INTERNATIONAL STANDARD

ISO/IEC/ IEEE 15289

First edition
2011-11-01

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

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

Reference number
ISO/IEC/IEEE 15289:2011(E)

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

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
E-mail inmail@iec.ch
Web www.iec.ch

Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York
NY 10016-5997, USA
E-mail stds.ipr@ieee.org
Web www.ieee.org

Published in Switzerland

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.

The main task of ISO/IEC JTC 1 is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is called to the possibility that implementation of this standard may require the use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. ISO/IEEE is 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 standard 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.

ISO/IEC/IEEE 15289 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 7, *Software and systems 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 first edition of ISO/IEC/IEEE 15289 cancels and replaces ISO/IEC 15289:2006, which has been technically revised.

Introduction

The purpose of this International Standard 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 International Standard 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 may be combined or subdivided as needed for project or organizational purposes.

This International Standard 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 15288:2008 (IEEE Std 15288-2008), *Systems and software engineering — System life cycle processes*; and the service management processes specified in ISO/IEC 20000-1:2005, *Information technology — Service management — Part 1: Specification*; and ISO/IEC 20000-2:2005, *Information technology — Service management — Part 2: Code of practice.*

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 this International Standard.

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

1 Scope

This International Standard 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 International Standard assumes an organization is implementing life-cycle processes in conformance with ISO/IEC 15288:2008 (IEEE Std 15288-2008), *Systems and software engineering — System life cycle processes*, or ISO/IEC 12207:2008 (IEEE Std 12207-2008), *Systems and software engineering — Software life cycle processes*, or practising service management in conformance with ISO/IEC 20000-1:2005, *Information technology — Service management — Part 1: Specification*, and ISO/IEC 20000-2:2005, *Information technology — Service management — Part 2: Code of practice.* ISO/IEC 12207:2008 (IEEE Std 12207-2008) and ISO/IEC 15288:2008 (IEEE Std 15288-2008) define a set of processes for managing and performing the stages of a systems life cycle. They define an Information Management process, but they do "not detail documentation in terms of name, format, explicit content, and recording media" [ISO/IEC 15288:2008 (IEEE Std 15288-2008), 1.4)]. ISO/IEC 12207:2008 (IEEE Std 12207-2008) establishes a common framework for software life-cycle processes and in passing identifies or requires a number of documentation items. The 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 20000-1:2005 establishes general requirements for documents and records (3.2). 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. This International Standard provides a mapping of ISO/IEC 15288:2008 (IEEE Std 15288-2008) and ISO/IEC 12207:2008 (IEEE Std 12207-2008) clauses with a set of information items.

The generic document types (which may be referred to as information item types) are to be used to identify the information necessary to support the ISO/IEC 15288:2008 (IEEE Std 15288-2008) agreement, enterprise, project, and technical processes; the ISO/IEC 12207:2008 (IEEE Std 12207-2008), primary, supporting, and organizational life-cycle processes; or the ISO/IEC 20000-1:2005 service management processes.

This International Standard identifies records and information items based on analysis of references in ISO/IEC 15288:2008 (IEEE Std 15288-2008), ISO/IEC 12207:2008 (IEEE Std 12207-2008), ISO/IEC 20000-1:2005 and ISO/IEC 20000-2:2005, which in some cases provide partial or complete outlines for the content of specific documents. However, the requirements for the life-cycle processes do not uniquely and unambiguously state the requirements for the information item contents or the information needed by a user of an information item. Moreover, the information from the life-cycle processes may overlap or may be created and revised at different times. In short, the analysed references do not result in a logically complete list of information items.

For each life-cycle process, it would be possible to prepare a 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 15288:2008 (IEEE Std 15288-2008) or ISO/IEC 12207:2008 (IEEE Std 12207-2008). As ISO/IEC 15288:2008 (IEEE Std 15288-2008) points out (1.4), "This International Standard does not detail the life-cycle processes in terms of methods or procedures required to meet the requirements and outcomes of a process." Thus, information items may be combined or subdivided as needed for project or organizational purposes, as further defined in Clause 2, Applicability, and Clause 3, Conformance.

Not included in the scope of this International Standard are 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 system and software life-cycle data, records, information items, or documentation, such as electronic publishing systems, content management systems, or data repositories;

d) detailed content for information items related to general business, organizational, and financial management that is not specific to systems and software engineering and information technology service management, such as business strategies, 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 15288:2008 (IEEE Std 15288-2008) or ISO/IEC 12207:2008 (IEEE Std 12207-2008) subclause not explicitly or implicitly identifying the recording of information about an 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 the life-cycle products and services that are not information items or records used in information items.

NOTE 1 ISO/IEC 26514:2008, *Systems and software engineering — Requirements for designers and developers of user documentation*, provides guidance on formats for software user documentation.

NOTE 2 ISO/IEC TR 15504-5:1999, *Information technology — Software Process Assessment — Part 5: An assessment model and indicator guidance*, details the content of work products as well as information items. Its guidance includes descriptions of a set of information items (documents) that an assessor may encounter. The information items in its guidance may be produced by combinations and subdivisions of the required information items in this International Standard.

2 Applicability

2.1 Purpose

The purpose of this International Standard is to provide requirements for users of ISO/IEC 12207:2008 (IEEE Std 12207-2008), ISO/IEC 15288:2008 (IEEE Std 15288-2008) and ISO/IEC 20000-1:2005 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 International Standard is intended for use as follows.

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

b) To specify information in an agreement process as described in ISO/IEC 15288:2008 (IEEE Std 15288-2008) or a two-party situation as described in ISO/IEC 12207:2008 (IEEE Std 12207-2008), ISO/IEC 20000-1:2005 and ISO/IEC 20000-2:2005. 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 15504, and to guide process improvement activities.

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

2.2 Intended users of this International Standard

This International Standard is applicable for use by:

a) project managers responsible for the Information Management process of ISO/IEC 15288:2008 (IEEE Std 15288-2008) (5.4.8) 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 occur, and what the contents of the documents should be;

c) acquirers responsible for determining what information items are needed to 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 15288:2008 (IEEE Std 15288-2008), or ISO/IEC 20000-1:2005;

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

2.3 Applicability to work efforts

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

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;

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.

2.4 Applicability to information item audiences

Users should map this International Standard to the requirements and needs of their agreements, or project and organizational procedures. The type of decision to be made, or 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 International Standard accurately and economically, since some information items are designed for various purposes and user groups:

- To provide information to specialized types of users who may not be a part of a particular project.
- To address the same type of user but in environments not normally coexisting in the same effort.
- To aid both users who are expected to be computer-literate and understand technical terminology, and users who may not have this background.

3 Conformance

3.1 Definition of conformance

This International Standard may be used as a conformance or a guidance document for projects and organizations claiming conformance to ISO/IEC 15288:2008 (IEEE Std 15288-2008), ISO/IEC 12207:2008 (IEEE Std 12207-2008), or ISO/IEC 20000-1:2005.

NOTE 1 Service providers should refer to ISO/IEC 20000-1:2005 and ISO/IEC TR 20000-5:2010 regarding claims of conformance for a defined certification scope, for example, organizational units, services, location.

To claim conformance to this International Standard, having tailored the selected system or software life-cycle processes, the users of this International Standard shall prepare the information items identified in this International Standard applicable to the selected and tailored ISO/IEC 15288:2008 (IEEE Std 15288-2008), ISO/IEC 12207:2008 (IEEE Std 12207-2008), or ISO/IEC 20000-1:2005 processes.

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

NOTE 2 Annex A of ISO/IEC 15288:2008 (IEEE Std 15288-2008) and ISO/IEC 12207:2008 (IEEE Std 12207-2008) provide requirements for the Tailoring Process.

In this International Standard, 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 International Standard.

