INTERNATIONAL STANDARD

ISO/IEC/IEEE 90003

First edition
2018-11

Software engineering — Guidelines for the application of ISO 9001:2015 to computer software

Ingénierie du logiciel — Lignes directrices pour l'application de l'ISO 9001:2015 aux logiciels informatiques

Reference number
ISO/IEC/IEEE 90003:2018(E)

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

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

Email: stds.ipr@ieee.org
Website: www.ieee.org

Published in Switzerland

Contents

Page

Foreword ..... **v**

Introduction ..... **vi**

1 Scope **1**

2 Normative references **1**

3 Terms and definitions **2**

4 Context of the organization **3**
4.1 Understanding the organization and its context 3
4.2 Understanding the needs and expectations of interested parties 4
4.3 Determining the scope of the quality management system 5
4.4 Quality management system and its processes 6
4.4.1 Quality management system processes 6
4.4.2 Information Management 7

5 Leadership **8**
5.1 Leadership and commitment 8
5.1.1 General 8
5.1.2 Customer focus 9
5.2 Policy 9
5.2.1 Establishing the quality policy 9
5.2.2 Communicating the quality policy 10
5.3 Organizational roles, responsibilities and authorities 10

6 Planning **11**
6.1 Actions to address risks and opportunities 11
6.1.1 Risk identification 11
6.1.2 Risk treatment 12
6.2 Quality objectives and planning to achieve them 12
6.2.1 Establishing quality objectives 12
6.2.2 Implementation of quality objectives 13
6.3 Planning of changes 14

7 Support **14**
7.1 Resources 14
7.1.1 General 14
7.1.2 People 15
7.1.3 Infrastructure 15
7.1.4 Environment for the operation of processes 16
7.1.5 Monitoring and measuring resources 17
7.1.6 Organizational knowledge 18
7.2 Competence 19
7.3 Awareness 20
7.4 Communication 20
7.5 Documented information 21
7.5.1 General 21
7.5.2 Creating and updating 22
7.5.3 Control of documented information 22

8 Operation **23**
8.1 Operational planning and control 23
8.1.1 General 24
8.1.2 Evidence of conformity to requirements 25
8.2 Requirements for products and services 25
8.2.1 Customer communication 25
8.2.2 Determining the requirements for products and services 27
8.2.3 Review of the requirements for products and services 29

8.2.4 Changes to requirements for products and services ... 31
8.3 Design and development of products and services ... 31
8.3.1 General ... 31
8.3.2 Design and development planning ... 32
8.3.3 Design and development inputs ... 35
8.3.4 Design and development controls ... 36
8.3.5 Design and development outputs ... 39
8.3.6 Design and development changes ... 40
8.4 Control of externally provided processes, products and services ... 41
8.4.1 General ... 41
8.4.2 Type and extent of control ... 43
8.4.3 Information for external providers ... 43
8.5 Production and service provision ... 44
8.5.1 Control of production and service provision ... 44
8.5.2 Identification and traceability ... 47
8.5.3 Property belonging to customers or external providers ... 49
8.5.4 Preservation ... 50
8.5.5 Post-delivery activities ... 51
8.5.6 Control of changes ... 51
8.6 Release of products and services ... 52
8.7 Control of nonconforming outputs ... 53
8.7.1 Identification and control of nonconforming outputs ... 53
8.7.2 Retaining documented information for nonconforming outputs ... 54

9 Performance evaluation ... 54
9.1 Monitoring, measurement, analysis and evaluation ... 54
9.1.1 General ... 54
9.1.2 Customer satisfaction ... 55
9.1.3 Analysis and evaluation ... 56
9.2 Internal audit ... 56
9.2.1 Conducting audits ... 56
9.2.2 Maintaining audit records ... 57
9.3 Management review ... 57
9.3.1 General ... 57
9.3.2 Management review inputs ... 58
9.3.3 Management review outputs ... 59

10 Improvement ... 59
10.1 General ... 59
10.2 Nonconformity and corrective action ... 60
10.2.1 Managing nonconformity ... 60
10.2.2 Maintaining nonconformity records ... 61
10.3 Continual improvement ... 61

Annex A (informative) **Summary of guidance on the implementation of ISO 9001:2015 available in ISO/IEC JTC 1/SC 7 and ISO/TC 176 standards ... 62**

Bibliography ... 68

IEEE notices and abstract ... 70

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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

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.

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

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

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

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

This first edition cancels and replaces ISO/IEC 90003:2014, which has been technically revised.

The main changes compared to the previous edition are as follows:

— updating structure and contents to reflect the total revision of ISO 9001:2015;

— updating contents to reflect the revision of ISO/IEC/IEEE 12207:2017 and other SC 7 standards.

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

Introduction

ISO 9001:2015, Quality management systems — Requirements

Introduction

0.1 General

The adoption of a quality management system is a strategic decision for an organization that can help to improve its overall performance and provide a sound basis for sustainable development initiatives.

The potential benefits to an organization of implementing a quality management system based on this International Standard are:

a) the ability to consistently provide products and services that meet customer and applicable statutory and regulatory requirements;

b) facilitating opportunities to enhance customer satisfaction;

c) addressing risks and opportunities associated with its context and objectives;

d) the ability to demonstrate conformity to specified quality management system requirements.

This International Standard can be used by internal and external parties.

It is not the intent of this International Standard to imply the need for:

— uniformity in the structure of different quality management systems;

— alignment of documentation to the clause structure of this International Standard;

— the use of the specific terminology of this International Standard within the organization.

The quality management system requirements specified in this International Standard are complementary to requirements for products and services.

This International Standard employs the process approach, which incorporates the Plan-Do-Check-Act (PDCA) cycle and risk-based thinking.

The process approach enables an organization to plan its processes and their interactions.

The PDCA cycle enables an organization to ensure that its processes are adequately resourced and managed, and that opportunities for improvement are determined and acted on.

Risk-based thinking enables an organization to determine the factors that could cause its processes and its quality management system to deviate from the planned results, to put in place preventive controls to minimize negative effects and to make maximum use of opportunities as they arise.

Consistently meeting requirements and addressing future needs and expectations poses a challenge for organizations in an increasingly dynamic and complex environment. To achieve this objective, the organization might find it necessary to adopt various forms of improvement in addition to correction and continual improvement, such as breakthrough change, innovation and re-organization.

In this International Standard, the following verbal forms are used:

— “shall” indicates a requirement;

— “should” indicates a recommendation;

— “may” indicates a permission;

— “can” indicates a possibility or a capability.

Information marked as “NOTE” is for guidance in understanding or clarifying the associated requirement.

0.2 Quality management principles

This International Standard is based on the quality management principles described in ISO 9000. The descriptions include a statement of each principle, a rationale of why the principle is important for the organization, some examples of benefits associated with the principle and examples of typical actions to improve the organization's performance when applying the principle.

The quality management principles are:

— customer focus;

— leadership;

— engagement of people;

— process approach;

— improvement;

— evidence-based decision making;

— relationship management.

0.3 Process approach

0.3.1 General

This International Standard promotes the adoption of a process approach when developing, implementing and improving the effectiveness of a quality management system, to enhance customer satisfaction by meeting customer requirements. Specific requirements considered essential to the adoption of a process approach are included in 4.4.

Understanding and managing interrelated processes as a system contributes to the organization's effectiveness and efficiency in achieving its intended results. This approach enables the organization to control the interrelationships and interdependencies among the processes of the system, so that the overall performance of the organization can be enhanced.

The process approach involves the systematic definition and management of processes, and their interactions, so as to achieve the intended results in accordance with the quality policy and strategic direction of the organization. Management of the processes and the system as a whole can be achieved using the PDCA cycle (see 0.3.2) with an overall focus on risk-based thinking (see 0.3.3) aimed at taking advantage of opportunities and preventing undesirable results.

The application of the process approach in a quality management system enables:

a) understanding and consistency in meeting requirements;

b) the consideration of processes in terms of added value;

c) the achievement of effective process performance;

d) improvement of processes based on evaluation of data and information.

Figure 1 gives a schematic representation of any process and shows the interaction of its elements. The monitoring and measuring check points, which are necessary for control, are specific to each process and will vary depending on the related risks.

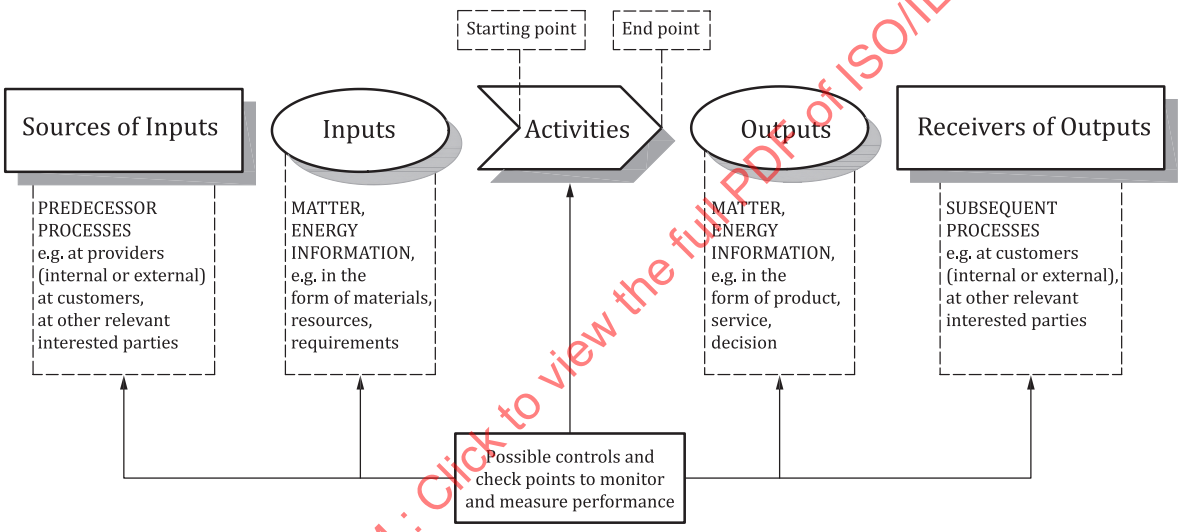
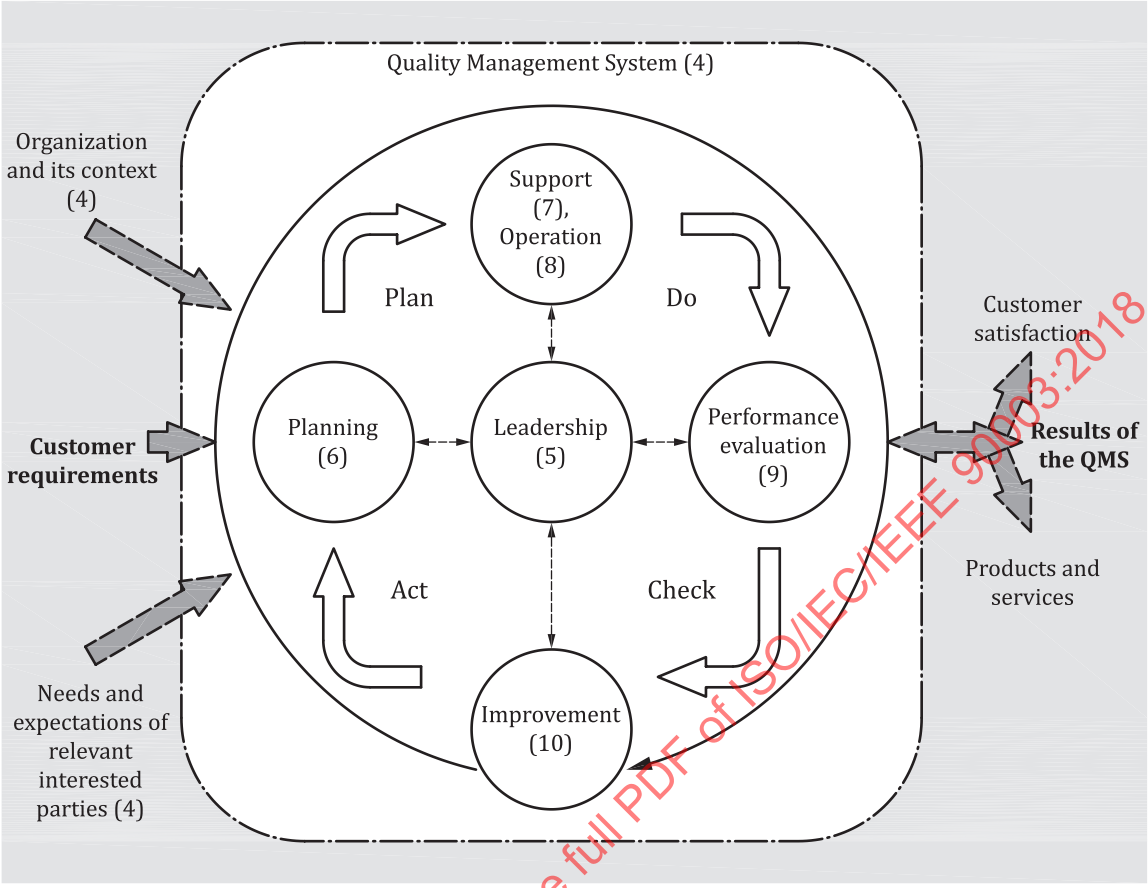


