INTERNATIONAL STANDARD

# ISO/IEC/IEEE 15289

Third edition
2017-06

# Systems and software engineering — Content of life-cycle information items (documentation)

*Ingénierie des systèmes et du logiciel — Contenu des articles d'information du cycle de vie (documentation)*



Reference number
ISO/IEC/IEEE 15289:2017(E)



ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Institute of Electrical and Electronics Engineers, Inc
3 Park Avenue, New York
NY 10016-5997, USA

stds.ipr@ieee.org
www.ieee.org

 

# Contents

Page

## List of Tables

## Foreword

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

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. The IEEE develops its standards through a consensus development process, approved by the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and serve without compensation. While the IEEE administers the process and establishes rules to promote fairness in the consensus development process, the IEEE does not independently evaluate, test, or verify the accuracy of any of the information contained in its standards.

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

Attention is called to the possibility that implementation of this document may require the use of subject matter covered by patent rights. By publication of this document, no position is taken with respect to the existence or validity of any patent rights in connection therewith. ISO/IEC and IEEE are not responsible for identifying essential patents or patent claims for which a license may be required, for conducting inquiries into the legal validity or scope of patents or patent claims or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance or a Patent Statement and Licensing Declaration Form, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this document are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from ISO or the IEEE Standards Association.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 7, *Systems and software engineering*, in cooperation with the Software & Systems Engineering Standards Committee of the IEEE Computer Society, under the Partner Standards Development Organization cooperation agreement between ISO and IEEE.

This third edition cancels and replaces the second edition (ISO/IEC/IEEE 15289:2015), of which it constitutes a minor revision. This third edition reflects ISO/IEC/IEEE 15288:2015, *Systems and software engineering—System life cycle processes,* which replaced ISO/IEC 15288:2008 (IEEE Std 15288:2008).

## Introduction

The purpose of this document is to provide requirements for identifying and planning the specific information items (information products) to be developed and revised during systems and software life cycles and service processes. This document specifies the purpose and content of all identified systems and software life-cycle information items, as well as information items for information technology service management. The information item contents are defined according to generic document types and the specific purpose of the document. Information items are combined or subdivided as needed for project or organizational purposes.

This document is based on the life-cycle processes specified in ISO/IEC 12207:2008 (IEEE Std 12207-2008), *Systems and software engineering — Software life cycle processes*; ISO/IEC/IEEE 15288:2015, *Systems and software engineering — System life cycle processes*; and the service management processes specified in ISO/IEC 20000-1:2011 (IEEE Std 20000-1:2013), *Information technology — Service management — Part 1: Service Management System Requirements*; and ISO/IEC 20000-2:2012 (IEEE Std 20000-2:2013), *Information technology — Service management — Part 2: Guidance on the application of service management systems*.

ISO/IEC 12207:2008 (IEEE Std 12207-2008) and ISO/IEC/IEEE 15288:2015 define a set of processes for managing and performing the stages of a system life cycle. They define an Information Management process, but they do "not detail information items in terms of name, format, explicit content, and recording media". ISO/IEC/IEEE 15288:2015, and ISO/IEC 12207:2008 (IEEE Std 12207-2008) establish a common framework for systems and software life-cycle processes and identify or require a number of documentation items. Their process reference model does not represent a particular process implementation approach, nor does it prescribe a system/software life-cycle model, methodology, or technique. ISO/IEC 12207:2008 (IEEE Std 12207-2008) does not always specify when software information items are to be prepared, nor does it identify information item contents. ISO/IEC 20000-1:2011 (IEEE Std 20000-1:2013) establishes comprehensive requirements for documents and records, with some specific requirements. ISO/IEC 20000-2:2012 (IEEE Std 20000-2:2013), Information technology — Service management — Part 2: Guidance on the application of service management systems provides guidance on the use of Part 1.

IEEE contributed IEEE 12207.1-1997, *Industry Implementation of International Standard ISO/IEC 12207:1995. (ISO/IEC 12207) Standard for Information Technology — Software life cycle processes — Life cycle data*, as a source for the first edition of this document.

# Systems and software engineering — Content of life-cycle information items (documentation)

## 1 Scope

This document specifies the purpose and content of all identified systems and software life-cycle and service management information items (documentation). The information item contents are defined according to generic document types, as presented in Clause 7, and the specific purpose of the document (Clause 10).

This document assumes an organization is performing life-cycle processes, or practicing service management, using one or more of the following:

— ISO/IEC 12207:2008 (IEEE Std 12207-2008), Systems and software engineering — Software life cycle processes;

— ISO/IEC/IEEE 15288:2015, Systems and software engineering — System life cycle processes;

— ISO/IEC 20000-1:2011 (IEEE Std 20000-1:2013), Information technology — Service management — Part 1: Service management system requirements; and

— ISO/IEC 20000-2 (IEEE Std 20000-2:2013), *Information technology — Service management — Part 2: Guidance on the application of service management systems.*

This document provides a mapping of processes from the above standards to a set of information items. It provides a consistent approach to meeting the information and documentation requirements of systems and software engineering and IT service management.

This document does not establish a service management system.

ISO/IEC 12207:2008 (IEEE Std 12207-2008) and ISO/IEC/IEEE 15288:2015 define a set of processes for managing and performing the stages of a software or system life cycle. They define an Information Management process, but do not "detail information items in terms of name, format, explicit content, and recording media".

ISO/IEC/IEEE 15288:2015 and ISO/IEC 12207:2008 (IEEE Std 12207-2008) establish a common framework for system and software life-cycle processes. They identify or require a number of documentation items. Their process reference model does not represent a particular process implementation approach, nor prescribe a system/software life-cycle model, methodology or technique.

ISO/IEC 20000-1:2011 (IEEE Std 20000-1:2013) establishes comprehensive requirements for documents and records, with some specific requirements.

ISO/IEC 20000-2:2012 (IEEE Std 20000-2:2013), provides guidance on the use of ISO/IEC 20000-1:2011 (IEEE Std 20000-1:2013).

The generic document types defined in this document are used to identify the information necessary to support the following:

— the ISO/IEC/IEEE 15288:2015 agreement;

— organizational project-enabling;

— technical management and processes;

— the ISO/IEC 12207:2008 (IEEE Std 12207-2008) primary, supporting, and organizational life-cycle processes; and

— the ISO/IEC 20000-1:2011 (IEEE Std 20000-1:2013) service management system (SMS), service delivery, relationship, resolution, and control processes.

The generic document types (which can be referred to as information item types) are used to identify the information necessary to support the ISO/IEC/IEEE 15288:2015 agreement, organizational project-enabling, technical management, and technical processes; the ISO/IEC 12207:2008 (IEEE Std 12207-2008) primary, supporting, and organizational life-cycle processes; or the ISO/IEC 20000-1:2011 (IEEE Std 20000-1:2013) service management system (SMS), service delivery, relationship, resolution, and control processes.

For each life-cycle process or service, it would be possible to prepare a policy, plan, procedures, and reports, as well as numerous records, requests, descriptions and specifications. Such an elaboration of the documentation schema would be more rigorous than specified by ISO/IEC/IEEE 15288:2015 or ISO/IEC 12207:2008 (IEEE Std 12207-2008). As ISO/IEC/IEEE 15288:2015 points out (1.4), "The users of this document are responsible for selecting a life cycle model for the project and mapping the processes, activities, and tasks in this document into that model. The parties are also responsible for selecting and applying appropriate methodologies, methods, models and techniques suitable for the project." Thus, information items are combined or subdivided consistent with the life cycle model, as needed for project or organizational purposes, as further defined in Clause 4, Applicability, and Clause 5, Conformance.

The scope of this document does not include the following:

a) the format or content of recommended input data or input information items, except for the content of those input items that are also output information items;

b) instructions on combining or subdividing information items and information item contents of a similar nature;

c) guidance on selecting an appropriate presentation format, delivery media, and maintenance technology for systems or software life-cycle data, records, information items, or documentation, such as electronic publishing systems, content management systems, or data repositories;

NOTE 1 ISO/IEC 12207:2008 (IEEE Std 12207-2008) does not always specify when software information items are to be prepared, nor does it identify information item contents.

NOTE 2 ISO/IEC/IEEE 26531, System and software engineering – Content management for product life-cycle, user, and service management documentation, provides requirements for content management and component content management systems.

d) detailed content for information items related to general business, contractual, organizational, and financial management that is not specific to systems and software engineering and information technology service management, such as business strategies, contract change notices, human resources and investment policies, personnel selection criteria, financial budgeting and accounting policies and procedures, cost reports, or payroll data;

e) information items showing only approval of an ISO/IEC 12207:2008 (IEEE Std 12207-2008) subclause, such as ISO/IEC 12207:2008 (IEEE Std 12207-2008), 6.1.2.3.4.5;

f) any ISO/IEC/IEEE 15288:2015 or ISO/IEC 12207:2008 (IEEE Std 12207-2008) subclause not explicitly or implicitly identifying the recording of information about a process, activity or task, for example, ISO/IEC 12207:2008 (IEEE Std 12207-2008), 6.4.4;

g) work products, models, software, and other artifacts of life-cycle products and services that are not information items or records used in information items.

NOTE 3 ISO/IEC 26514:2008, Systems and software engineering — Requirements for designers and developers of user documentation, provides guidance on formats for user documentation.

## 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 12207:2008 (IEEE Std 12207-2008), *Systems and software engineering — Software life cycle processes*

— ISO/IEC/IEEE 15288:2015, *Systems and software engineering — System life cycle processes*

— ISO/IEC 20000-1:2011 (IEEE Std 20000-1:2013), *Information technology — Service management — Part 1: Service management system requirements*

## 3 Terms, definitions, and abbreviated terms

For the purposes of this document, the terms and definitions given in ISO/IEC/IEEE 24765 (available at www.computer.org/sevocab) apply.

ISO, IEC, and IEEE maintain terminological databases for use in standardization at the following addresses:

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

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

— IEEE Standards Dictionary Online: available at http://ieeexplore.ieee.org/xpls/dictionary.jsp

NOTE ISO/IEC 20000-1:2011 contains different definitions for the terms document, procedure, record and service request. Those definitions are applicable when conforming to that document..

### 3.1 Terms and definitions

**3.1.1**
**approval**
notification by an authorized representative that a deliverable item appears to satisfy requirements and is complete

Note 1 to entry: Such approval does not shift responsibility from the supplier to meet requirements under a two-party situation.

**3.1.2**
**complaint**
record of perceived non-compliance with a service level agreement or customer dissatisfaction with service

**3.1.3**
**complete [documentation]**
including all critical information and any necessary, relevant information for the intended audience

**3.1.4**
**consistent**
without internal conflicts

**3.1.5**
**Commercial-Off-The-Shelf**
**COTS**
product available for purchase and use without the need to conduct development activities

**3.1.6**
**criteria**
rules on which a judgment or decision can be based, or by which a product, service, result, or process can be evaluated

**3.1.7**
**critical information**
information describing the safe use of the software, the security of the information created with the software, or the protection of the sensitive personal information created by or stored with the software

[SOURCE: ISO/IEC 26514:2008]

**3.1.8**
**database**
collection of data organized according to a conceptual structure describing the characteristics of the data and the relationships among their corresponding entities, supporting one or more application areas

**3.1.9**
**description**
information item that represents a planned or actual concept, function, design, or object

**3.1.10**
**document**
uniquely identified unit of information for human use

EXAMPLE A report, specification, manual or book, in printed or electronic form.

Note 1 to entry: A document can be a single information item, or part of a larger information item.

**3.1.11**
**documentation plan**
plan identifying the documents to be produced during the system or software life cycle

**3.1.12**
**include [information]**
having either the information or a reference to the information present in the document

**3.1.13**
**information item**
separately identifiable body of information that is produced, stored, and delivered for human use

Note 1 to entry: "Information product" is a synonym. A document produced to meet information requirements can be an information item, or part of an information item, or a combination of several information items.

Note 2 to entry: An information item can be produced in several versions during a project or system life cycle.

**3.1.14**
**information item content**
information included in an information item, associated with a system, product or service, to satisfy a requirement or need

**3.1.15**
**information item type**
group of information items consistent with a pre-arranged set of generic criteria

Note 1 to entry: A "generic document type" is a synonym.

EXAMPLE A "plan" is the information item type for all plans and "report" is the information item type for all reports.

**3.1.16**
**modifiable**
structured and has a style such that changes can be made completely, consistently, and correctly while retaining the structure

**3.1.17**
**plan**
information item that presents a systematic course of action for achieving a declared purpose, including when, how, and by whom specific activities are to be performed

**3.1.18**
**policy**
clear and measurable statement of preferred direction and behavior to condition the decisions made within an organization

[SOURCE: ISO/IEC 38500:2008]

**3.1.19**
**presentable**
retrievable and viewable

**3.1.20**
**procedure**
information item that presents an ordered series of steps to perform a process, activity, or task

Note 1 to entry: A procedure defines an established and approved way or mode of conducting business in an organization. It details permissible or recommended methods in order to achieve technical or managerial goals or outcomes.

Note 2 to entry: According to ISO 9000:2015, procedures can be documented or not.

**3.1.21**
**process**
set of interrelated or interacting activities which transforms inputs into outputs

**3.1.22**
**record**
set of related data items treated as a unit

**3.1.23**
**report**
information item that describes the results of activities such as investigations, observations, assessments, or tests

**3.1.24**
**request**
information item that initiates a defined course of action or change to fulfill a need

**3.1.25**
**service request**
request for information, or for a routine change or procedure with previously evaluated risk

EXAMPLE A request to provide access to a controlled application, a request to move hardware.

**3.1.26**
**software item**
identifiable part of a software product

EXAMPLE Identification and descriptions of the software product, source code, software life-cycle data, archive and release data, and instructions for building the executable object code.

**3.1.27**
**specification**
information item that identifies, in a complete, precise, and verifiable manner, the requirements, design, behavior, or other expected characteristics of a system, service, or process

**3.1.28**
**traceable**
having components whose origin can be determined

**3.1.29**
**unambiguous**
described in terms that allow only a single interpretation, aided, if necessary, by a definition

**3.1.30**
**verifiable**
can be checked for correctness by a person or tool

### 3.2 Abbreviated terms

CFP Call for Proposals

CM Configuration management

COTS Commercial-Off-The-Shelf

ITT Invitation to Tender

RFP Request for Proposal

SLA Service level agreement

SMS Service management system

## 4 Applicability

### 4.1 Purpose

The purpose of this document is to provide requirements for users of ISO/IEC 12207:2008 (IEEE Std 12207-2008), ISO/IEC/IEEE 15288:2015, and ISO/IEC 20000-1:2011 (IEEE Std 20000-1:2013) for identifying and planning the specific information items (information products) to be developed and revised during systems and software life cycles and service management processes. This document is intended for use as follows:

a) To address the technical information needed by those involved in ISO/IEC/IEEE 15288:2015 and ISO/IEC 12207:2008 (IEEE Std 12207-2008) processes;

b) To specify information in an agreement process as described in ISO/IEC/IEEE 15288:2015 or a two-party situation as described in ISO/IEC 12207:2008 (IEEE Std 12207-2008), ISO/IEC 20000-1:2011 (IEEE Std 20000-1:2013) and ISO/IEC 20000-2:2012 (IEEE Std 20000-2:2013). The two-party situation may range from an informal agreement within an organization to a legally binding contract between organizations;

c) To develop information items that provide evidence for process assessment performed with respect to ISO/IEC 33001, and to guide process improvement activities; and

d) To guide a single party in self-imposed tasks.

### 4.2 Intended users of this document

This document is applicable for use by the following:

a) project managers responsible for the Information Management process of ISO/IEC/IEEE 15288:2015 (6.3.6) during a system life cycle;

b) project managers responsible for identifying information item requirements and document contents when using ISO/IEC 12207:2008 (IEEE Std 12207-2008), or any other software engineering life-cycle process, to help determine what should be documented, when the documentation should be developed, and what the contents of the documents should be;

c) acquirers responsible for determining what information items are needed to help ensure the quality of the project, or delivered system, product or service;

d) individuals who write or support the design and development of service, systems and software information items;

e) individuals responsible for identifying information items required to claim conformance with ISO/IEC 12207:2008 (IEEE Std 12207-2008), ISO/IEC/IEEE 15288:2015, or ISO/IEC 20000-1:2011 (IEEE Std 20000-1:2013); and

f) individuals undertaking service, systems or software process improvement in their organizations.

### 4.3 Applicability to work efforts

Use of this document is not limited by size, complexity or criticality of the project. It may be applied to the following:

a) any type of project and life-cycle process;

b) any of the activities and tasks of a project and system or software product or service life cycle;

c) all forms of information items, information item content and document delivery media; and

d) documentation in Commercial-Off-The-Shelf (COTS) products when the COTS product is specified as a deliverable under a two-party situation.

NOTE See ISO/IEC 12207:2008 (IEEE Std 12207-2008), 1.2.

### 4.4 Applicability to information item audiences

Users of this document should determine the relationship of the requirements in this document to the requirements and needs of their audience (customers or users of information), or project and organizational procedures. The type of decision to be made, or the work to be performed, by users of the information should be considered before an information item is prepared. Reviewing and understanding the requirements, needs, and background of users and stakeholders are essential to applying this document accurately and economically, since some information items are designed for various purposes and user groups:

a) To provide information to specialized types of users who may not be a part of a particular project;

b) To address the same type of user but in environments not normally coexisting in the same effort; and

c) To aid both users who are expected to understand technical concepts and terminology, and users who may not have this background.

## 5 Conformance

### 5.1 Definition of conformance

This document may be used as a conformance or a guidance document for projects and organizations claiming conformance to ISO/IEC/IEEE 15288:2015, ISO/IEC 12207:2008 (IEEE Std 12207-2008), or ISO/IEC 20000-1:2011 (IEEE Std 20000-1:2013).

NOTE 1 Service providers can refer to ISO/IEC 20000-1:2011 (IEEE Std 20000-1:2013) and ISO/IEC TR 20000-3:2012 regarding claims of conformance for a defined certification scope, for example, organizational units, services, location.

NOTE 2 ISO/IEC 20000-1:2011 is a management system standard stating requirements for service providers. Some requirements of this document are not requirements of ISO/IEC 20000-1. Some requirements of ISO/IEC 20000-1 are not requirements of this document.

If the selected systems or software life-cycle processes have been tailored in conformance with ISO/IEC 15288 or ISO/IEC 12207, to claim conformance to this document, the user of this document shall prepare the information items identified in this document applicable to the selected and tailored ISO/IEC/IEEE 15288:2015 or ISO/IEC 12207:2008 (IEEE Std 12207-2008), processes.

The generic and specific record and information item titles and contents in Clauses 7, 9, and 10 of this document may be tailored to satisfy requirements of an organization, its projects, or agreements based on the tailored conformance to ISO/IEC/IEEE 15288:2015 or ISO/IEC 12207:2008 (IEEE Std 12207-2008). In tailoring, information items provided in this document may be modified (added to, combined or retitled). The contents of the information items shall correspond to the selected and tailored processes.

NOTE 3 Annex A of ISO/IEC/IEEE 15288:2015 and ISO/IEC 12207:2008 (IEEE Std 12207-2008) provide requirements for the Tailoring process.

In this document, for simplicity of reference, each information item is described as if it were published as a separate document. However, information items shall be considered as conforming if they are unpublished but available in a repository for reference, divided into separate documents or volumes, or combined with other information items into one document. Use of the nomenclature of the specific records in Clause 9 or the information item titles in Clause 10 is not required to claim conformance with this document.

Throughout this document, "shall" is used to express a provision that is normative, "should" to express a recommendation among other possibilities, and "may" to indicate a course of action permissible within the limits of this document.

The verb "include" used in this document indicates that either (1) the information is present or (2) a reference to the information is given.

## 5.2 Conformance situations

Conformance may be claimed for organizations, projects, multi-supplier projects, services, and information items, as identified in the claim of conformance:

a) When conformance is claimed for an organization or a service provider, the organization or service provider shall produce a document declaring its tailoring of the records and information items, and its interpretation of any clauses of this document that reference "the contract."

b) When conformance is claimed for a project (or program), the project plans or the contract shall document the tailoring of the records and information items, and the interpretation of any clauses of this document that reference "the contract."

c) When conformance is claimed for multi-supplier projects, it may be the case that no individual project can claim conformance because no single contract calls for all the required records and information items. Nevertheless, the projects, as a whole, may claim conformance if each of the required records and information items is produced by an identified party. The program plans shall document the tailoring of the records and information items, and their assignment to the various parties, as well as the interpretation of any clauses of this document that reference "the contract."

d) When conformance is claimed for an information item, the item shall contain the generic contents required in Clause 7 of this document and the specific content required in Clause 10.

NOTE 1 One possible way for an organization to deal with clauses that cite "the contract" is to specify that they will be interpreted in the project plans for any particular project. A project's claim of conformance is typically specified with respect to the organization's claim of conformance.

NOTE 2 In accordance with ISO/IEC 17000:2004, *Conformity assessment — Vocabulary and general principles*, an organization or a project or a multi-supplier program can be said to comply with this document when its products (the information items) fulfill the requirements, but the organization, project or program has not met the specific requirements for conformance stated in items (a), (b) or (c) above.

### 5.3 Type of conformance

One of the following types of conformance shall be asserted. The selected type shall be identified in the claim of conformance:

a) Tailored: The minimum set of required information items is determined by tailoring of processes and activities in accordance with Annex A of ISO/IEC 12207:2008 (IEEE Std 12207-2008) or Annex A of ISO/IEC/IEEE 15288:2015.

b) Absolute: The minimum set of required information items is all of those specified as normative (that is, clauses containing "shall") in the text of the normative reference standards.

Absolute conformance may be claimed for selected processes or information items even if absolute conformance with all requirements of this document is not claimed.

## 6 Life-cycle data and information items

### 6.1 Life-cycle data characteristics

This document specifies how life-cycle data is managed in information items. The required data from the life-cycle or service process shall be organized into records and presented in one or more information items, and shall be consistent with an information item generic type. An information item shall include its generic information item contents (Clause 7).

Each set of records and each information item produced as a document described in this document shall support the following life-cycle data characteristics:

a) unambiguous;

b) complete;

c) verifiable;

d) consistent;

e) modifiable;

f) traceable; and

g) presentable.