Throughout this International Standard, “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 International Standard.

The verb “include” used in this International Standard indicates that either (1) the information is present or (2) a reference to the information is listed.

3.2 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 make public a document declaring its tailoring of the records and information items, and its interpretation of any clauses of the standard 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 the standard 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 the standard 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 International Standard 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 shall 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 may be said to comply with this document when its products (the information items) fulfil the requirements, but the organization, project or program has not met the specific requirements for conformance stated in items (a), (b) or (c) above.

3.3 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 15288:2008 (IEEE Std 15288-2008).

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.

NOTE Absolute conformance may be claimed for selected processes or information items even if absolute conformance with the entire standard is not claimed.

4 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies.

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

ISO/IEC 15288:2008 (IEEE Std 15288-2008), *Systems and software engineering — System life cycle processes*

ISO/IEC 20000-1:2005, *Information technology — Service management — Part 1: Specification*

ISO/IEC/IEEE 24765:2010, *Systems and software engineering — Vocabulary*

5 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 12207:2008 (IEEE Std 12207-2008), ISO/IEC/IEEE 24765:2010 and the following apply.

5.1
approval
written notification, by an authorized representative, that a deliverable item appears to satisfy requirements and is complete

NOTE Such approval does not shift responsibility from the supplier to meet requirements under a two-party situation.

5.2
complete [documentation]
including all critical information and any necessary, relevant information for the intended audience

5.3
consistent
without internal conflicts

5.4
COTS
Commercial-Off-The-Shelf
product available for purchase and use without the need to conduct development activities

5.5
criteria
rules on which a judgment or decision can be based, or by which a product, service, result, or process can be evaluated

5.6
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

[ISO/IEC 26514:2008]

5.7
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

5.8
description
information item that represents a planned or actual concept, function, design, or object

5.9
document
uniquely identified unit of information for human use, such as a report, specification, manual or book, in printed or electronic form

5.10
documentation plan
plan identifying the documents to be produced during the system or software life cycle

5.11
information item
separately identifiable body of information that is produced, stored, and delivered for human use

NOTE 1 “information product” is a synonym.

NOTE 2 An information item can be produced in several versions during a project life cycle.

5.12
include information
having either the information or a reference to the information present in the document

5.13
information item content
information included in an information item, associated with a system, product or service, to satisfy a requirement or need

5.14
information item type
group of information items consistent with a pre-arranged set of generic criteria

NOTE "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.

5.15
modifiable
structured and has a style such that changes can be made completely, consistently, and correctly while retaining the structure

5.16
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

5.17
policy
clear and measurable statement of preferred direction and behaviour to condition the decisions made within an organization

[ISO/IEC 38500:2008]

5.18
presentable
retrievable and viewable

5.19
procedure
information item that presents an ordered series of steps to perform a process, activity, or task

NOTE 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.

5.20
record
set of related data items treated as a unit

5.21
report
information item that describes the results of activities such as investigations, observations, assessments, or tests

5.22
request
information item that initiates a defined course of action or change to fulfil a need

5.23
software item
identifiable part of a software product

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

5.24
specification
information item that identifies, in a complete, precise, and verifiable manner, the requirements, design, behaviour, or other expected characteristics of a system, service, or process

5.25
traceable
having components whose origin can be determined

5.26
unambiguous
described in terms that allow only a single interpretation, aided, if necessary, by a definition

5.27
verifiable
can be checked for correctness by a person or tool

6 Life cycle data and information items

6.1 Life cycle data characteristics

This International Standard 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 information item produced as a document described in this International Standard shall support the life cycle data characteristics:

a) unambiguous

b) complete

c) verifiable

d) consistent

e) modifiable

f) traceable

g) presentable

6.2 Records compared to information items (documents)

A record is a special type of information containing a set of structured data treated as a unit. Table 4 in Clause 9 identifies records. Consistent with the ISO 9000 series, the purpose of a record is to state results achieved or to provide evidence of activities performed by an organizational entity. In fact, ISO/IEC 20000-1:2005 defines record as “document stating results achieved or providing evidence of activities performed” and considers any document or information item to be a record. However, this International Standard 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. 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 activities and tasks of the standard. Many of the clauses in ISO/IEC 15288:2008 (IEEE Std 15288-2008) and ISO/IEC 12207:2008 (IEEE Std 12207-2008) require life cycle data to be produced or recorded. However, the clauses of ISO/IEC 15288:2008 (IEEE Std 15288-2008) 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, users 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. 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 15288:2008 (IEEE Std 15288-2008), and 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 15288:2008 (IEEE Std 15288-2008) clause 6.2.4. 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.

Appendix A of this International Standard 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 tailored system processes, phases, and stakeholder needs.

The documentation management process shall include these activities:

a) Identify the documents to be produced by the organization, service, process or project;

b) Specify the content and purpose of all documents and plan and schedule their production;

c) Identify the standards to be applied for development of documents;

d) Develop and publish all documents in accordance with identified standards and in accordance with nominated plans;

e) Maintain all documents in accordance with specified criteria.

NOTE Annex A provides a procedure for identifying information items and their contents during information management and documentation planning.

6.4.1 Developing the documentation plan

The tasks to be performed in the Documentation 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 Documentation Management Process for each project should be considered as part of a repeatable process for the acquirer and supplier.

NOTE 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, 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 International Standard defines the life cycle data of ISO/IEC 12207:2008 (IEEE Std 12207-2008) and ISO/IEC 15288:2008 (IEEE Std 15288-2008) 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

g) specification.

NOTE Clause 9 identifies the generic content of data records.

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.

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

j) Change history

Identified information items:

- Concept of operations
- Database design description
- Interface description
- Proposal
- Service catalog
- Software architecture description
- Software design description
- Software unit description
- System architecture description
- 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) Approach for technical and management review and reporting

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

h) Planned activities and tasks

i) Identification of tools, methods, and techniques

j) Schedules

k) Budgets and cost estimates

l) Resources and their allocation

m) Responsibilities and authority, including the senior responsible owner and immediate process owner

n) Interfaces among parties involved

o) Risks and risk identification, assessment and mitigation activities

p) Quality assurance and control measures

q) Environment, infrastructure, security, and safety

r) Training

s) Glossary

t) Change procedures and history

u) 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
- Reuse plan
- Risk management policy and plan
- Service Availability and continuity plan
- Service management plan
- Training plan
- Validation plan
- 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

h) Change history

NOTE Policies can 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:

- Configuration management plan and policy (change management policy, release policy)
- Improvement policy
- Information security policy
- Life cycle policy and procedure
- Quality management policy and procedure
- Risk management policy and plan

7.5 Procedure – generic content

Reference: ISO/IEC 15288:2008 (IEEE Std 15288-2008), 5.3.1

Purpose: Define in detail when and how to perform certain 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

k) Change history

Identified information items:

- Audit procedure
- Capacity management procedure
- Configuration management procedure (change management procedure, release management procedure)
- Complaint procedure
- Implementation procedure
- Incident management procedure
- Life cycle policy and procedure
- Maintenance 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

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

g) Context (assumptions)

h) Body (including methods of obtaining results)

i) Conclusions and recommendations

j) References

k) Bibliography

l) Glossary

m) Change history

Identified information items:

- Acceptance review and testing 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 analysis report
- Product need assessment
- Progress report
- Qualification test report
- Review minutes
- Service report
- Software unit test report
- User notification
- Validation report
- 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 may be a Specification.