Figure 1 — Schematic representation of the elements of a single process

0.3.2 Plan-Do-Check-Act cycle

The PDCA cycle can be applied to all processes and to the quality management system as a whole. Figure 2 illustrates how Clauses 4 to 10 can be grouped in relation to the PDCA cycle.



NOTE Numbers in brackets refer to the clauses in this International Standard.

Figure 2 — Representation of the structure of this International Standard in the PDCA cycle

The PDCA cycle can be briefly described as follows:

— **Plan**: establish the objectives of the system and its processes, and the resources needed to deliver results in accordance with customers' requirements and the organization's policies, and identify and address risks and opportunities;

— **Do**: implement what was planned;

— **Check**: monitor and (where applicable) measure processes and the resulting products and services against policies, objectives, requirements and planned activities, and report the results;

— **Act**: take actions to improve performance, as necessary.

0.3.3 Risk-based thinking

Risk-based thinking is essential for achieving an effective quality management system. The concept of risk-based thinking has been implicit in previous editions of this International Standard including, for example, carrying out preventive action to eliminate potential nonconformities, analysing any nonconformities that do occur, and taking action to prevent recurrence that is appropriate for the effects of the nonconformity.

To conform to the requirements of this International Standard, an organization needs to plan and implement actions to address risks and opportunities. Addressing both risks and opportunities establishes a basis for increasing the effectiveness of the quality management system, achieving improved results and preventing negative effects.

Opportunities can arise as a result of a situation favourable to achieving an intended result, for example, a set of circumstances that allow the organization to attract customers, develop new products and services, reduce waste or improve productivity. Actions to address opportunities can also include consideration of associated risks. Risk is the effect of uncertainty and any such uncertainty can have positive or negative effects. A positive deviation arising from a risk can provide an opportunity, but not all positive effects of risk result in opportunities.

0.4 Relationship with other management system standards

This International Standard applies the framework developed by ISO to improve alignment among its International Standards for management systems.

This International Standard enables an organization to use the process approach, coupled with the PDCA cycle and risk-based thinking, to align or integrate its quality management system with the requirements of other management system standards.

This International Standard relates to ISO 9000 and ISO 9004 as follows:

— ISO 9000 *Quality management systems — Fundamentals and vocabulary* provides essential background for the proper understanding and implementation of this International Standard;

— ISO 9004 *Managing for the sustained success of an organization — A quality management approach* provides guidance for organizations that choose to progress beyond the requirements of this International Standard.

This International Standard does not include requirements specific to other management systems, such as those for environmental management, occupational health and safety management, or financial management.

Sector-specific quality management system standards based on the requirements of this International Standard have been developed for a number of sectors. Some of these standards specify additional quality management system requirements, while others are limited to providing guidance to the application of this International Standard within the particular sector.

A matrix showing the correlation between the clauses of this edition of this International Standard and the previous edition (ISO 9001:2008) can be found on the ISO/TC 176/SC 2 open access web site at: www.iso.org/tc176/sc02/public.

This document provides guidance for organizations in the application of ISO 9001:2015 to the acquisition, supply, development, operation and maintenance of computer software.

It identifies the issues that should be addressed and is independent of the technology, life cycle models, development processes, sequence of activities and organizational structure used by an organization. The guidance and identified issues are intended to be comprehensive but not exhaustive. Where the scope of an organization's activities includes areas other than computer software development, the relationship between the computer software elements of that organization's quality management

system and the remaining aspects should be clearly documented within the quality management system as a whole.

Clauses 4, 5, and 6 and parts of Clauses 8, 9 and 10 of ISO 9001:2015 are applied mainly at the “global” level in the organization, although they do have some effect at the “project/product level”. Each project or product development may tailor the associated parts of the organization’s quality management system to suit project/product-specific requirements.

This document provides guidance to assist in understanding how the provisions of ISO 9001:2015 apply in the context of software.

In addition to the software-specific guidance provided by this document, an organization can find generic guidance, applicable in all sectors, including software, in ISO/TS 9002:2016 helpful in gaining an understanding of how the requirements of ISO 9001:2015 can apply, in the context of software development. No new requirements are introduced in the guidance text of either document (i.e., no "shall"). In either document, where "should" is used, it is a recommendation of a requirement in ISO 9001:2015.

Organizations with quality management systems for developing, operating or maintaining software based on this document may choose to use processes from ISO/IEC/IEEE 12207 to support or complement the ISO 9001:2015 quality management system (QMS) requirements. The related clauses of ISO/IEC/IEEE 12207:2017 are referenced in each clause of this document; however, they are not intended to imply requirements additional to those in ISO 9001:2015. Further guidance to the use of ISO/IEC/IEEE 12207 can be found in ISO/IEC TR 24748–3. For additional guidance, references are provided to the International Standards for software engineering developed by ISO/IEC JTC 1/SC 7, and for information technology, developed by ISO/IEC JTC 1/SC 27. Where these references are specific to a clause or sub-clause of ISO 9001:2015, they appear after the guidance for that clause or sub-clause.

Where they apply generally across the parts of a clause or sub-clause, the references are included at the end of the last part of the clause or sub-clause.

Where text has been quoted from ISO 9001:2015, that text is enclosed in a box for ease of identification.

Software engineering — Guidelines for the application of ISO 9001:2015 to computer software

1 Scope

ISO 9001:2015, Quality management systems — Requirements

1 Scope

This International Standard specifies requirements for a quality management system when an organization:

a) needs to demonstrate its ability to consistently provide products and services that meet customer and applicable statutory and regulatory requirements, and

b) aims to enhance customer satisfaction through the effective application of the system, including processes for improvement of the system and the assurance of conformity to customer and applicable statutory and regulatory requirements.

All the requirements of this International Standard are generic and are intended to be applicable to any organization, regardless of its type or size, or the products and services it provides.

NOTE 1 In this International Standard, the terms "product" or "service" only apply to products and services intended for, or required by, a customer.

NOTE 2 Statutory and regulatory requirements can be expressed as legal requirements.

This document provides guidance for organizations in the application of ISO 9001:2015 to the acquisition, supply, development, operation and maintenance of computer software and related support services. It does not add to or otherwise change the requirements of ISO 9001:2015.

Annex A provides a table pointing to additional guidance on the implementation of ISO 9001:2015, available in ISO/IEC JTC 1/SC 7, ISO/IEC JTC 1/SC 27 and ISO/TC 176 International Standards.

The guidelines provided in this document are not intended to be used as assessment criteria in quality management system registration/certification. However, some organizations can consider it useful to implement the guidelines proposed in this document and can be interested in knowing whether the resultant quality management system is compliant or not with this document. In this case, an organization can use both this document and ISO 9001 as assessment criteria for quality management systems in the software domain.

2 Normative references

ISO 9001:2015, Quality management systems — Requirements

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 9000:2015, *Quality management systems — Fundamentals and vocabulary*

3 Terms and definitions

ISO 9001:2015, Quality management systems — Requirements

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 9000:2015 apply.

For the purposes of this document, the terms and definitions given in ISO 9000:2015 and the following apply.

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

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

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

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

3.1
baseline
formally approved version of a *configuration item* (3.2), regardless of media, formally designated and fixed at a specific time during the *configuration item's* (3.2) life cycle

[SOURCE: ISO/IEC/IEEE 12207:2017, 3.1.11]

3.2
configuration item
item or aggregation of hardware, software, or both, that is designated for configuration management and treated as a single entity in the configuration management process

[SOURCE: ISO/IEC/IEEE 12207:2017, 3.1.15, modified — The EXAMPLE has been removed.]

3.3
COTS
Commercial-Off-The-Shelf
product available for purchase and use without the need to conduct development activities

3.4
implementation
process of translating a design into hardware components, software components, or both

3.5
life cycle model
framework of processes and activities concerned with the life cycle that can be organized into stages, which also acts as a common reference for communication and understanding

[SOURCE: ISO/IEC/IEEE 12207:2017, 3.1.27, modified — The word "acting" has been replaced with "which also acts".]

3.6
regression testing
testing following modification to a test item or to its operational environment, to identify whether regression failures occur

Note 1 to entry: The sufficiency of a set of regression test cases depends on the item under test and on the modifications to that item or its operational environment.

[SOURCE: ISO/IEC/IEEE 29119-1:2013, 4.32]

3.7
replication
copying a *software product* (3.9) from one medium to another

3.8
software element
identifiable part of a *software product* (3.9)

3.9
software product
set of computer programs, procedures, and possibly associated documentation and data

Note 1 to entry: A software product may be designated for delivery, an integral part of another product, or used in development.

Note 2 to entry: This is different from the term "product" in ISO 9000:2015, 3.7.6.

Note 3 to entry: For the purposes of this document, “software” is synonymous with “software product”.

