities. 5) Incident and problem reporting, including resulting action taken, is tracked through the incident and process management activity of the Quality Assurance process. 6) - Customer satisfaction is measured and monitored with system and maintenance support.

Table C.1 *(continued)*

Reference	Name	Category	Characteristics
			7) ISO 10004:2012 contains guidelines for monitoring and measuring customer satisfaction. When customer satisfaction data is collected, it is then used in the Quality Management process. [ISO/IEC/IEEE 12207:2017, 6.4.13.3 d) 1)] 8) Record incidents and problems, including their resolutions, and significant maintenance and logistics results. [ISO/IEC/IEEE 12207:2017, 6.4.13.3 d) 2)] 9) Identify and record trends of incidents, problems, and maintenance and logistics actions. [ISO/IEC/IEEE 12207:2017, 6.4.13.3 d) 5)] 10) Monitor and measure customer satisfaction with system and maintenance support.
08-41	Manage architecture	Record	1) - The architecture governance approach is formalized and governance-related roles and responsibilities, accountabilities, and authorities related to design, quality, security, and safety are specified. 2) - Explicit acceptance of the architecture by stakeholders is obtained. 3) The Validation process is used to confirm that the architecture models and views reflect stakeholder requirements, that stakeholder concerns are addressed, and to help ensure that future iterations of software system architecture better address stakeholder concerns. 4) - Concordance and completeness of the architectural entities and their architectural characteristics is maintained. 5) The entities to be checked are not only technical. These are also, for example, legal, economical, organizational and operational entities that are normally part of stakeholder requirements and concerns. 6) - The evolution of the architecture models and views is organized, assessed and controlled to help ensure that the architectural intent is met and the architectural vision and key concepts are correctly implemented. 7) - The architecture definition and evaluation strategy is maintained. [ISO/IEC/IEEE 12207:2017, 6.4.4.3 f) 1)] 8) Formalize the architecture governance approach and specify governance-related roles and responsibilities, accountabilities, and authorities related to design, quality, security, and safety. [ISO/IEC/IEEE 12207:2017, 6.4.4.3 f) 2)] 9) Obtain explicit acceptance of the architecture by stakeholders. [ISO/IEC/IEEE 12207:2017, 6.4.4.3 f) 3)] 10) Maintain concordance and completeness of the architectural entities and their architectural characteristics. [ISO/IEC/IEEE 12207:2017, 6.4.4.3 f) 4)] 11) Organize, assess and control evolution of the architecture models and views to help ensure that the architectural intent is met and the architectural vision and key concepts are correctly implemented. [ISO/IEC/IEEE 12207:2017, 6.4.4.3 f) 5)] 12) Maintain the architecture definition and evaluation strategy.
08-42	Manage software elements	Record	1) - The software system element is packaged and stored. 2) Contain the software system element in order to achieve continuance of its characteristics. Conveyance and storage, and their durations, can influence the specified containment. For software, a master copy of the implemented software (electronic or on physical media) is stored in a controlled location and made available to authorized roles (e.g., for use in the Integration and Transition processes). Configuration and product information is captured by the Configuration Management and Information Management processes when the element is stored. 3) - Objective evidence that the software system element meets requirements is recorded. 4) Evidence is provided in accordance with supply agreements, legislation and organization policy. Evidence includes element modifications made due to processing changes or non-conformances found during the Verification and Validation processes. The objective evidence is part of the element's as-implemented configuration baseline established through the Configuration Management process and includes the results of unit testing, analysis, inspections, walkthrough events, demonstrations, product or technical reviews, or other verification exercises. [ISO/IEC/IEEE 12207:2017, 6.4.7.3 b) 5)] 5) Package and store the software system element. [ISO/IEC/IEEE 12207:2017, 6.4.7.3 b) 6)] 6) Record objective evidence that the software system element meets requirements.