Identified information items:

- Change request
- Customer satisfaction survey
- Request for proposal (RFP)
- Resource request
- Risk action request

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. Each requirement should be uniquely identified. 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

j) Change history

Identified information items:

- Contract
- Service level agreement (SLA)
- Software requirements specification
- System requirements specification
- 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 15288:2008 (IEEE Std 15288-2008) or ISO/IEC 12207:2008 (IEEE Std 12207-2008) or ISO/IEC 20000-1:2005. These references may be normative requirements, recommended output, informative material, examples, or notes. This International Standard identifies information items that are not explicitly specified by title in ISO/IEC 15288:2008 (IEEE Std 15288-2008) or ISO/IEC 12207:2008 (IEEE Std 12207-2008) or ISO/IEC/IEEE 20000-1:2005. 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 15288:2008 (IEEE Std 15288-2008) 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 20000-1:2005 and 20000-2:2005 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 1-3 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 1-3 also show the specific reference citations from the source standards for each specified information item, not all references for a process.

In numerous clauses, the life cycle standards indicate that something (for example, a strategy) is to be "defined." However, definition does not in itself indicate that a specific information item will be 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 International Standard 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, five organizational processes, seven project processes, and eleven technical 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. Requirements Analysis
3. Architectural Design
4. Implementation
5. Integration
6. Verification
7. Transition
8. Validation
9. Operation
10. Maintenance
11. Disposal

Table 1 — Mapping of ISO/IEC 15288:2008 (IEEE Std 15288-2008), Clauses to Information Items for Each System Life Cycle Process

Typical Input information items	ISO/IEC 15288: 2008 (IEEE Std 15288 -2008) reference	Output information item
ACQUISITION		
Proposal, other contracts	6.1.1.2d) 6.1.1.3c)	Contract
Needs assessment	6.1.1.3a)	System requirements specification
Concept of operations, system requirements specification, software requirements specification, acceptance strategy, other requests for proposal	6.1.1.3a)	Request for proposal (RFP)
SUPPLY		
Request for proposal, other proposals	6.1.1.3.a), 6.1.1.3b), 6.1.2.2b) 6.1.2.3b)	Proposal

Typical Input information items	ISO/IEC 15288: 2008 (IEEE Std 15288 -2008) reference	Output information item
Proposal, other contracts and agreements	6.1.2.2c) 6.1.2.2f) 6.1.2.3c) 6.1.3.3f)	Contract
Problem report	6.1.2.3b)	Product need assessment
Project management plan	6.1.2.3d)	Progress report
Organizational procedure, other project management plans, contract	6.1.2.3c) 6.1.2.3d)	Project management plan
LIFE CYCLE MODEL MANAGEMENT		
Organizational procedure	6.2.1.2a) 6.2.1.3a)	Life cycle policy and procedure
Assessment report, organizational procedure	6.2.1.3c)	Improvement plan
Organizational procedure, process assessment procedure, process assessment results, audit report, customer satisfaction report, assessment report, progress report, problem report	6.2.1.3c)	Process improvement analysis report
INFRASTRUCTURE MANAGEMENT		
Organizational procedure, other system requirements specification	6.2.2.2	System requirements specification
PROJECT PORTFOLIO MANAGEMENT		
Organizational procedure, project plan, business action plan	6.2.3.3a)	Project management plan
System life cycle policies and procedures	6.2.3.3a)6)	Progress 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	6.2.4.3b)	Training documentation
QUALITY MANAGEMENT		
Project management plan	6.2.5.3	Quality management plan
Organizational procedure, quality management plan, customer satisfaction report, problem report	6.2.5.2a) 6.2.5.3a)	Quality management policy and procedure
Survey, interview, requirements specification	6.2.5.3b)	Evaluation report
PROJECT PLANNING		
Contract, organizational procedure, other plans	6.3.1.1 6.3.1.2, 6.3.1.3	Project management plan
Product need assessment, contract	6.3.1.3b)	Acceptance plan
Product need assessment	6.3.1.3b)	Acquisition plan

Typical Input information items	ISO/IEC 15288: 2008 (IEEE Std 15288 -2008) reference	Output information item
Organizational quality management policy and procedure	6.3.1.3c)	Quality management plan
Project management plan, work breakdown structure, budget	6.3.1.3.d),	Resource request
PROJECT ASSESSMENT AND CONTROL		
Contract, organizational procedure, project plan, quality assurance plan	6.3.2.2	Problem report
Contract, organizational procedure, project plan, quality assurance plan, other progress report	6.3.2.2d) 6.3.2.3a)9)	Progress report
Problem report, analysis of metrics and variations	6.3.2.3.b)4	Monitoring and control report
Project management plan, work breakdown structure, budget, progress report	6.3.2.3.b)	Resource request
DECISION MANAGEMENT		
Organizational procedure, contract	6.3.3.3a)2), 6.3.3.3c)1)	Problem report
Organizational procedure, contract	6.3.3.2.d)	Report *(see generic Report information item)*
RISK MANAGEMENT		
Project management plan	6.3.4.3a)	Risk management policy and plan
Risk management plan, risk profile	6.3.4.3d)	Risk action request
Risk management plan, risk profile, quality assurance procedure, problem report	6.3.4.3b)	Monitoring and control report
CONFIGURATION MANAGEMENT		
project management plan, information management plan	6.3.5.3a)	Configuration management plan
INFORMATION MANAGEMENT		
Organizational procedure, project management plan, configuration management plan	6.3.6.3 a)	Information management plan
MEASUREMENT		
Organizational procedure, project management plan	6.3.7.3 a)	Measurement plan
Measurement data, information management plan	6.3.7.1 6.3.7.3 b)	Monitoring and control report
Measurement plan, evaluation report	6.3.7.3 c)	Process improvement analysis report
STAKEHOLDER REQUIREMENTS DEFINITION		
Contract, needs assessment	6.4.1.2a), D.4.a	Concept of operations
Contract, needs assessment, concept of operations	6.4.1.3c)	System requirements specification

Typical Input information items	ISO/IEC 15288: 2008 (IEEE Std 15288 -2008) reference	Output information item
REQUIREMENTS ANALYSIS		
Organizational procedure, stakeholder requirements	6.4.2.2, 6.4.2.3	System requirements specification
ARCHITECTURAL DESIGN		
Development plan, system requirements specification	6.4.3.1 6.4.3.2a), 6.4.3.3.c)	System architecture description
System architecture description	6.4.3.2b)	System element description
System architecture description, system design description	6.4.3.3a), c)	Interface description
IMPLEMENTATION		
Agreement, organizational procedure, system description, integration procedure, interface control description	6.4.4.3	Integration plan (implementation plan)
Implementation plan, system design	6.4.4.3.a) 6.4.4.3.b)	Implementation procedure
INTEGRATION		
agreement, System requirements specification, interface description, system test plan	6.4.5.3a)	Integration plan
configuration record	6.4.5.3b)	Problem report
VERIFICATION		
system requirements specification, system description, interface description	6.4.6.3a)	Verification plan
Organizational procedure, requirements specification, verification plan, design definition, interface control description, test procedures, progress report, problem report, test case	6.4.6.3b)	Verification report
Test procedures, test report	6.4.6.2.c) 6.4.6.3b)	Problem report
TRANSITION		
Agreement, system description, system requirements specification, interface description	6.4.7.3a)	Installation plan
Installation plan, problem report, progress report	6.4.7.3b)	Installation report
Quality management procedure	6.4.7.2.e) 6.4.7.3b)	Problem report
VALIDATION		
Stakeholder requirements, project management plan, verification plan	6.4.8.3a)	Validation plan
Quality management plan, validation plan	6.4.8.3b)	Validation report
Test procedure	6.4.8.2.d) 6.4.8.3b)	Problem report