Note 4 to entry: Software includes firmware.

[SOURCE: ISO/IEC/IEEE 12207:2017, 3.1.54, modified — The original Note 1 to entry has been removed; Notes 1, 2, 3 and 4 to entry have been added.]

4 Context of the organization

4.1 Understanding the organization and its context

ISO 9001:2015, Quality management systems — Requirements

4.1 Understanding the organization and its context

The organization shall determine external and internal issues that are relevant to its purpose and its strategic direction and that affect its ability to achieve the intended result(s) of its quality management system.

The organization shall monitor and review information about these external and internal issues.

NOTE 1 Issues can include positive and negative factors or conditions for consideration.

NOTE 2 Understanding the external context can be facilitated by considering issues arising from legal, technological, competitive, market, cultural, social and economic environments, whether international, national, regional or local.

NOTE 3 Understanding the internal context can be facilitated by considering issues related to values, culture, knowledge and performance of the organization.

Software specific internal and external issues can include:

— Use of “Cloud” (i.e., network accessed systems provided by a third party) applications, tools and storage services. This can be of economic benefit as well as to provide for business continuity, but needs research to ensure there is no increased risk to the organization in using the cloud services provider.

— In some countries employees are encouraged to use personal devices such as mobile phones and computers (bring your own device — byod) rather than those provided by the employer. Employees’ own devices can represent a security risk for employers’ data and a risk of transfer of malware or computer viruses if poorly managed.

— An external risk for all software organizations is that of safety, security and assurance of data and systems from external attack by unauthorised access to networks or transfer of malware or viruses to organizations' computer systems.

— The delivery of the software as an end product in itself or part of an integrated delivery with general purpose or special purpose hardware can result in external issues for an organization.

— After release and in operational use changes to the software or context (e.g. need for evolution) can present an external risk.

— The legal and operational context of the organisation for use of its software products can dictate organisational focus on assurance of software product characteristics relating to safety, security and business/mission assurance.

NOTE 1 ISO/IEC 27001 provides a complementary set of requirements to this document, for a computer security management system that can be used to address those elements of security that provide a risk to the organization's operations.

NOTE 2 ISO/IEC/IEEE 12207:2017, 6.4.1 provides a Business or Mission Analysis process to define the business or mission problem or opportunity, characterize the solution space and determine potential solution class(es) that could address a problem or take advantage of an opportunity. Although this process addresses the context of the software end product rather than the organisation's context for the development of one or more software products, the same process can be useful in understanding the organisation and its context.

NOTE 3 Additional information and guidance for assurance of cybersecurity requirements are found in the following:

— the ISO/IEC 15026 series for systems and software engineering — systems and software assurance;

— ISO/IEC 27000 for information security management.

4.2 Understanding the needs and expectations of interested parties

ISO 9001:2015, Quality management systems — Requirements

4.2 Understanding the needs and expectations of interested parties

Due to their effect or potential effect on the organization's ability to consistently provide products and services that meet customer and applicable statutory and regulatory requirements, the organization shall determine:

a) the interested parties that are relevant to the quality management system;

b) the requirements of these interested parties that are relevant to the quality management system.

The organization shall monitor and review information about these interested parties and their relevant requirements.

Relevant interested parties could include: customers, partners, outsourcing organizations, competitors, those responsible for software life cycle processes and activities (e.g., architects, developers, testers), end users and staff.

NOTE ISO/IEC/IEEE 12207 has a Business or Mission Analysis process (ISO/IEC/IEEE 12207:2017, 6.4.1) and a Stakeholder Needs and Requirements process, especially ISO/IEC/IEEE 12207:2017, 6.4.2.3 a) 2), that can assist in understanding the needs and expectations of interested parties.

4.3 Determining the scope of the quality management system

ISO 9001:2015, Quality management systems — Requirements

4.3 Determining the scope of the quality management system

The organization shall determine the boundaries and applicability of the quality management system to establish its scope.

When determining this scope, the organization shall consider:

a) the external and internal issues referred to in 4.1;

b) the requirements of relevant interested parties referred to in 4.2;

c) the products and services of the organization.

The organization shall apply all the requirements of this International Standard if they are applicable within the determined scope of its quality management system.

The scope of the organization's quality management system shall be available and be maintained as documented information. The scope shall state the types of products and services covered, and provide justification for any requirement of this International Standard that the organization determines is not applicable to the scope of its quality management system.

Conformity to this International Standard may only be claimed if the requirements determined as not being applicable do not affect the organization's ability or responsibility to ensure the conformity of its products and services and the enhancement of customer satisfaction.

The application of this document is appropriate to software that is:

— acquired from another organisation (e.g., part of a commercial contract or other form of agreement);

— a product available for a market sector;

— used to support the processes of an organization;

— embedded in a hardware product;

— related to software services.

Some organizations may be involved in all of the above activities; others may specialize in one area.

Whatever the situation, the determined scope of the organization's quality management system should cover all aspects (software related and non-software related) of the business, apart from any justification for requirements determined as not being applicable.

4.4 Quality management system and its processes

4.4.1 Quality management system processes

ISO 9001:2015, Quality management systems — Requirements

4.4.1 The organization shall establish, implement, maintain and continually improve a quality management system, including the processes needed and their interactions, in accordance with the requirements of this International Standard.

The organization shall determine the processes needed for the quality management system and their application throughout the organization, and shall:

a) determine the inputs required and the outputs expected from these processes;

b) determine the sequence and interaction of these processes;

c) determine and apply the criteria and methods (including monitoring, measurements and related performance indicators) needed to ensure the effective operation and control of these processes;

d) determine the resources needed for these processes and ensure their availability;

e) assign the responsibilities and authorities for these processes;

f) address the risks and opportunities as determined in accordance with the requirements of 6.1;

g) evaluate these processes and implement any changes needed to ensure that these processes achieve their intended results;

h) improve the processes and the quality management system.

NOTE Guidance is provided for items a) and b) of ISO 9001:2015, 4.4.1 in relation to the organizational processes as follows.

4.4.1.1 Process identification and application

The organization should also identify the processes for software development, testing, operation or maintenance, as applicable.

4.4.1.2 Process sequence and interaction

The organization should also define the sequence and interaction of the processes in:

1) life cycle models for software development, e.g. incremental, spiral, iterative and evolutionary (adaptive);

2) quality and development planning, which should be based upon a life cycle model;

3) the software quality system, data, documentation, procedures and processes and controls should be integrated into the overall quality system based on ISO 9001; all areas of management should take responsibility for all software processes, software development and end products that may contain software.

4.4.1.3 Evidence of effective operation

Examples of evidence of effective operation of the quality management system may include:

a) changes (and the reasoning) to resources (people, software and equipment);

b) estimates, e.g. project size and effort (people, cost, schedule);

c) how and why tools, methodologies and suppliers were selected and qualified;

d) software license agreements (both for software supplied to customers and software procured to aid development);

e) minutes of meetings;

f) software release records.

NOTE For further information, see the following:

— ISO/IEC/IEEE 12207, which defines a set of software life cycle processes that may be used for reference. The life cycle model management process (ISO/IEC/IEEE 12207:2017, 6.2.1) in particular would be useful to define one or more life cycles for use within a quality management system;

— ISO/IEC/IEEE 24748–1 and ISO/IEC/TR 24748–3, which provide guidance on how to use processes from ISO/IEC/IEEE 12207 in different life cycles.

4.4.2 Information Management

ISO 9001:2015, Quality management systems — Requirements

4.4.2 To the extent necessary, the organization shall:

a) maintain documented information to support the operation of its processes;

b) retain documented information to have confidence that the processes are being carried out as planned.

The emphasis on documentation in ISO 9001:2015 has changed to that of supporting the operation of processes and retaining documented information (records) to substantiate that processes are carried out as planned. There is a need to consider where the information is held, which may be in computer tools, and the ability to access versions of information applicable to particular process steps, such as the version requirements of a design that underwent a particular review step.

Retaining information, and ensuring the ability to access retained information, may require the maintenance of obsolete tools or the transfer of historic/archived information to new tools.

NOTE The Information Management process of ISO/IEC/IEEE 12207:2017, 6.3.6 has requirements for maintaining and retaining documented information. ISO/IEC/IEEE 12207:2017, B.1 details recommended software-related information items.

5 Leadership

5.1 Leadership and commitment

5.1.1 General

ISO 9001:2015, Quality management systems — Requirements

5.1.1 General

Top management shall demonstrate leadership and commitment with respect to the quality management system by:

a) taking accountability for the effectiveness of the quality management system;

b) ensuring that the quality policy and quality objectives are established for the quality management system and are compatible with the context and strategic direction of the organization;

c) ensuring the integration of the quality management system requirements into the organization's business processes;

d) promoting the use of the process approach and risk-based thinking;

e) ensuring that the resources needed for the quality management system are available;

f) communicating the importance of effective quality management and of conforming to the quality management system requirements;

g) ensuring that the quality management system achieves its intended results;

h) engaging, directing and supporting persons to contribute to the effectiveness of the quality management system;

i) promoting improvement;

j) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

NOTE Reference to "business" in this International Standard can be interpreted broadly to mean those activities that are core to the purposes of the organization's existence, whether the organization is public, private, for profit or not for profit.

This clause applies to software but no software specific guidance is provided.

5.1.2 Customer focus

ISO 9001:2015, Quality management systems — Requirements

5.1.2 Customer focus

Top management shall demonstrate leadership and commitment with respect to customer focus by ensuring that:

a) customer and applicable statutory and regulatory requirements are determined, understood and consistently met;

b) the risks and opportunities that can affect conformity of products and services and the ability to enhance customer satisfaction are determined and addressed;

c) the focus on enhancing customer satisfaction is maintained.

NOTE Management support for customer focus and meeting customer needs for software quality is attained primarily through the Portfolio Management process (ISO/IEC/IEEE 12207:2017, 6.2.3.1) and the Quality Management process (ISO/IEC/IEEE 12207:2017, 6.2.5.1) of ISO/IEC/IEEE 12207.

5.2 Policy

5.2.1 Establishing the quality policy

ISO 9001:2015, Quality management systems — Requirements

5.2.1 Establishing the quality policy

Top management shall establish, implement and maintain a quality policy that:

a) is appropriate to the purpose and context of the organization and supports its strategic direction;

b) provides a framework for setting quality objectives;

c) includes a commitment to satisfy applicable requirements;

d) includes a commitment to continual improvement of the quality management system.

Management are responsible for the control of software development and should ensure the integrity of software deliveries and products that contain software.

NOTE Establishing the quality policy is a primary outcome [ISO/IEC/IEEE 12207:2017, 6.2.5.2 a)] and activity [ISO/IEC/IEEE 12207:2017, 6.2.5.3 a) 1)] of the Quality Management process of ISO/IEC/IEEE 12207.

5.2.2 Communicating the quality policy

ISO 9001:2015, Quality management systems — Requirements

5.2.2 Communicating the quality policy

The quality policy shall:

a) be available and be maintained as documented information;

b) be communicated, understood and applied within the organization;

c) be available to relevant interested parties, as appropriate.