### 6.2 Records compared to information items (documents)

A record is a special type of documented information containing a set of structured data treated as a unit. Table 4 in Clause 9 identifies records. Consistent with ISO 9000:2015, the purpose of a record is to state results achieved or to provide evidence of activities performed. In fact, ISO/IEC 20000-1:2011 (IEEE Std 20000-1:2013) considers any document or information item to be a record. However, this document distinguishes between records of data and documents (information items).

Data records gain their value from being combined with other records in a set, typically by inclusion in structured databases, registers, or repositories where the individual records are available for retrieval and analysis. Records hold the factual data (evidence) for the other generic information types. Data can be aggregated into records, and these records may be included in a report which is already defined as a particular information item (e.g. test report), or they may exist separately for other uses defined by the project. A single record, a selection of records, or a complete listing of the repository's contents is not suitable for issuance as a complete communication product as are the information items (documents) such as a plan or procedure. The information items (documents) are produced and communicated for human use and contain formal elements (such as purpose, scope, and summary), intended to make them usable by their intended audience.

## 6.3 Management of life-cycle data (records)

Life-cycle data results from the execution of the process or service management system activities and tasks. Data can be a work product or an element in other information items. Many of the clauses in ISO/IEC/IEEE 15288:2015 and ISO/IEC 12207:2008 (IEEE Std 12207-2008) require life-cycle data to be produced or recorded. However, the clauses of ISO/IEC/IEEE 15288:2015 and ISO/IEC 12207:2008 (IEEE Std 12207-2008) do not dictate the content, location, format, or media to be used to record and maintain the data. When choosing appropriate data to be recorded, record managers should also determine where in the organization or project's record-keeping systems the data should be recorded. Records may be maintained in databases, registers, repositories, archives, or other data management systems. Organizations or projects shall establish record retention policies in consideration of system life-cycle and organizational or service management needs for the data. Clause 9 defines the content of generic records and recommends content for specific records.

NOTE Requirements and guidance for records management are found in ISO/IEC 16175:2010, *Information and documentation — Principles and functional requirements for records in electronic office environments — Part 1: Overview and statement of principles.*

## 6.4 Management of information items (documents)

The management of information items shall be performed by applying the Information Management process of ISO/IEC 12207:2008 (IEEE Std 12207-2008) and ISO/IEC/IEEE 15288:2015, the Documentation Management and Software Documentation Management processes of ISO/IEC 12207:2008 (IEEE Std 12207-2008), including the knowledge management activities of ISO/IEC/IEEE 15288:2015 clause 6.2.4, or the documentation management activities of ISO/IEC 20000-1:2011 (IEEE Std 20000-1:2013). The Information Management process should support the needs of a project and the related product or service. It should include procedures for preparing, collecting, identifying, classifying, distributing, storing, updating, archiving, and retrieving information.

Annex A of this document provides a summary procedure for identifying and planning for information items and their contents. Information items should be defined to be applicable to multiple related processes used by a project or organization, or to related services (such as incident and problem management). Information items may be combined or subdivided consistent with the project, service, or system processes, phases, and stakeholder needs.

The information management process shall produce these outcomes:

a) Information to be managed is identified.

b) Information representations are defined.

c) Information is obtained, developed, transformed, stored, validated, presented, and disposed of.

d) The status of information is identified.

e) Information is available to designated stakeholders.

### 6.4.1 Developing the documentation plan

The tasks to be performed in the Information Management process shall be identified in a Documentation Plan. When developing the Documentation Plan, consideration should be given to policies and procedures of the acquirer and supplier. The Information Management process for each project should be considered as part of a

repeatable process for the acquirer and supplier. A Documentation Plan may be created for an entire organization or for multiple projects and services that reuse document content.

### 6.4.2 Managing and controlling information items

Projects, organizations, and services may include their record descriptions and tailored information item descriptions in a data dictionary or work breakdown structure. This practice helps the document management, development, and maintenance activities. An established hierarchy of information items should be prescribed and a mechanism developed for resolving conflicts between items. For example, there should be one master schedule for the entire suite of plans relating to a single project, and schedule information given in specific plans should relate to this master schedule.

Commercial or other existing information items may be substituted for all or part of an information item if they contain the desired information, meet applicable quality characteristics, and are properly referenced. When existing information items are readily available to users, organizations should consider providing a reference to these information items rather than reproducing the information.



## 7 Generic types of information items

### 7.1 General

The use of generic types simplifies the application of consistent structure, content, and formats for similar information items (records and documents), to support usability. This document defines the life-cycle data of ISO/IEC 12207:2008 (IEEE Std 12207-2008), ISO/IEC/IEEE 15288:2015, and ISO/IEC 20000-1:2011 (IEEE Std 20000-1:2013) and ISO/IEC 20000-2:2012 (IEEE Std 20000-2:2013) by relating tasks and activities to the following generic types of information items:

a) description;

b) plan;

c) policy;

d) procedure;

e) report;

f) request; and

g) specification.

NOTE 1 Clause 9 identifies the generic content of data records.

NOTE 2 In ISO/IEC 20000, documents, except for records, state the intent to be achieved.

The generic information item contents shall be included in each applicable information item. Generic information item (document) contents are mapped to the identified output information items shown in column 3 of Tables 1, 2, and 3.

The lists of contents of generic types of information items do not specify a normative sequence, structure of parts, or a list of section titles.

### 7.2 Description – generic content

Purpose: Represent a planned or actual context of use, function, design, service, or item

NOTE A description of something that is required is a specification. The level of detail involved and the presentation for human use or for data storage determine whether information is presented as a description or as a preformatted record.

A description shall include the following elements:

a) Date of issue and status;

b) Scope;

c) Issuing organization;

d) References;

e) Context;

f) Notation for description;

g) Body;

h) Summary;

i) Glossary; and

j) Change history.

**Identified information items:**

— Concept of operations (operational concept);

— Database design description;

— Interface description;

— Proposal;

— Service catalog;

— Software architecture description;

— Software design description;

— Software unit description;

— System architecture description; and

— System element description.



### 7.3 Plan – generic content

Purpose: Define when, how, and by whom specific processes or activities are to be performed.

A plan shall include the following elements:

a) Date of issue and status;

b) Scope;

c) Issuing organization;

d) References (applicable policies, laws, standards, contracts, requirements, and other plans and procedures);

e) Approval authority;

f) Introduction, containing the purpose, audience, and scope of the plan;

g) Planned activities and tasks;

h) Identification of tools, methods, and techniques;

i) Schedules;

j) Budgets and cost estimates;

k) Resources and their allocation, including human resources, technical resources (infrastructure), and tools;

l) Responsibilities and authority, including the senior responsible owner and immediate process or service owner;

m) Interfaces among parties involved;

n) Risks and risk identification, assessment and mitigation activities;

o) Quality assurance and performance measures;

p) Environment, infrastructure, security, and safety;

q) Training;

r) Approach for technical and management review and reporting;

s) Other plans (plans or task descriptions that expand on the details of a plan);

t) Glossary;

u) Change procedures and history; and

v) Termination process.

**Identified information items:**

— Acceptance plan;

— Acquisition plan;

— Asset management plan;

— Audit plan;

— Capacity plan;

— Configuration management plan and policy;

— Development plan;

— Disposal plan;

— Documentation plan;

— Domain engineering plan;

— Improvement plan (process improvement plan, service improvement plan);

— Information management plan;

— Information security plan;

— Installation plan;

— Integration plan (implementation plan);

— Maintenance plan;

— Measurement plan;

— Project management plan;

— Quality management plan (quality assurance plan);

— Release plan (deployment plan);

— Reuse plan;

— Risk management policy and plan;

— Service continuity and availability plan;

— Service management plan;

— Service plan (plan for new or changed services);

— Training plan;

— Validation plan; and

— Verification plan.

## 7.4 Policy – generic content

Purpose: Establish an organization's high-level intention and approach to achieve objectives for, and ensuring effective control of, a service, process, or management system.

A policy shall include the following elements:

a) Date of issue, effective date, and status;

b) Scope;

c) Issuing organization;

d) Approval authority and identification of those accountable for enforcing the policy;

e) Authoritative references for compliance or conformance (such as policies, laws and regulations, standards, contracts, requirements, and vision or mission statements);

f) Body, including objectives;

g) Glossary; and

h) Change history.

Policies may be communicated in various media or included in plans, procedures, specifications, or other documents. Policies are implemented through Plans and Procedures. Policies may be defined for any life-cycle process or service process.

**Identified information items:**

- Budgeting and accounting policy (out of scope for this document);
- Configuration management plan and policy (change management policy);
- Improvement plan (and continual improvement policy);
- Information security policy;
- Life-cycle policy and procedure;
- Quality management policy and procedure;
- Release plan (and policy);
- Risk management policy and plan; and
- Service management plan (and policy).

## 7.5 Procedure – generic content

ISO/IEC/IEEE 15288:2015, reference: 5.5.1

ISO/IEC 20000-1:2011 (IEEE Std 20000- 1:2013) reference: 5.3

Purpose: Define in detail when and how to perform certain processes, activities or tasks, including tools needed. A procedure shall include the following elements:

a) Date of issue and status;

b) Scope;

c) Issuing organization;

d) Approval authority;

e) Relationship to plans and other procedures;

f) Authoritative references;

g) Inputs and outputs;

h) Ordered description of steps to be taken by each participant;

i) Error and problem resolution;

j) Glossary; and

k) Change history.

**Identified information items:**

- Audit procedure;

- Capacity management procedure;
- Communication procedure;
- Complaint procedure;
- Configuration management procedure (asset management procedure, change management procedure, release and deployment procedure);
- Documentation procedure;
- Implementation procedure;
- Improvement procedure;
- Incident management procedure;
- Information management procedure;
- Information security procedure;
- Life-cycle policy and procedure;
- Maintenance procedure;
- Measurement procedure;
- Operational test procedure
- Problem management procedure;
- Process assessment procedure;
- Qualification test procedure;
- Quality management policy and procedure;
- Software unit test procedure;
- Supplier management procedure;
- Supplier selection procedure;
- Training documentation;
- User documentation;
- Validation procedure; and
- Verification procedure.



### 7.6 Report – generic content

Purpose: Describe the results of activities such as investigations, assessments, and tests. A report communicates decisions.

A report shall include the following elements:

a) Date of issue and status;

b) Scope;

c) Issuing organization;

d) Contributors;

e) Summary;

f) Introduction, including the purpose, audience, and scope of the report;

g) Context (assumptions);

h) Body (including methods of obtaining results);

i) Conclusions and recommendations;

j) References;

k) Bibliography;

l) Glossary; and

m) Change history.

**Identified information items:**

- Acceptance report;
- Audit acknowledgement report;
- Audit report;
- Configuration status report;
- Evaluation report;
- Incident report;
- Installation report;
- Integration and test report;
- Monitoring and control report;
- Problem report;
- Process improvement report;
- Product need assessment;
- Progress report;

— Qualification test report;

— Review minutes;

— Service report;

— Software unit test report;

— User notification;

— Validation report; and

— Verification report.

## 7.7 Request – generic content

Purpose: Record information needed to solicit a response.

A request shall include the following elements:

a) Date of initiation;

b) Scope;

c) Subject;

d) Originator of request;

e) Identification of requested item, service, or response;

f) Detailed description of requested item, service, or response, including due date;

g) Justifications.

NOTE The identification of the requested item can be a Specification.

**Identified information items:**

— Change request;

— Customer satisfaction survey;

— Request for proposal (RFP);

— Resource request;

— Risk action request; and

— Service request (record).

## 7.8 Specification – generic content

Purpose: provide requirements for a required service, product, or process.

Specifications should use a well-defined syntax. Specifications should be internally consistent in terminology, definitions, and constraints. Unique specifications should be defined once to prevent inconsistent updates. A specification shall include the following elements:

a) Date of issue and status;

b) Scope;

c) Issuing organization;

d) References;

e) Approval authority;

f) Body;

g) Assurance requirements;

h) Conditions, constraints, and characteristics;

i) Glossary; and

j) Change history.

**Identified information items:**

— Contract;

— Service level agreement (SLA);

— Software requirements specification;

— System requirements specification (or service requirements); and

— Validation test specification.

## 8 Mapping of information items to the life cycle and service management processes

In Tables 1, 2, and 3, column 3, information items are identified and mapped to the process where they are identified as output in ISO/IEC/IEEE 15288:2015 or ISO/IEC 12207:2008 (IEEE Std 12207- 2008) or ISO/IEC 20000-1:2011 (IEEE Std 20000-1:2013) and ISO/IEC 20000-2:2012 (IEEE Std 20000-2:2013). These references may be normative requirements, recommended output, informative material, examples, or notes. This document identifies information items that are not explicitly specified by title in the base standards. In these cases, the base standards explicitly call out information to be documented, described, planned, specified, reported, recorded, requested or specified. Annex B, Table B.1, compares information items by source.

Table 1 maps ISO/IEC/IEEE 15288:2015 clauses (column 2), processes, and output information items.

Table 2 maps ISO/IEC 12207:2008 (IEEE Std 12207-2008) clauses (column 2), processes, and output information items.

Table 3 maps ISO/IEC 20000-1:2011 (IEEE Std 20000-1:2013) and ISO/IEC 20000-2:2012 (IEEE Std 20000-2:2013) clauses (column 2), processes, and output information items.

Tables 1, 2, and 3 also list recommended input information items (source documents and data) in column 1 to help produce the output information items. Tables 1, 2, and 3 do not show all the possible inputs, nor all the required outputs for a process. They show the recommended input information items for each output information item developed or revised during the process. Tables 1, 2, and 3 also show the specific reference citations from the base standards for each specified information item, not all references for a process.

In numerous clauses, the base standards indicate that something (for example, a strategy) is to be “defined.” However, definition does not in itself indicate that a specific information item is produced. Similarly, clauses indicating that 'communication is maintained' do not necessarily mean that an information item (a document) is produced.

For nearly every process, ISO/IEC/IEEE 15228:2008 and ISO/IEC 12207:2008 (IEEE Std 12207-2008) specify that organizational policies and procedures are a source for process activities and outputs. In Tables 1, 2, and 3,

"organizational policies and procedures" are not listed, but should be considered as input for every information item. In contractual work, the contract/agreement and requirements should also be considered as input for every information item, whether or not the source standard states that the process should be performed "as specified in the contract."

This document does not specify the format or content of recommended input data or input information items, except for the content of those items that are also output information items.

## 8.1 Mapping of information items to the system life cycle

As defined in ISO/IEC/IEEE 15288 and shown in Table 1 headings, in addition to the Tailoring process, there are two Agreement processes, six Organizational Project-Enabling processes, eight Technical Management processes, and fourteen Technical processes:

**Agreement processes**

1. Acquisition
2. Supply

**Organizational Project-Enabling processes**

1. Life Cycle Model Management
2. Infrastructure Management
3. Portfolio Management
4. Human Resource Management
5. Quality Management
6. Knowledge Management

**Technical Management processes**

1. Project Planning
2. Project Assessment and Control
3. Decision Management
4. Risk Management
5. Configuration Management
6. Information Management
7. Measurement
8. Quality Assurance

**Technical processes**

1. Business or Mission Analysis
2. Stakeholder Needs and Requirements Definition
3. System Requirements Definition

4. Architecture Definition
5. Design Definition
6. System Analysis
7. Implementation
8. Integration
9. Verification
10. Transition
11. Validation
12. Operation
13. Maintenance
14. Disposal

**Table 1 — Mapping of ISO/IEC/IEEE 15288:2015, clauses to information items for each system life-cycle process**

| Typical Input information items | ISO/IEC/IEEE 15288:2015 reference | Output information item |
|---|---|---|
| **ACQUISITION** | | |
| Proposal, other contracts, needs assessment, requirements specification | 6.1.1.2.c), 6.1.1.3.c), B.1 | Contract (agreement) |
| Concept of operations, system requirements specification, software requirements specification, acceptance strategy, other requests for proposal | 6.1.1.2.a), 6.1.1.3.a.2), B.1 | Request for proposal (RFP) (Request for supply) |
| Request for proposal, Proposal, Contract | 6.1.1.3.b), 6.1.1.3.d), B.1 | Evaluation Report (Supplier selection report, Supply assessment report). |
| Problem report, monitoring and control report, complaint | 6.1.1.3.c)2) | Change Request |
| Release report | 6.1.1.3.e)1), B.1 | Acceptance Report (Acceptance Record) |
| **SUPPLY** | | |
| Request for proposal, other proposals | 6.1.2.2.b), 6.1.2.3.b), B.1 | Proposal |
| Proposal, other contracts and agreements | 6.1.2.2.c), 6.1.2.3.c), B.1 | Contract (agreement) |
| Problem report, monitoring and control report, complaint | 6.1.2.1, 6.1.2.3.c)2), B.1 | Change Request |
| **LIFE CYCLE MODEL MANAGEMENT** | | |
| Organizational procedure | 6.2.1.1, 6.2.1.2a), 6.2.1.3a), B.1 | Life-cycle policy and procedures |
| Assessment report, organizational procedure | 6.2.1.3.c) | Improvement plan |
| Organizational procedure, process assessment procedure, process assessment results, audit report, customer satisfaction report, assessment report, progress report, problem report | 6.2.1.3.c), B.1 | Process improvement report |
| **INFRASTRUCTURE MANAGEMENT** | | |
| Organizational procedure, other system requirements specification, project management plan | 6.2.2.2.a), 6.2.2.3.a), 6.2.2.3.b), B.1 | System requirements specification |
| System architecture description | 6.2.2.2.b) | System element description |
| System architecture description, problem report, monitoring and control report | B.1 | Change Request |

| Typical Input information items | ISO/IEC/IEEE 15288:2015 reference | Output information item |
|---|---|---|
| **PORTFOLIO MANAGEMENT** | | |
| Organizational procedure, project plan, business action plan | 6.2.3.3.a)8 | Project management plan |
| Agreement, project life-cycle policies and procedures | 6.2.3.3.a)7). B.1 | Progress report (Progress Initiation Report, Project Closure Report) |
| Agreement, Business strategy, risk management plan | 6.2.3.3.a)7), B.1 | Evaluation report (Portfolio analysis report) |
| **HUMAN RESOURCE MANAGEMENT** | | |
| Employee Skill record, project management plan | 6.2.4.3.b) | Training plan |
| Knowledge management policy, training plan, user documentation, validation procedure | 6.2.4.3.b) | Training documentation |
| Project management plan, staffing plan, training plan | 6.2.4.3.a)1), B.1 | Evaluation report (required skills) |
| **QUALITY MANAGEMENT** | | |
| Project management plan | 6.2.5.3.a), 6.2.5.3.c) | Quality management plan |
| Organizational procedure, quality management plan, customer satisfaction report, problem report | 6.2.5.2.a), 6.2.5.3.a), B.1 | Quality management policy and procedure |
| Survey, interview, requirements specification, quality assurance evaluation results, customer satisfaction assessment results | 6.2.5.3.c.3),, B.1 | Monitoring and control report (Corrective and preventive action report) |
| **KNOWLEDGE MANAGEMENT** | | |
| Project management plan, configuration management plan, | 6.2.6.3.a) | Information management plan (Knowledge management plan) |
| Knowledge assets, reference architectures, process models, lessons learned, domains and types of knowledge, skills, and knowledge assets to be collected and maintained | 6.2.6.3.c)2), B.1 | Training documentation |
| **PROJECT PLANNING** | | |
| Contract, organizational procedure, other plans, project objectives and constraints | 6.3.1.1, 6.3.1.2, 6.3.1.3, B.1 | Project (technical) management plan (systems engineering management plan, software development plan) |
| Product need assessment, contract | 6.3.1.3.b)6) | Acceptance plan |
| Product need assessment | 6.3.1.3.b)6) | Acquisition plan |
| Project management plan, work breakdown structure, budget | 6.3.1.3.c)2) | Resource request |
| **PROJECT ASSESSMENT AND CONTROL** | | |
| Contract, organizational procedure, other plans | 6.3.2.3.a) | Project management plan |
| Contract, organizational procedure, project plan, quality assurance plan, other progress report | 6.3.2.2.f), 6.3.2.3.b)6) | Progress report |
| Problem report, analysis of metrics and variations | 6.3.2.3.b)10), B.1 | Monitoring and control report (project assessment report) |
| Monitoring and control report, decision record | 6.3.2.3.c)1) | Review minutes |
| Contract, complaint, measurement results | 6.3.2.3.c)3), B.1 | Change request (project control request) |
| **DECISION MANAGEMENT** | | |
| Organizational procedure, contract | 6.3.3.3.a)2), 6.3.3.3.c)3) | Problem report |
| Organizational procedure, contract | 6.3.3.3.c), B.1 | Report (*see generic Report information item*) |
| **RISK MANAGEMENT** | | |
| Project management plan | 6.3.4.3.a) | Risk management plan |
| Risk management plan, risk profile | 6.3.4.3.b)2), B.1 | Risk action request |
| Risk management plan, risk profile, quality assurance procedure, problem report | 6.3.4.3.b), B.1 | Monitoring and control report (risk profile report) |
| **CONFIGURATION MANAGEMENT** | | |
| Project management plan, information management plan | 6.3.5.3.a) | Configuration management plan |