Typical Input information items	ISO/IEC 15288: 2008 (IEEE Std 15288 -2008) reference	Output information item
OPERATION		
problem report, evaluation report	6.4.9.3b)	User documentation
User documentation, incident report, service level agreement	6.4.9.2.c)	Problem report
MAINTENANCE		
Organizational procedure, operations plan, development plan	6.4.10.3a)	Maintenance plan
Maintenance plan, user documentation	6.4.10.3.a 6.4.10.3b)	Maintenance procedure
Maintenance procedures	6.4.10.2.e), 6.4.10.3b)	Problem report
DISPOSAL		
Project management plan, system requirements specification, interface description, installation procedure, operations procedures	6.4.11.3a)	Disposal plan
TAILORING		
Standard life cycle model, standard, organizational policies and procedures, tailoring decision, agreement, stakeholder requirement	A.2.3a), B.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, acquisition report, other acquisition plans	6.1.1.3.1.8, 6.1.1.3.1.9, 6.1.1.3.1.12	Acquisition plan
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)

Typical Input information items	ISO/IEC 12207: 2008 (IEEE Std 12207 -2008)	Output information item
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	6.1.2.2, 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

Typical Input information items	ISO/IEC 12207: 2008 (IEEE Std 12207 -2008)	Output information item
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		
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.b)4	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

Typical Input information items	ISO/IEC 12207: 2008 (IEEE Std 12207 -2008)	Output information item
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

Typical Input information items	ISO/IEC 12207: 2008 (IEEE Std 12207 -2008)	Output information item
IMPLEMENTATION		
[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		
Systems requirement 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

Typical Input information items	ISO/IEC 12207: 2008 (IEEE Std 12207 -2008)	Output information item
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
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

Typical Input information items	ISO/IEC 12207: 2008 (IEEE Std 12207 -2008)	Output information item
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
Database design 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

Typical Input information items	ISO/IEC 12207: 2008 (IEEE Std 12207 -2008)	Output information item
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		
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 13 service management processes as defined in ISO/IEC 20000-1:2005 and ISO/IEC 20000-2:2005. There are six Service Delivery processes, two Relationship Processes, two Resolution Processes, two Control Processes, and a Release Process. In addition, there are a number of information items required by all service management processes as part of the Plan-Do-Check-Act cycle.

NOTE 1 ISO/IEC 20000-2:2005, *Information technology — Service management — Part 2: Code of practice* 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 compliance are not misleading.

NOTE 2 As stated in Table 3 and required by ISO/IEC 20000-1:2005, subclauses 3.1 and 3.2, all processes require policies, plans and procedures. In Table 3, policies, plans and procedures are shown for specific services when additional detail is available in the referenced ISO/IEC 20000-1 or ISO/IEC 20000-2 clause.

Service Delivery Processes

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

Relationship Processes

1. Business Relationship Management
2. Supplier Management

Resolution Processes

1. Incident Management
2. Problem Management

Control Processes

1. Configuration Management
2. Change Management

Release Process

1. Release Management

Table 3 — Mapping of ISO/IEC 20000-1:2005 and ISO/IEC 20000-2:2005 Clauses to Information Items for Each Service Management Process

Typical Input information items	ISO/IEC 20000-1: 2005 or ISO/IEC 20000-2: 2005 clause	Output information item
APPLICABLE ACROSS SERVICE MANAGEMENT PROCESSES (MANAGEMENT SYSTEM)		
Organizational policy	**1:** 3.1, 3.2, 4, 4.2 **2:** 3.1	Service management policy *(see generic Policy information item)*
Service management policy, contract	**1:** 3.1, 3.2, 4.1, 4.2, 4.4.3, 5 **2:** 3.2, 4.1.1, 4.1.2, 4.1.3, 4.1.4,	Service management plan
Service management plan, SLA	**1:** 3.2, 4.4.3 **2:** 3.2	Procedure *(Plan generic information item)*
Contract (if applicable), service management plan	**1:** 3.2, 5	Service level agreement (SLA)
SLA, service management plan	**1:** 4.2, 4.4.2, 4.4.3, 5	Progress report
SLA, service management plan	**1:** 4.3 **2:** 4.3	Audit plan
Contract, SLA	**2:** 7.2.1	Review minutes
Audit plan, SLA	**1:** 4.3	Audit procedure
Audit procedure	**1:** 4.3	Audit report
Organizational policies, service plans	**1:** 4.4.1	Improvement policy
Service management plan, SLA, service improvement policy, measurement plan, monitoring and control reports, review minutes, audit results	**1:** 4.3, 4.4.2, 4.4.3 2:4.3	Improvement plan
Service management plan	**2:** 4.3	Measurement plan
SERVICE LEVEL MANAGEMENT		
Service management plan, contract, service catalog, change request, service report, service management procedures, organizational procedures, or customer procedures	**1:** 6.1 **2:** 6.1.2	Service level agreement (SLA)
SLA, service procedure	**1:** 6.1 **2:** 6.1.3	Monitoring and control report

Typical Input information items	ISO/IEC 20000-1: 2005 or ISO/IEC 20000-2: 2005 clause	Output information item
Review minutes, monitoring and control report, problem report	**1:** 6.1 **2.** 6.1.3	Improvement plan
Service management plan, SLA	**2:** 6.1.1,	Service catalog
SERVICE REPORTING		
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 **2:** 6.2, 6.2.1, 6.2.2, 6.2.3	Service report
SERVICE CONTINUITY AND AVAILABILITY MANAGEMENT		
business plan; SLA; risk assessment; service availability and continuity requirements; service recovery procedure; change request	**1:** 6.3 **2:** 6.1.2, 6.3.4	Service availability and continuity plan
Availability records, service level agreement, service availability and continuity plan, test results, action plans	**2:** 6.3.2	Monitoring and control report
BUDGETING AND ACCOUNTING FOR IT SERVICES		
Business policies and financial procedures, previous budgets and cost reports, financial forecast reports *NOTE: Business policies and financial procedures relating to budgeting, financial accounting, and reporting on costs are outside the scope of this standard.*	**1:**6.4 **2:** 6.4.1, 6.4.2	*Financial management, budgeting, and accounting policies and procedures* *Budget* *Cost report* *NOTE: The contents of these financial items are not further specified in this Standard.*
CAPACITY MANAGEMENT		
Service management plan, SLA, capacity and performance requirements (current and future), capacity usage data and analyses, change management reports	**1:** 6.5 **2:** 6.5	Capacity plan
Capacity plan	**1:**: 6.5	Capacity management procedure
INFORMATION SECURITY MANAGEMENT		
Organizational policies, regulations	**1:** 6.6 **2:** 6.6.1, 6.6.6	Information security policy
Information security requirements specification, Information security risk assessment procedure, security control procedure	**1:** 6.6 **2:** 6.6.6, 6.6.7	Information security plan
information security plan, incident management plan	**1:** 6.6	Incident management procedure
Information Security plan, monitoring and control report, incident management procedures, incident records	**1:** 6.6 **2:** 6.6.6	Incident report