NOTE ISO/IEC/IEEE 12207:2017, B.1 covers making documented information available concerning the quality management policies.

5.3 Organizational roles, responsibilities and authorities

ISO 9001:2015, Quality management systems — Requirements

5.3 Organizational roles, responsibilities and authorities

Top management shall ensure that the responsibilities and authorities for relevant roles are assigned, communicated and understood within the organization.

Top management shall assign the responsibility and authority for:

a) ensuring that the quality management system conforms to the requirements of this International Standard;

b) ensuring that the processes are delivering their intended outputs;

c) reporting on the performance of the quality management system and on opportunities for improvement (see 10.1), in particular to top management;

d) ensuring the promotion of customer focus throughout the organization;

e) ensuring that the integrity of the quality management system is maintained when changes to the quality management system are planned and implemented.

For a software-producing organization or a software maintenance organization, there is benefit if the persons allocated specific quality roles, responsibilities and authorities have had experience with software development.

For a software acquisition organization or a software operation organization, there is benefit if the persons allocated specific quality roles, responsibilities and authorities have had experience with software configuration control and software integration.

Also for a software services organization there is a benefit from service delivery and software product management experience.

NOTE In ISO/IEC/IEEE 12207, the life cycle model management process includes defining the applicable roles, responsibilities, accountabilities and authorities for each process and for strategic management [ISO/IEC/IEEE 12207:2017, 6.2.1.3 a) 3)]. The Quality Assurance process [ISO/IEC/IEEE 12207:2017, 6.3.8.3 a) 1) ii)] applies this to quality assurance strategy.

6 Planning

6.1 Actions to address risks and opportunities

6.1.1 Risk identification

ISO 9001:2015, Quality management systems — Requirements

6.1.1 When planning for the quality management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to:

a) give assurance that the quality management system can achieve its intended result(s);

b) enhance desirable effects;

c) prevent, or reduce, undesired effects;

d) achieve improvement.

It is imperative to understand the level of risk associated with the use of the software and the consequences of its potential failure so that adequate measures (processes) can be put in place to prevent failures from occurring.

For software apply constraints in proportion to the level of risk and consequence of failure. For example software life cycle constraints (e.g., level of testing) can then become commensurate with the level of risk.

The following risks may be relevant when reviewing software:

a) criticality, safety and security issues;

b) capabilities and experience of the organization or its suppliers;

c) reliability of estimates of resources and the duration required for each activity;

d) significant differences between the times required to deliver products or services, and the times determined from plans through the optimization of cost and quality goals;

e) significant geographical dispersion of the organization, customers, users and suppliers;

f) high technical novelty, including novel methods, tools, technologies and supplied software;

g) low quality or availability of supplied software and tools;

h) low precision, accuracy and stability of the definition of the customer requirements and external interfaces;

i) use of publicly available tools or code reuse.

NOTE For further information, see the following standards for software risk management, assurance and software process measurement that can be useful in determining risks and opportunities:

— ISO/IEC/IEEE 12207:2017, 6.3.4 for Risk Management process;

— the ISO/IEC 15026 series for assurance and ISO/IEC 15026-3 for integrity levels;

— ISO/IEC 16085 for risk management process;

— ISO 31000 for risk management guidelines;

— ISO/IEC 33001, ISO/IEC TR 33014, ISO/IEC 33020, ISO/IEC TS 33053 and ISO/IEC TS 33073 for process assessment.

6.1.2 Risk treatment

ISO 9001:2015, Quality management systems — Requirements

6.1.2 The organization shall plan:

a) actions to address these risks and opportunities;

b) how to:

1) integrate and implement the actions into its quality management system processes (see 4.4);

2) evaluate the effectiveness of these actions.

Actions taken to address risks and opportunities shall be proportionate to the potential impact on the conformity of products and services.

NOTE 1 Options to address risks can include avoiding risk, taking risk in order to pursue an opportunity, eliminating the risk source, changing the likelihood or consequences, sharing the risk, or retaining risk by informed decision.

NOTE 2 Opportunities can lead to the adoption of new practices, launching new products, opening new markets, addressing new customers, building partnerships, using new technology and other desirable and viable possibilities to address the organization's or its customers' needs.

NOTE The risk management process of ISO/IEC/IEEE 12207:2017, 6.3.4.3 a) 1) has related activities to define the risk management strategy.

6.2 Quality objectives and planning to achieve them

6.2.1 Establishing quality objectives

ISO 9001:2015, Quality management systems — Requirements

6.2.1 The organization shall establish quality objectives at relevant functions, levels and processes needed for the quality management system.

The quality objectives shall:

a) be consistent with the quality policy;

b) be measurable;

c) take into account applicable requirements;

d) be relevant to conformity of products and services and to enhancement of customer satisfaction;

e) be monitored;

f) be communicated;

g) be updated as appropriate.

The organization shall maintain documented information on the quality objectives.

NOTE 1 Quality objectives are an outcome of the quality management process in ISO/IEC/IEEE 12207:2017, 6.2.5.2 a), with related activities in ISO/IEC/IEEE 12207:2017, 6.2.5.3 a) 1).

NOTE 2 Information on attributes of software processes suitable for setting objectives can be found in ISO/IEC 33001, ISO/IEC TR 33014, ISO/IEC 33020, ISO/IEC TS 33053 and ISO/IEC TS 33073, and can be used for assessing process capabilities and for setting objectives for improving process capabilities.

NOTE 3 Information on quality characteristics, sub-characteristics and attributes of a software product suitable for setting quality objectives are defined in ISO/IEC 25010. ISO/IEC 25001, ISO/IEC 25040, ISO/IEC 25041 and ISO/IEC 25051 are useful for defining quality requirements and for setting quality objectives of a software product.

NOTE 4 Objectives can also include software assurance (see the ISO/IEC 15026 series) and software integrity levels (see ISO/IEC 15026-3).

6.2.2 Implementation of quality objectives

ISO 9001:2015, Quality management systems — Requirements

6.2.2 When planning how to achieve its quality objectives, the organization shall determine:

a) what will be done;

b) what resources will be required;

c) who will be responsible;

d) when it will be completed;

e) how the results will be evaluated.

Planning for the agreement of quality objectives may occur at organizational, project, product and service levels.

Quality management system planning at the organizational level may include the following:

a) defining appropriate software life cycle models to be used for the types of project that the organization or its supplier(s) undertakes, including how the organization normally implements software life cycle processes;

b) defining the work products of software development, such as software requirements documents, architectural design documents, detailed design documents, program code and software user documentation;

c) defining the content of software management plans, such as software project management plans, software configuration management plans, software verification and validation plans, software quality assurance plans hardware and firmware resources, graphical user interfaces (GUIs), interface requirements specifications, interface control documents and training plans;

d) defining how software engineering methods are tailored for the organization's projects within the life cycle;

e) planning of future human resources and skills needed to meet the future work;

f) identifying the tools and environment for software development, operations or maintenance, any specific instructions and tools which will be required for decommissioning and for maintenance and retention of software-related information, documentation and records;

g) specifying conventions for the use of programming languages, e.g. coding rules, software libraries and frameworks;

h) identifying any software reuse.

The organization's management representative should consider any change to a software life cycle model which may affect the quality management system and should consider if such changes compromise any quality management system controls.

Software quality planning at the project/product level is discussed in 8.1.

NOTE Planning for quality management is addressed in ISO/IEC/IEEE 12207:2017, 6.2.5.3 a) and planning for quality assurance is covered in ISO/IEC/IEEE 12207:2017, 6.3.8.3 a).

6.3 Planning of changes

ISO 9001:2015, Quality management systems — Requirements

6.3 Planning of changes

When the organization determines the need for changes to the quality management system, the changes shall be carried out in a planned manner (see 4.4).

The organization shall consider:

a) the purpose of the changes and their potential consequences;

b) the integrity of the quality management system;

c) the availability of resources;

d) the allocation or reallocation of responsibilities and authorities.

The organization's management should consider any change to a software life cycle model which may affect the quality management system and should verify that such changes continue to address the risks in proportion to the impact on software conformity and do not unnecessarily compromise any quality management system controls.

NOTE ISO/IEC/IEEE 12207:2017, 5.7 discusses process change.

7 Support

7.1 Resources

7.1.1 General

ISO 9001:2015, Quality management systems — Requirements

7.1.1 General

The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the quality management system.

The organization shall consider:

a) the capabilities of, and constraints on, existing internal resources;

b) what needs to be obtained from external providers.

NOTE ISO/IEC/IEEE 12207:2017, 6.2.3.3 a) 5) covers the provision of resources in the Portfolio Management process.

7.1.2 People

ISO 9001:2015, Quality management systems — Requirements

7.1.2 People

The organization shall determine and provide the persons necessary for the effective implementation of its quality management system and for the operation and control of its processes.

For a software-producing, software maintenance or software services organization, there is benefit if the persons allocated specific quality roles, responsibilities and authorities have had education and experience with software development, testing, operation and maintenance.

For a software acquisition organization or a software operation organization, there is benefit if the persons allocated specific quality roles, responsibilities and authorities have had experience with software configuration control and software integration.

Software quality assurance activities should be conducted by personnel who are independent from the software development process and should be given the responsibility to define, monitor, control, review and approve software procedures and determine process methods and outcomes.

NOTE ISO/IEC/IEEE 12207:2017, 6.2.4.3 c) covers the provision of human resources in the Human Resource Management process. The provision of resources for quality management activities is covered in the Quality Management process, ISO/IEC/IEEE 12207:2017, 6.2.5.3 a).

7.1.3 Infrastructure

ISO 9001:2015, Quality management systems — Requirements

7.1.3 Infrastructure

The organization shall determine, provide and maintain the infrastructure necessary for the operation of its processes and to achieve conformity of products and services.

NOTE Infrastructure can include:

a) buildings and associated utilities;

b) equipment, including hardware and software;

c) transportation resources;

d) information and communication technology.

The infrastructure should include any hardware, software, tools or facilities for development, testing, operation or maintenance of software, including the following:

a) tools for analysis, design and development, configuration management, testing, project management, documentation;

b) tools for code creation, generation or complexity analysis;

c) tools for application development and support environments;

d) knowledge management, intranet, extranet tools;

e) network tools, including tools for disaster recovery, security, backup, virus protection, firewall;

f) access control tools;

g) help desk and maintenance tools;

h) operational control tools such as for network monitoring, systems management and storage management.

Whether these tools and techniques are developed internally or are purchased, the organization should evaluate whether or not they are fit for purpose. Tools used in the implementation of the product, such as analysis tools, design and development tools, operation, support and maintenance tools, compilers and assemblers should be evaluated, approved and placed under an appropriate level of configuration management control prior to use. The scope of use of such tools and techniques may be documented with appropriate guidance, and their use reviewed periodically, as appropriate, to determine whether there is a need to improve and/or upgrade them. Tools used for software requiring a high level of assurance may also need corresponding assurance of function (see ISO/IEC 15026-3).