| Typical Input information items | ISO/IEC/IEEE 15288:2015 reference | Output information item |
|---|---|---|
| Configuration management plan, quality management plan | 6.3.5.3.c) | Configuration management procedure |
| Needs analysis | 6.3.5.3.c), B.1 | Change request (Request for change, request for variance) |
| Change records, inventories, configuration management plan, CM procedures | 6.3.2.3.d), B.1 | Configuration status report (system release report) |
| Change records, inventories, configuration management plan, CM procedures | 6.3.5.3.e), B.1 | (Configuration) evaluation report |
| **INFORMATION MANAGEMENT** | | |
| Organizational procedure, project management plan, configuration management plan | 6.3.6.1, 6.3.6.3.a) | Information management plan |
| Information item records, release records, information management plan | 6.3.6.3.b), B.1 | Configuration status report (Information management report) |
| **MEASUREMENT** | | |
| Measurement data, information management plan | 6.3.7.1, 6.3.7.3.b) | Monitoring and control report |
| Project management plan, quality assurance plan, measurement strategy, requirements specification | 6.3.7.3.a)5) | Measurement procedures |
| Measurement results, quality assurance plan, measurement procedures | 6.3.7.2.a), 6.3.7.3.a)3), B.1 | Evaluation report (Measurement information needs) |
| Measurement results | 6.3.7.3.b)4) | Review minutes |
| Measurement results, quality assurance plan, measurement procedures | 6.3.7.1, 6.3.7.2.e), 6.3.7.3.b)3) | Report (*see generic Report information item*) |
| **QUALITY ASSURANCE** | | |
| Quality management plan, measurement procedures, system quality requirements, quality assurance records, incident record, problem record, customer satisfaction report, complaint | 6.3.8.2.d), 6.3.8.3.d), B.1 | (QA) Evaluation report |
| Quality management procedures, quality management plan, test procedures | 6.3.8.2.a) | Quality management (assurance) procedures |
| **BUSINESS OR MISSION ANALYSIS** | | |
| Needs assessment, portfolio evaluation report, use case | 6.4.1.1, 6.4.1.2, 6.4.1.3.c), B.1 | Concept of Operations (Preliminary life cycle concepts or preliminary operational concepts) |
| **STAKEHOLDER NEEDS AND REQUIREMENTS DEFINITION** | | |
| Contract, needs assessment, life cycle concepts, scenarios, use cases | 6.4.2.2.b), 6.4.2.3.b), 6.4.2.3.c), B.1 | Concept of operations (operational concept) |
| Contract, needs assessment, concept of operations | 6.4.2.1, 6.4.2.2.e), 6.4.2.3.c), 6.4.2.3.d), 6.4.2.3.e), B.1 | System (stakeholder) requirements specification |
| Business strategy, customer satisfaction survey | 6.4.2.1, 6.4.2.2.d), 6.4.2.3.b) | Product need assessment |
| **SYSTEM REQUIREMENTS DEFINITION** | | |
| Organizational procedure, stakeholder requirements | 6.4.3.1, 6.4.3.2, 6.4.3.3.b), 6.4.3.3.c), B.1 | System requirements specification |
| Concept of operation, system requirements specification | 6.4.3.2.a), B.1 | System architecture description |
| **ARCHITECTURE DEFINITION** | | |
| Development plan, system requirements specification, concept of operations (operational concept), technology roadmaps | 6.4.4.1, 6.4.4.2, 6.4.4.3.b), 6.4.4.3.c), B.1 | System architecture description (architecture report) |
| System architecture description, system design description | 6.4.4.3.c), 6.4.4.3.d) | Interface description |
| System architecture description, stakeholder and system requirements specifications | 6.4.3.3.e), B.1 | Evaluation report (architecture assessment report) |
| **DESIGN DEFINITION** | | |
| System architecture description | 6.4.5.2.d), 6.4.5.3.d), B.1 | Interface description |
| System architecture description, technology assessment report, product specifications | 6.4.5.1, 6.4.5.2.b), 6.4.5.3, B.1 | System element description (design characteristics report) |
| **SYSTEM ANALYSIS** | | |

| Typical Input information items | ISO/IEC/IEEE 15288:2015 reference | Output information item |
|---|---|---|
| System requirements specification, change request, problem report, test report | 6.4.6.1, 6.4.6.3.c), B.1 | Evaluation report (system analysis report) |
| **IMPLEMENTATION** | | |
| System design descriptions, interface descriptions | 6.4.7.3.a) | Implementation procedure |
| Stakeholder requirements, use case, concept of operations, design descriptions | 6.4.7.3.b) | User documentation |
| Implementation procedure | 6.4.7.3.b), B.1 | Integration and test report (implementation report) |
| **INTEGRATION** | | |
| Integration procedure, test procedure | 6.4.8.2.g), B.1 | Integration and test report |
| Integration procedures, design description | 6.4.8.3.b) | User documentation (assembly procedure) |
| Configuration record | 6.4.8.3.c) | Problem report |
| **VERIFICATION** | | |
| Requirements specification, verification strategy, design definition, interface control description, test procedures, progress report, problem report, test case | 6.4.9.3.b) | Verification procedure |
| Verification procedures, progress report, problem report, test case | 6.4.9.3.c), B.1 | Integration and test report (verification report) |
| Test procedures, test report | 6.4.9.2.d) | Problem report |
| **TRANSITION** | | |
| Installation procedure, transition strategy, operational procedures | 6.4.10.3.a) | Release plan (contingency back-out plan) |
| Installation plan, problem report, progress report | 6.4.10.3.c), B.1 | Installation report (Transition report) |
| Problem management procedure | 6.4.10.1, 6.4.10.3.c) | Problem report |
| **VALIDATION** | | |
| Stakeholder requirements, validation strategy, test procedures, test case, problem report | 6.4.11.3.b) | Validation procedure |
| Quality management plan, validation procedures | 6.4.11.2.f), B.1 | Validation report |
| Test procedure, test report | 6.4.11.3.c) | Problem report |
| **OPERATION** | | |
| Problem report, evaluation report | 6.4.12.3.d) | User documentation |
| Information security plan, operational strategy, threat analysis | 6.4.12.3.a) | Information security procedure |
| Operational procedures, safety strategy, service level agreement, measurement data | 6.4.12.3.b), B.1 | Monitoring and control report (operation report) |
| Incident and problem reports, complaints, operational procedures | 6.4.12.3.d) | Customer satisfaction survey |
| User documentation, incident report, service level agreement | 6.4.12.3.c), B.1 | (Operational) problem report |
| **MAINTENANCE** | | |
| Organizational procedure, operations plan, development plan | 6.4.13.3.d) | Maintenance plan (life cycle support plan) |
| Maintenance plan, user documentation | 6.4.13.3.b), 6.4.13.3.c) | Maintenance procedure |
| Problem report, incident report, product need assessment, complaint | 6.4.13.3.b), B.1 | Change request (maintenance request) |
| Problem report, maintenance plan, system analysis report | 6.4.13.3.d), B.1 | Service report (logistics report) |
| Maintenance procedures, change requests, incident reports, service requests | 6.4.13.3.b), B.1 | (Maintenance) problem report |
| **DISPOSAL** | | |
| Disposal records, knowledge management records, asset management records | 6.4.14.3.c), B.1 | Configuration status report (archive report) |
| **TAILORING** | | |
| Standard life-cycle model, standard, organizational policies and procedures, tailoring decision, agreement, stakeholder requirement | A.2.3 | Life-cycle procedure |

## 8.2 Mapping of information items to the software life cycle

Table 2 maps information items to the software life cycle as defined in ISO/IEC 12207:2008 (IEEE Std 12207-2008). ISO/IEC/IEEE 12207 has processes the same as the system life cycle: two Agreement processes, five Organizational Project-Enabling processes, and seven Project processes. There are also distinctive processes for the software life cycle: eleven Technical processes, seven Software Implementation processes, eight Software Support processes, and three Software Reuse processes.

**Agreement processes**

1. Acquisition
2. Supply

**Organizational Project-Enabling processes**

1. Life Cycle Model Management
2. Infrastructure Management
3. Project Portfolio Management
4. Human Resource Management
5. Quality Management

**Project processes**

1. Project Planning
2. Project Assessment and Control
3. Decision Management
4. Risk Management
5. Configuration Management
6. Information Management
7. Measurement

**Technical processes**

1. Stakeholder Requirements Definition
2. System Requirements Analysis
3. System Architectural Design
4. Implementation
5. System Integration
6. System Qualification Testing
7. Software Installation
8. Software Acceptance Support

9. Software Operation
10. Software Maintenance
11. Software Disposal

**Software Implementation processes**

1. Software Implementation
2. Software Requirements Analysis
3. Software Architectural Design
4. Software Detailed Design
5. Software Construction
6. Software Integration
7. Software Qualification Testing

**Software Support processes**

1. Software Documentation Management
2. Software Configuration Management
3. Software Quality Assurance
4. Software Verification
5. Software Validation
6. Software Review
7. Software Audit
8. Software Problem Resolution

**Software Reuse processes**

1. Domain Engineering
2. Reuse Asset Management
3. Reuse Program Management



**Table 2 — Mapping of ISO/IEC 12207:2008 (IEEE Std 12207-2008) clauses to information items for each software life-cycle process**

| Typical Input information items | ISO/IEC 12207: 2008 (IEEE Std 12207 -2008) | Output information item |
|---|---|---|
| **ACQUISITION** | | |
| Acquisition report, contract product need assessment, acquisitio report, other acquisition plans | 6.1.1.3.1.8, 6.1.1.3.1.9, 6.1.1.3.1.12 | Acquisition plan |

| Typical Input information items | ISO/IEC 12207: 2008 (IEEE Std 12207 -2008) | Output information item |
|---|---|---|
| Proposal, other contracts | 6.1.1.2, 6.1.1.3.4.2, B.3.1.2.2, B.3.1.3.2, F.3.3.1.1, F.3.3.1.2, F.3.3.5.1 | Contract |
| Other product need assessments | 6.1.1.2, 6.1.1.3.1.1 | Product need assessment |
| other system descriptions, concept of operations | 6.1.1.3.1.1 | Concept of operations |
| Request for proposal, product needs assessment, acquisition report, previous requests for proposals (RFPs); concept; system requirement; software requirements definition and analysis result; past: scope statement, bidder instructions, terms and conditions; acceptance strategy and condition, acquisition recommendation. | 6.1.1.3.1.10 | Request for proposal (RFP) |
| System requirements specification, product need assessment | 6.1.1.3.1.2, 6.1.1.3.1.7, 6.1.1.3.1.8, 6.1.1.3.1.11 | Software requirements specification |
| Acquisition plan, system requirements specification | 6.1.1.3.1.7 | Maintenance plan |
| Acquisition plan, acceptance plan, requirements specification, contract | 6.1.1.3.6.1, 6.1.1.3.6.2 | Qualification test procedure |
| Other supplier selection procedures, acquisition plan, other requests for proposals | 6.1.1.3.3.1 | Supplier selection procedure |
| Contract, problem report, monitoring and control report | F.3.2, F.3.3.2.1 | Change request |
| **SUPPLY** | | |
| Requirements specification, request for proposal | 6.1.2, 6.1.2.3.3.1, 6.1.2.3.6.2, B.3.2.2.1, B.3.2.2.2 | Contract |
| Contract, supplier's project management plan, quality assurance plan | 6.1.2.3.4.8, 6.1.2.3.4.15 | Evaluation report |
| Project management plan | 6.1.2.3.4.15 | Review minutes |
| Monitoring result | 6.1.2.3.4.8, 6.1.2.3.4.15 | Monitoring and control report |
| Proposal review record, proposal, contract, other project management plans, information security policy | 6.1.2.3.4.3, 6.1.2.3.4.5 | Project Management Plan |
| Customer inquiry or request, request for proposal, other proposals | 6.1.2.2b), B.3.2.1.2 | Proposal |
| Problem management procedure | 6.1.2.3.4.15, B.3.2.3.2 | Problem report |
| Project management plan | 6.1.2.3.4.15 | Progress report |
| Audit plan, contract | 6.1.2.3.4.15 | Audit report |
| **LIFE CYCLE MODEL MANAGEMENT** | | |
| Organizational procedures | 6.2.1.1, 6.2.1.2, 6.2.1.3.1.1, 6.2.1.3.3.1 | Life-cycle policy and procedure |
| Assessment report, organizational procedure | 6.2.1.3 | Improvement plan |
| Life-cycle procedure, process description, review minutes, process improvement analysis report, audit report, improvement plan, project management plan | 6.2.1.3.2.2 | Audit plan |
| Life-cycle policies, process description | 6.2.1.3.2.1 | Process assessment procedure |
| Assessment report, progress report, problem report, audit report, customer satisfaction report | 6.2.1.3.3.2, B.3.3.1.2, B.3.3.2.2, B.3.3.3.2 | Process improvement analysis report |
| **INFRASTRUCTURE MANAGEMENT** | | |
| Organizational procedure, strategic plan, system requirements specification | 6.2.2.2, 6.2.2.3.1.1, 6.2.2.3.2.1 | System requirements specification |
| Work breakdown structure, infrastructure system requirements specification. | 6.2.2.3.1.2 | Project management plan |
| **PROJECT PORTFOLIO MANAGEMENT** | | |
| Organizational procedures, project plan, business action plan, life-cycle procedure | 6.2.3.3.2.1, 6.2.3.3.1.6 | Project management plan |
| **HUMAN RESOURCE MANAGEMENT** | | |

| Typical Input information items | ISO/IEC 12207: 2008 (IEEE Std 12207 -2008) | Output information item |
|---|---|---|
| Employee Skill records, project management plans | 6.2.4.3.2.1, 6.2.4.3.4.1 | Training plan |
| Knowledge area schema, evaluation reports | 6.2.4.3.4.1 | Information management plan |
| Training plan, user documentation, validation procedures | 6.2.4.3, B.3.4.1.2 | Training documentation |
| **QUALITY MANAGEMENT** | | |
| Project management plan | 6.2.5.3.1.5 | Quality management plan |
| Organizational procedures, quality management plan, customer satisfaction report, problem report | 6.2.5.2, 6.2.5.3.1.1 | Quality management policy and procedure |
| Surveys, interviews, requirements specification | 6.2.5.3.1.4 | Service report |
| **PROJECT PLANNING** | | |
| Proposal, contract, other plans, budget requests, organizational procedures, contract modification, other plans | 6.3.1.1, 6.3.1.2.e), 6.3.1.3.2.1 | Project management plan |
| Project management plan, contract | 6.3.1.3.3.2 | Resource request |
| **PROJECT ASSESSMENT AND CONTROL** | | |
| Contract, organizational procedures, project plan, quality assurance plan | 6.3.2.3.2.1 | Problem report |
| Contract, organizational procedures, project plan, quality assurance plan, other progress report | 6.3.2.2, 6.3.2.3.1.1, 6.3.2.3.2.2 | Progress report |
| Problem reports, analysis of metrics and variations | 6.3.2.3.2, 6.3.2.3.3 | Monitoring and control report |
| **DECISION MANAGEMENT** | | |
| Organizational procedures, contract | 6.3.3.3.1.3, 6.3.3.3.3.1 | Problem report |
| Organizational procedures, contract | 6.3.3.2d) | Report |
| **RISK MANAGEMENT** | | |
| Risk management policies, organizational procedures | 6.3.4.3.1.1, 6.3.4.3.1.2, 6.3.4.3.2.1 | Risk management plan |
| Risk management plan | 6.3.4.3.1.5 | Improvement plan |
| Quality assurance procedures, problem reports | 6.3.4.3.3.4, 6.3.4.3.6.3 | Monitoring and control report |
| Change request, monitoring and control report, risk register, risk profile | 6.3.4.3.4.1 | Risk action request |
| **CONFIGURATION MANAGEMENT** | | |
| Project management plan, system requirements specification, | 6.3.5.3.1.1 | Configuration management plan and policy |
| **INFORMATION MANAGEMENT** | | |
| Organizational procedures, project management plan | 6.3.6.3.1, 6.3.6.3.2.5 | Information management plan |
| Information management plan | 6.3.6.3.1 | Documentation plan |
| **MEASUREMENT** | | |
| Organizational policies, project management plan, contract, information management plan | 6.3.7.2.c), 6.3.7.3.1.1, 6.3.7.3.1.3, 6.3.7.3.1.4 | Measurement plan |
| Measurement plan, measurement procedures | 6.3.7.1, 6.3.7.3.2.4 | Monitoring and control report |
| **STAKEHOLDER REQUIREMENTS DEFINITION** | | |
| Contract, needs assessment, concept of operations | 6.4.1.3.2 | System requirements specification |
| Contract, needs assessment | 6.4.1.2, 6.4.1.3.2.3 | Concept of operations |
| **SYSTEM REQUIREMENTS ANALYSIS** | | |
| Organizational procedures, contracts, quality requirements | 6.4.2.2, 6.4.2.3.1.1 | System requirements specification |
| System requirements specification, needs assessment | 6.4.2.3.2.1 | Evaluation report |
| **SYSTEM ARCHITECTURAL DESIGN** | | |
| Development plan, system requirements specification | 6.4.3.2, 6.4.3.3.1.1 | Software architecture description |
| System architecture description, system design description | 6.4.3.2d) | Interface description |
| System requirements specification, system architecture description, concept of operations | 6.4.3.3.2.1 | Evaluation report |
| **IMPLEMENTATION** | | |

| Typical Input information items | ISO/IEC 12207: 2008 (IEEE Std 12207 -2008) | Output information item |
|---|---|---|
| [*Replaced by the Software Implementation process*] | | |
| **SYSTEM INTEGRATION** | | |
| System requirements specification, system architecture description, software user documentation, software integration test plan | 6.4.5.3.1.1 | Integration and test report |
| System requirements specification, Integration and test report | 6.4.5.3.2.2 | Evaluation report |
| **SYSTEM QUALIFICATION TESTING** | | |
| System requirements specification, validation plan | 6.4.5.3.2.1 | Qualification test procedure |
| Requirements, design definition, interface control description, verification plan, test procedures, test case | 6.4.6.3.1.2 | Evaluation report |
| System requirements specification, contract | 6.4.6.3.1.3 | Audit report |
| **SOFTWARE INSTALLATION** | | |
| Contract, development plan, system requirements specification, system architecture description, other installation plans | 6.4.7.3.1.1 | Installation plan |
| Contract, installation plan | 6.4.7.3.1.2 | Installation report |
| **SOFTWARE ACCEPTANCE SUPPORT** | | |
| Contract, acceptance plan, acceptance procedure | 6.4.8.3.1.1 | Acceptance review and testing report |
| Test procedures | 6.4.8.2, 6.4.8.3.1.1 | Problem report |
| **SOFTWARE OPERATION** | | |
| System requirements specification | 6.4.9.3.1.1 | Service management plan |
| Software requirements specification, detailed system design description, concept of operation | 6.4.9.3.3.1, 6.4.9.3.4.1 | User documentation |
| Software user documentation, problem reports; change requests, other operational test procedures | 6.4.9.3.1.3 | Operational test procedure |
| Problem reports, other operational procedures | 6.4.9.3.1.2, 6.4.9.3.1.3 | Problem management procedure |
| Problem reports, problem management procedure | 6.4.9.3.4.2, 6.4.9.3.5.2 | Problem report |
| Operations plan, user documentation, problem report, customer satisfaction survey | 6.4.9.3.4.2 | Change request |
| **SOFTWARE MAINTENANCE** | | |
| Organizational procedures, operations plan, development plan, contract, software user documentation, | 6.4.10.1, 6.4.10.3.1.1 | Maintenance plan |
| Maintenance plan, user documentation, installation procedures, test procedures | 6.4.10.3.1.1 | Maintenance procedure |
| Software requirements specification, modification report, low-level software design document. | 6.4.10.2, 6.4.10.3.3.1 | Software design description |
| Release record, change request, detailed design document | 6.4.10.2 | User documentation |
| Problem report, low-level software design description, verification plan | 6.4.10.3.3.2 | Software unit test procedure |
| Maintenance procedures | 6.4.10.3.1.2, 6.4.10.3.2.4 | Problem report |
| Software unit test plan, problem report, change request | 6.4.10.3.3.2 | Software unit test report |
| Maintenance plan, modification test and evaluation criteria specification, modification requirement report, modification notification report, modification test report, migration plan | 6.4.10.3.5.6 | Review minutes |
| Contract, maintenance plan, installation plan, verification plan, configuration management plan | 6.4.10.3.5.2 | Release plan |
| Release plan | 6.4.10.3.5.3, 6.4.10.3.5.5 | User notification |
| **SOFTWARE DISPOSAL** | | |
| Retirement constraints, contract | 6.4.11.2 | Software requirements specification |
| Disposal plan | 6.4.11.3.2.2 | User notification |
| Organizational procedures, contract, project management plan | 6.4.11.3.1.1 | Disposal plan |
| **SOFTWARE IMPLEMENTATION** | | |
| Life-cycle model, software requirements specification, software architecture description | 7.1.1.3.1.2 | Software design description |

| Typical Input information items | ISO/IEC 12207: 2008 (IEEE Std 12207 -2008) | Output information item |
|---|---|---|
| Software design description, software requirements specification | 7.1.1.3.1.2 | User documentation |
| Incidents, problem records | 7.1.1.3.1.2 | Problem report |
| Contract, supplier's project management plan, software requirements specification, quality assurance plan | 7.1.1.3.1.3, 7.1.1.3.1.4 | Development plan |
| **SOFTWARE REQUIREMENTS ANALYSIS** | | |
| Contract, system requirements specification, development plan, system architecture description, stakeholder requirements, product needs assessment, risk assessment, evaluations of prototypes | 7.1.2.2, 7.1.2.3.1.1 | Software requirements specification |
| Software requirements specification, concept of operations | 7.1.2.3.1.2 | Evaluation report |
| **SOFTWARE ARCHITECTURAL DESIGN** | | |
| Contract, development plan, system requirements specification, software requirements specification | 7.1.3.3.1.1 | Software architecture description |
| System architecture description, concept of operations, system requirements specification, software requirements specification | 7.1.3.3.1.2 | Interface description |
| Software requirements specification, high- level software design description | 7.1.3.3.1.3 | Database design description |
| System architecture description, concept of operations, interface description | 7.1.3.3.1.4 | User documentation |
| Development plan, system design description | 7.1.3.3.1.5 | Software requirements specification |
| Test requirements, project management plan (master schedule) | 7.1.3.3.1.5 | Development plan |
| System architecture description, software requirements specification, concept of operations, interface description, database design description | 7.1.3.3.1.6 | Evaluation report |
| **SOFTWARE DETAILED DESIGN** | | |
| Development plan, software requirements specification, system architecture description, | 7.1.4.3.1.1 | Software design description |
| Software detailed design, system architecture description, software requirements specification | 7.1.4.3.1.2 | Interface description |
| Software requirements specification, system architecture description | 7.1.4.3.1.3 | Database design description |
| Documentation plan, software requirements specification, high-level software design description, other software user documentation, database description | 7.1.4.3.1.4 | User documentation |
| Development plan, acceptance plan, software requirements specification, low-level software design description, database detailed design description | 7.1.4.3.1.5 | Software unit test procedure |
| System architecture description, Software detailed design, software requirements specification, software unit test plan | 7.1.4.3.1.7 | Evaluation report |
| **SOFTWARE CONSTRUCTION** | | |
| Software items, databases, software unit test plan | 7.1.5.3.1.1 | Software unit test procedure |
| Software design description | 7.1.5.3.1.1 | Software unit description |
| Software unit description, software unit test procedures | 7.1.5.3.1.2 | Software unit test report |
| Documentation plan, software requirements specification, software design description, other software user documentation, database description, software unit test procedures, software unit test report | 7.1.5.3.1.3 | User documentation |
| Software unit test plan, software unit test report, software requirements specification, concept of operations, integration and test report | 7.1.5.3.1.5 | Evaluation report |
| **SOFTWARE INTEGRATION** | | |
| Software requirements specification, software design description, software architecture description, interface specifications | 7.1.6.3.1.1, 7.1.6.3.1.5 | Integration plan |
| Integration plan, test plan, test procedures, test result records | 7.1.6.3.1.2 | Integration and test report |
| Documentation plan, integration and test report, software design description | 7.1.6.3.1.3 | User documentation |