Typical Input information items	ISO/IEC 20000-1: 2005 or ISO/IEC 20000-2: 2005 clause	Output information item
Incident record, problem record	**2:** 6.6.7	Improvement plan
BUSINESS RELATIONSHIP MANAGEMENT		
SLA, contract, service management plan, problem report, monitoring and control report, cost report, business relationship management procedure	**1:** 7.2 **2:** 7.2.1	Review minutes
SLA, contract, service management plan, problem report, incident report (complaint)	**1:** 7.2	Change request
SLA, service management plan, complaint procedure	**1:** 7.2 **2:** 7.2.2	Complaint
Agreement, SLA, service management plan	**2:** 7.2.2, 7.2.3	Complaint procedure
Problem report, customer satisfaction survey (measurements)	**2:** 7.2.2, 7.2.3	Improvement plan
SLA, contract, compliment, complaint	**2:** 7.2.3	Customer satisfaction survey
SUPPLIER MANAGEMENT		
Organizational policy, service management plan, service level agreement	**1:** 7.3 **2:** 7.3.1, 7.3.3, 7.3.4	Supplier management procedure
Service management plan, contract	**1:** 7.3	Service level agreement (SLA)
System requirements specification	**1:** 7.3	Interface description
Service level agreement, service management plan, service catalog, change request	**2:** 7.3.2, 7.3.3, 7.3.4	Contract (and contract changes)
Contract, SLA, monitoring and control report	**2:** 7.3.2	Service report
Service management plan	**2:** 7.3.3	Service catalog
INCIDENT MANAGEMENT		
known error and problem resolution, service request	**1:** 8.2 **2:** 8.2.1	Incident report
Change management procedure, service management plan, configuration management database	**1:** 8.2 **2:** 8.2.2	Incident management procedure
Problem report, Review minutes	**2:** 8.2.2	Improvement plan
PROBLEM MANAGEMENT		
Incident report	**1:** 8.3	Problem report
SLA, service management plan	**1:** 8.3 **2:** 8.3.7	Problem management procedure
Service management plan, SLA, problem report, monitoring and control report, review minutes	**1:** 8.3, 8.3.9	Improvement plan
Problem report, Review minutes, user documentation	**2:** 8.3.10	Training documentation
Problem report	**1:** 8.3 **2:** 8.3.4	Change request
Problem report, Review minutes	**2:** 8.3.9, 8.3.10	User documentation

Typical Input information items	ISO/IEC 20000-1: 2005 or ISO/IEC 20000-2: 2005 clause	Output information item
CONFIGURATION MANAGEMENT		
System design description	**1:** 9.1	Interface description
System management policies, System design description, service level agreement, system requirements specification, configuration management policy	**1:** 9.1 **2:** 9.1.1	Configuration management plan and policy
Configuration management plan	**1:** 9.1	Configuration management procedure
Configuration management procedure, configuration records	**2:** 9.1.4	Configuration status report
Configuration management procedure	**2:** 9.1.5	Audit report
incident record, monitoring and control report	**2:** 9.1.5	Improvement plan
CHANGE MANAGEMENT		
System management policies, change requests, service catalog, service availability and continuity plan, Service management plan, problem management procedure, SLA, service availability and continuity plan, changes to cost estimates	**1:** 9.2 **2:** 9.2.1	Configuration management plan and policy (change management plan and policy)
Problem report, configuration status report	**1:** 9.2 **2:** 5.1.2, 9.2.1, 9.2.2	Change request
Configuration management plan, problem management procedure, SLA,	**1:** 9.2	Configuration management procedure (change management procedure)
SLA, change request, Configuration management procedure,	**1:** 9.2 **2:** 9.2.1, 9.2.4	Monitoring and control report
SLA, problem report	**1:** 9.2 **2:** 9.2.2	Improvement plan
Change request	**2:** 9.2.2	Evaluation report
Configuration management plan, audit plan, Configuration management database	**1:** 9.2	Audit procedure
RELEASE MANAGEMENT		
Change management policy, Release policy and plan, Release record	**1:** 10.1 **2:** 10.1.4	Configuration management plan and policy (release management plan and policy)
Test plan, verification plan, acceptance plan, disposal plan	**2:** 10.1.2, 10.1.3, 10.1.8	Release plan
Release record, release management plan	**2:** 10.1.1, 10.1.7	Service level agreement (SLA)
Change request, SLA	**1:** 10.1 **2:** 10.1.2, 10.1.7	Configuration management procedure (release management procedure)
SLA, problem report	**1:** 9.3 **2:** 10.1.9	Improvement plan
Release plan, installation plan, integration and test plan	**2:** 10.1.5, 10.1.7, 10.1.8	User documentation
Service level agreement, release plan	**2:** 10.1.8	Customer satisfaction survey

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 15288:2008 (IEEE Std 15288-2008), and ISO/IEC 20000-1:2005 and ISO/IEC 20000-2:2005. 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, 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.

NOTE Consistent with the ISO 9000 series, the purpose of a record is to state results achieved or to provide evidence of activities performed by an organizational entity.

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

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 15288:2008 (IEEE Std 15288-2008), ISO/IEC 20000-1:2005, and ISO/IEC 20000-2:2005. 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” may 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 and ISO/IEC 20000-2:2005 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 standard, 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
Assessment record	Life cycle model management, Project assessment and control, Service management, Information security management	**12207:** 6.2.1.3.2.1, 6.2.1.3.3.2, 6.3.2.2, B.3.3.2.2 **20000-2:** 4.3, 6.6.3, 9.1.5	Information and data related to the use of the standard process for specific projects and services
Availability record	Service continuity and availability management	**20000-2:** 6.3.2	Response time compared to SLA, actual available time divided by planned available time
Complaint record (compliment record)	Business relationship management	**20000-1:** 7.2 **20000-2:** 7.2.2, 7.3.5	Variance, defect, or non-conformance; complaint category, correction actions, known error, assigned responsibility, resolution. *See* problem report, change request
Configuration record (asset record, change record)	Configuration Management, Implementation, Maintenance, Disposal, Reuse Asset Management, Domain engineering Transition, Information security management, Problem management, Release management	**15288:** 6.2.5.3b), 6.4.4.3b) **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 **20000-1:** 9.1, 9.2, 10.1, **20000-2:** 5.1.2, 6.6.2, 8.3.3, 9.1.1, 9.1.2, 9.1.4, 9.1.5, 9.2.1, 9.2.4, 10.1.8	Functional and physical characteristics, configuration status; approvals and authorizations; 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. *See also* change request, problem record, release record, software item configuration record, system element description.
Decision record	Decision Making	**15288:** 6.3.3.1, 6.3.3.3.1 **12207:** 5.1.2, 6.3.3.1	Decision, assumptions, and rationale
Disposal record	Disposal	**12207:** 6.4.11.1, 6.4.11.2.e)	Disposal actions for future risk and impact analysis
Incident record (security incident record, service request record)	Maintenance, Supply, Information security management, Incident management, Change management, Problem Management, Release management	**15288:** 6.4.10.3.b)2) **20000-1:** 6.6, 7.2, 8.2 **20000-2: 8.2.1**, **8.3.3,** 8.3.6, 8.3.7, 9.2.1, 9.2.2, 10.1.7	Incident, variance, defect, or non-conformance; incident category, fault correction actions, known error, assigned responsibility, resolution. *See* incident report, change request

Record	Process	Reference	Record Contents
Information item storage record	Information Management	**12207:** 6.3.6.2, 6.3.6.3.2.2 **15288:** 6.3.6.2d), 6.3.6.3 b)	Information status, version description, distribution record, security classification
Knowledge management record	Human resource Management, Disposal, Incident management, Problem management	**12207:** 6.2.4.3.3.5 **15288:** 6.2.4.3, 6.4.11.3b) **20000-2:** 8.1.2, 8.2.1, 8.3.3	Knowledge, recommended applicability
Personnel skills record	Human resource management	**15288:** 6.2.4.3a)2) **20000-2:** 3.3.1	Employee identifier, skill, level of proficiency. *See also* Skill development record
Problem record	Decision management, Integration, Maintenance, Project assessment and control, Software review, Software audit, Software operations, Software quality assurance, Software problem resolution, Software verification, Software validation, Domain engineering, Reuse management, Configuration management, Incident management, Problem management	**15288:** 6.3.3.3, 6.4.5.3, 6.4.10.1, 6.4.10.2 **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 **20000-1:** 8.2, 8.3, 9.1 **20000-2:** 6.3.2, 8.2.1, 8.3.3, 8.3.6, 8.3.7, 9.2.1, 10.1.7	Problem, variance, defect, or non-conformance; problem category, associated configuration item, fault correction actions, known error, assigned responsibility, resolution. *See also* problem report, change request
Process control record	Service Management	**20000-2:** 3.2, 4.4.2	Data on the results of applying the process, service quality level
Quality activity record	Software quality assurance, Improvement	**12207:** 7.2.3.3.1.3.c), 7.2.3.3.1.4, 7.2.3.3.1.5	Execution of the quality activity, Assessment activity
Quality cost data	Life Cycle Model Management	**12207:** 6.2.1.3.3.3	Establish the cost of preventing and resolving problems and non-conformities and support process improvement