The technologies employed in software development, operation and maintenance should be continually monitored and evaluated in order to determine requirements for updating staff skills.

NOTE For further information, see the following:

— ISO/IEC/IEEE 12207:2017, 6.2.2 for Infrastructure Management Process;

— ISO/IEC 25001 (Acquisition), ISO/IEC 25040, ISO/IEC 25041 (Evaluation of a Software Product) and ISO/IEC 14102.

7.1.4 Environment for the operation of processes

ISO 9001:2015, Quality management systems — Requirements

7.1.4 Environment for the operation of processes

The organization shall determine, provide and maintain the environment necessary for the operation of its processes and to achieve conformity of products and services.

NOTE A suitable environment can be a combination of human and physical factors, such as:

a) social (e.g. non-discriminatory, calm, non-confrontational);

b) psychological (e.g. stress-reducing, burnout prevention, emotionally protective);

c) physical (e.g. temperature, heat, humidity, light, airflow, hygiene, noise).

These factors can differ substantially depending on the products and services provided.

NOTE ISO/IEC/IEEE 12207:2017, 5.2.1 and 5.2.3 discusses the environment for a process (operation of a system). The operational environment is addressed in ISO/IEC/IEEE12207:2017, 6.4.12.

7.1.5 Monitoring and measuring resources

7.1.5.1 General

ISO 9001:2015, Quality management systems — Requirements

7.1.5.1 General

The organization shall determine and provide the resources needed to ensure valid and reliable results when monitoring or measuring is used to verify the conformity of products and services to requirements.

The organization shall ensure that the resources provided:

a) are suitable for the specific type of monitoring and measurement activities being undertaken;

b) are maintained to ensure their continuing fitness for their purpose.

The organization shall retain appropriate documented information as evidence of fitness for purpose of the monitoring and measurement resources.

NOTE For further information for software, see the following:

— ISO/IEC/IEEE 15939 for a software measurement process;

— ISO/IEC/IEEE 12207:2017, 6.3.7 details the measurement process for software systems;

— ISO/IEC 19770-4 for resource utilization measurement.

7.1.5.2 Measurement traceability

ISO 9001:2015, Quality management systems — Requirements

7.1.5.2 Measurement traceability

When measurement traceability is a requirement, or is considered by the organization to be an essential part of providing confidence in the validity of measurement results, measuring equipment shall be:

a) calibrated or verified, or both, at specified intervals, or prior to use, against measurement standards traceable to international or national measurement standards; when no such standards exist, the basis used for calibration or verification shall be retained as documented information;

b) identified in order to determine their status;

c) safeguarded from adjustments, damage or deterioration that would invalidate the calibration status and subsequent measurement results.

The organization shall determine if the validity of previous measurement results has been adversely affected when measuring equipment is found to be unfit for its intended purpose, and shall take appropriate action as necessary.

Calibration is a technique that often has been perceived as not directly applicable to software. However, the equivalent to 'calibration' may be applicable to hardware and software tools used to test and validate software products. Consequently, items a) to c) in ISO 9001:2015, 7.1.5.2, may be applicable to the environment used when testing the software.

Where the organization uses tools, facilities and techniques in the conduct of any tests verifying conformance of the software product to specified requirements, the organization should consider the

effect of such tools on the quality of the software product, when approving them. In addition, such tools should be placed under configuration management prior to use.

The suitability of test tools, techniques and data should be verified prior to use, to determine if there is a need to improve and/or upgrade them. The organization should have procedures for determining how the test software is checked.

Measuring and monitoring devices used in software development, testing, maintenance and operation include:

a) data used for testing the software product;

b) software tools (e.g. for debugging, simulation, collecting performance, resource utilization and coverage information, recording);

c) computer hardware;

d) instrumentation interfacing to the computer hardware.

The organization should control measuring and monitoring devices by means of a configuration management system (see 8.5.2), to meet the intent of ISO 9001:2015.

7.1.6 Organizational knowledge

ISO 9001:2015, Quality management systems — Requirements

7.1.6 Organizational knowledge

The organization shall determine the knowledge necessary for the operation of its processes and to achieve conformity of products and services.

This knowledge shall be maintained and be made available to the extent necessary.

When addressing changing needs and trends, the organization shall consider its current knowledge and determine how to acquire or access any necessary additional knowledge and required updates.

NOTE 1 Organizational knowledge is knowledge specific to the organization; it is generally gained by experience. It is information that is used and shared to achieve the organization's objectives.

NOTE 2 Organizational knowledge can be based on:

a) internal sources (e.g. intellectual property; knowledge gained from experience; lessons learned from failures and successful projects; capturing and sharing undocumented knowledge and experience; the results of improvements in processes, products and services);

b) external sources (e.g. standards; academia; conferences; gathering knowledge from customers or external providers).

As well as needing knowledge related to software, staff also need knowledge relevant to the domain (e.g. finance, flight control dynamics, medical imagery, privacy, etc.)

NOTE ISO/IEC/IEEE 12207:2017, 6.2.6 covers the Knowledge Management process.

7.2 Competence

ISO 9001:2015, Quality management systems — Requirements

7.2 Competence

The organization shall:

a) determine the necessary competence of person(s) doing work under its control that affects the performance and effectiveness of the quality management system;

b) ensure that these persons are competent on the basis of appropriate education, training, or experience;

c) where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken;

d) retain appropriate documented information as evidence of competence.

NOTE Applicable actions can include, for example, the provision of training to, the mentoring of, or the re-assignment of currently employed persons; or the hiring or contracting of competent persons.

The training needs should be determined considering the requirements, design methods, specific programming languages, tools, techniques and computer resources to be used in the development, testing, operation and management of the software product/project. It might also be useful to include training in the skills and knowledge of the specific field within which the software is applied and in other topics such as project management.

Individuals should be trained and assessed on the use of software development and associated tools.

Individuals should be able to demonstrate competency in areas of their expertise and have evidence of adequate training/experience in the applicable field. Individuals should also be able to demonstrate (prove) that they are capable of developing systems and software to the required standard and be able to follow the associated levels or constraints.

The form of training may not necessarily be traditional training courses but could be workshops, computer-based training, self-study, mentoring, training on-the-job or web-based training.

Evaluation of the effectiveness of training may be performed using measurements of products and processes, or identifying areas of improvement in team or personal performance (among other areas for improvement).

NOTE ISO/IEC/IEEE 12207:2017, 6.2.4.3 a) and b) covers determining and improving competence in the Human Resource Management process.

7.3 Awareness

ISO 9001:2015, Quality management systems — Requirements

7.3 Awareness

The organization shall ensure that persons doing work under the organization's control are aware of:

a) the quality policy;

b) relevant quality objectives;

c) their contribution to the effectiveness of the quality management system, including the benefits of improved performance;

d) the implications of not conforming with the quality management system requirements.

Individuals should be aware of specific software standards, procedures and tools used for the development of software as defined by the organisation.

Individuals should be aware of associated risks in the use of these processes, tools, process outcomes and their potential impact.

7.4 Communication

ISO 9001:2015, Quality management systems — Requirements

7.4 Communication

The organization shall determine the internal and external communications relevant to the quality management system, including:

a) on what it will communicate;

b) when to communicate;

c) with whom to communicate;

d) how to communicate;

e) who communicates.

The following should be considered, regarding communications carried out in the organization:

a) communicating to the organization the importance of satisfying the client's requirements;

b) quality policy (see 5.2.2);

c) communication with the customer (see 8.2.1):

   1) communication with the customer during development (see 8.2.1.3);

   2) communication with the customer during operation and maintenance (see 8.2.1.4);

d) help desk [see 8.5.1.6 a)];

e) customer property (see 8.5.3).

7.5 Documented information

7.5.1 General

ISO 9001:2015, Quality management systems — Requirements

7.5.1 General

The organization's quality management system shall include:

a) documented information required by this International Standard;

b) documented information determined by the organization as being necessary for the effectiveness of the quality management system.

NOTE The extent of documented information for a quality management system can differ from one organization to another due to:

— the size of organization and its type of activities, processes, products and services;

— the complexity of processes and their interactions;

— the competence of persons.

The level of documentation for software can be affected by:

a) organisational responsibilities for different parts of the system and the way in which these can change over the lifecycle (e.g., one organisation taking over ongoing maintenance from another);

b) the level of software assurance, i.e., greater levels can need more detailed, formal documentation (see the ISO/IEC 15026 series for assurance and ISO/IEC 15026-3 for integrity levels).

For software the interpretation of this requirement includes the control of data, tools and systems, not just documents.

The control of issue status for data and documentation for software is usually part of configuration management, see 8.5.2 and control of changes in 8.5.6.

The software development lifecycle process should be documented or controlled by approved tools.

NOTE For further information for software, see the following:

— The Information Management process in ISO/IEC/IEEE 12207:2017, 6.3.6 has requirements for maintaining and retaining documented information. ISO/IEC/IEEE 12207:2017, B.1 details recommended Quality Management information items.

— ISO/IEC/IEEE 15289 for content of life-cycle information items (documentation) also.

— ISO/IEC/IEEE 26511 for users of systems, software, and services.

— ISO/IEC/IEEE 26515 for users in an agile environment.

7.5.2 Creating and updating

ISO 9001:2015, Quality management systems — Requirements

7.5.2 Creating and updating

When creating and updating documented information, the organization shall ensure appropriate:

a) identification and description (e.g. a title, date, author, or reference number);

b) format (e.g. language, software version, graphics) and media (e.g. paper, electronic);

c) review and approval for suitability and adequacy.

This clause applies to software but no software specific guidance is provided, other than the mechanism for identification of data and software including documentation is usually part of configuration management (see 8.5.2).

7.5.3 Control of documented information

7.5.3.1 Quality management system documentation

ISO 9001:2015, Quality management systems — Requirements

7.5.3.1 Documented information required by the quality management system and by this International Standard shall be controlled to ensure:

a) it is available and suitable for use, where and when it is needed;

b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).

This clause applies to software but no software specific guidance is provided, other than the mechanism for control of data and software including documentation is usually part of configuration management (see 8.5.2).

7.5.3.2 Maintaining quality management system documentation

ISO 9001:2015, Quality management systems — Requirements

7.5.3.2 For the control of documented information, the organization shall address the following activities, as applicable:

a) distribution, access, retrieval and use;

b) storage and preservation, including preservation of legibility;

c) control of changes (e.g. version control);

d) retention and disposition.

Documented information of external origin determined by the organization to be necessary for the planning and operation of the quality management system shall be identified as appropriate, and be controlled.

Documented information retained as evidence of conformity shall be protected from unintended alterations.

NOTE Access can imply a decision regarding the permission to view the documented information only, or the permission and authority to view and change the documented information.

7.5.3.2.1 Control of data and documentation

For software, encryption may be used to control access to data and documentation and in its' transmission across internal and external networks.

7.5.3.2.2 Evidence of conformity

All conformity evidence (data and documentation) should be controlled and traceable across the software life cycle processes employed.