| Typical Input information items | ISO/IEC 12207: 2008 (IEEE Std 12207 -2008) | Output information item |
|---|---|---|
| Acceptance plan, software user documentation, development plan, system requirements specification, integration plan, software design description, database design description, software requirements specification, system architecture description | 7.1.6.3.1.4 | Qualification test procedure |
| Integration plan, software requirements specification, concept of operations, integration and test report | 7.1.6.3.1.5 | Evaluation report |
| **SOFTWARE QUALIFICATION TESTING** | | |
| Software requirements specification, integration and test report, qualification test procedures | 7.1.7.3.1.1, 7.1.7.3.1.3 | Qualification test report |
| Documentation plan, integration and test report, software design description | 7.1.7.3.1.2 | User documentation |
| Concept of operations, user documentation, qualification test procedures, qualification test report | 7.1.7.3.1.3 | Evaluation report |
| Acceptance plan, software user documentation, development plan, software requirements specification, software design description, database design description, test report | 7.1.7.3.1.4 | Audit report |
| **SOFTWARE DOCUMENTATION MANAGEMENT** | | |
| Program management plan, development plan, audit reports, evaluation reports, contract, other documentation plans | 7.2.1.2, 7.2.1.3.1.1 | Documentation plan |
| **SOFTWARE CONFIGURATION MANAGEMENT** | | |
| Contract, other configuration management plans | 7.2.2.3.1.1 | Configuration management plan |
| Configuration records, other configuration status reports | 7.2.2.2.e, 7.2.2.3.4.1, 7.2.2.3.5.1 | Configuration status report |
| **SOFTWARE QUALITY ASSURANCE** | | |
| Contract, project management plan, system requirements specification | 7.2.3.3.1.3 | Quality management plan (quality assurance plan) |
| **SOFTWARE VERIFICATION** | | |
| Contract, software requirements specification | 7.2.4.3.1.5, 7.2.4.3.1.6 | Verification plan |
| Verification plan, test specifications, test records | 7.2.4.3.1.5 | Verification report |
| **SOFTWARE VALIDATION** | | |
| Contract, other validation plans, software requirements specification | 7.2.5.3.1.4 | Validation plan |
| Contract, qualification test report, system requirements specifications, software requirements specification | 7.2.5.3.2.1, 7.2.5.3.2.2 | Validation test specification |
| Validation test specification | 7.2.5.3.1.4.d) | Validation report |
| **SOFTWARE REVIEW** | | |
| Contract, review agenda, problem reports, plans, schedules, standards | 7.2.6.2, 7.2.6.3.1.5 | Review minutes |
| **SOFTWARE AUDIT** | | |
| Organizational policies and procedures, | 7.2.7.3.1.4 | Audit procedure |
| Audit report | 7.2.7.3.1.6 | Audit acknowledgement report |
| Contract, software requirements specification, test plans, validation test specification, test reports, user documentation, plans, monitoring results, standards | 7.2.7.3.1.6 | Audit report |
| **SOFTWARE PROBLEM RESOLUTION** | | |
| Problem management procedure, review minutes, incident reports | 7.2.8.2, 7.2.8.3.1.1, 7.2.8.3.2.1 | Problem report |
| **DOMAIN ENGINEERING** | | |
| Configuration status report, evaluation report, domain architecture description | 7.3.1.3.1.3 | Change request |
| Project management plan, organizational procedures, business strategy, development plan | 7.3.1.3.1.1 | Domain engineering plan |
| Domain engineering plan, test report, change request | 7.3.1.3.1.3 | Problem report |
| Domain model, interface description | 7.3.1.2, 7.3.1.3.3.1, 7.3.1.3.3.3 | Software architecture description |
| **REUSE ASSET MANAGEMENT** | | |

| Typical Input information items | ISO/IEC 12207: 2008 (IEEE Std 12207 -2008) | Output information item |
|---|---|---|
| Strategic plan, project management plan, maintenance plan, domain engineering plan | 7.3.2.2, 7.3.2.3.1.1, 7.3.2.3.2.2, | Asset management plan |
| Configuration status report | 7.3.2.3.3.6 | Change request |
| Change request, problem report | 7.3.2.3.3.6 | Maintenance plan |
| Problem report | 7.3.2.3.3.8 | User notification |
| Asset reuse data | 7.3.2.3.3.5, 7.3.2.3.3.7 | Monitoring and control report |
| Test report, audit report | 7.3.2.3.3.6 | Problem report |
| **REUSE PROGRAM MANAGEMENT** | | |
| Project management plan, organizational procedures, business strategy, development plan, domain engineering plan | 7.3.3.1, 7.3.3.3.2.1, 7.3.3.3.3.3, 7.3.3.3.4.1, 7.3.3.3.4.2, 7.3.3.3.4.3 | Reuse plan |
| Reuse plan, configuration management procedure | 7.3.3.3.5.3 | Problem report |
| **TAILORING** | | |
| Standards, organizational policies and procedures | A.2.3.1 | Life-cycle procedure |

## 8.3 Mapping of information items to the service management processes

Table 3 maps information items to the 14 service management processes as defined in ISO/IEC 20000-1:2011 (IEEE Std 20000-1:2013) and ISO/IEC 20000-2:2012 (IEEE Std 20000-2:2013). The 14 processes include the design and transition of new or changed services, six Service Delivery processes, two Relationship processes, two Resolution processes, and three Control processes. In addition, Clause 4 of ISO/IEC 20000-1:2011 (IEEE Std 20000-1:2013) requires some information items for the service management system in general, applicable to all processes. In Table 3, policies, plans and procedures are shown for specific services when additional detail is available in the referenced ISO/IEC 20000-1 (IEEE Std 20000-1:2013) or ISO/IEC 20000-2 (IEEE Std 20000-1:2013) Clauses 5 to 9.

ISO/IEC 20000-2:2012, *Information technology — Service management — Part 2: Guidance on the application of service management systems* takes the form of guidance and recommendations. It should not be quoted as if it were a specification and particular care should be taken to ensure that claims of conformance are not misleading.

**Design and transition of new or changed services process**

**Service Delivery processes**

1. Service Level Management
2. Service Reporting
3. Service Continuity and Availability Management
4. Budgeting and Accounting for Services
5. Capacity Management
6. Information Security Management

**Relationship processes**

1. Business Relationship Management
2. Supplier Management

**Resolution processes**

1. Incident and Service Request Management

2. Problem Management

**Control processes**

1. Configuration Management

2. Change Management

3. Release and Deployment Management

**Table 3 — Mapping of ISO/IEC 20000-1:2011 (IEEE Std 20000-1:2013) and ISO/IEC 20000-2:2012 (IEEE Std 20000-2:2013) clauses to information items for each service management process**

| Typical Input information items | ISO/IEC 20000-1:2011 (IEEE Std 20000- 1:2013) or ISO/IEC 20000-2: 2012 (IEEE Std 20000-2:2013) clause | Output information item |
|---|---|---|
| ***APPLICABLE ACROSS THE SERVICE MANAGEMENT SYSTEM TO ALL PROCESSES*** | | |
| **SERVICE MANAGEMENT** | | |
| Service management policy, contract, objectives, scope, customer requirements, performance reports | **1:** 1.1, 4.1.1, 4.1.2, 4.3.1, 4.5.1, 4.5.2<br>**2:** 4.1.1.1, 4.1.1.4, 4.1.1.5, 4.1.1.6, 4.1.2.1, 4.1.2.2, 4.1.3.1, 4.1.4.2, 4.2.4, 4.3.1.1, 4.5.2.1, 4.5.2.2, 4.5.2.4, 4.5.4.1 | Service management plan (includes service management policy) |
| Service management plan including policy | **1:** 4.1.3<br>**2:** 4.1.1.3, 4.1.3.2 | Communication procedure |
| Service management plan, SLA | **1:** 4.3.1<br>**2:** 4.3.1.1 | Service catalog |
| Contract (or agreement), service management plan, service catalog | **1:** 4.3.1<br>**2:** 4.1.1.3, 4.3.1.1, | Service level agreement (SLA) |
| Documentation plan, information management plan | **1:** 4.3.1, 4.3.2<br>**2:** 4.1.3.1, 4.3.1.2, 4.3.2 | Documentation procedure |
| Configuration management plan, information management plan | **1:** 4.3.3<br>**2:** 4.3.3, 4.4.2.2 | Information management procedure (records management procedure) |
| Service description, process description | **1:** 4.5.2<br>**2:** 4.2.4, 4.5.2.4 | Interface description |
| Service management plan, service level agreement, audit report | **1:** 4.1.4.e), 4.5.3.f), 4.5.5.2<br>**2:** 4.1.4.4, 4.5.4.2 | Service report |
| SLA, service management plan | **1:** 4.5.4.1, 4.5.4.2<br>**2:** 4.5.4.2 | Audit plan |
| Contract, SLA, Service management plan, customer satisfaction survey, resource information, risk register, audit results, changes, improvements meeting decisions and actions, | **1:** 4.5.4.1,4.5.4.3<br>**2:** 4.1.1.2, 4.1.2.1.f) | Review minutes |
| Audit plan | **1:** 4.5.4.2<br>**2:** 4.5.4.2 | Audit procedure |
| Audit procedure | **1:** 4.5.4.2<br>**2:** 4.5.4.2 | Audit report |
| Service management plan, SLA, improvement policy, measurement plan, monitoring and control reports, review minutes, audit results | **1:** 4.5.5.1<br>**2:** 4.5.5.2 | Improvement procedure |

| Typical Input information items | ISO/IEC 20000-1:2011 (IEEE Std 20000- 1:2013) or ISO/IEC 20000-2: 2012 (IEEE Std 20000-2:2013) clause | Output information item |
|---|---|---|
| Organizational policies, service plans Improvement policy, service management plan, problem reports, test reports | **1:** 4.5.5.1, 4.5.5.2<br>**2:** 4.5.5.1, 4.5.5.2 | Improvement plan (includes improvement policy) |
| Service management plan, service requirements, service design | **2:** 4.2.1, 4.2.5, 4.3.1.1, 4.5.2.3, 4.5.3, | Contract (agreement) |
| **DESIGN AND TRANSITION OF NEW OR CHANGED SERVICES** | | |
| Service management policy, change management policy, contract, customer requirements | **1:** 5.1, 5.2, 5.3 | System requirements specification (service requirements) |
| Service management policy, change management policy, contract, objectives, customer requirements, service requirements, performance reports | **1:** 5.2, 5.3<br>**2:** 5.2.7, 5.3.3.1 | Service Plan (plan for new or changed services) |
| Service management plan, service requirements, service design | **1:** 5.2. 5.3<br>**2:** 5.2.8 | Contract (agreement) |
| Service management plan, service plan, service design | **1:** 5.2<br>**2:** 5.2.8.h | Interface description |
| Service management plan, service catalog | **1:** 5.2<br>**2:** 5.2.8 | Disposal plan |
| Service management plan, SLA | **1:** 5.3 | Service catalog |
| Contract (or agreement), service management plan, service catalog | **1:** 5.3<br>**2:** 5.3.1, 5.5 | Service level agreement (SLA) |
| Service management plan, SLA | **1:** 5.3 | Procedure (generic information item) |
| Service management plan, service level agreement, audit report | **1:** 5.4<br>**2:** 5.2.8, 5.4, 5.5 | Service report |
| **SERVICE LEVEL MANAGEMENT** | | |
| SLA, service management plan | **1:** 6.1<br>**2:** 6.1.4 | Contract (agreement) |
| Service management plan, contract (underpinning or operational level agreement), service catalog, change request, service report, service management procedures, organizational procedures, or customer procedures, security policy, service performance, continuity, and availability requirements | **1:** 6.1,<br>**2:** 6.1.3.2, 6.1.3.3, 6.1.3.4, 6.1.4 | Service level agreement (SLA) |
| Service management plan, SLA | **1:** 6.1<br>**2:** 6.1.3.4, 6.1.4 | Service catalog |
| SLA, contract, service plan, problem report, monitoring and control report, cost report, business relationship management procedure | **1:** 6.1<br>**2:** 6.1.4 | Review minutes |
| Service report, service management plan | **2:** 6.1.4 | Improvement plan |
| SLA, availability record, incident record, complaint record | **2:** 6.1.3.1, 6.1.3.4, 6.1.4 | Service report |
| SLA, service procedure | **2:** 6.1.4 | Monitoring and control report |
| **SERVICE REPORTING** | | |
| Service continuity plan, monitoring and control report; SLA; incident report; problem report; release record; service reporting requirements specification; monitoring and control records for performance data, non-conformity with standards, workload characteristics and volume information, trend information by period (e.g. day, week, month, period); future and scheduled workloads | **1:** 6.2<br>**2:** 6.2.1, 6.2.2, 6.2.3, Table A.3 | Service report |
| SLA, audit plan | **2:** 6.2.3.c) | Audit report |
| **SERVICE CONTINUITY AND AVAILABILITY MANAGEMENT** | | |
| Business plan; SLA; risk assessment; service availability and continuity requirements; capacity plan, service recovery procedure; change request | **1:** 6.3<br>**2:** 6.3.2, 6.3.3.2, 6.3.3.3, 6.3.4, 6.3.5 | Service availability and continuity plan (includes service availability and continuity policy) |

| Typical Input information items | ISO/IEC 20000-1:2011 (IEEE Std 20000- 1:2013) or ISO/IEC 20000-2: 2012 (IEEE Std 20000-2:2013) clause | Output information item |
|---|---|---|
| Availability records, service level agreement, service availability and continuity plan, test results, action plans, Risk management plan, service continuity plan | **1:** 6.3.3<br>**2:** 6.3.4.3, 6.3.5 | Evaluation report |
| SLA, Verification plan | **2:** 6.3.5 | Integration and test report (service continuity and availability test report) |
| Service availability and continuity plan, SLA | **2:** 6.3.5 | Monitoring and control report |
| Service availability and continuity plan, SLA | **2:** 6.3.5 | Verification plan (service continuity and availability test plan) |
| **BUDGETING AND ACCOUNTING FOR SERVICES** | | |
| Business policies and financial procedures, previous budgets and cost reports, financial forecast reports, service management plan, SLA<br>NOTE : Business policies and financial procedures relating to budgeting, financial accounting, and reporting on costs are outside the scope of this document. | **1:** 6.4<br>**2:** 4.4.1.2, 6.4.1, 6.4.2 | Financial management, budgeting, and accounting policies and procedures Budget<br>Financial accounting report (cost report)<br>NOTE : The contents of these financial items are not further specified in this document. |
| **CAPACITY MANAGEMENT** | | |
| Capacity plan | **1:** 6.5<br>**2:** 6.5.3.2, 6.5.4 | Capacity management procedure |
| Service management plan. SLA, capacity and performance requirements (current and future), capacity usage data and analyses, change management reports | **1:** 6.5<br>**2:** 6.5.1, 6.5.2, 6.5.3.2, 6.5.4 | Capacity plan |
| Capacity and performance data, problem report, monitoring and control report | **2:** 6.5.3.1, 6.5.4 | Service report |
| **INFORMATION SECURITY MANAGEMENT** | | |
| Organizational policies, regulations | **1:** 6.6.1<br>**2:** 6.6.2, 6.6.3.1, 6.6.4, Table A.7 | Information security policy |
| Information security plan, security control description, incident report; problem report, process assessment | **1:** 6.6.2<br>**2:** 6.6.4 | Evaluation report |
| Information security policy and plan, problem management procedures | **1:** 6.6.2<br>**2:** 6.6.2, 6.6.4 | Information security procedures |
| Information security plan, monitoring and control report, incident management procedures, incident records | **1:** 6.6.2, 6.6.3<br>**2:** 6.6.3.4, 6.6.4 | Incident report |
| Information security policy, requirements specification, information security risk assessment procedure, risk management plan, security control procedure | **2:** 6.6.2, 6.6.4 | Information security plan |
| Information security policy and plan | **2:** 6.6.3.4.n) | Training plan |
| Incident report, problem report, assessment report | **2:** 6.6.3.5 | Change request |
| **BUSINESS RELATIONSHIP MANAGEMENT** | | |
| SLA, service management plan, complaint procedure | **1:** 7.1<br>**2:** 7.1.3.1, 7.1.3.3, 7.1.4, Table A.8 | Complaint (record) |
| Agreement, SLA, service management plan | **1:** 7.1<br>**2:** 7.1.3.3, 7.1.4 | Complaint procedure |
| SLA, Communications plan | **2:** 7.1.1 | Communications procedure |
| SLA, contract, compliment, complaint | **1:** 6.2.5.3.1.4, 7.1<br>**2:** 7.1.3.3, 7.1.4, Table A.8 | Customer satisfaction survey |
| SLA, contract, service management plan, problem report, monitoring and control report, cost report, business relationship management procedure | **1:** 7.1<br>**2:** 7.1.4 | Review minutes |

| Typical Input information items | ISO/IEC 20000-1:2011 (IEEE Std 20000- 1:2013) or ISO/IEC 20000-2: 2012 (IEEE Std 20000-2:2013) clause | Output information item |
|---|---|---|
| SLA, Problem report, customer satisfaction survey, Performance measurements | **2:** 7.1.4 | Service report |
| **SUPPLIER MANAGEMENT** | | |
| Service level agreement, service management plan, service catalog, change request, information security policy | **1:** 7.2<br>**2:** 7.2.2, 7.2.3.1, 7.2.4 | Contract (and contract changes) |
| Contract, supplier management procedure | **1:** 7.2<br>**2:** 7.2.4 | Interface description |
| Service management plan, contract, supplier's SLA | **1:** 7.2<br>**2:** 7.2.2, 7.2.3.2 | Service level agreement (SLA) |
| Contract, SLA, monitoring and control report | **1:** 7.2<br>**2:** 7.2.3.1 | Service report |
| Organizational policy, service management plan, service level agreement | **1:** 7.2<br>**2:** 7.2.2 | Supplier management procedure |
| **INCIDENT AND SERVICE REQUEST MANAGEMENT** | | |
| Change management procedure, service management plan, configuration management database, known errors, catalog of services, SLA | **1:** 8.1<br>**2:** 8.1.2, 8.1.4, 8.1.5 | Incident management procedure or service request management procedure |
| Incident procedure, known error and problem resolution, configuration records | **2:** 8.1.5 | Incident report |
| **PROBLEM MANAGEMENT** | | |
| Problem report | **1:** 8.2 | Change request |
| SLA, service management plan, | **1:** 8.2<br>**2:** 8.2.2, 8.2.3, 8.2.4 | Problem management procedure and policy |
| Incident report, information on known errors, problem management procedure | **1:** 8.2<br>**2:** 8.2.4 | Problem report |
| Problem review, problem reports | **1:** 8.2<br>**2:** 8.2.4.f) | Review minutes |
| **CONFIGURATION MANAGEMENT** | | |
| Configuration management procedure, configuration status report | **1:** 9.1<br>**2:** 9.1.3.2, 9.1.4 | Audit report |
| Configuration management procedure | **1:** 9.1<br>**2:** 9.1.3.5 | Change request |
| Configuration management plan | **1:** 9.1<br>**2:** 9.1.3.2, 9.1.3.3, 9.1.4. | Configuration management procedure |
| Service management plan | **1:** 9.1 | Interface description |
| System management policies, System design description, service level agreement, system requirements specification, configuration management policy | **2:** 9.1.2, 9.1.3.2, 9.1.3.3, 9.1.4 | Configuration management plan and policy |
| Audit plan, configuration management plan and policy, configuration records | **2:** 9.1.3.2, 9.1.3.5. | Audit procedure |
| Configuration management procedure, configuration records | **2:** 9.1.1, 9.1.4 | Configuration status report |
| **CHANGE MANAGEMENT** | | |
| Incident report, Problem report, configuration status report | **1:** 9.2<br>**2:** 9.2.2, 9.2.3.2, 9.2.3.3, 9.2.4 | Change request |
| Contract, System management policies, change requests, service catalog, service availability and continuity plan, Service management plan, service requirements, problem management procedure, SLA, service continuity and availability plan, capacity plan, changes to cost estimates | **1:** 9.2<br>**2:** 9.2.3.1, 9.2.3.2, 9.2.4 | Configuration management plan and policy (change management plan and policy) |
| Configuration management plan, problem management procedure, SLA, | **1:** 9.2<br>**2:** 9.2.2, 9.2.4 | Configuration management procedure (change management procedure) |

| Typical Input information items | ISO/IEC 20000-1:2011 (IEEE Std 20000- 1:2013) or ISO/IEC 20000-2: 2012 (IEEE Std 20000-2:2013) clause | Output information item |
|---|---|---|
| Change request, change management plan, change management procedures | **2:** 9.2.4 | Release plan (deployment plan) |
| Change request | **2:** 9.2.3.2, 9.2.4 | Evaluation report |
| **RELEASE AND DEPLOYMENT MANAGEMENT** | | |
| Change request, SLA | **1:** 9.3<br>**2:** 9.3.3.2, 9.3.3.3 | Configuration management procedure (release management procedure) |
| Release plan, release management plan | **1:** 9.3<br>**2:** 9.3.4 | Evaluation report |
| Change management policy, service management plan, test plan, verification plan, acceptance plan, disposal plan, release schedule, change request | **1:** 9.3<br>**2:** 9.3.3.1, 9.3.3.2, 9.3.4 | Release plan and policy |
| Test plan, incident reports or records | **2:** 9.3.3.4, 9.3.4 | Integration and test report |
| Release management plan, release plan; change request, problem report | **2:** 9.3.3.4, 9.3.4 | Verification plan (Test plan) |
| Release plan, service management plan | **2:** 9.3.4 | Communication procedure (communications plan). |
| Release management plan, service management plan | **2:** 9.3.4 | Training plan |
| Release plan, installation plan, integration and test plan | **2:** 9.3.4 | User documentation |

# 9 Records

This clause identifies the generic and specific content of records called out in ISO/IEC 12207:2008 (IEEE Std 12207-2008), ISO/IEC/IEEE 15288:2015, ISO/IEC 20000-1:2011 (IEEE Std 20000-1:2013) and ISO/IEC 20000-2:2012 (IEEE Std 20000-1:2013). The project, organization, or service shall maintain the records needed for the required information items (documents). Records contain data structured in a permanent, readable form. Records may be generated for any life-cycle process, task, or activity in a project or organization, to include data on requirements, policies, decisions and their rationale, designs, source code, problems, reviews, requests, measurements, and test data, as well as product, quality, legal and official, financial, and historical data. Records should be maintained for retrieval in registers, repositories, or databases.