Record	Process	Reference	Record Contents
Release record	Supply, Software Operation, Release management, Configuration management	**12207:** 6.4.9.3.1.3, B.3.2.3.2 **20000-2**: 9.1.2	Identifies, tracks, and controls a configuration item 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.
Requirement record	Stakeholder requirements definition Service reporting	**15288:** 6.4.1.3 **12207:** 6.4.1.3.5.1 **20000-2:** 6.2.1	Traceability, priority, constraints, required services, usability of interactions, health and safety, security, environment
Risk profile	Risk Management, Stakeholder Requirements Definition. Operations, Software review, Service Management, Information Security Management	**15288:** 6.3.4.3 b) **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) **20000-1**: 4.2 **20000-2**: 6.6.3	Source, probability, consequence, acceptability threshold, priority, risk action requests, treatment strategy, status. Stored in a *risk register*.
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
Skill development record (training record)	Human Resource Management	**12207:** 6.2.4.3.2.3, 6.2.4.3.3.5 **15288:** 6.2.4.3b)4) **20000-2**: 3.3.1, 3.3.2	Skill area, employee identifying data, duration of training, proficiency level, certifying authority

Record	Process	Reference	Record Contents
Test result	Development, 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 **20000-1**: 6.3 **20000-2:** 6.3.4	Result of testing, 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 tem, 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 15288:2008 (IEEE Std 15288-2008), and ISO/IEC 20000-1:2005 and 20000-2:2005.

In this International Standard, 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.

10.2 Acceptance plan

ISO/IEC 15288:2008 (IEEE Std 15288-2008) reference: 6.3.1.3.b)

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

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 review and testing report

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

Generic type: Report

The acceptance review and testing report states that an acquirer has reviewed and tested a product. It indicates whether the product is accepted.

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

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

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

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 20000-1:2005 reference: 4.3

ISO/IEC 20000-2:2005 reference: 4.3

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, the subjects of the audits, including work products and records to be reviewed, 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 20000-1:2005 reference: 4.3, 9.1, 9.2

Generic type: Procedure

The audit procedure includes the audit criteria, scope, frequency, and methods for conducting audits. It outlines how deficiencies will be recorded and reported and who is responsible for 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 20000-1:2005 reference: 4.3

ISO/IEC 20000-2:2005 reference: 9.1.5

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 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 findings.

10.10 Capacity plan

ISO/IEC 20000-1:2005 reference: 6.5

ISO/IEC 20000-2:2005 reference: 6.5

Generic type: plan

The capacity plan documents the predicted or actual performance of the infrastructure systems in terms of component and resource utilization. It includes estimates of future workload (capacity requirements). It defines the approach for predictive analysis to determine when and how much additional capacity should be acquired to upgrade the service. It includes or references proposals with cost estimates for recommended solutions. The capacity plan should be updated at least annually.

10.11 Capacity management procedure

ISO/IEC 20000-1:2005 reference: 6.5

The capacity management procedures explain how the organization monitors and provides adequate capacity, and tunes service performance.

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, 6.3.9.3.4.3, 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 20000-1:2005 reference: 2.11, 4.4.2, 6.5, 7.2, 9.1, 9.2, 10.1.

ISO/IEC 20000-2:2005 reference: 5.1.2, 9.1.3, 9.2.1, 9.2.2

Generic type: Request

A change request identifies a configuration item, system, service, hardware, software, interface, asset, or documentation problem or desired improvement, and requests modifications. 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, functions or problem to be corrected; priority, assumptions and constraints. It may address the impact to schedules, cost, products, and test.

See also: problem report

NOTE Change requests should be recorded and may use the same system that records complaints, incidents and problems.

10.13 Complaint procedure

ISO/IEC 20000-1:2005 reference: 7.2

ISO/IEC 20000-2:2005 reference: 7.2.2

Generic type: Procedure

The complaint procedure defines what constitutes a complaint (a record of perceived non-compliance with a service level agreement or customer dissatisfaction with service). 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.

See also: incident management procedure, incident report, problem management procedure, problem report

10.14 Concept of operations

ISO/IEC 15288:2008 (IEEE Std 15288-2008) reference: 6.4.1.2.a), D.4.a

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

Generic type: Description

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

a) a description of how a system will work 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

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

The concept of operations may include the following:

a) 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.

b) 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

c) 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

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

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

See also: product need assessment, system requirements specification

NOTE IEEE 1362-1998 (R2007) *IEEE Guide for Information Technology-System Definition -Concept of Operation Document* provides additional guidance.

10.15 Configuration management plan and policy

ISO/IEC 15288:2008 (IEEE Std 15288-2008) reference: 6.3.5.3

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

ISO/IEC 20000-1:2005 reference: 9.1, 9.2, 10.1

ISO/IEC 20000-2:2005 reference: 9.1.1, 10.1.2, 10.1.4

Generic type: Plan, Policy

The configuration management (CM) policy (or change management or release policy) includes the policy for how a configuration item and its components are defined. The change management policy defines what constitutes an emergency change, and responsibilities for authorizing and implementing normal and emergency changes. The release policy establishes the expected frequency and type of releases, authority for the release into acceptance test and production environments, schema for uniquely identifying a release and its contents, and the approaches for grouping changes into a uniquely identified release, automating the release, and verifying and accepting the release.

NOTE 1 Configuration management policy may be included in the configuration management plan or as a separate set of policies. Similarly, Release policy may be included in a release management plan or as a separate set of policies.

As stated in ISO/IEC 20000-1:2005, configuration management should be planned and implemented with change and release management. The configuration management (CM) plan (or change management or release 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 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 will perform:

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

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

A Release management plan provides overall direction for release planning. A specific Release plan includes the applicable details for a specific release.

NOTE 2 IEEE 828-2005 *IEEE Standard for Software Configuration Management Plans* provides additional guidance.

See also: release plan

10.16 Configuration management procedure

ISO/IEC 20000-1:2005 reference: 9.1, 9.2. 10.1

ISO/IEC 20000-2:2005 reference: 9.2.1, 10.1.2, 10.1.7

Generic type: Procedure

The configuration management procedure (or change management or release management procedure) presents how to perform the detailed activities for the configuration management or change management or release processes. As stated in ISO/IEC 20000-1:2005, the release management process should be integrated with the configuration and change management processes.

The procedures include the following:

a) process implementation

b) configuration identification

c) configuration control

d) change management

e) procedures to validate the completeness and correctness of systems and software releases

f) configuration status accounting

g) configuration evaluation

h) release management and delivery

i) a defined procedure for management of emergency changes or releases when the normal procedure is insufficient.

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

They should include the following:

a) procedures for initial baselining of work products

b) logging and analysis of the impact of change requests

c) documenting the scope of changes

d) change control board operations

e) tracking of changes in progress

f) updating configuration data

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

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

10.17 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 20000-2:2005 reference 6.5, 9.1.1, 9.1.4, 9.2.1

Generic type: Report

The configuration status report (or change management report) provides the status of controlled configuration items, including baselines, release identifiers, and location of the item or software master version. 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.