7.5.3.2.3 Retention and disposition

Where records are held on electronic media, consideration of the retention times and accessibility of the records should take into account the rate of media degradation, the availability of the devices and software needed to access the records. Records may include information held in email systems. Protection from computer viruses and unapproved or illegal access should be considered.

The proprietary nature of the information stored on records should be assessed, in determining the methods of data erasure from the media, at the end of its required retention period. Destruction of the media rather than reuse may be necessary at the end of the defined retention period.

8 Operation

8.1 Operational planning and control

ISO 9001:2015, Quality management systems — Requirements

8.1 Operational planning and control

The organization shall plan, implement and control the processes (see 4.4) needed to meet the requirements for the provision of products and services, and to implement the actions determined in Clause 6, by:

a) determining the requirements for the products and services;

b) establishing criteria for:

   1) the processes;

   2) the acceptance of products and services;

c) determining the resources needed to achieve conformity to the product and service requirements;

d) implementing control of the processes in accordance with the criteria;

e) determining, maintaining and retaining documented information to the extent necessary:

   1) to have confidence that the processes have been carried out as planned;

   2) to demonstrate the conformity of products and services to their requirements.

The output of this planning shall be suitable for the organization's operations.

The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.

The organization shall ensure that outsourced processes are controlled (see 8.4).

8.1.1 General

Software operational planning should result in a definition of what products are to be produced, who is to produce them and when they are to be produced (see also 8.3.2). Software quality planning at the project/product level should result in a description of how specific products are to be developed, assessed or maintained.

Quality planning provides the means for tailoring the application of the quality management system to a specific project, product or contract. Quality planning may include or reference generic and/or project/product/contract-specific procedures, as appropriate. Quality planning should be revisited along with the progress of design and development, and items concerned with each stage should be completely defined when starting that stage. Quality planning may be reviewed and agreed by all organizations concerned in its implementation, as appropriate.

A document that describes quality planning may be an independent document (entitled quality plan), a part of another document, or composed of several documents, including a design and development plan.

Software quality planning at the project level should address the following:

a) inclusion of, or reference to, the plans for development (see 8.3.2);

b) quality requirements related to the product and/or processes;

c) quality management system tailoring and/or identification of specific procedures and instructions, appropriate to the scope of the quality management system and any stated applicability of requirements (ISO 9001:2015, 4.3 and A.5);

d) project-specific procedures and instructions, such as software test specifications detailing plans, designs, test cases and procedures for unit, integration, system and acceptance testing (see 8.3.2);

e) methods, life cycle model(s), tools, programming language conventions, libraries, frameworks and other reusable assets to be used in the project;

f) criteria for starting and ending each project stage;

g) types of review, and other verification and validation activities to be carried out (see 8.3.4);

h) configuration management procedures to be carried out (see 8.5.2);

i) monitoring and measurement activities to be carried out;

j) the person(s) responsible for approving the outputs of processes for subsequent use;

k) training needs in the use of tools and techniques, and scheduling of the training before the skill is needed;

l) records to be maintained (see 7.5.3);

m) change management, such as for resources, schedule and contract changes.

Quality planning, however abbreviated, is particularly useful to clarify limited quality objectives for software being designed for a limited purpose. Examples of limited-purpose software include proof-of- concept demonstration prototypes, a research computation used only by its designer, an interim solution lacking features such as security or full operational performance that will be implemented in a future output, and one-time data analysis reports.

Limited-purpose software should be tested in ways that are consistent with its planned use (purpose) to reduce the possible occurrence of unintended omissions and errors.

8.1.2 Evidence of conformity to requirements

Evidence of conformity to requirements may include:

a) documented test results;

b) problem reports, including those related to tools problems;

c) change requests;

d) documents marked with comments;

e) audit and assessment reports;

f) review and inspection records, such as those for requirements reviews, design reviews, code inspections and walkthroughs.

NOTE For further general guidance related to ISO 9001:2015, 8.1, see the following:

— ISO/IEC/IEEE 12207:2017, 6.3.1, (Project Planning process) and ISO/IEC/IEEE 12207:2017, 6.3.8 (Quality Assurance process).

— ISO/IEC/IEEE 24748-5 for software development planning.

— ISO/IEC 25001 for Software product Quality Requirements and Evaluation (SQuaRE) — planning and management.

— ISO/IEC/IEEE 16326 for systems and software engineering — life cycle processes — project management.

8.2 Requirements for products and services

8.2.1 Customer communication

ISO 9001:2015, Quality management systems — Requirements

8.2.1 Customer communication

Communication with customers shall include:

a) providing information relating to products and services;

b) handling enquiries, contracts or orders, including changes;

c) obtaining customer feedback relating to products and services, including customer complaints;

d) handling or controlling customer property;

e) establishing specific requirements for contingency actions, when relevant.

8.2.1.1 General

For computer software, depending on the type, the method of communication may vary depending on the type of agreement, and on the scope of the contract for development, operations or maintenance.

The following guidance for communicating with customers is separated into advice for development and advice for operations/maintenance life cycle processes.

8.2.1.2 Customer representative

The customer may have responsibilities under the contract. Particular issues may include the need for the customer to cooperate with the organization, to provide necessary information in a timely manner, and to resolve action items. When assigned to monitor life cycle activities, a customer representative

may represent the eventual users of the product, as well as executive management, and have the authority to deal with contractual matters which include, but are not limited to, the following:

a) dealing with customer-supplied software items, data, facilities and tools that are found unsuitable for use;

b) providing review and approval of the outputs of the development process on behalf of the customer;

c) organizing access to end-users, where appropriate.

8.2.1.3 Customer communication during development

Joint reviews involving the organization and the customer may be scheduled on a regular basis, or at significant project events, to cover the following aspects, as appropriate:

1) product information, including:
    a) development plans;
    b) conformance of outputs, such as design and development documents, to the customer's agreed requirements;
    c) communications to convey progress and provide assurance to the customer that the planned processes are being followed;
    d) demonstrations of outputs of the development processes, such as prototypes;
    e) acceptance test results;
2) enquiries, contracts and amendments, including:
    a) the progress of activities concerning the eventual users of the system under development, such as deployment and training;
    b) the progress of software development work undertaken by the organization;
    c) the progress of agreed activities being undertaken by the customer;
    d) the processing of risk management issues, problems and change control items;
    e) the methods by which the customer will be advised of current or planned future changes.

8.2.1.4 Customer communication during operations and maintenance

Sources of information that involve customer communication in operations and maintenance may include the following:

1) product information, including:
    a) online help, user manuals describing the product and its use;
    b) descriptions of new releases and upgrades;
    c) product web sites;
2) enquiries, contracts and amendments, including:
    a) progress on product or service delivery, and/or maintenance activities;
    b) processing service or product risks, issues and change requests;
3) customer feedback, including:
    a) help desk arrangements and effectiveness;

b) progress on customer complaints processing;

c) surveys, user groups, conferences.

NOTE For further information, see the following:

— ISO/IEC 14764 (Software Maintenance).

— The Business and Mission Analysis process in ISO/IEC/IEEE 12207:2017, 6.4.1 has requirements for use of customer feedback. Customer support and communication is a primary activity of the Operation and Maintenance processes in ISO/IEC/IEEE 12207:2017, 6.4.12 and 6.4.13.

8.2.2 Determining the requirements for products and services

ISO 9001:2015, Quality management systems — Requirements

8.2.2 Determining the requirements for products and services

When determining the requirements for the products and services to be offered to customers, the organization shall ensure that:

a) the requirements for the products and services are defined, including:

1) any applicable statutory and regulatory requirements;

2) those considered necessary by the organization;

b) the organization can meet the claims for the products and services it offers.

Software may be developed as part of a contract, as a product available for a market sector, as software embedded in a system or in support of the business processes of the organization. Requirements determination is applicable in all of these circumstances.

Specific actions may include:

1) the establishment of the following for developing the requirements:

a) methods for agreement of requirements and authorizing and tracking changes, especially during iterative development;

b) methods for the evaluation of prototypes or demonstrations, where used;

c) methods for recording and reviewing discussion results from all parties involved;

2) the development of the requirements in close cooperation with the customer or users, and efforts to prevent misunderstandings by, for example, the provision of definition of terms, explanation of the background of requirements;

3) the obtainment of the customer's approval of the requirements;

4) the establishment of a method for traceability of the requirements to the final product (such as a requirements traceability matrix);

5) identifying any formal claims of software products or services that need to be provided. Claims for software products may address properties relating to safety, reliability, performance or cyber-worthiness.

The requirements may be provided by the customer, may be developed by the organization or may be jointly developed.

When the requirements are provided and agreed in the form of a system specification, methods should be in place to allocate them into hardware and software items with any appropriate interface

specifications. Changes to the requirements should be controlled. The contract may need to be amended when requirements change.

In contractual situations, the requirements may not be fully defined at contract acceptance, and some may be developed during a project.

Formal claims relating to products may need to be supported by an assurance case. This should include one or more claims about properties; arguments that logically link the evidence and any assumptions to the claim(s); a body of evidence and possibly assumptions supporting these arguments for the claim(s); and justification of the choice of top-level claim and the method of reasoning. The requirements for such claims needs to be well understood as they can have significant impact on product development and acceptance.

The requirements should take the operational environment into account. The requirements may include, but not be limited to, the following characteristics: functionality, reliability, usability, efficiency, maintainability and portability. Other characteristics may be specified, for example security, safety and statutory or regulatory obligations. Some of these characteristics may be mission and/or safety critical.

The type and scope of software requirement content and rate of update will be commensurate with the type of software life cycle being applied, e.g., Waterfall or Agile.

If the software product needs to interface with other software or system products, the interfaces between the software product to be developed and other software or system products should be specified, as far as possible, either directly or by reference, in the requirements. Development arrangements may also need to allow for co-development of interfaces or define the respective roles in the development of interfaces.

NOTE 1 For further information, see the following:

— ISO/IEC/IEEE 12207:2017, 6.4.2 for Stakeholder Needs and Requirements Definition and ISO/IEC/IEEE 12207:2017, 6.4.3 for System/Software Requirements Definition;

— ISO/IEC/IEEE 29148;

— ISO/IEC 25010;

— ISO/IEC 15026–3;

— ISO/IEC 25051.

8.2.3 Review of the requirements for products and services

8.2.3.1 Requirements review

ISO 9001:2015, Quality management systems — Requirements

8.2.3.1 The organization shall ensure that it has the ability to meet the requirements for products and services to be offered to customers. The organization shall conduct a review before committing to supply products and services to a customer, to include:

a) requirements specified by the customer, including the requirements for delivery and post-delivery activities;

b) requirements not stated by the customer, but necessary for the specified or intended use, when known;

c) requirements specified by the organization;

d) statutory and regulatory requirements applicable to the products and services;

e) contract or order requirements differing from those previously expressed.

The organization shall ensure that contract or order requirements differing from those previously defined are resolved.

The customer's requirements shall be confirmed by the organization before acceptance, when the customer does not provide a documented statement of their requirements.

NOTE In some situations, such as internet sales, a formal review is impractical for each order. Instead, the review can cover relevant product information, such as catalogues.