## 9.1 Record – generic content

Purpose: Organize the data an organizational entity retains.

A record shall include the following elements:

a) Date of record, date recorded, and status;

b) Scope;

c) Subject or category;

d) Issuing organization;

e) References;

f) Body; and

g) Unique record identifier.

## 9.2 Specific record contents

Table 4 provides references for the applicable life-cycle process and content of specific records referenced in ISO/IEC 12207:2008 (IEEE Std 12207-2008), ISO/IEC/IEEE 15288:2015, ISO/IEC 20000-1:2011 (IEEE Std 20000-1-2013), and ISO/IEC 20000-2:2012 (IEEE Std 20000-2-2013). The generic content of records is presented in clause 9.1. Table 4 does not include every reference to records of results that are required to be collected, stored, and verified, such as measurement data. Problem records are included in the Problem Report in Clauses 8 and 10. Annex B, Table B.2 compares Records by Source.

NOTE 1 The term "configuration record" can be used for either a record of an individual component (item) in a configuration or the record of a system's configuration at a point in time (baseline).

NOTE 2 ISO/IEC 20000-1:2011 (IEEE Std 20000-1:2013) and ISO/IEC 20000-2:2012 (IEEE Std 20000-2:2013) distinguish between complaints, incidents and problems. A problem is the underlying root cause of one or more incidents or complaints. For information management purposes in this document, the records for complaints, incidents, and problems have similar content and often use the same or related records management systems.

**Table 4 — Record references and contents**

| Record | Process | Reference | Record Contents |
|---|---|---|---|
| Acceptance record | Acquisition<br>Service management | **15288:** 6.1.1.3.e.1)<br>**20000-2:** 5.4, 7.2.3.2 | Acquirer acknowledgment that acceptance criteria have been met |
| Assessment record (audit record) | Life-cycle model management, project assessment and control, service management, information security management, configuration management | **12207:** 6.2.1.3.2.1, 6.2.1.3.3.2, 6.3.2.2, B.3.3.2.2<br>**15288:** B.1<br>**20000-1**: 4.5.4.1, 4.5.4.2, 5.2<br>**20000-2:** 6.6.3.3, 9.1.3.2 | Information and data related to the use of the standard process for specific projects and services; result of the audit or assessment. |
| Availability record | Service continuity and availability management | **20000-1:** 6.3.3<br>**20000-2**: 6.3.4.2, 6.3.5 | Response time compared to SLA, actual available time divided by planned available time |
| Complaint record (compliment record) | Business relationship management, supplier management | **20000-1:** 7.1<br>**20000-2:** 7.1.3.3, 7.1.4, 7.2.3.4, Table A.8 | Customer, customer type, variance, defect, conflicting requirement, or non-conformance; complaint category, correction actions, known error, dispute information, assigned responsibility, resolution. See problem report, change request |
| Configuration record (asset record, change record, maintenance record) | Configuration management, infrastructure management, implementation, transition, maintenance, disposal, reuse asset management, domain engineering, asset management, information security management, problem management, change management, release and deployment management | **12207:** 6.3.5.3.1.2, 6.3.5.3.2.1, 6.3.5.3.2.2, 7.2.2.3.3.1<br>**15288:** 6.2.2.3.2, 6.2.5.3.b), 6.4.4.3.b), 6.4.10.3.c), 6.4.13.3.d), B.1<br>**20000-1:** 3.4, 9.1, 9.2<br>**20000-2:** 4.1.4.3, 4.3.2, 4.3.3, 9.1.1, 9.1.2, 9.1.3.1, 9.1.3.3, 9.1.3.4, 9.1.3.5, 9.1.4, 9.1.5, 9.2.2, 9.2.3.3, 9.2.4 | Functional and physical characteristics, version, location, configuration status; approvals and authorizations; associated items, associated incident or problem records, associated known errors, associated change requests, associated incident or service requests, the rationale for approval of the baseline; changes to baseline; association to requirements; indication that the item or element fulfilled the agreement or requirements; maintenance, failure and lifetime data; disposal record; owner, use and criticality of asset; and activities performed, such as backup, storage, archiving, handling and delivery of configured items.<br>Stored in a configuration management database (CMDB) or change log<br>See also change request, incident record, problem record, release record, software item configuration record, system element description. |

| Record | Process | Reference | Record Contents |
|---|---|---|---|
| Decision record | Decision management, supplier management, systems analysis | **12207:** 5.1.2, 6.3.3.1<br>**15288:** 6.3.3.1, 6.3.3.3.1, 6.4.6.3.b), B.1<br>**20000-1:** 4.5.4.3<br>**20000-2:** 4.1.1.2, 5.4, 7.2.4 | Decision, assumptions, and rationale; outstanding actions. |
| Disposal record | Disposal | **12207:** 6.4.11.1, 6.4.11.2.e)<br>**15288:** 6.4.14.1, 6.4.14.2.e) | Disposal actions for future risk and impact analysis |
| Incident record (transition record, security incident record, service request record, major incident record, customer support record) | Maintenance, supply, verification, transition, validation, operation, service continuity and availability management, capacity management, information security management, incident and service request management, change management, problem management, release and deployment management | **15288:** 6.4.8.3.c), 6.4.9.1, 6.4.9.3.c), 6.4.10.2.f), 6.4.10.3.c), 6.4.11.3.c), 6.4.12.3.b), 6.4.12.3.c), 6.4.12.3.d), 6.4.13.1, 6.4.13.2.d), 6.4.13.3.b), 6.4.13.3.d), B.1<br>**20000-1**: 6.6.3, 8.1<br>**20000-2:** 4.2.3,.3.1.2,4.3.3, 5.5 6.3.3.3, 6.3.4.2, 6.5.4, 6.6.3.4, 6.6.3.5, 6.6.4, 8.1.2, 8.1.3.1, 8.1.3.2, 8.1.5, 8.2.1, 9.3.3.5, 9.3.4, Table A.2, Table A.10 | Incident summary, service request, associated configuration items, variance, anomaly, defect, or non- conformance; priority, incident category, root cause, fault correction actions, known error, assigned responsibility and escalation, resolution and closure.<br>*See* incident report, change request |
| Information item (storage) record | Information management | **12207:** 6.3.6.2, 6.3.6.3.2.2<br>**15288:** 6.3.6.2.d), 6.3.6.3.b), 6.2.6.3.d) | Information status, version description, distribution record, security classification |
| Knowledge management record | Life cycle model management, Human resource management, knowledge management, disposal, incident and service request management, problem management | **12207:** 6.2.4.3.3.5<br>**15288:** 6.2.1.3.c), 6.2.4.3, 6.2.6.3.d), 6.4.13.3.d), 6.4.14.3.b), B.1 | Knowledge, recommended applicability, usage of knowledge assets |
| Performance control record | Service management, supplier management | **20000-1:** 6.1, 7.2<br>**20000-2:** 7.2.3.2 | Data on service performance against targets, the results of applying the process, service quality level |
| Personnel skills record (staff assignment record) | Human resource management, maintenance | **15288:** 6.2.4.3.a)2), 6.4.13.3.c), B.1<br>**20000-1:** 4.4.2<br>**20000-2:** 4.4.2.2, | Employee identifier, skill, level of proficiency.<br>*See also* Skill development record |
| Problem record (known error record) | Decision management, integration, maintenance, project assessment and control, quality assurance, verification, transition, validation, operation, software review, software audit, software operations, software quality assurance, software problem resolution, software verification, software validation, domain engineering, reuse management, configuration management, problem management, release and deployment management | **12207:** 6.1.2.3.4.8, 6.3.2.3.2.1, 6.3.3.3.1.3, 6.3.3.3.3.2, 6.4.9.3.1.2, 6.4.9.3.4.1, 6.4.10.3.1.2, 7.2.3.2.c), 7.2.3.3.1.4, 7.2.4.2.d), 7.2.5.2.d), 7.2.6.2.e), 7.2.6.3.1.4, 7.2.7.2, 7.2.7.3.1.5, 7.2.8.2.b). 7.2.8.3.1.1, 7.3.3.3.5.3<br>**15288:** 6.3.2.3.c), 6.3.3.3, 6.4.9.3.c), 6.4.10.3.c), 6.4.11.3.c), 6.4.12.3.c), 6.4.13.3.b), 6.4.13.3.d), B.1<br>**20000-1**: 3.19, 8.2, 9.1<br>**20000-2**: 4.5.5.2, 6.3.4.2, 8.2.2, 8.2.3, 8.2.4, 8.2.5, 9.3.3.5, 9.3.4, Table A.10 | Problem, variance, defect, or non-conformance; problem category, associated configuration item, fault correction actions, known error, root cause, assigned responsibility, resolution.<br>*See also* problem report, change request |
| Project authorization record | Portfolio management, project planning, project assessment and control | **15288**: 6.2.3.3.a), 6.3.1.3.c), B.1 | Project description, responsible organization, authorization period |
| Quality activity record | Quality assurance, software quality assurance, improvement, | **15288:** B.1<br>**12207:** 7.2.3.3.1.3.c), 7.2.3.3.1.4, 7.2.3.3.1.5<br>**20000-1:** 4.3.3<br>**20000-2:** 4.3.3 | Execution of the quality activity, such as document review or assessment activity |

| Record | Process | Reference | Record Contents |
|---|---|---|---|
| Quality cost data | Life-cycle model management | **12207:** 6.2.1.3.3.3 | Establishes the cost of preventing and resolving problems and non-conformities and support process improvement |
| Release record | Supply, software operation, release and deployment management, configuration management | **12207:** 6.4.9.3.1.3, B.3.2.3.2<br>**20000-1:** 9.3<br>**20000-2:** 9.1.2, 9.3.3.5, 9.3.4 | Identifies, tracks, and controls a release and its configuration items at the time a version (including the baseline version) is released. For software, it identifies a software version consisting of one or more software items. It lists items being delivered, including system and software item versions, traceability to specifications or previous releases, what has been changed; known errors, problems and workarounds. It may refer to installation or delivery procedures and information on the success of the release or associated problems. |
| Requirement record | Stakeholder requirements definition, system requirements definition, portfolio management, business or mission analysis; infrastructure management, operation, maintenance, All service management processes and services | **12207:** 6.4.1.3.5.1<br>**15288:** 6.2.3.3.a), 6.4.1.3, 6.4.2.1, 6.4.2.2.e), 6.4.2.3.a), 6.4.2.3.d), 6.4.3.1, 6.4.3.2.b), 6.4.3.3.b), 6.4.12.1, 6.4.12.3.a), 6.4.13.3.b), B.1<br>**20000-1** 3.34, 4.1.4, 4.5.2, 5.2, 6.3.1, 6.5, 7.1, 7.2,<br>**20000-2:** 4.1.1.3, 4.1.1.7, 4.1.1.8, 4.1.1.9, 4.1.1.10, 4.1.4.3, 4.5.2.1, 4.5.2.2, 4.5.2.4, 5.2.4, 5.2.5, 5.2.7, 5.3.1, 5.5, 6.1.4, 6.2.3, 6.3.5, 6.5.4 | Traceability, priority, resources, constraints, capacity, continuity and availability, usability of interactions, health and safety, information security, environment, statutory, regulatory, financial, reporting, quality<br>*See also*: software requirements specification, system requirements specification (service requirements) |
| Risk record or profile (opportunity) | Risk management, stakeholder requirements definition. operations, software review, service management, service continuity management, information security management, change management | **12207:** 6.3.4.3.2, 6.3.4.3.3.4, 6.4.1.3.2.5, 6.4.9.3.1.1, 7.2.6.2.e)<br>**15288:** 6.3.4.3 b)<br>**20000-1:** 4.1.1, 4.5.5.1, 5.2, 6.3.1, 6.6.1, 9.2<br>**20000-2:** 4.1.1.10, 4.1.1.11, 5.2.3, 5.2.6, 6.6.3.3, 9.2.4 | Source, probability, consequence, acceptability threshold, priority, risk action requests, treatment strategy, status; also opportunities for improvement.<br>Stored in a risk register. |
| Skill development record (Training record) | Human resource management, information security management | **12207:** 6.2.4.3.2.3, 6.2.4.3.3.5<br>**15288:** 6.2.4.3.b)4)<br>**20000-1**: 4.4.2.e<br>**20000-2:** 4.4.2.2, 6.3.5, 6.6.3.4.n) | Skill area, employee identifying data, duration of training, proficiency level, certifying authority<br>*See also:* Personnel skills record |
| Software item configuration record (software asset record) | Software configuration management | **12207:** 7.2.2.2.e), 7.2.2.3.2.1, 7.2.2.3.4.1, 7.3.1.2.e), 7.3.1.3.4.2, 7.3.2.2.e) | A software configuration index may contain software item configuration records for one software item or a set of software items. A software item configuration record should identify generic record information, the software product (source), executable object code, archive and release data, instructions for building the executable object, and data integrity checks for the executable object, and reuse of assets |

| Record | Process | Reference | Record Contents |
|---|---|---|---|
| Test result record (implementation record) | Development, implementation, verification, validation, system qualification testing, software integration, software qualification testing, service continuity and availability management | **12207:** 6.4.6.2, 7.1.6.2.e), 7.1.7.2, 7.1.7.3.1.1<br>**15288:** 6.4.7.3.c), 6.4.9.3.c), 6.4.11.3.c), B.1<br>**20000-1:** 6.3.3<br>**20000-2:** 5.3.3.2, 9.3.3.2, 9.3.3.4 | Result of testing or implementation, includes verification and validation records |

# 10 Specific information item (document) contents

## 10.1 General

Specific contents of the information items shall be provided as required in this clause. For each information item, the generic contents as specified in Clause 7 shall be part of the required item content. The information item contents serve as a checklist that can be satisfied by the organization's content mapping, templates and information models. This clause is not intended to address all possible information item contents, or to mandate the title of the information item, nor the order or titles of the sections in an information item.

Some contents are duplicated or adapted in multiple information items and information item types. A single source repository (such as a content management system) should be used for similar contents for consistency and ease of development. The Information Management Plan, Development Plan, and Documentation Plan should include the type of information and level of detail to be provided in each information item where duplications in content exist.

The contents of the information items identified in Clause 10 include those explicitly identified (but may not be required for conformance) and those implicitly identified in ISO/IEC 12207:2008 (IEEE Std 12207-2008), ISO/IEC/IEEE 15288:2015, and ISO/IEC 20000-1:2011 (IEEE Std 20000-1:2013) and ISO/IEC 20000-2:2012 (IEEE Std 20000-1:2013).

In this document, the project has been chosen as the context for describing processes concerned with planning, assessment and control. The principles related to these processes may be applied in any area of an organization's management (for example, for a program or organization).

Qualifiers and adjectives (such as "Software," "Architecture," "Component", "Summary", "Preliminary", "Customer's," "Stakeholders", "Enterprise") may be applied as part of the information item or document title.

Information items for systems may be specialized for software.

EXAMPLE A system element description produced for a software item may be called a software element description. A change request for software may be called a software modification request.

NOTE ISO/IEC/IEEE 26531 includes requirements for content management of life-cycle information

## 10.2 Acceptance plan

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 6.1.1.3.1.9

ISO/IEC/IEEE 15288:2015 reference: 6.3.1.3.b)6)

Generic type: Plan

The acceptance plan should prepare for acceptance based on the defined acceptance strategy and criteria. It specifies objective criteria for determining acceptability of the deliverable work products, and any technical processes, methods, or tools required for product acceptance. Methods such as testing, demonstration, analysis, and inspection should be specified. It indicates the extent of supplier involvement. If acceptance is based on tests, it may reference or provide an overall test plan.

See also: software integration test plan

## 10.3 Acceptance report

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 6.4.8.3.1.1

ISO/IEC/IEEE 15288:2015 reference: 6.1.1.3.e.1), B.1

Generic type: Report

The acceptance report states that an acquirer has reviewed (and possibly tested) a deliverable. It indicates whether the product is accepted, and the reasons for non-acceptance if the product or service is rejected.

## 10.4 Acquisition plan

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 6.1.1.3.1.8, 6.1.1.3.1.9, 6.1.1.3.1.12

ISO/IEC/IEEE 15288:2015 reference: 6.3.1.3.b)6)

Generic type: Plan

The acquisition plan includes the following:

a) a definition of the technical and managerial processes necessary to satisfy the software acquisition requirements, that is, the following acquisition activities: process initiation, request for proposal (RFP) (tender) preparation, contract preparation and maintenance, supplier monitoring, and acceptance and completion;

b) system requirements, planned employment of the system, contract type, organizational responsibilities, and the concept of support;

c) risks and methods to manage risks; and

d) acquisition options and criteria to include risk, cost, and benefits for each option considered.

Acquisition options include off-the-shelf product, product developed internally or contracted out, and reuse or enhancement of existing product or service, or any combination thereof.

The acquisition plan should include the following:

a) supplier selection criteria;

b) the purpose of the system or software;

c) a description of the general nature of the system and components, including software;

d) an outline of the expected life-cycle processes and the need for system development, operation, and maintenance;

e) identification of the project sponsor, acquirer organization, user organizations, and support agencies;

f) the project review and audit milestones; and

g) current and planned operating sites.

The acquisition plan may include costs and budgets for the acquisition.

## 10.5 Asset management plan

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference 7.3.2.2, 7.3.2.3.1.1, 7.3.2.3.1.3, 7.3.2.3.2.2

Generic type: Plan

The asset management plan defines the strategy, management and technical processes for asset management. It defines an asset classification scheme, the asset storage, handling and retrieval mechanism; and asset acceptance, certification, and retirement procedures.

## 10.6 Audit acknowledgement report

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 7.2.7.3.1.6

Generic type: Report

The audit acknowledgement report acknowledges audit results and presents the planned resolution of problems to the auditing party.

### 10.7 Audit plan

ISO/IEC 12207:2008 (IEEE Std 12207-2008): 6.2.1.3.2.2, 7.2.7.3.2.1

ISO/IEC 20000-1:2011 (IEEE Std 20000-1:2013) reference: 4.5.4.1, 4.5.4.2

ISO/IEC 20000-2:2012 (IEEE Std 20000-2:2013) reference: 4.5.4.2

Generic type: Plan

The audit plan defines the overall audit program, as well as the specific processes, services, or other activities to be audited. It includes the audit objectives and priorities and the subjects of the audits, including work products and records to be reviewed. It defines roles and responsibilities for the audit and plans for recording and communicating the audit results.

### 10.8 Audit procedure

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 7.2.7.3.1.4,

ISO/IEC 20000-1:2011 (IEEE Std 20000-1:2013) reference: 4.5.4.2,

ISO/IEC 20000-2:2012 (IEEE Std 20000-2:2013) reference: 4.5.4.2, 9.1.3.5

Generic type: Procedure

The audit procedure includes the audit criteria, scope, frequency, and methods for conducting audits. It outlines how deficiencies are recorded and reported. It identifies who is responsible for planning and conducting the audit, reporting the results, maintaining the audit records, and initiating and performing corrective action.

### 10.9 Audit report

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 6.1.2.3.4.15, 6.4.6.3.1.3, 7.1.7.3.1.4, 7.2.7.3.1.6

ISO/IEC 20000-1:2011 (IEEE Std 20000-1:2013) reference: 4.5.4.2, 9.1

ISO/IEC 20000-2:2012 (IEEE Std 20000-2:2013) reference: 4.3.1.1, 4.5.4.2, 6.2.3.c), 9.1.3.2, 9.1.4

Generic type: Report

The audit report provides audit results and is delivered to the audited party. It identifies participants, certification of auditor's independence, agreement on resources involved in the audit, audit schedule, list of items to be audited, audit scope, audit procedures, entry and exit criteria, reference to problem records, action item responsibilities and closure criteria and status of corrective actions, compliance/conformity. It may include an audit strategy, the names of organizations audited, product or service being audited, name of auditor, date and location of audit, audit criteria, status of previous audit action items, new action items (including responsible person or organization and due date), and observations and findings.

### 10.10 Capacity plan

ISO/IEC 20000-1:2011 (IEEE Std 20000-1:2013) reference: 6.5

ISO/IEC 20000-2:2012 (IEEE Std 20000-2:2013) reference: 6.5.1, 6.5.2, 6.5.3.2, 6.5.4

Generic type: plan

The capacity plan documents how the supplier meets the capacity and performance requirements for a service, including continuity and availability. It identifies factors affecting capacity, including current and anticipated demand, legal and regulatory changes, changes in agreements or organizations, and implementation of new technology or procedures. It defines the approach for predictive analysis to determine thresholds when additional capacity should be provided to upgrade the service. It describes how schedules and cost estimates are prepared for recommended changes in capacity. The capacity plan should be updated at least annually.