10.18 Contract

ISO/IEC 15288:2008 (IEEE Std 15288-2008) reference: 6.1.1.2, 6.1.1.3, 6.1.2.2, 6.1.2.3, 6.1.3.3

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 20000-2:2005 reference: 7.3.2, 7.3.3, 7.3.4

Generic type: Specification

A contract is the formal agreement between an acquirer and a supplier. It addresses the following:

a) identification of the performing organizations

b) statement of work to be performed, with tasks based on a service management process or a system 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 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

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.

Informally, commitments or agreements may be specified between parts of the same organization (sometimes called a memorandum of understanding).

10.19 Customer satisfaction survey

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

ISO/IEC 20000-2:2005 reference: 7.2.3, 10.1.8

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.

10.20 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

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:

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

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

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

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

e) the types of errors affecting the database and the handling of those errors

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

The database detailed design may specify

a) database access methods

b) data entities and their relationships

c) security and integrity constraints

d) data retention requirements

e) expected size of the data elements.

10.21 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 system 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

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

10.22 Disposal plan

ISO/IEC 15288:2008 (IEEE Std 15288-2008) reference: 6.4.11.3

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

ISO/IEC 20000-1:2005 reference: 5

Generic type: Plan

The disposal plan (or retirement plan) presents how activities will be 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; and plans for system disposal or archiving of the software and documentation. 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.

10.23 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 will receive or have access to restricted documents. The documentation plan should include the controlling template or standard for each document.

See also: information management plan.

10.24 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.

10.25 Evaluation report

ISO/IEC 15288:2008 (IEEE Std 15288-2008) reference: 6.2.5.3

ISO/IEC 12207:2008 (IEEE Std 12207-2008) reference: 6.1.2.3.1.15, 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 20000-2:2005 reference: 9.2.2

Generic type: Report

The evaluation report provides results of reviews and evaluations, such as an evaluation of design constraints, customer satisfaction, analysis of change records, or financial variances. It includes evaluation criteria. Evaluations may be based on criteria of traceability, consistency, testability, usability and customer

satisfaction, and feasibility. It 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, review minutes, service report, validation report, and verification report.

10.26 Implementation procedure

ISO/IEC 15288:2008 (IEEE Std 15288-2008) reference: 6.4.4.3.b)

Generic type: Procedure

The implementation procedure details how the system or system elements will be 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

10.27 Improvement plan

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

ISO/IEC 15288:2008 (IEEE Std 15288-2008) reference: 6.2.1.3, 6.3.4.3

ISO/IEC 20000-1:2005 reference: 4.3, 4.4.2, 4.4.3, 6.1, 8.3, 8.3.9, 9.2, 9.3, 10.1

ISO/IEC 20000-2:2005 reference: 4.3, 4.4.2, 6.1.3, 6.6.7, 7.2.2, 7.2.3, 8.2.2, 8.3.9, 9.1.5, 9.2.2, 10.1.9

Generic type: Plan

The improvement plan 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 plan includes how processes will be reviewed, and recommended improvements and change requests will be 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) will 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 15504-4, *Information technology — Process assessment — Part 4: Guidance on use for process improvement and process capability determination* provides additional guidance.

10.28 Improvement policy

ISO/IEC 20000-1:2005 reference: 4.4.1

ISO/IEC 20000-2:2005 reference: 4.4.1

Generic type: Policy

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 improvement will be incorporated into plans for specific processes and services. It identifies roles and responsibilities for improvement activities.

10.29 Incident management procedure

ISO/IEC 20000-1:2005 reference: 6.6, 8.2, 8.3

ISO/IEC 20000-2:2005 reference: 6.6.6, 8.2.2, 8.3.7.

Generic type: Procedure

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

See also: problem management procedure

10.30 Incident report

ISO/IEC 20000-1:2005 reference: 6.6, 8.2

ISO/IEC 20000-2:2005 reference: 6.6.6, 8.2.1

Generic type: Report

The incident report, or security incident report, addresses issues or non-conformance (deviance) with contract requirements, reported customer concerns. The report may be a consolidation 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

a) reporting control number and related control information

b) identification of the incident reporter

c) the 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

h) 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

l) information from organizational (internal) reviews.

NOTE ISO/IEC 20000-1:2005 and ISO/IEC 20000-2:2005 distinguish between incident reports and problem reports. 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: problem report, change request

10.31 Information management plan

ISO/IEC 15288:2008 (IEEE Std 15288-2008) reference: 6.3.6.3, D.4.m)

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

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

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 will receive or have access to restricted information

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

The knowledge management plan includes the definition of the infrastructure and training to support the contributors and the users of the organization's knowledge assets, the classification schema for the assets, and the asset criteria.

See also: Documentation plan

10.32 Information security plan

ISO/IEC 20000-1:2005 reference: 6.6

ISO/IEC 20000-2:2005 reference: 6.6.6, 6.6.7

Generic type: plan

The information security plan includes the following:

a) description of how the organization will identify, control, and protect the physical and logical security of systems, assets, and information

b) description of how requirements for confidentiality, integrity, and availability of information will be implemented

c) description of how the system or service will deny unauthorized access, permit authorized access, secure data in transmission, storage, and processing, and provide security in a cost-effective manner

d) description of how security risks and related controls, including access controls, will be identified

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

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

NOTE ISO/IEC 27002:2005, *Information technology — Security techniques — Code of practice for information security management* provides guidelines for information security management. ISO/IEC 27001:2005, *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.

10.33 Information security policy

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

ISO/IEC 20000-1:2005 reference: 6.6

ISO/IEC 20000-2:2005 reference: 6.6.1, 6.6.5

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 risk management and for establishing and monitoring security controls, including audits

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

10.34 Installation plan

ISO/IEC 15288:2008 (IEEE Std 15288-2008) reference 6.4.7.3

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.

10.35 Installation report

ISO/IEC 15288:2008 (IEEE Std 15288-2008) reference 6.4.7.3

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

Generic type: Report

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

10.36 Integration and test report

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

ISO/IEC 20000-2:2005 reference: 9.1.2

Generic type: Report

Based on the system or software requirements, the integration and test report presents the results from 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 integration 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 test procedures.

10.37 Integration plan

ISO/IEC 15288:2008 (IEEE Std 15288-2008) reference: 6.4.4.3, 6.4.5.3

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 approach to 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 tools and equipment. For software, the integration plan defines how the software units and components will be 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.

See also: Improvement plan

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

10.38 Interface description

ISO/IEC 15288:2008 (IEEE Std 15288-2008) reference: 6.4.3.3

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

ISO/IEC 20000-1:2005 reference: 7.3, 9.1

Generic type: Description

The interface description describes the interface entity 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, 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.

10.39 Life cycle policy and procedure

ISO/IEC 15288:2008 (IEEE Std 15288-2008) reference: 6.2.1.2, 6.2.1.3, 6.2.3.3 b) 1) iii), A.2.3, B.2.3

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

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.

10.40 Maintenance plan

ISO/IEC 15288:2008 (IEEE Std 15288-2008) reference: 6.4.10.3

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

Generic type: Plan

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

a) the objectives, strategy, and approach for the system 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

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.

10.41 Maintenance procedure

ISO/IEC 15288:2008 (IEEE Std 15288-2008) reference: 6.4.10.3

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

Generic type: Procedure

The maintenance procedure covers the processes for receiving, recording, and tracking problem reports and change requests (modification requests) from users, 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 system 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.

10.42 Measurement plan

ISO/IEC 15288:2008 (IEEE Std 15288-2008) reference: 6.3.7.3

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

ISO/IEC 20000-2:2005 reference: 4.3

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 will be evaluated. Items to be measured include the achievement of service targets, customer satisfaction, resource utilization, major issues, and trends.

10.43 Monitoring and control report

ISO/IEC 15288:2008 (IEEE Std 15288-2008) reference: 6.3.2.3, 6.3.4.3b), 6.3.7.1, 6.3.7.3 b)

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 20000-1:2005 reference: 4.c), 6.1, 9.2

ISO/IEC 20000-2:2005 reference: 6.1.3, 6.3.2, 1: 9.2, 9.2.1, 9.2.4

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

e) 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.