8.2.3.1.1 Customer's requirements

Requirements should be recorded or captured in a formal manner or within an appropriate tool (e.g., JIRA). All requirements including software requirements should be reviewed and approved before use.

The review process and methods used should be approved by management. Care should be taken to differentiate between system and software requirements.

8.2.3.1.2 Organization's concerns

Issues which may be relevant during the organization's review of software tenders, contracts or orders include, but are not limited to the following:

1) the feasibility of meeting and validating the requirements and product characteristics, including identifying the required software characteristics (e.g. functionality, reliability, usability, maintainability, portability and efficiency);

2) software design and development standards and procedures to be used;

3) the identification of facilities, tools, software items and data, to be provided by the customer, the definition and documentation of methods to assess their suitability for use;

4) the operating system or hardware platform;

5) agreement on the control of external interfaces with the software product;

6) replication and distribution requirements;

7) customer related issues:

   1) life cycle processes imposed by the customer;

   2) period of obligation of the organization to supply copies and the capability of reading master copies;

8) management issues:

   1) risk management should be addressed;

   2) organization's responsibility with regard to subcontracted work;

   3) scheduling of progress, technical reviews and outputs;

   4) scope and schedule for customer test witnessing if applicable, as well as the respective roles of organization and customer during this process;

   5) installation, maintenance and support requirements;

   6) timely availability of technical, human and financial resources;

9) legal, security and confidentiality issues:

   1) information handled under the contract may be subject to concerns regarding intellectual property rights, licence agreements, statutory and regulatory requirements, confidentiality and the protection of information including patents and copyrights;

   2) guardianship of the master copy of the product and the rights of the customer to access or verify that master;

   3) level of information disclosure, to the customer, needs to be mutually agreed to by the parties;

   4) definition of warranty terms;

   5) liabilities/penalties associated with the contract.

Review of requirements may be performed by internal or external organizations. This may include reviews of requirements related to contracts, engineering, maintenance or quality.

The implications of any contract changes on resources, schedules and costs should be evaluated, particularly for changes to scope, functionality or risk. The above issues should be re-evaluated, as appropriate. For products where failure may cause injury or danger to people, or damage or corruption of property or the environment, requirements should specify the desired immunity from, and response to, potential failure conditions.

NOTE For software specific aspects of review of the requirements for products and services, see also ISO/IEC/IEEE 12207:2017, 6.4.2.3 d) and e) in Stakeholder Needs and Requirements Definition.

8.2.3.2 Maintaining requirements records

ISO 9001:2015, Quality management systems — Requirements

8.2.3.2 The organization shall retain documented information, as applicable:

a) on the results of the review;

b) on any new requirements for the products and services.

c) The maintenance of requirements records should be conducted in a systematic manner.

d) It should be possible to conduct traceability throughout the software life cycle processes, both from requirements to delivery and from test back to the initial design requirements. This is usually through configuration management (see 8.5.2).

NOTE 1 The Quality Assurance process has requirements for management of QA records and reports in ISO/IEC/IEEE 12207:2017 6.3.8.3 d).

NOTE 2 For further information on requirements review, see ISO/IEC/IEEE 12207:2017, 6.1.2 (Supply Process), 6.4.9 (Verification) and 6.4.11 (Validation Process).

NOTE 3 For further information on requirements engineering for eliciting, analysing, verifying and validating customer requirements, see ISO/IEC/IEEE 29148.

NOTE 4 For further information on risk management, see ISO/IEC/IEEE 12207:2017, 6.3.4 (Risk Management) and ISO/IEC 16085.

NOTE 5 For further information on review of quality requirements using quality characteristics, see ISO/IEC 25010.

8.2.4 Changes to requirements for products and services

ISO 9001:2015, Quality management systems — Requirements

8.2.4 Changes to requirements for products and services

The organization shall ensure that relevant documented information is amended, and that relevant persons are made aware of the changed requirements, when the requirements for products and services are changed.

See 8.5.2.2 for configuration management of changes.

NOTE ISO/IEC/IEEE 12207:2017 6.4.3.3 d) covers changes to requirements in the System/Software Requirements Definition process.

8.3 Design and development of products and services

8.3.1 General

ISO 9001:2015, Quality management systems — Requirements

8.3.1 General

The organization shall establish, implement and maintain a design and development process that is appropriate to ensure the subsequent provision of products and services.

NOTE The Architecture Definition (ISO/IEC/IEEE 12207:2017, 6.4.4), Design Definition (ISO/IEC/IEEE 12207:2017, 6.4.5), Implementation (ISO/IEC/IEEE 12207:2017, 6.4.7) and Integration (ISO/IEC/IEEE 12207:2017, 6.4.8) processes, as well as related technical processes of ISO/IEC/IEEE 12207 have requirements for design and development of software.

8.3.2 Design and development planning

ISO 9001:2015, Quality management systems — Requirements

8.3.2 Design and development planning

In determining the stages and controls for design and development, the organization shall consider:

a) the nature, duration and complexity of the design and development activities;

b) the required process stages, including applicable design and development reviews;

c) the required design and development verification and validation activities;

d) the responsibilities and authorities involved in the design and development process;

e) the internal and external resource needs for the design and development of products and services;

f) the need to control interfaces between persons involved in the design and development process;

g) the need for involvement of customers and users in the design and development process;

h) the requirements for subsequent provision of products and services;

i) the level of control expected for the design and development process by customers and other relevant interested parties;

j) the documented information needed to demonstrate that design and development requirements have been met.

8.3.2.1 General

Design and development should be carried out in a disciplined manner to prevent or minimize the occurrence of problems in development or in the software product. This approach reduces dependence on verification and validation as the sole methods for identifying problems. The acquirer's organization should therefore check that the software products are developed in compliance with specified requirements and in accordance with design and development planning and/or quality planning (see 8.1 for quality planning).

NOTE Some items in the following list have been included in the quality planning list in 8.1.2. These are noted in square brackets.

Design and development planning should address the following items, as appropriate:

1) the activities of requirements analysis, design and development, coding, integration, testing, installation and support for acceptance of software products; this includes the identification of, or reference to:

   a) activities to be carried out;

   b) required inputs to each activity;

   c) required outputs from each activity;

   d) verification required for each activity output (as 8.3.4);

   e) management and supporting activities to be carried out;

   f) required team training [as 8.1.1 k)];

2) planning for the control of product and service provision;

3) the organization of the project resources, including the team structure, responsibilities, use of suppliers and material resources to be used;

4) organizational and technical interfaces between different individuals or groups, such as sub-project teams, suppliers, partners, users, customer representatives, quality assurance representative;

5) the analysis of the possible risks, assumptions, dependencies and problems associated with the design and development;

6) the schedule identifying:

   a) the stages of the project;

   b) the work breakdown structure;

   c) the associated resources and timing;

   d) the associated dependencies;

   e) the milestones and milestone entry/exit criteria;

   f) verification and validation activities (as 8.3.4);

7) the identification of:

   a) standards, rules, practices and conventions, methodology, life cycle model, statutory and regulatory requirements [as 8.1.1 d) and e)];

   b) statutory and regulatory requirements [as 8.3.2 and 8.2.3.1.2 9) 1)];

   c) tools and techniques for development, including the qualification of, and configuration controls placed on, such tools and techniques;

   d) facilities, hardware and software for development;

   e) configuration management practices (as 8.5.2.3);

   f) method of controlling nonconforming software products;

   g) methods of control for software used to support development;

   h) procedures for archiving, back-up, recovery and controlling access to software products;

   i) methods of control for virus protection;

   j) security controls;

   k) infrastructure needed to rapidly build completed versions of the executable software;

   l) instrumentation and forensic support to find faults in reasonable time frames;

8) the identification of related planning (including planning of the system) addressing topics such as quality, risk management, configuration management, supplier management, integration, testing, release management, installation, training, migration, maintenance, re-use, communication and measurement;

9) documentation control including document/record archive and distribution;

10) supportability and maintenance;

11) for a COTS product in which the organization does not have control over the design, the organization should assure that the product meets the acceptance criteria.

Planning should be reviewed periodically and any plans amended if appropriate.

A document defining design and development planning and any of these related planning topics may be an independent document, a part of another document or composed of several documents.

8.3.2.2 Software life cycle

Processes, activities and tasks should be planned and performed using life cycle models suitable to the nature of a software project, considering size, complexity, safety, risk and integrity. ISO 9001:2015 is intended for application irrespective of the life cycle models used and is not intended to indicate a specific life cycle model or process sequence.

Design and development can be an evolutionary process and procedures may therefore need to be changed or updated as the project progresses, after consideration of changes to related activities and tasks.

Consideration should be given to the suitability of the design and development method for the type of task, product or project and the compatibility of the application, the methods and the tools to be used.

8.3.2.3 Review, verification and validation

The review, verification and validation for software design and development are covered in 8.3.4 to 8.3.6. In software operations and maintenance, they may be covered in service level agreements or maintenance procedures.

8.3.2.4 Responsibilities and authorities

Responsibilities and authorities are applicable to software but there is no software specific guidance.

8.3.2.5 Interfaces

The boundaries of responsibility for each part of the software product and the way that technical information will be transmitted between all parties should be clearly defined in the design and development planning of suppliers. The organization may require review of a supplier's design and development planning.

In defining interfaces, care should be taken to consider parties, other than the customer and organization, who have an interest in the design and development, installation, operation, maintenance and training activities. These may include customer representatives, suppliers, partners, quality assurance representatives, engineering process group representatives, regulatory authorities, associated development project staff and help desk staff. In particular, the end-users and any intermediate operations function may need to be involved to consider if appropriate capacity and training are available to achieve committed service levels.

NOTE 3 For further information see the following:

— ISO/IEC/IEEE 16326 (Software project management).

— ISO/IEC/IEEE 24748-5 for systems and software engineering — life cycle management — software development planning.

— The life cycle model management (ISO/IEC/IEEE 12207:2017, 6.2.1), Portfolio Management (ISO/IEC/IEEE 12207:2017, 6.2.3), and Project Planning process (ISO/IEC/IEEE 12207:2017, 6.3.1) as well as related technical processes of ISO/IEC/IEEE 12207 have requirements for planning design and development of software and software projects.

— ISO/IEC 25010 for Software product Quality Requirements and Evaluation (SQuaRE) — system and software quality models.

8.3.3 Design and development inputs

ISO 9001:2015, Quality management systems — Requirements

8.3.3 Design and development inputs

The organization shall determine the requirements essential for the specific types of products and services to be designed and developed. The organization shall consider:

a) functional and performance requirements;

b) information derived from previous similar design and development activities;

c) statutory and regulatory requirements;

d) standards or codes of practice that the organization has committed to implement;

e) potential consequences of failure due to the nature of the products and services.

Inputs shall be adequate for design and development purposes, complete and unambiguous.

Conflicting design and development inputs shall be resolved.

The organization shall retain documented information on design and development inputs.

In system architectural design, system requirements are allocated to hardware, software components and manual operations. The inputs to software requirements analysis are the system requirements allocated to software and specifications of the interfaces between the system components.