## 10.11 Capacity management procedure

ISO/IEC 20000-1:2011 (IEEE Std 20000-1:2013) reference: 6.5

ISO/IEC 20000-2:2012 (IEEE Std 20000-2:2013) reference: 6.5.3.2, 6.5.4

Generic type: procedure

The capacity management procedures explain how the organization performs predictive analyses of capacity based on system monitoring data, such as modelling predicted or actual performance of the infrastructure systems in terms of component and resource utilization.

## 10.12 Change request

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 6.1.1.3.4.3, 6.1.2.3.3.2, 6.3.5.3.1, 6.4.9.3.1.3, 6.4.9.3.4.1, 6.4.9.3.4.2, 6.4.10.3.1.2, 6.4.10.3.2.1, 6.4.10.3.2.4, 7.2.2.3.3.1, 7.2.8.2, 7.3.1.3.1.3, 7.3.1.3.5.1, 7.3.2.3.3.6, 7.3.2.3.3.7, F.3.2, F.3.3.2.1

ISO/IEC/IEEE 15288:2015 reference:6.1.2.1, 6.1.1.3.c)2), 6.1.2.3.c)2), 6.3.2.3.c)3), B.1

ISO/IEC 20000-1:2011 (IEEE Std 20000-1-2013) reference: 8.2, 9.1, 9.2

ISO/IEC 20000-2:2012 (IEEE Std 20000-2-2013) reference: 6.6.3.5, 9.1.3.5, 9.2.2, 9.2.3.2, 9.2.3.3, 9.2.4, Table A.14

Generic type: Request

A change request (or request for change) identifies a problem, maintenance need, or desired improvement and requests modifications. The requested change may affect a contract, configuration item, system, service, hardware, software, interface, asset, or documentation. It is the input to initiate contract changes and the change management process. It may reflect requests and related actions from customers and users for assistance and consultation, or a request to retire a configuration item. The change request should present the benefit and scope of the change, including the new or modified asset, service or functions, or problem to be corrected; with the priority, assumptions and constraints. It may address the impact to schedules, cost, products, and test.

Routine, preapproved maintenance requests are treated as service requests. Change requests should be recorded and can use the same system that records complaints, service requests, incidents, or problems.

See also: problem report, service request (record)

## 10.13 Communication procedure

ISO/IEC 20000-1:2011 (IEEE Std 20000-1:2013) reference: 4.1.3, 7.1

ISO/IEC 20000-2:2012 (IEEE Std 20000-1:2013) reference: 4.1.1.3, 4.1.3.2, 7.1.1, 9.3.4

Generic type: Procedure

The communication procedure aligns the objectives of written and oral communication with the occasions, frequency, media, and types of communication, such as reviews, meetings, briefings, workshops, notifications, and unscheduled discussions, as well as electronic or printed communications. It identifies communication audiences and parties who should communicate, such as managers and team members or stakeholders, supplier and acquirer, or service provider and customers, users, and interested parties. It explains how communications can be escalated, with contact details. It covers how contact information on communication recipients (distribution list) is maintained, schedules for periodic communications, who is responsible for communicating, and who has access to communication tools and source information (records). Types of information to be communicated may include policies, new or changed requirements, alignment of a service with objectives and customer expectations, and understanding of the environment for services.

## 10.14 Complaint procedure

ISO/IEC 20000-1:2011 (IEEE Std 20000-1:2013) reference: 7.1

ISO/IEC 20000-2:2012 (IEEE Std 20000-1:2013) reference: 7.1.3.3, 7.1.4

Generic type: Procedure

The complaint procedure defines what constitutes a complaint. It identifies the service provider's point of contact for formal complaints. It documents how to receive record, prioritize, investigate, review, escalate,

resolve, and close complaints, and how to report on complaints and provide feedback. It may explain when complaints become recorded as incidents.

See also: complaint (record), incident (service request) management procedure, incident report, problem management procedure, problem report, service level agreement

## 10.15 Concept of operations

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 6.1.1.3.1.1, 6.4.1.2, 6.4.1.3.2.3

ISO/IEC/IEEE 15288:2015 reference: 6.4.1.1, 6.4.1.2, 6.4.1.3.c), 6.4.2.2.b), 6.4.2.3.b), 6.4.2.3.c), B.1

Generic type: Description

The concept of operations (or operational concept) includes the following:

a) a description of how a system works from the users' point of view;

b) identification of stakeholder needs and the anticipated types of system users;

c) identification of interfaces to existing and future systems;

d) summary of operational, organizational, and development impacts; and

e) reviews of cost, criticality and feasibility of the intended system.

NOTE ISO/IEC/IEEE 15288:2015 distinguishes between the Concept of Operations, first developed in business or Mission Analysis, and the Operational Concept, a detailed strategy for the performance of system operations.

The concept of operations may include the following:

1) the intended interaction of the system in its operational environment, such as scenarios, models, or activity sequences of business processes handled by the system, as the basis for defining the system requirements. Scenarios (or use cases) should include events, actions, stimuli, information, and interactions.

2) context of use of services, such as user culture, system constraints, operational situation, needs and requirements imposed by society, the constraints imposed by a supplier organization, and the capabilities and limiting characteristics of staff

3) a description of the current system or situation, including background, operational policies and constraints, modes of operation, operational environment, user classes, interfaces to external systems or procedures, capabilities/functions, performance characteristics, and support environment

4) comparison of the as-is processes to the future processes to be handled by a new system

5) Identification of change issues, including priorities, assumptions and constraints, and changes considered but not recommended.

See also: product need assessment, system requirements specification.

NOTE 2 ISO/IEC/IEEE 29148:2011 *Systems and software engineering — Life cycle processes — Requirements engineering* provides additional guidance.

## 10.16 Configuration management plan and policy

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 6.3.5.3.1.1, 7.2.2.3.1.1

ISO/IEC/IEEE 15288:2015 reference: 6.3.5.3.a)

ISO/IEC 20000-1: (IEEE Std 20000-1:2013) reference: 5.1, 9.2, 9.3

ISO/IEC 20000-2:2012 (IEEE Std 20000-2:2013) reference 9.1.2, 9.1.3.2, 9.1.3.3, 9.1.4, 9.2.3.1, 9.2.3.2, 9.2.3.4, 9.2.4, 9.3.3.1, 9.3.3.2, 9.3.3.3, 9.3.3.5, 9.3.4

Generic type: Plan, Policy

The configuration management (CM) policy (or change management policy) includes the policy for how a configuration item and its components are defined and what items are subject to change control and release management.

Configuration or change management policy may be included in the configuration or change management plan or as a separate set of policies.

The change management policy defines what constitutes a major change and an emergency change (emergency release), and responsibilities for authorizing and implementing normal and emergency changes.

The configuration management (CM) plan (or change management or release and deployment management plan) describes the responsible organization for authorizing and performing these activities, and their relationship with other organizations, such as software development, asset management, suppliers and subcontractors, and maintenance. For a review board or special organization established for authorizing and performing CM activities on a project, the plan shall describe its purpose and objectives; membership and affiliations; scope of authority; and operational practices.

For software, the CM plan should include how the organization performs:

a) configuration identification, including the scheme for the identification and classification of software item records and information items and their versions, and the establishment of baselines;

b) configuration control and change management;

c) configuration status accounting; and

d) configuration audit and evaluation, including recording deficiencies, initiating corrective actions, and reporting.

NOTE IEEE Std 828-2012, *IEEE Standard for Configuration Management in Systems and Software Engineering,* provides additional guidance.

See also: release plan

## 10.17 Configuration management procedure

ISO/IEC 15288:2015 reference: 6.3.5.3.c)

ISO/IEC 20000-1:2011 (IEEE Std 20000-1:2013) reference: 9.1, 9.2, 9.3.

ISO/IEC 20000-2:2012 (IEEE Std 20000-2:2013) reference: 4.1.4.3, 5.3.3.2.l, 9.1.3.2, 9.1.3.3, 9.1.3.5, 9.1.4., 9.2.2, 9.2.4, 9.3.3.2, 9.3.3.3

Generic type: Procedure

The configuration management procedure (or asset management or change management or release and deployment procedure) presents how to perform the detailed activities for the configuration management or change management or release and deployment processes.

NOTE ISO/IEC 20000-1:2011 (IEEE Std 20000-1:2013) requires that planning for the release and deployment management process be coordinated with the change management process.

The procedures include the following:

a) process implementation;

b) configuration identification and recording;

c) configuration control;

d) configuration status accounting (tracking);

e) configuration evaluation;

f) logging and analysis of the impact of change requests;

g) procedures to verify the completeness and correctness of systems and software releases;

h) Release and deployment management and delivery;

i) management of emergency changes or releases when the normal procedure is insufficient; and

j) how an unsuccessful change or release can be backed out or corrected.

They should include the following:

1) procedures for initial baselining of work products and configuration items;

2) documenting the scope of changes;

3) change control board authority, membership, and procedures for approval or denial of change requests;

4) tracking of changes in progress;

5) updating configuration data; and

6) notifying concerned parties when baselines are first established or later changed.

They may include asset management procedures, such as asset retirement.

### 10.18 Configuration status report

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 7.2.2.2.e), 7.2.2.3.4.1, 7.2.2.3.5.1

ISO/IEC/IEEE 15288:2015 reference: 6.3.2.3.d), 6.3.6.3.b), 6.4.14.3.c), B.1

ISO/IEC 20000-2:2012 (IEEE Std 20000-2:2013) reference 9.1.1, 9.1.4, 9.2.3.3

Generic type: Report

The configuration status report (or change management report, information management report, system release report, or archive report) provides the status of controlled configuration items, including baselines, release identifiers, and location of the item or software master version. For deactivated systems, it contains information about system disposal to trace potential future environmental, safety, or security impacts. It may include the number of changes for a project, version history, number of releases, and comparisons of releases. It may be in the same format as an Audit Report.

### 10.19 Contract

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 6.1.1.2, 6.1.1.3.4.2, 6.1.1.3.4.3, 6.1.2.2, 6.1.2.3.3.1, 6.1.2.3.6.2, 6.4.1.3.2.1, B.3.2.2.1, B.3.2.2.2, B.3.1.2.2, B.3.1.3.2, F.3.3.1.1, F.3.3.1.2, F.3.3.5.1

ISO/IEC/IEEE 15288:2015 reference: 6.1.1.2.c), 6.1.1.3.c), 6.1.2.2.c), 6.1.2.3.c), 6.3.1.3, B.1

ISO/IEC 20000-1:2011 (IEEE Std 20000-1:2013) reference: 5.2, 5.3, 6.1, 7.2

ISO/IEC 20000-2:2012 (IEEE Std 20000-2:2013) reference: 4.2.1, 4.2.5, 4.3.1.1, 4.5.2.3, 4.5.3, 5.2.8, 6.1.3, 6.1.4, 7.2.2, 7.2.3.1, 7.2.4, Table A.14

Generic type: Specification

A contract (or agreement) is the formal agreement between an acquirer and a supplier. Informally, commitments or agreements may be specified between parts of the same organization (sometimes called a memorandum of understanding). A contract or agreement addresses the following:

a) identification of the performing organizations and their responsibilities;

b) statement of work to be performed, with tasks based on a service management process or a systems or software life-cycle model, and scope of tasks;

c) system requirements and software requirements definition and analysis results;

d) negotiated price and payment schedule;

e) deliverables, including documentation, records, and off-the-shelf products identified;

f) schedule for suppliers to deliver the product or service;

g) proprietary rights to systems and technical data and software intellectual property rights: usage, ownership, warranty and licensing rights;

h) provisions for monitoring; reporting, verification, validation, and acceptance criteria; and

i) procedures for contract changes, exceptions, resolving disputes, and closeout, such as supplier responsibilities in the event of expected or early termination of the contract or formal agreement and the transfer of services to another party.

The contract may specify best practices, to include standards and strategies for processes, activities and tasks.

### 10.20 Customer satisfaction survey

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 6.2.5.3.1.4, 7.1

ISO/IEC/IEEE 15288:2015 reference: 6.4.12.3.d)

ISO/IEC 20000-2:2012 (IEEE Std 20000-2:2013) reference: 7.1.3.3, 7.1.4, Table A.8

Generic type: request

The customer satisfaction survey requests opinions on service performance from the customers. Series of surveys may be issued to track trends in customer satisfaction.

### 10.21 Database design description

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 7.1.3.3.1.3, 7.1.4.3.1.3

Generic type: Description

The database design description is the top-level design for databases. It includes the following:

a) database overview and identification;

b) database design (including descriptions of applicable design levels, for example, conceptual, internal, logical, and physical);

c) reference to design descriptions of software used for database access or manipulation;

d) rationale for database design; and

e) database-wide design decisions about its activity from a user's viewpoint, in meeting its functional and performance requirements.

The database detailed design description covers software items used to access or manipulate data. It provides visibility into the design and information needed for database management. It is used as the basis for implementing a database and related software items. It includes the following:

1) a summary of the history of the database development, use and maintenance;

2) the database design at the conceptual, internal, logical and physical levels;

3) identification of each software item used for database access or manipulation;

4) any constraints, limitations or unusual features in the design of the database software items;

5) the types of errors affecting the database and the handling of those errors; and

6) traceability between each database or related software item, and the system or software item requirements.

The database detailed design may specify the following:

i. database access methods;

ii. data entities and their relationships;

iii. security and integrity constraints;

iv. data retention requirements; and

v. expected size of the data elements.

## 10.22 Development plan

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 7.1.1.3.1.3, 7.1.1.3.1.4, 7.1.3.3.1.5

Generic type: Plan

The development plan presents how the organization or project plans to conduct development activities (the software implementation strategy). It includes the following:

a) identification of the objectives and standards to be used in the system or software development process;

b) identification of the systems or software life-cycle model to be used to satisfy the product or service requirements, based on the project's scope, magnitude and complexity;

c) mapping of development process activities and best practices to the selected life-cycle model;

d) schedule, resources, methodology, tools, reuse strategy, action items, roles and responsibilities to be used in development and test;

e) qualification of all requirements, including safety and security;

f) references to separate plans or procedures to address different activities in the development stage or process, such as development process implementation, system requirements analysis, system architecture design, system and software requirements specification, high-level and low-level system or software design, software construction or coding, system element test or software unit test, system or software integration test, system or software qualification test, system or software installation, and acceptance; and

g) identification of notations and naming conventions used in development.

## 10.23 Disposal plan

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 6.4.11.3.1.1

ISO/IEC 20000-1:2011 (IEEE Std 20000-1-2013) reference: 5.2

ISO/IEC 20000-2:2012 (IEEE Std 20000-2-2013) reference: 5.2.8

Generic type: Plan

The disposal plan (or retirement plan or service removal plan) presents how activities are conducted to retire systems or software items or services and related documents. It identifies stakeholders and user organizations or users to be notified of the planned withdrawal from service, replacement systems and services, if any; a schedule for cessation of support. Plans for system disposal or archiving of the software and

documentation should include the removal of sensitive or secured information. It includes the schedules, actions and resources for disassembly or destruction of a system, bringing it into a socially and physically acceptable state in accordance with relevant safety, security, privacy and environmental standards, directives and laws, and avoiding subsequent adverse effects on stakeholders, society and the environment. It considers the associated enabling systems and storage locations.

### 10.24 Documentation plan

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 6.3.6.3, 7.2.1.2, 7.2.1.3.1.1

Generic type: Plan

The documentation plan identifies and specifies the project's documentation (information items). It specifies the purpose, audience, content, structure, media, and format of each document and document set. It identifies the documents and information to be acquired, re-used, or developed, and includes schedule, resources, methodology, tools, content management or reuse strategy for the documentation, action items, and roles and responsibilities, consistent with the information management plan. It includes schedules for document development, review and approval. It identifies who receives or have access to restricted documents. The documentation plan should include the controlling template or standard for each document.

See also: information management plan.

### 10.25 Documentation procedure

ISO/IEC 20000-1:2011 (IEEE Std 20000-1:2013) reference: 4.3.1, 4.3.2

ISO/IEC 20000-2:2012 (IEEE Std 20000-1:2013) reference: 4.1.3.1, 4.3.1.2, 4.3.2

Generic type: Procedure

The documentation procedure (or document management procedure) details how documents are identified, including versions; how they are reviewed and approved, how documents are made available to users; and how stakeholders are notified about new, changed, or archived documents. It describes how documents are controlled to prevent unauthorized change or damage. It applies to printed, electronic, or web-accessible documentation.

NOTE ISO/IEC/IEEE 26513-2009 *Systems and software engineering — Requirements for testers and reviewers of user documentation* provides additional detail on documentation review and approval.

See also: documentation plan, information management plan

### 10.26 Domain engineering plan

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 7.3.1.3.1.1

Generic type: Plan

The domain engineering plan presents how the organization intends to conduct domain engineering procedures and activities. It describes the process for handling change requests.

### 10.27 Evaluation report

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 6.1.2.3.4.5, 6.1.2.3.4.8, 6.1.2.3.4.15, 6.4.2.3.2.1 6.4.3.3.2.1, 6.4.5.3.2.2, 6.4.6.3.1.2, 7.1.2.3.1.2, 7.1.3.3.1.6, 7.1.4.3.1.7, 7.1.5.3.1.5, 7.1.6.3.1.5, 7.1.7.3.1.3

ISO/IEC/IEEE 15288:2015 reference: 6.2.3.3.a)7), 6.2.4.3.a)1, 6.3.5.3.e), 6.3.8.2.d), 6.3.8.3.d), 6.4.3.3.e), B.1

ISO/IEC 20000-1:2011 (IEEE Std 20000-1-2013): 6.3.3, 6.6.2

ISO/IEC 20000-2:2012 (IEEE Std 20000-2-2013) reference: 5.5, 6.3.4.3, 6.3.5, 9.2.3.2, 9.2.4, 9.3.4

Generic type: Report

The evaluation report provides results of reviews and evaluations, such as a risk assessment, quality assurance evaluation, or an evaluation of project portfolios, design constraints, candidate architectures, suppliers, customer satisfaction, effectiveness of security controls, analysis of change records or change requests, personnel needs, measurement needs or financial variances. It includes evaluation criteria. Evaluations may be based on criteria

of traceability, consistency, testability, risk reduction, usability and customer satisfaction, and feasibility. The report provides information and recommendations to assist future decision-making, and it may indicate trends and recommendations for future comparable situations. For software configuration management evaluations, the report provides information about functional completeness of the software items against their requirements and the physical completeness of the software items (whether their design and code reflect an up-to-date technical description).

See also: audit report, monitoring and control report, progress report, review minutes, service report, validation report, and verification report.

### 10.28 Implementation procedure

ISO/IEC/IEEE 15288:2015 reference: 6.4.4.3.b) Generic type: Procedure

The implementation procedure details how the system or system elements are produced to satisfy the design requirements. Implementation procedures may address system hardware and software configuration; software creation and compilation, and operational readiness.

See also: operational test procedure, training documentation

### 10.29 Improvement plan

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 6.2.1.3, 6.3.4.3.1.5

ISO/IEC/IEEE 15288:2015 reference: 6.2.1.3

ISO/IEC 20000-1:2011 (IEEE Std 20000-1:2013) reference: 4.5.5.1, 4.5.5.2

ISO/IEC 20000-2:2012 (IEEE Std 20000-2:2013) reference: 4.5.5.1, 4.5.5.2, 6.1.3.1, 6.1.4, 9.2.3.3

Generic type: Plan

The improvement plan (which may include the improvement policy) presents how the organization plans to improve a service (service improvement plan) or process (process improvement plan). The improvement should be linked to organizational objectives. The Improvement Policy may be included in the Improvement Plan or as a separate set of policies.

The improvement policy expresses the organization's commitment to improving its services or products by making them more effective and efficient. Following the 'Plan-Do-Check-Act' methodology for continual improvement, the policy outlines how opportunities for improvement are evaluated and how improvement is incorporated into plans for specific processes and services. It identifies roles and responsibilities for improvement activities.

The plan includes how processes are reviewed, and recommended improvements and change requests are identified, recorded, prioritized, authorized, performed, measured, assessed, and communicated. The improvement plan references baseline documentation of the process or service level to be improved and may specify a service or process improvement target (new level). The improvement plan identifies what information items (policies, procedures, and plans) need to be updated to reflect the improved process or service. The improvement plan may include an assessment of the organizational culture and managers' attitudes and ability to adapt; the available resources, facilities, and tools; and financial constraints on the improvement project.

NOTE ISO/IEC TR 33014:2013 Information technology — Process assessment —Guide for process improvement provides additional guidance.

### 10.30 Improvement procedure

ISO/IEC 20000-1:2012 reference: 4.5.5.1

ISO/IEC 20000-2:2012 reference: 4.5.5.2

Generic type: Procedure

The improvement procedure presents how improvements are identified, recorded, evaluated, prioritized, authorized, performed, measured, assessed, and reported, to improve a management system, service (service improvement procedure) or process (process improvement)

## 10.31 Incident management procedure

ISO/IEC 20000-1:2011 (IEEE Std. 20000-1:2013) reference: 6.6.3, 8.1

ISO/IEC 20000-2:2012 (IEEE Std. 20000-2:2013) reference: 6.6.6, 8.1.2, 8.1.3.1, 8.1.4, 8.1.5

Generic type: Procedure

The incident management procedure (or service request management procedure or security incident management procedure) defines how to receive, record and update, classify and assign responsibility, prioritize, escalate, resolve, and close incidents or service requests, including security incidents; and how to provide feedback. It includes the definition of what constitutes a service request or an incident, a major incident, and a problem. It covers action initiation, assignment of a responsible individual for major incidents, notification, trend analysis, status tracking and reporting, and incident records management. It includes a procedure to help ensure that all security incidents are investigated and receive management response.

See also: problem management procedure

## 10.32 Incident report

ISO/IEC 20000-1:2011 (IEEE Std. 20000-1:2013) reference: 6.6.2, 6.6.3

ISO/IEC 20000-2:2012 (IEEE Std. 20000-2:2013) reference: 6.6.3.4, 6.6.4, 8.1.5

Generic type: Report

The incident report or security incident report, addresses performance in resolving issues, statistical reports on incident processing, issues or non-conformance (deviance) with service level agreements or contract requirements, and reported customer concerns, links to customer complaints or problems, and improvements made in response to incidents. The report may be a compilation or analysis of incidents or complaints.

It should include information for future reference to prevent problems (lessons learned) and identify a duplication of issues and trends.