Table C.1 *(continued)*

Reference	Name	Category	Characteristics
08-43	Manage software system element design	Record	1) - The design and rationale is captured. 2) Commonly captured information includes the software system elements and affiliated requirements and design data, e.g., for software elements, internal and external interfaces, data structures, implementation and test requirements, unit aggregation data for integration, and test cases. Rationale typically includes information about major implementation options and enablers. The resultant design is controlled in accordance with the strategy. 3) - Traceability is established between the detailed design elements, the system/software requirements, and the architectural entities of the software system architecture. 4) This task facilitates providing feedback to the Architecture Definition process for potential modifications, for example, to modify the allocation of software system elements in order to obtain the expected architectural characteristics; or possibly to modify the expected architectural characteristic due to factors discovered during the design process, or to make stakeholders aware of the potential impacts. 5) Through the life cycle, bidirectional traceability is maintained between the design and the verification methods or techniques, and software system element requirements. Allocations and design properties are assigned to software elements, software units and affiliated artifacts, at a detailed enough level to permit software testing and implementation, including construction. [ISO/IEC/IEEE 12207:2017, 6.4.5.3 d) 1)] 6) Capture the design and rationale. [ISO/IEC/IEEE 12207:2017, 6.4.5.3 d) 3)] 7) Determine the status of the software system and element design.
08-44	Manage stakeholder requirements	Record	1) - Explicit agreement is obtained with designated stakeholders on the stakeholder requirements. 2) This includes confirming that stakeholder requirements are expressed correctly, comprehensible to originators, and that the resolution of conflict in the requirements has not corrupted or compromised stakeholder intentions. [ISO/IEC/IEEE 12207:2017, 6.4.2.3 f) 1)] 3) Obtain explicit agreement with designated stakeholders on the stakeholder requirements.
08-45	Manage system requirements	Record	1) - Explicit agreement is obtained on the system/software requirements. 2) This includes confirming that system/software requirements are expressed correctly, comprehensible to originators and implementers, and that the resolution of conflict in the requirements is consistent with stakeholder decisions. [ISO/IEC/IEEE 12207:2017, 6.4.3.3 d) 1)] 3) Obtain explicit agreement on the system/software requirements.
08-46	Operation actions	Record	1) - The software system is used in its intended operational environment. 2) Where agreed, continuous service capacity and quality is maintained when the software system replaces an existing system or element that is being retired. 3) - Materials and other resources area applied, as required, to operate the software system and sustain its services. 4) This includes energy sources for hardware, connectivity for software, and human or automated operators. 5) - Software system operation is monitored, including consideration of the following: i) Managing adherence to the operation strategy (e.g. , operational procedures); ii) Recording and reporting significant events, such as possible breaches of software and data confidentiality and integrity; iii) Operating the software system in a safe manner and compliant with legislated guidelines e.g. , those concerning occupational safety and environmental protection; and iv) Recording when software system or service performance is not within acceptable parameters.

Table C.1 *(continued)*

Reference	Name	Category	Characteristics
			6) This includes anomalies due to the operation strategy, the operation enabling systems, execution of the operation, or incorrect software system definition. The system sometimes exhibits unacceptable performance when system elements implemented in hardware have degraded or exceeded their useful life or the system's operational environment affects the software operation, e.g., workload above capacity thresholds, utilization by contending applications, security hacks, or software defects. 7) - Where feasible, automated operational procedures are developed to minimize the risk of operational anomalies, consistent with the operational strategy. 8) This includes procedures for handling routine (pre-approved) change requests and service requests, troubleshooting and incident reporting, especially for security incidents. 9) - Measurements are analysed to confirm that: i) Service performance is within acceptable parameters or agreed service levels for the agreed workload; ii) System and service availability and response times are acceptable; iii) Cost of operation is consistent with objectives and constraints; and iv) Potential improvements are identified and prioritized, consistent with the operational strategy. 10) Operator feedback and suggestions are often useful input for improving software system operational performance. The Quality Assurance and Measurement processes can be applied. 11) - Contingency operations are performed, if necessary. 12) This includes operating the software system in a degraded mode, performing back-out and restore operation, system shutdown, implementation of work-around procedures to restore operation, or other modes for special conditions. If needed, the operator performs steps necessary to enter into contingency operations and possibly power down the system. Contingency operations are performed in accordance with pre-established procedures for such an event. Often these procedures are accompanied by a continuity plan.. [ISO/IEC/IEEE 12207:2017, 6.4.12.3 b) 1)] 13) Use the software system in its intended operational environment. [ISO/IEC/IEEE 12207:2017, 6.4.12.3 b) 2)] 14) Apply materials and other resources, as required, to operate the software system and sustain its services. [ISO/IEC/IEEE 12207:2017, 6.4.12.3 b) 3)] 15) Monitor software system operation, including consideration of the following: i) Managing adherence to the operation strategy (e.g. , operational procedures); ii) Recording and reporting significant events, such as possible breaches of software and data confidentiality and integrity; iii) Operating the software system in a safe manner and compliant with legislated guidelines e.g. , those concerning occupational safety and environmental protection; and iv) Recording when software system or service performance is not within acceptable parameters. [ISO/IEC/IEEE 12207:2017, 6.4.12.3 b) 4)] 16) Consistent with the operational strategy, develop and, where feasible, automate operational procedures to minimize the risk of operational anomalies. [ISO/IEC/IEEE 12207:2017, 6.4.12.3 b) 5)] 17) Consistent with the operational strategy, analyse measurements to confirm that: i) Service performance is within acceptable parameters or agreed service levels for the agreed workload; ii) System and service availability and response times are acceptable; iii) Cost of operation is consistent with objectives and constraints; and iv) Potential improvements are identified and prioritized. [ISO/IEC/IEEE 12207:2017, 6.4.12.3 b) 6)] 18) Perform contingency operations, if necessary.