10.44 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 ensure testing occurred as planned. It explains use of the organization's problem resolution procedure.

See also: qualification test procedure

10.45 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 20000-1:2005 reference: 6.6, 8.3

ISO/IEC 20000-2:2005 reference: 7.2.2, 7.2.3, 8.3.7.

Generic type: Procedure

The problem management procedure defines how to receive record, prioritize, escalate, resolve, and close problems; how to control 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, classification, root cause analysis, trend analysis, problem escalation, problem resolution, status tracking and reporting, and problem records management.

NOTE For ISO/IEC 20000, the problem management procedures are separate from, but related to the procedures for incidents, fulfilment of service requests, and customer complaints.

See also: incident management procedure

10.46 Problem report

ISO/IEC 15288:2008 (IEEE Std 15288-2008) reference: 6.3.3.3a) 2), 6.4.5.3b), 6.4.6.2.b), 6.4.6.3b), 6.4.7.2.e), 6.4.7.3b), 6.4.8.3b), 6.4.9.2.c), 6.4.10.2.e, 6.4.10.3b)

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 20000-1:2005 reference: 8.3

ISO/IEC 20000-2:2005 reference: 8.3.6

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) 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

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 20000-1:2005 and ISO/IEC 20000-2:2005 distinguish between incident reports and problem reports. 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

10.47 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.

10.48 Process improvement analysis report

ISO/IEC 15288:2008 (IEEE Std 15288-2008) reference: 6.2.1.3 c), 6.3.7.3 c)

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

Generic type: Report

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

10.49 Product need assessment

ISO/IEC 15288:2008 (IEEE Std 15288-2008) reference: 6.1.2.3

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

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

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

a) analysis of improvements, disadvantages and limitations, and considered alternatives and tradeoffs

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

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

d) preliminary information on contract type

e) current and potential organizational responsibilities

f) risk identification and risk management methods.

See also: concept of operations

10.50 Progress report

ISO/IEC 15288:2008 (IEEE Std 15288-2008) reference: 6.1.2.3, 6.2.3.3, 6.3.2.2, 6.3.2.3, 6.3.3.2, 6.3.3.3

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 20000-1:2005 reference: 4.2, 4.3, 4.4.2, 4.4.3, 5

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 service 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; corrective actions; risk treatment actions; and problem tracking and problem analysis.

10.51 Project management plan

ISO/IEC 15288:2008 (IEEE Std 15288-2008) reference: 6.1.2.3, 6.2.3.3, 6.3.1.1, 6.3.1.2, 6.3.1.3

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

Generic type: Plan

The project management plan presents how the project processes and activities will be 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

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:

a) procedures for replanning

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

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

d) 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.

See also: service management plan

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

NOTE 2 IEEE 1058-1998, *IEEE Standard for Software Project Management Plans* provides additional guidance.

10.52 Proposal

ISO/IEC 15288:2008 (IEEE Std 15288-2008) reference: 6.1.1.3, 6.1.2.2, 6.1.2.3

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

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.

10.53 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 will be conducted, and the conditions that are 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.

10.54 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.

10.55 Quality management plan

ISO/IEC 15288:2008 (IEEE Std 15288-2008) reference: 6.2.5.3, 6.3.1.3

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

Generic type: Plan

The quality management plan (or quality assurance plan), in accordance with ISO/IEC 9001:2008 or other quality standard, presents the approach to fulfil the quality aspects of the 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

d) standards, 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 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 system or software configuration items and media

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

10.56 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 15288:2008 (IEEE Std 15288-2008) reference: 6.2.5.2, 6.2.5.3, 6.2.5.3.1.1

ISO/IEC 20000-2:2005 reference: 4.4.1

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 will be 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 will be 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, software quality assurance, software audit, verification, validation, and process improvement processes.

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

10.57 Release plan

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

ISO/IEC 20000-1:2005 reference: 10.1

ISO/IEC 20000-2:2005 reference: 10.1.1, 10.1.3, 10.1.8

Generic type: Plan

The release plan (or migration plan or roll-out plan or deployment plan) presents how a system, service, or software product or software release will be transferred to a new environment, with the release dates. It includes the deliverables, including updates to related SLA, operational procedures, and user documentation. It references the related change requests, identified configuration items, known errors, and problems. It should include identified risks, potential problems, and suggested resolutions. It covers how the release is authorized, scheduled, coordinated, and tracked. The migration plan includes the description of deliverables, dependencies, and scheduled dates, the expected configuration of the target environment at the time of migration, the backout or recovery plans, verification and acceptance procedures, and communication and training for the customer and support staff. It should include planning for decommissioning of replaced systems or services.

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

10.58 Request for proposal (RFP)

ISO/IEC 15288:2008 (IEEE Std 15288-2008) reference: 6.1.1.3

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

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)

j) supporting processes and their performing organizations, including responsibilities (if other than supplier), so suppliers may, 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.

10.59 Resource request

ISO/IEC 15288:2008 (IEEE Std 15288-2008) reference: 6.3.1.3.d), 6.3.2.3.b

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

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.

10.60 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 will be conducted to support the reuse of systems or software assets and related documents. It defines the reuse strategy, domains where reuse will be managed, and the implementation approach, including infrastructure support.

10.61 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 20000-1:2005 reference: 7.2

ISO/IEC 20000-2:2005 reference: 7.2.1

Generic type: Report

The Review minutes (or joint review minutes or service review minutes) provide a report of a review conducted by the acquirer and the supplier. Minutes include attendees, agenda, product or service under review, entry and exit points for the review, main discussion topics, assumptions, presentation material, 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.

10.62 Risk action request

ISO/IEC 15288:2008 (IEEE Std 15288-2008) reference: 6.3.4.3.

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

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.

10.63 Risk management policy and plan

ISO/IEC 15288:2008 (IEEE Std 15288-2008) reference: 6.3.4.3

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

Generic type: Plan, policy

The risk management policy and plan presents the conditions under which risk management will be 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.

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

10.64 Service availability and continuity plan

ISO/IEC 20000-1:2005 reference: 6.3

ISO/IEC 20000-2:2005 reference: 6.1.2, 6.3.4

Generic type: Plan

The service availability and continuity plan describes the provisions to make services available in the event of failure of a site or a system component. The service continuity plan shall be available in printed media to all concerned. A copy of the service continuity plan and applicable agreements and contracts shall be available at a secure remote location where it is planned that alternate service will be provided. It includes the following:

a) availability requirements for the service as stated in the service level agreements

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

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

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

e) procedures for restoring service

f) procedures for testing the continuity plan

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

10.65 Service catalog

ISO/IEC 20000-2:2005 reference: 6.1.1, 7.3.3

Generic type: Description

The service catalog describes the information technology services available for customers. 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 contact points for requesting assistance or reporting incidents; and summarizes service levels as further specified in the service level agreement (SLA).

10.66 Service level agreement (SLA)

ISO/IEC 20000-1:2005 reference: 2.13, 3.2, 5, 6.1, 7.3

ISO/IEC 20000-2:2005 reference: 6.1.2, 10.1.1, 10.1.7

Generic type: Specification

The service level agreement (SLA) is between a service provider and a customer, and should be authorized by the service supplier and acquirer. It specifies the following:

a) the requirements for the service

b) scope, and workload limits (upper and lower)

c) responsibilities of both supplier and customer

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

e) the procedures for incident and problem management, escalation, notifications, and complaints

f) the measures and acceptance criteria, such as performance, availability, service period, and operator and maintenance responsiveness

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

It may include targets beyond the minimal acceptable level of service.