It may include the following:

a) reporting control number and related control information;

b) identification of the incident reporter;

c) date and time of incident occurrence, escalation, resolution, and closure;

d) location (environment) of the incident in the system, software or information configuration item;

e) applicable contract provision or conformance requirement;

f) cause, nature, and impact (severity) of the incident;

g) immediate corrective action recommended or performed;

h) opportunities for improvement, related action items, the responsible person or organization, and the due date;

i) references to similar incidents, previously reported problems, and known errors;

j) responsible person or organization, along with appropriate confirmation showing approval and implementation of the solution;

k) incident closure information; and

l) information from organizational (internal) reviews.

NOTE ISO/IEC 20000-1:2011 (IEEE Std 20000-1:2013) and ISO/IEC 20000-2:2012 (IEEE Std 20000-2:2013) distinguish between incidents and problems. An incident response deals with the restoration of service to the users, whereas a

problem resolution is concerned with identifying and removing the causes of incidents. An opportunity report is similar, but includes analysis of potential positive events.

See also: change request, incident (record), problem report, service request (record)

## 10.33 Information management plan

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 6.2.3.3.3.2, 6.2.4.3.4.1, 6.2.4.3.4.5, 6.3.6.3.1, 6.3.6.3.2.5, 7.2.4.3.2.5

ISO/IEC/IEEE 15288:2015 reference: 6.2.6.3.a), 6.3.6.1, 6.3.6.3.a)

Generic type: Plan

The information management plan (or documentation management plan or knowledge management plan) presents how the project or service provider plans to conduct information management or knowledge management activities during the life cycle. It includes the following:

a) descriptions of the process and activities for authorizing, developing, reviewing, storing, communicating, and maintaining knowledge or information in electronic and printed media;

b) identification of the information to be acquired, re-used, produced, and maintained;

c) resources, methodology, tools, action items, and roles and responsibilities, consistent with the overall project management plan;

d) provisions for content management or reuse strategy and version control (document configuration management);

e) schedules for information development, review, and approval;

f) who may receive or have access to restricted information; and

g) the organizational policy and process for retention or disposal of information and records after project closure.

The knowledge management plan includes the knowledge taxonomy (classification schema), definition of the infrastructure to control and retrieve knowledge assets, and training to support the contributors and the users of the organization's knowledge assets, the and the asset retention criteria.

See also: documentation plan

## 10.34 Information management procedure

ISO/IEC 20000-1:2011 (IEEE Std 20000-1:2013) reference: 4.3.3

ISO/IEC 20000-2:2012 (IEEE Std 20000-2:2013) reference: 4.3.3, 4.4.2.2, 6.1.3.4, Table A.11

Generic type: Procedure

The information management procedure (or records management procedure) details how information, such as content or records, is managed and controlled. It includes procedures to identify, update, store, retrieve, and archive or remove information.

See also: documentation procedure

## 10.35 Information security plan

ISO/IEC 20000-2:2012 (IEEE Std 20000-2:2013) reference: 6.6.2, 6.6.3.2, 6.6.4, Table A.14

Generic type: Plan

The information security plan includes the following:

a) description of how the organization identifies, controls, and protects the physical and logical security of

systems, assets, and information;

b) description of how requirements for confidentiality, integrity, and availability of information are implemented;

c) description of how the system or service denies unauthorized access, permits authorized access, secures data in transmission, storage, and processing; and provides security in a cost-effective manner;

d) description of security risks and related controls, including access controls, and how security controls are operated and maintained;

e) description of systems monitoring, monitoring to detect security incidents, and security trends analysis;

f) specific procedures for the protection of sensitive personal data and security-classified data, investigation of security problems, and reporting; and

g) procedures for analyzing the effectiveness of information security policy, procedures, and activities.

NOTE ISO/IEC 27002:2013, *Information technology — Security techniques — Code of practice for information security* controls provides guidelines for information security management. ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements* addresses the Information Security Management System (ISMS) processes for establishing, implementing, operating, monitoring, reviewing, maintaining and improving information security.

### 10.36 Information security policy

ISO/IEC 12207:2008 (IEEE Std 12207-2008): reference 6.1.2.3.4.5 l)

ISO/IEC 20000-1:2011 (IEEE Std 20000-1:2013) reference: 6.6.1

ISO/IEC 20000-2:2012 (IEEE Std 20000-2:2013) reference: 6.6.2, 6.6.3.1, 6.6.4, Table A.7

Generic type: Policy

The information security policy includes the following:

a) the organization's commitment to identify, control, and protect the physical and logical security of information and systems used to store, transmit, and process information;

b) objectives for preserving the confidentiality, integrity, and availability of information;

c) rules for need-to-know and access-to-information at each project organization level;

d) methodology for managing information security risks;

e) approach for establishing, documenting, and monitoring security controls, including audits;

f) approach for information security training and awareness for employees and customers.

NOTE The ISO/IEC 27000 series includes detailed requirements for information security, including detection and recovery from intrusions.

### 10.37 Information security procedure

ISO/IEC/IEEE 15288:2015 reference: 6.4.12.3.a)

ISO/IEC 20000-1:2011 (IEEE Std 20000-1:2013) reference: 6.6.2, 6.6.3

ISO/IEC 20000-2:2012 (IEEE Std 20000-2:2013) reference: 6.6.4, Table A.9

Generic type: Procedure

The information security procedure details how the organization controls and protects the physical and logical security of information and systems used to store, transmit, and process information. Procedures cover how

the organization establishes, documents, and monitors security controls. It includes how the organization manages information security threats, events and incidents. It includes how the organization protects sensitive and personally identifiable information.

See also: incident management procedure

### 10.38 Installation plan

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 6.4.7.3.1.1

Generic type: Plan

The installation plan provides the approach for installing a configuration item in its target environment. It includes software and hardware prerequisites, problems resolved, workarounds for unresolved problems, provisions for user training, conversion from existing systems, an installation checklist, and installation instructions. It provides a point of contact for questions relating to the installation, supporting material and any issues concerning security, safety and privacy. For software installation, it provides information on software application and database initialization, execution, and termination.

### 10.39 Installation report

ISO/IEC/IEEE 15288:2015 reference 6.4.10.3.c), B.1

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 6.4.7.3.1.2

Generic type: Report

The installation report (or transition report) provides results of the installation, including the related events, installation location, version being installed, installation dates, and completed installation checklist.

### 10.40 Integration and test report

ISO/IEC/IEEE 15288:2015 reference: 6.4.7.3.b), 6.4.8.2.g), 6.4.9.3.c), B.1

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 6.4.5.3.1.1, 7.1.6.3.1.2

ISO/IEC 20000-2:2012 (IEEE Std 20000-2:2013) references: 6.3.5, 9.3.3.4, 9.3.4

Generic type: Report

Based on the system or software requirements, the integration and test report (or service continuity and availability test report, or verification report, or implementation report) presents the results from implementation or integration and testing of the system, which may include software components or software combined with the hardware configuration items and manual operations. The results should demonstrate conformance with the test plan and item requirements and the integration of items into the next version of the integrated baseline. It includes an item identification, date of testing, integration and test requirements and criteria, test identifier, overview of results, detailed results, and rationale for decisions. It describes problems encountered and deviations from the planned procedures.

### 10.41 Integration plan

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 7.1.6.3.1.1, 7.1.6.3.1.2, 7.1.6.3.1.5

Generic type: Plan

The integration plan (or implementation plan) describes the strategy (approach) for implementation, integration or assembly of system elements, including provision of facilities, tools and resources and preparation for integration testing. For systems. The implementation plan defines the scheme of actions, timing and resources governing the build, buy or reuse actions that make available a system element ready for system assembly. It defines the tasks for the design of system elements; the fabrication processes and constraints appropriate to the selected fabrication medium, technology, enabling systems, tools and equipment. For software, the integration plan defines how the software units and components are linked or combined to form the deliverable software item. It includes traceability to the system or software requirements. It includes or references the test plan with test requirements and test procedures.

NOTE In service management, an implementation plan can be prepared for the project of implementing a new service or improving an existing service, as described in ISO/IEC TR 20000-5: 2010.

See also: Improvement plan

### 10.42 Interface description

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 6.3.5.3.2.2, 6.4.3.2.d), 7.1.3.3.1.2, 7.1.4.3.1.2

ISO/IEC/IEEE 15288:2015 reference: 6.4.4.3.c), 6.4.4.3.d), 6.4.5.2.d), 6.4.5.3.d), B.1

ISO/IEC 20000-1:2011 (IEEE Std 20000-1:2013) reference: 4.5.2, 5.2, 7.2, 9.1

ISO/IEC 20000-2:2012 (IEEE Std 20000-2:2013) reference: 4.2.4, 4.5.2.4, 5.2.8.h), 7.2.4

Generic type: Description

The interface description describes the interface characteristics of one or more systems, subsystems, domains, hardware items, software items, manual operations (processes) or other system components. It presents interface characteristics, including systems or configuration items performing the interface (including human-system and human-human interfaces), standards and protocols, responsible parties, information or data records transmitted by the interface, interface operational schedule, and error handling. It includes interface diagrams to depict the interfaces. It should define existing or permanent interface characteristics and those that are being developed or modified.

### 10.43 Life-cycle policy and procedure

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 6.2.1.1, 6.2.1.2, 6.2.1.3.1.1, 6.2.1.3.3.1, A.2.3.1

ISO/IEC/IEEE 15288:2015 reference: 6.2.1.1, 6.2.1.2.a), 6.2.1.3.a), A.2.3, B.1

Generic type: Policy, Procedure

The life-cycle policy and procedure includes high-level policy guidance and specific steps to select, tailor, and implement a life-cycle model in a project. It defines roles, responsibility, accountability, and authority for life-cycle process management, including process improvement. It identifies the criteria for entering and completing each life-cycle stage. It identifies and describes the organization's processes to be applied in projects.

### 10.44 Maintenance plan

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 6.1.1.3.1.7, 6.4.10.1, 6.4.10.3.1.1, 7.3.2.3.3.6

ISO/IEC/IEEE 15288:2015 reference: 6.4.10.3

Generic type: Plan

The maintenance plan presents how the organization or project plans to meet systems availability requirements and conduct maintenance (logistics) activities. It includes the following:

a) the objectives, strategy, and approach for the systems or software maintainer to resolve problems, update the system and test new updates;

b) criteria for performing maintenance;

c) the approach to the following activities: maintenance process implementation (how to request maintenance); problem and modification analysis; modification implementation; maintenance update, review, and acceptance; migration; and software retirement;

d) the outputs of the maintenance process;

e) the resources (for example, facilities, software, hardware, tools, and personnel) needed to perform all aspects of maintenance, and the interrelationships among resources;

f) scheduled periods for performing maintenance; and

g) special procedural requirements during maintenance (for example, security, access rights, and documentation control).

It should identify the specific standards, methods, tools, and responsibilities for scheduled and preventive maintenance activities.

### 10.45 Maintenance procedure

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 6.4.10.3.1.1

ISO/IEC/IEEE 15288:2015 reference: 6.4.10.3

ISO/IEC 20000-2:2012 (IEEE Std 20000-2:2013) reference: Generic type: Procedure

The maintenance procedure covers the processes for performing preventive and corrective maintenance, and providing customer support feedback to the users. It should identify the specific standards, methods, tools, and responsibilities for maintenance activities. It may identify systems or software areas that could change and needs for training. Maintenance procedures for systems cover the disassembly strategy, fault diagnosis techniques, and re-assembly and testing sequences. Maintenance procedures for software include procedures for archiving, backup, and recovery.

See also: problem management procedure

### 10.46 Measurement plan

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 6.3.7.2.c), 6.3.7.3.1.1, 6.3.7.3.1.3, 6.3.7.3.1.4, 6.3.7.3.2.1

Generic type: Plan

The measurement plan identifies the needs and requirements for measurement in an organization, project, or service. It identifies the selected measures and the data collection, storage, analysis, and reporting procedures. It defines how the process and the measurements are evaluated. Items to be measured include the achievement of service targets, customer satisfaction, resource utilization, major issues, and trends.

### 10.47 Measurement procedure

ISO/IEC/IEEE 15288:2015 reference: 6.3.7.3.a)5)

Generic type: Plan

The measurement procedures define how to obtain measurements in an organization, project, or service, or how the measurements are analyzed and evaluated. Items to be measured may include the achievement of technical performance or service targets, customer satisfaction, and resource utilization.

### 10.48 Monitoring and control report

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 6.1.2.3.4.8, 6.1.2.3.4.15, 6.3.2.3, 6.3.4.3.3.4, 6.3.4.3.6.3, 6.3.7.1, 6.3.7.3.2.4, 7.3.2.3.3.5, 7.3.2.3.3.7

ISO/IEC/IEEE 15288:2015 reference: 6.2.5.3.c), 6.3.2.3.b)10), 6.3.4.3.b), 6.3.7.1, 6.3.7.3.b), 6.4.12.3.b), B.1

ISO/IEC 20000-1:2011 (IEEE Std 20000-1:2013) reference: 6.3.3

ISO/IEC 20000-2:2012 (IEEE Std 20000-2:2013) reference: 6.1.4, 6.3.5

Generic type: Report

The monitoring and control report provides monitoring results. It may include the following:

a) a history of all monitoring results and control actions and results of individual monitoring audits;

b) measurements of processes and services against objectives and requirements;

c) monitoring the progress of technical performance, risk mitigation, cost and schedules; and reporting of project status;

d) actions taken to correct deficiencies in service availability and continuity;

e) an analysis of the effects of risks on the achievement of system quality, timeliness and profitability; and

f) results of asset reuse, including information on the original developer or owner of the asset, cost of reusing the asset, and savings and benefits derived from reusing the asset.

### 10.49 Operational test procedure

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 6.4.9.3.1.3, 6.4.9.3.2.2

Generic type: Procedure

The operational test procedure defines how to test a system or software before its operational release, in its intended environment. It includes acceptance criteria, version identification of the system or software being tested, test data, and post-test analysis procedure to help ensure testing occurred as planned. It explains use of the organization's problem resolution procedure.

See also: qualification test procedure

### 10.50 Problem management procedure

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 6.2.1.3.2.1, 6.4.9.3.1.2, 6.4.9.3.1.3, 7.2.8.3.1.1

ISO/IEC 20000-1:2011 (IEEE Std 20000-1:2013) reference: 8.2

ISO/IEC 20000-2:2012 (IEEE Std 20000-2:2013) reference: 8.2.2, 8.2.3, 8.2.4

Generic type: Procedure

The problem management procedure defines how to receive, record, classify and assign, prioritize, escalate, resolve, and close problems; how to control and minimize or avoid the impact of problems; and how to provide feedback. It includes the definition of what constitutes a major problem or an incident. It covers action initiation, notification, root cause analysis, trend analysis, status tracking and reporting, and problem records management. It may include the policy for prioritizing, investigating, and resolving problems.

See also: incident management procedure

### 10.51 Problem report

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 6.1.2.3.4.15, 6.3.2.3.2.1, 6.3.3.3.1.3, 6.3.3.3.3.1, 6.4.8.2, 6.4.8.3.1.1, 6.4.8.3.1.3, 6.4.9.3.1.3, 6.4.9.3.4.2, 6.4.9.3.5.2, 6.4.10.3.1.2, 6.4.10.3.2.1, 6.4.10.3.2.4, 7.1.1.3.1.2, 7.2.8.2.f), 7.2.8.3.1.1, 7.2.8.3.2.1, 7.3.1.3.1.3, 7.3.2.3.3.6, 7.3.3.3.5.3, B.3.2.3.2

ISO/IEC/IEEE 15288:2015 reference: 6.3.3.3.a)2), 6.4.8.3.b), 6.4.9.2.d), 6.4.10.1, 6.4.10.3.c), 6.4.11.3.c), 6.4.12.3.c), B.1

ISO/IEC 20000-1:2011 (IEEE Std 20000-1:2013) reference: 8.2

ISO/IEC 20000-2:2012 (IEEE Std 20000-2:2013) reference: 8.2.4

Generic type: Report

The problem report (also called non-conformance report or corrective action request) reports problems or non-conformance (deviance) with contract requirements. It may be a consolidation of problem records. It serves as input to the ISO/IEC 12207:2008 (IEEE Std 12207-2008) problem resolution process.

It should include information for future reference to prevent problems (lessons learned) and identify a duplication of issues and trends.

It may include:

a) a problem reporting control number and related control information;

b) identification of the problem reporter;

c) the date and time of problem occurrence, escalation, resolution, and closure;

d) location (environment) of the problem in the system, software or information configuration item;

e) applicable contract provision or conformance requirement;

f) cause, nature, and impact (severity) of the problem;

g) problem analyses and decisions, solution or corrective action recommended;

h) related action items, the responsible person or organization, and the due date;

i) references to similar problems previously reported;

j) responsible person or organization, along with appropriate confirmation showing approval and implementation of the solution;

k) problem closure information; and

l) information from organizational (internal) reviews.

For problems occurring during testing or operation, it should include the inputs, expected results, actual results, anomalies, date and time, procedure step, environment, attempts to repeat the problem, and observers. It may report a temporary or permanent solution to a problem.

NOTE ISO/IEC 20000-1:2011 (IEEE Std 20000-1:2013) and ISO/IEC 20000-2:2012 (IEEE Std 20000-2:2013) distinguish between incidents and problems. An incident response deals with the restoration of service to the users, whereas a problem resolution is concerned with identifying and removing the causes of incidents. An opportunity report is similar, but includes analysis of potential positive events.

See also: change request, incident report, problem record.

### 10.52 Process assessment procedure

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 6.2.1.3.2.1

Generic type: Procedure

The process assessment procedure describes how to conduct life-cycle process improvement and how to evaluate the suitability and effectiveness of organizational processes. It may include assessment goals.

### 10.53 Process improvement report

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 6.2.1.3.3.2, B.3.3.1.2, B.3.3.2.2, B.3.3.3.2, 6.3.7.3.3

ISO/IEC/IEEE 15288:2015 reference: 6.2.1.3 c), B.1

Generic type: Report

Based on historical, technical and evaluation data, the process improvement report presents the results of process improvement activities, recommended changes, and technology advancement needs. It may include quality cost data to improve an organization's processes and to determine the cost of quality.

### 10.54 Product need assessment

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 6.1.1.2, 6.1.1.3.1.1

ISO/IEC/IEEE 15288:2015 reference: 6.4.2.1, 6.4.2.2.d), 6.4.2.3.b)

Generic type: Report

The product need assessment is used to obtain consensus among an acquirer, developer, and support and user organizations on the demand for a proposed system. It may focus on communicating the user's needs to a developer or a developer's ideas to a user and other stakeholders. It includes the following:

a) the decision and rationale to acquire, develop, or enhance a system, software product or service; and

b) description of a proposed system in terms of user needs to be fulfilled, the system's relationship to existing or planned systems or procedures, and the way the system should be used (the concept of operations).

The product need assessment may include the following:

1) analysis of improvements, disadvantages and limitations, and considered alternatives and tradeoffs;

2) assessments for technical, strategic, economic and market bases, and trade-off studies;

3) preliminary information on system requirements, system prototypes, possible system employment, possible support concepts

4) preliminary information on contract type;

5) current and potential organizational responsibilities; and

6) risk identification and risk management methods.

See also: concept of operations

### 10.55 Progress report

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 6.1.2.3.4.15, 6.3.2.2, 6.3.2.3.1.1, 6.3.2.3.2.2, 6.3.3.2, 6.3.3.3.3.1, 6.3.3.3.3.1

ISO/IEC/IEEE 15288:2015 reference: 6.2.3.3.a)7), 6.3.2.2.f), 6.3.2.3.b)6), B.1

Generic type: Report

The progress report provides results of monitoring the execution of the defined plan or processes for internal or external distribution. It includes a summary of decisions, monitoring results, action items, process or performance data, and recorded process improvements. It assesses the degree of adherence to the plans. It provides information about projected cost, performance, and schedule risks; any changes to previously approved plans and the related impact to the project or organization; corrective actions; risk treatment actions; and problem tracking and problem analysis.

See also: service report

### 10.56 Project management plan

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 6.1.1.3.4.3, 6.1.2.3.4.3, 6.1.2.3.4.5, 6.1.2.3.4.6, 6.2.2.3.1.2, 6.2.3.3.1.6, 6.2.3.3.2.1, 6.3.1.1, 6.3.1.2, 6.3.1.3.2.1, 6.3.1.3.3.3, 6.3.2.3.2.1, 6.2.3.3.1.6, 7.2.6.3.1.1, 7.2.6.3.2.1, F.3.3.5.3

ISO/IEC/IEEE 15288:2015 reference: 6.2.3.3.a.8, 6.3.1.1, 6.3.1.2, 6.3.1.3, 6.3.2.3.a), B.1

Generic type: Plan

The project management plan presents how the project processes and activities are executed to assure the project's successful completion, and the quality of the deliverable product or service. It includes the following:

a) identification of the selected system or software life-cycle model to satisfy contractual requirements, and mapping of processes, activities and tasks to the selected life-cycle model;

b) the project's organizational structure, showing authority and responsibility of each organizational unit, including external organizations and responsibilities of acquirers, suppliers, and users;

c) requirements for resource needs and the acquirer's involvement in providing resources;

d) the expected acquirer involvement in joint reviews, audits, informal meetings, reports, change requests, implementation, approval, acceptance, and access to facilities;

e) the expected user involvement in requirements specification, reviews, and evaluations;

f) security policies for the control of access to systems and software items, project information, data, and infrastructures;

g) the means of reporting and the documents and information items to be delivered;

h) other plans to be produced as separate documents during the project; and

i) risks and risk analysis for technical, cost, and schedule risks.

It should include a Work Breakdown Structure (WBS) of the life-cycle processes and activities, including the products, services, and non-deliverable items to be provided, such as establishing the project infrastructure.

It may include the following:

1) procedures for re-planning;

2) options for developing the product or providing the service and an analysis of the risks associated with each option;

3) plans for subcontractor management, including subcontractor selection and involvement between the subcontractor and the acquirer, if any; and

4) plans for project closeout, including debriefings of project personnel and staff reassignment, archiving project materials, and preparation of a final report to include lessons learned and analysis of project objectives achieved.

NOTE 1 In addition to projects, management plans can be prepared for programs, organizations, processes, including the portfolio management process.

NOTE 2 Depending on the project, the project management plan can be called a project technical management plan, systems engineering management plan (SEMP) or software development plan (SDP).

NOTE 3 ISO/IEC/IEEE 16326-2009 *Systems and software engineering — Lifecycle processes — Project management*, provides extensive detail on the contents of the project management plan.

See also: service management plan

### 10.57 Proposal

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 6.1.2.2.b), B.3.2.1.2

ISO/IEC/IEEE 15288:2015 reference: 6.1.1.3, 6.1.2.2.b), 6.1.2.3.b), B.1

Generic type: Description

The proposal is information prepared by a potential supplier to support the offer of a contract bid, including cost, schedule, risk statements, methodology to satisfy the Request for Proposal (RFP), experiences and capabilities, any recommendations to tailor the RFP or contract, and the signature of the supplier's approving authority. Informally, proposals may be prepared within an organization, such as for software reuse.

### 10.58 Qualification test procedure

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 6.1.1.3.6.1, 6.1.1.3.6.2, 6.4.5.3.2.1. 7.1.6.3.1.4, 7.2, 7.3.2.1

Generic type: Procedure

The qualification test procedure (acceptance procedure) documents how acceptance review and testing of a deliverable product or service is conducted, and the conditions to be satisfied before acceptance. The acceptance procedure is initially prepared by the acquirer consistent with the Acquisition Plan. The qualification test procedure provides a set of tests so that each qualification requirement is addressed for the system or software items. It includes mapping of requirements to qualification tests and overall requirements to perform qualification testing, test objectives, test criteria, test configurations, preparations, test cases (inputs, steps, and outputs), expected results, and post-test analysis procedures.

## 10.59 Qualification test report

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 7.1.7.3.1.1, 7.1.7.3.1.3, 7.2.7.3.2.1.

Generic type: Report

The qualification test report indicates that the system was tested for conformity with each system requirement, produced the expected results, and is feasible to operate and maintain. It provides the results of each qualification test and states whether all requirements were satisfied. It includes system identification and overview, qualification requirements and criteria, overview of results, identification of items tested and dates of testing, detailed results, problems encountered, and rationale for decisions.

## 10.60 Quality management plan

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 6.1.2.3.4.3, 6.2.5.3.1.5, 6.3.1.3, 7.2.3.3.1.3

ISO/IEC/IEEE 15288:2015 reference: 6.2.5.3.a), 6.2.5.3.c)

Generic type: Plan

The quality management plan (or quality assurance plan) presents the approach to fulfil the quality objectives of the organization, program, project, product or service. It includes the following:

a) the project or organization's quality objectives and the organization’s quality policies;

b) product or service improvement plans;

c) product and service assessment plans, with assessment requirements, criteria, responsibilities, and allocations to standards,

d) methods, procedures or tools needed for quality management;

e) identification of required records of the quality activities and tasks, as well as records of problems and problem resolutions;

f) the configuration management of quality-related records;

g) specific reviews, assessments and audits to be performed, with references to the associated testing, verification, validation, problem reporting, and corrective action processes;

h) assessment of configuration control practices for systems or software configuration items and media; and

i) required coordination of software quality assurance activities with other project activities.

NOTE ISO 9001:2015 contains requirements for life-cycle planning as part of a quality management system. See also ISO 1005, *Quality management systems – Guidelines for quality plans*.

## 10.61 Quality management policy and procedure

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 6.2.5.2, 6.2.5.3.1.1

ISO/IEC/IEEE 15288:2015 reference: 6.2.5.2.a), 6.2.5.3.a), 6.3.8.2.a), B.1

Generic type: Policy, Procedure

The quality management policy and procedure (or quality assurance procedure) defines the framework for establishing and reviewing quality objectives. It explains how quality objectives are met and expresses the personal contribution of all involved to the quality of the product or service. The quality procedure details how the quality aspects of the program, product or service are performed. It includes procedures for contract reviews, inspections, assessments, reviews and audits. It addresses procedures for the tasks of testing, problem reporting, process improvement, and corrective action; as included in the quality management, quality assurance, software audit, verification, validation, and process improvement processes.

NOTE Quality management policy can be included in the quality management plan or quality management procedures or in a separate set of policies.

## 10.62 Release plan (and policy)

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 6.4.10.3.5.2, 6.4.11.3.2.1

ISO/IEC/IEEE 15288: 6.4.10.3.a)

ISO/IEC 20000-1:2011 (IEEE Std 20000-1:2013) reference: 9.3

ISO/IEC 20000-2:2012 (IEEE Std 20000-1:2013) reference: 9.3.3.1, 9.3.3.2, 9.3.4

Generic type: Plan

The release plan (or transition plan, deployment plan, migration plan, or roll-out plan) presents how a system, service, or software product or software release is transitioned to a new environment, with the release dates and schedule.

A release management plan provides overall direction for release planning, including coordination with configuration management and change management, and identification of standard types of releases routinely performed. A specific release plan includes the applicable details for a specific release. The release plan includes the following:

a) the deliverables, including updates to related SLA, operational procedures, and user documentation;

b) the related change requests, identified configuration items, known errors, and problems;

c) identified risks, potential problems;

d) plans for reversing or correcting an unsuccessful release (contingency back-out plan); and

e) how the release is authorized, scheduled, coordinated, and tracked.

The migration plan includes the following:

1) the description of deliverables;

2) dependencies and scheduled dates;

3) the expected configuration of the target environment at the time of migration;

4) the back-out or recovery plans;

5) verification and acceptance procedures; and

6) communications with and training for the customer and support staff.

It should include planning for decommissioning of replaced systems or services.

A release policy may be included in a release and deployment management plan or as a separate set of policies.

The release policy establishes the following:

i. the expected frequency and types of releases, including emergency releases;

ii. authority for the release into acceptance test and production environments;

iii. schema for uniquely identifying a release and its contents;

iv. the approach for grouping changes and configuration items into a uniquely identified release and versions;

v. approach for automating releases; and

vi. approach for verifying (testing) and accepting the release.

See also: configuration management plan and policy, configuration management procedure (release procedure).

### 10.63 Request for proposal (RFP)

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 4.24, 4.36, 6.1.1.3.1.10, 6.1.1.3.1.11, 6.1.1.3.2.1, 6.1.2.2, 6.1.2.3.2.1, 6.1.2.3.2.3, 6.4.1.3.2.1

ISO/IEC/IEEE 15288:2015 reference: 6.1.1.2.a), 6.1.1.3.a)2), B.1

Generic type: Request

The request for proposal (RFP) is the acquirer's request for information and commitments needed from the supplier that are required to be included in the potential supplier's proposal. It announces the acquirer's intention to potential bidders to acquire a specified system, software product or software service. It includes the following:

a) the stakeholders' system requirements;

b) scope statement;

c) bidder instructions;

d) the scope of tasks to be referenced in the draft contract;

e) deliverable product list;

f) terms and conditions;

g) contract milestones (for example, review and audit of supplier progress);

h) control of subcontracts;

i) procedural and technical constraints (for example, target environment); and

j) supporting processes and their performing organizations, including responsibilities (if other than supplier), so suppliers can, in their proposals, define the approach to each of the specified supporting processes.

It may outline the supplier selection criteria.

NOTE Actual contents depend upon the legal environment. Also known as acquisition requirements, acquisition document, call for proposals (CFP), invitation to tender (ITT), request for tender.

### 10.64 Resource request

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 6.3.1.3.3.2

ISO/IEC/IEEE 15288:2015 reference: 6.3.1.3.c)2)

A request for resources arises from project or service planning and is directed to management who can commit the resources and, if necessary, approve modifying the contract.

### 10.65 Reuse plan

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 7.3.3.1, 7.3.3.3.2.1, 7.3.3.3.3.3, 7.3.3.3.4.1, 7.3.3.3.4.2, 7.3.3.3.4.3, 7.3.3.3.5.2

Generic type: Plan

The reuse plan presents how activities are conducted to support the reuse of systems or software assets and related documents. It defines the reuse strategy, domains where reuse is managed, and the implementation approach, including infrastructure support.

### 10.66 Review minutes

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 6.1.2.3.4.15, 6.4.10.3.5.6, 7.2.6.2, 7.2.6.3.1.5

ISO/IEC/IEEE 15288:2015 reference: 6.2.3.3.c)1), 6.3.7.3.b)4)

ISO/IEC 20000-1:2011 (IEEE Std 20000-1:2013) reference: 4.5.4.1, 4.5.4.3, 6.1, 7.1, 7.2

ISO/IEC 20000-2:2012 (IEEE Std 20000-2:2013) reference: 4.1.1.2, 4.1.2.1.f), 6.1.4, 7.1.4, 7.2.4, 8.2.4.f)

Generic type: Report

The review minutes (or joint review minutes or service review minutes) provide a report of a review, such as a meeting between the acquirer and the supplier or the service provider and the customer. Minutes include attendees, agenda, product or service under review, objectives, entry and exit points for the review, main discussion topics, assumptions, presentation material, decisions relating to resources and improvement of the service management system and services, approvals, action items and their status and closure criteria. Minutes document the evaluation of status and conformity of products and services, and activities and schedule status. Minutes include problems found and their resolution or anticipated resolution.

### 10.67 Risk action request

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 6 3.4.3.2.3, 6.3.4.3.4.1

ISO/IEC/IEEE 15288:2015 reference: 6.3.4.3.b)2), B.1.

Generic type: Request

The risk action request is submitted from the project or service management organization to the stakeholders. It includes recommended alternatives for risk treatment.

### 10.68 Risk management policy and plan

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 6.3.4.3.1.1, 6.3.4.3.1.2, 6.3.4.3.2.1

ISO/IEC/IEEE 15288:2015 reference: 6.3.4.3.a)

Generic type: Plan, policy

The risk management policy and plan presents the conditions under which risk management is performed and the context of risk management, such as management and technical objectives, assumptions, and constraints. It defines the approach to the identification, assessment, treatment (including avoidance, mitigation, and contingency plans), and monitoring of risks, as well as the approach for registering risks, creating and maintaining risk profiles (records), and reporting risk status. It establishes risk categories and risk assessment criteria. It identifies the risks to service continuity and availability.

NOTE ISO/IEC 16085:2006, *Systems and software engineering — Life cycle processes — Risk management*, provides additional guidance.

### 10.69 Service catalog

ISO/IEC 20000-1:2011 (IEEE Std 20000-1:2013) reference: 4.3.1, 5.3, 6.1

ISO/IEC 20000-2:2012 (IEEE Std 20000-2:2013) reference: 4.3.1.1, 6.1.3.2, 6.1.3.3, 6.1.3.4, 6.1.4

Generic type: Description

The service catalog describes the information technology services available for customers, with the dependencies between services and service components. For each service, it defines the service; identifies those responsible for providing the service; includes the schedule of service availability and unavailability, access control provisions and security arrangements, and contact points for requesting assistance or reporting incidents. It summarizes target service levels as further specified in the service level agreement (SLA).

See also: complaint procedure, risk management plan.

### 10.70 Service continuity and availability plan

ISO/IEC 20000-1:2011 (IEEE Std 20000-1:2013) reference: 6.3.1, 6.3.2

ISO/IEC 20000-2:2012 (IEEE Std 20000-2:2013) reference: 4.1.1.5, 6.3.2, 6.3.3.2, 6.3.3.3, 6.3.4, 6.3.5, Table A.4, Table A.14

Generic type: Plan

The service continuity and availability plan, also known as a continuity of operations plan (COOP) or disaster recovery plan, may also include service continuity and availability strategy and policy. It describes the provisions to make services available under normal conditions and in the event of failure of a site or a system component (recovery procedure). The service continuity and availability plan shall be available in printed media to all concerned, for ready access in the event of system unavailability. A copy of the service continuity plan, applicable agreements and contracts shall be available at a secure remote or virtual location where it is planned that alternate service are provided. It includes the following:

a) availability requirements for the service as stated in the service level agreements, including access rights, end-to-end availability, and service restoration times;

b) availability targets for service restoration;

c) the business impact of services unavailability for various durations, and priorities for restoring services;

d) criteria for invoking the plan (threshold for events and major incidents);

e) procedures and alternate means of providing service (such as paper-based records) while automated systems are being restored;

f) roles and responsibilities for system recovery, including points of contact of people authorized to invoke contingency plans and act in emergencies;

g) procedures for restoring service;

h) procedures for testing the continuity plan; and

i) advance activities to prepare for service disruptions, such as off-site system backups or arrangements with emergency service providers.

See also: verification plan

### 10.71 Service level agreement (SLA)

ISO/IEC 20000-1:2011 (IEEE Std 20000-1:2013) reference: 3.29, 4.3.1, 5.3, 6.1, 7.2

ISO/IEC 20000-2: 2912 (IEEE Std 20000-2:2013) reference: 4.1.1.3, 4.3.1.1, 5.3.1, 5.5, 6.1.3.3, 6.1.3.4, 6.1.4, 7.2.2, 7.2.3.2

Generic type: Specification

A Service Level Agreement (SLA) is a documented agreement between the service provider and customer that identifies services and service targets. The SLA is the service level requirements document. The SLA should be authorized by the service supplier and acquirer. It specifies the following:

a) Requirements and scope of the service;

b) Service targets and workload limits (upper and lower) and exceptions;

c) Responsibilities of both supplier and customer;

d) Details of service availability (hours of service), which may be referenced in the service catalog;

e) Procedures and points of contact for incident and problem management, escalation, notifications, and complaints;

f) Measures and acceptance criteria, such as performance, availability, reliability, service period, and

operator and maintenance responsiveness; and

g) Communication process for periodic reporting on the achieved service level to the customer.

## 10.72 Service management plan (and policy)

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 6.4.9.3.1.1

ISO/IEC 20000-1:2011 (IEEE Std 20000-1:2013) reference: 4.1.1, 4.1.2, 4.3.1, 4.5.1, 4.5.2

ISO/IEC 20000-2:2012 (IEEE Std 20000-2:2013) reference: 4.1.1.1, 4.1.1.4, 4.1.1.5, 4.1.1.6, 4.1.2.1, 4.1.2.2, 4.1.3.1, 4.1.4.2, 4.3.1.1, 4.5.2.1, 4.5.2.2, 4.5.2.3, 4.5.3, 4.5.4.1, 7.1.3.1

Generic type: Plan

The service management plan (or operations plan) includes the service management policy. It presents how the service provider's processes and activities are managed, executed, measured, and controlled to successfully deliver the service.

NOTE When applied to a new, modified, or improved service, the service management plan can be called a plan for new or changed service or service plan.

It identifies the following:

a) the service management system scope, policy, objectives, and requirements and business needs, including customer requirements along with expected outcomes and acceptance criteria;

b) the processes included in the service management system, including the responsible organization; process inputs, activities, and outcomes; interfaces to other processes and services; and records and documentation needed to govern the process;

c) resource plans for human, technical, information, and financial resources, and succession plans to staff the service;

d) constraints and limitations affecting the service management system;

e) descriptions of the organizations or roles involved in approving, designing, developing, transitioning, changing, implementing, operating, maintaining, and improving the service and the service management plan, and the relationships of those involved, including suppliers and customers;

f) the coordination of interfaces among related services, processes and activities;

g) plans for reports, reviews and communications with stakeholders and assurance of customer satisfaction; and

h) how the organization measures, audits, reports on, and improves the SMS and the services.

See also: audit plan, complaint procedure, implementation plan, improvement plan, interface specification, information management plan, project management plan, disposal plan, risk management plan, service plan.

## 10.73 Service plan

ISO/IEC 20000-1:2011 (IEEE Std 20000-1: 2013) reference: 5.2, 5.3

ISO/IEC 20000-2:2012 (IEEE Std 20000-2: 2013) reference: 5.2.7, 5.3.3.1, 5.4, 5.5

Generic type: Plan

The service plan (plan for new or changed services) presents plans for designing and implementing a major change or major new service. A service plan may be prepared for a new, existing, modified, or improved service. It includes the following:

a) description of the new or changed service, including service requirements, expected outcomes and outputs,

service measurements, and activities to be performed for service delivery;

b) analysis of required resources, such as human, financial, and technological, and dependencies on other services;

c) analysis of risks in the new service and risks to existing services;

d) testing and acceptance criteria for the new or changed service;

e) responsibilities and authorities for service delivery;

f) communication planning; and

g) needed changes in other documents, including plans and policies, agreements, SLAs, service catalog, and procedures.

See also: concept of operations, disposal plan, implementation plan, improvement plan, project management plan, retirement plan, risk management plan, service catalog, service management plan

## 10.74 Service report

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 6.2.5.3.1.4

ISO/IEC/IEEE 15288:2015 reference: 6.4.13.3.d), B.1

ISO/IEC 20000-1:2011 (IEEE Std 20000-1: 2013) reference: 4.1.4.e, 4.5.3.f, 4.5.5.2, 5.4, 6.2, 7.2

ISO/IEC 20000-2:2012 (IEEE Std 20000-2: 2013) reference: 4.1.1.1, 4.1.4.4, 4.5.4.1, 4.5.4.2, 5.2.8, 5.4, 5.5, 6.1.2, 6.1.3.1, 6.1.3.4.c), 6.1.4, 6.2.1, 6.2.2, 6.2.3, 6.3.2, 6.3.4.3, 6.4. 6.5.3.1, 6.5.4, 7.1.4, 7.2.3.1, 8.1.2, Table A.3, Table A.7, Table A.8

Generic type: Report

The service report informs management or customers about the performance of service management activities, and the level of service provided. It reports results and reviews of performance by the service provider against the service targets, SLA and other contractual commitments and customer satisfaction measurements and analyses. It is issued periodically or following major events, transitions, and changes in the service. It includes a summary of significant events, monitoring results, trends and historical analysis, customer satisfaction measurements, and recorded service improvements. It provides information about non-conformities, options for changes, complaints, action items, corrective actions; anticipated problems, and risk treatment actions. It includes information concerning workload volume and scheduled workloads, trends and periodic changes. It may include cost reports and comparisons of capacity to service performance for the service, specific components, or exceptional events.

See also: audit report, evaluation report, incident report, monitoring and control report, progress report.

## 10.75 Software architecture description

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 6.4.3.2, 6.4.3.3.1.1, 7.1.1.2, 7.1.3.2, 7.1.3.3.1, 7.1.3.3.1.1, 7.3.1.2, 7.3.1.3.3.1, 7.3.1.3.3.3

Generic type: Description

The software architecture description includes the following:

a) the fundamental conception of the software for the system-of-interest in terms of its purpose, software qualities (such as performance, usability and security), constraints, and decisions;

b) the architecture's stakeholders and the stakeholders' architecture-related concerns. Key stakeholders include the client, users, developers, acquirers, suppliers and maintainers;

c) definitions of viewpoints to document the procedures for creating, interpreting, analyzing and evaluating architectural data; and

d) one or more views of the system. Each architecture view is a representation of the complete system from the perspective of one or more concerns, for its stakeholders.

The software architecture description should do the following:

1) provide rationale for architectural decisions, with traceability information to both software and system requirements;

2) establish the principles for partitioning the software into design elements;

3) record the important properties of, and relationships among, those elements in a manner consistent with the work breakdown structure;

4) demonstrate that architecturally significant requirements are met and allocated to design elements; and

5) provide a basis for software requirements specification and design refinement.

The software architecture description may present the following:

i. the concept of operation in terms of its elements; and

ii. a domain model or reference architecture for a family of, or system of, software systems. See also: system architecture description.

NOTE The software architecture description can be considered as a specification for the software design. For more information on architecture description, refer to ISO/IEC/IEEE 42010:2011, *Systems and software engineering — Architecture description*.

## 10.76 Software design description

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 6.4.10.2, 6.4.10.3.3.1, 7.1.1.3.1.2, 7.1.4.3.1.1, 7.2.2.3.5.1, 7.3.1.3.3.3

Generic type: Description

The software design description presents the characteristics of one or more systems, subsystems, software items, or other system components, and their interfaces. It includes the following:

a) identification of external interfaces, software components, software units, and other interfaces;

b) allocation of software item requirements to software components, further refined, as needed, to facilitate detail design;

c) description of the items (systems, configuration items, users, hardware, software, etc.) that communicate with other items to pass and receive data, instructions or information;

d) the concept of execution including data flow and control flow;

e) security considerations;

f) reuse elements; and

g) error handling.

It should include the following:

1) traceability information to both architectural components and software requirements;

2) specification of protocols; and

3) partitioning of the software into design entities and description of the important properties and relationships among those entities.

The low-level software design description describes the design of a software item or interface, including software item-wide design decisions, software item architectural design and the detailed design needed to implement software. The low-level description permits software development or selection of items for reuse without the need for further information. It provides visibility into the design and information needed for software reuse and support. It is used as the basis for implementing software. It includes the following:

i. the detailed structure description of software components (to the software unit level to be coded, compiled and tested);

ii. allocation of software component requirements to software items, further refined, as needed, to facilitate detail design and traceability from each software item to the software item requirements allocated to it;

iii. the software item-wide design decisions about the software item's behavioral design (how it behaves, from a user's viewpoint, in meeting its requirements, ignoring internal implementation);

iv. decisions affecting the selection and design of the software items making up a software item;

v. detailed design for software components' external interfaces to the software item, between related software components, and between related software units; and

vi. the interface entity characteristics of one or more systems, subsystems, hardware items, software items, manual operations or other system components.

It should include the following:

— descriptions of the size, frequency or other characteristics of the data elements;

— reference to known timing constraints;

— specification of protocols.

See also: system element description

NOTE IEEE Std 1016-2008, IEEE Recommended Practice for Software Design Descriptions provides further guidance.

## 10.77 Software requirements specification

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 6.1.1.3.1.2, 6.1.1.3.1.7, 6.1.1.3.1.8, 6.1.1.3.1.11, 6.4.11.2, 7.1.2.2, 7.1.2.3.1.1, 7.1.3.3.1.5

Generic type: Specification

The software requirements specification includes the following:

a) precedence and criticality of requirements;

b) description of the methods and tools used to define traceability from system requirements to system architecture, software requirements, software architecture, and software items and units;

c) product assumptions and dependencies;

d) references for design and testing standards and procedures;

e) product functions and system functional requirements;