Software architectural design needs to consider high level requirements and long term business objectives and make system wide design decisions that impact all the software, providing additional constraints on each element.

Design and development input may be determined from functional, performance, quality, relevant safety and security requirements and system design constraints, or derived through techniques such as prototyping. Design and development input may also be determined from design change requests originating from previous phases in the iterative development model (cycle), problems to be fixed, or requirements arising from acceptance criteria. Input may also come from contract review activities.

When design and development input documents are being reviewed (this often happens in conjunction with the customer), they should be checked for:

a) ambiguities and contradictions;

b) inconsistent, incomplete or unfeasible information or requirements;

c) unrealistic performance specifications;

d) requirements that cannot be verified or validated;

e) unstated or assumed requirements;

f) inaccurate description of user environment and actions;

g) lack of design and development decisions in a requirements document;

h) omissions of key performance measures.

NOTE 1 Review of requirements by the customer does not absolve the organization of the need to independently review requirements for their adequacy, as per 8.3.3.

NOTE 2 For further information, see:

— ISO/IEC 25010 for software quality requirements as software quality characteristics.

— ISO/IEC/IEEE 12207:2017, 6.4.4.3 a) considers requirements as inputs to design and development in the Architecture Definition process.

8.3.4 Design and development controls

ISO 9001:2015, Quality management systems — Requirements

8.3.4 Design and development controls

The organization shall apply controls to the design and development process to ensure that:

a) the results to be achieved are defined;

b) reviews are conducted to evaluate the ability of the results of design and development to meet requirements;

c) verification activities are conducted to ensure that the design and development outputs meet the input requirements;

d) validation activities are conducted to ensure that the resulting products and services meet the requirements for the specified application or intended use;

e) any necessary actions are taken on problems determined during the reviews, or verification and validation activities;

f) documented information of these activities is retained.

NOTE Design and development reviews, verification and validation have distinct purposes. They can be conducted separately or in any combination, as is suitable for the products and services of the organization.

8.3.4.1 Design and development review

The degree of formality and rigour of the activities associated with the review processes should be appropriate for the complexity of the product, the quality requirements and the degree of risk associated with the specified use of the software product. The organization should establish procedures for dealing with process and product deficiencies or nonconformities identified during these activities (see 8.7). It is recommended that these procedures be documented.

During design and development reviews, criteria such as feasibility, security, safety, programming rules and testability should be taken into account.

Collaboration tools are often used to track design and development reviews as well as follow-up actions taken to resolve issues.

Review of design and development should be performed in accordance with planned arrangements. The elements of the review to be considered are the following:

a) what is to be reviewed, when and the type of review, such as demonstrations, formal proof of correctness, inspections, walkthroughs and joint reviews;

b) what functional groups would be concerned in each type of review and, if there is to be a review meeting, how it is to be organized and conducted;

c) what records have to be produced, e.g. meeting minutes, issues, problems, actions and action status;

d) the methods for monitoring the application of rules, practices and conventions to enable requirements to be met;

e) what has to be done prior to the conduct of a review, such as establishment of objectives, meeting agenda, documents required and roles of review personnel;

f) what has to be done during the review, including the techniques to be used and guidelines for all participants;

g) the success criteria for the review;

h) methods of monitoring supplier performance;

i) what follow-up activities are used to ensure that issues identified at the review are resolved;

j) further design and development activities should proceed only when the consequences of all known deficiencies are understood, or the risk of proceeding otherwise is known and agreed; any findings should be addressed and resolved, as appropriate.

8.3.4.2 Design and development verification

Verification of software is aimed at providing assurance that the output of a design and development activity conforms to the input requirements.

Verification should be performed as appropriate during design and development. Verification may comprise reviews of design and development output (e.g. by inspections and walkthroughs), analysis, demonstrations including prototypes, simulations or tests. Verification may be conducted on the output from other activities, e.g. COTS, purchased and customer-supplied products.

The verification results and any further actions should be recorded and checked when the actions are completed.

When the size, complexity or criticality of a software product warrants, specific assurance methods should be used for verification, such as complexity metrics, peer reviews, condition/decision coverage or formal methods.

Only verified design and development outputs should be submitted for acceptance and subsequent use.

Any findings should be addressed and resolved, as appropriate.

8.3.4.3 Design and development validation

Validation of software is aimed at providing reasonable confidence that it will meet its operational requirements and user needs.

Before offering the product for customer acceptance, the organization should validate the operation of the product in accordance with its specified intended use, under conditions similar to the application environment, as specified in the contract. Any differences between the validation environment and the actual application environment, and the risks associated with such differences, should be identified and justified as early in the life cycle as possible, and recorded. In the course of validation, configuration audits or evaluations may be performed, where appropriate, before release of a configuration baseline.

Configuration audits or evaluations confirm, by examination of the review, inspection and test records, that the software product complies with its contractual or specified requirements. This may require analysis, simulation or emulation where validation is not practicable in operational conditions.

In software development, it is important that the validation results and any further actions required to meet the specified requirements are recorded and checked when the actions are completed.

In some cases, it can be impossible, or unfeasible, to validate fully the software product by measurement and monitoring. An example can be where safety-related software cannot be tested under actual circumstances without risking serious consequences, or perhaps the actual circumstances themselves are rare and difficult to simulate.

The inability to test some software products exhaustively and conclusively may lead the organization to decide

a) how confidence can be gained from the development and tools used, and

b) what types of testing or analysis can be performed to increase confidence that the product will perform correctly under the "untestable" circumstances, e.g. static code analysis.

Whatever methods are used, they should be commensurate with the risk and consequences of design and development failures.

Tools should be validated for their specific intended use.

8.3.4.4 Testing

Testing is often performed to support verification and validation. Testing may be required at several levels, from the individual software item to the complete software product. There are several different approaches to testing, and the extent of testing and the degree of controls on the test environment, test inputs and test outputs may vary with the approach, the complexity of the product and the risk associated with the use of the product. Test planning should address test types, objectives, sequence and scope of testing, test cases, test data and expected results. Test planning should identify the human and physical resources needed for testing and define the responsibilities of those involved.

Specific software tests may include establishing, documenting, reviewing and implementing plans for the following:

a) unit tests, i.e. stand-alone tests of software components;

b) integration and system tests, i.e. tests of aggregations of software components (and the complete system);

c) qualification tests, i.e. tests of the complete software product prior to delivery to confirm the software meets its defined requirements;

d) acceptance tests, i.e. tests of the complete software product to confirm the software meets its acceptance criteria.

Regression testing should be performed to verify or validate that the capabilities of the software have not been compromised by a change.

Acceptance tests are those that are performed for the customer's benefit with the aim of determining the acceptability of the product. Acceptance may be with or without defects or deviations from requirements, by agreement of the parties involved.

Testing tools and the environment to be used should be qualified and controlled, and any limitations to testing recorded.

Testing procedures should cover recording of results and may also include analysis and problem and change management.

Test requirements are often tracked with a change management tool, where records of reviews of test plans, test cases, and approval of test results are maintained in the tool.

NOTE 1 For further information on verification through quality evaluation using quality characteristics and measures, see ISO/IEC 25001, ISO/IEC 25010, ISO/IEC 25040, ISO/IEC 25041 and ISO/IEC 25051.

NOTE 2 ISO/IEC/IEEE 12207 includes the related processes for verification (ISO/IEC/IEEE 12207:2017, 6.4.9) and validation (ISO/IEC/IEEE 12207:2017, 6.4.11).

NOTE 3 The ISO/IEC/IEEE 29119 series gives information on software testing. Organization can establish their own test processes based on principles and processes given in the ISO/IEC/IEEE 29119 series.

8.3.5 Design and development outputs

ISO 9001:2015, Quality management systems — Requirements

8.3.5 Design and development outputs

The organization shall ensure that design and development outputs:

a) meet the input requirements;

b) are adequate for the subsequent processes for the provision of products and services;

c) include or reference monitoring and measuring requirements, as appropriate, and acceptance criteria;

d) specify the characteristics of the products and services that are essential for their intended purpose and their safe and proper provision.

The organization shall retain documented information on design and development outputs.

The output from the design and development process should be defined and documented in accordance with the prescribed or chosen method. This output should be complete, accurate and consistent with the requirements, and may be produced using computer design and development tools. Design and development outputs may be expressed in textual form, by diagrams or using symbolic modelling notation, and may include:

a) design, development and test specifications;

b) data models;

c) pseudo code or source code;

d) user guides, operator documentation, training material, maintenance documentation;

e) developed product;

f) formal methods.

Prototyping, when used, should result in design and development (output) documentation. The acceptance criteria for design and development outputs should be defined in order to demonstrate that the inputs to each design and development stage are correctly reflected in the outputs.

Specified outputs of design and development should be retained for a period of time consistent with the organizational records management policy.

NOTE ISO/IEC/IEEE 12207:2017, B.1 identifies typical outputs of its Architecture Definition (ISO/IEC/IEEE 12207:2017, 6.4.4), Design Definition (ISO/IEC/IEEE 12207:2017, 6.4.5), Implementation (ISO/IEC/IEEE 12207:2017, 6.4.7) and Integration (ISO/IEC/IEEE 12207:2017, 6.4.8) processes. Process outcomes are identified for each process.

8.3.6 Design and development changes

ISO 9001:2015, Quality management systems — Requirements

8.3.6 Design and development changes

The organization shall identify, review and control changes made during, or subsequent to, the design and development of products and services, to the extent necessary to ensure that there is no adverse impact on conformity to requirements.

The organization shall retain documented information on:

a) design and development changes;

b) the results of reviews;

c) the authorization of the changes;

d) the actions taken to prevent adverse impacts.

In the software development environment, control of design and development changes is usually addressed as part of configuration management (see 8.5.2).

NOTE 1 ISO/IEC/IEEE 12207:2017, 6.3.5 covers the Configuration Management process.

Changes to a software specification or component should maintain appropriate consistency among requirements, designs, code, tests specifications, user manuals and, where relevant, other additional items.

NOTE 2 For further general guidance related to ISO 9001:2015, 8.3, see the following:

— ISO/IEC 25051 for guidance on any procured COTS software products;

— ISO/IEC 19761, ISO/IEC 20926 and ISO/IEC 20968 for guidance on estimation of size methods.

8.4 Control of externally provided processes, products and services

8.4.1 General

ISO 9001:2015, Quality management systems — Requirements

8.4.1 General

The organization shall ensure that externally provided processes, products and services conform to requirements.

The organization shall determine the controls to be applied to externally provided processes, products and services when:

a) products and services from external providers are intended for incorporation into the organization's own products and services;

b) products and services are provided directly to the customer(s) by external providers on behalf of the organization;

c) a process, or part of a process, is provided by an external provider as a result of a decision by the organization.

The organization shall determine and apply criteria for the evaluation, selection, monitoring of performance, and re-evaluation of external providers, based on their ability to provide processes or products and services in accordance with requirements. The organization shall retain documented information of these activities and any necessary actions arising from the evaluations.

8.4.1.1 Purchased products

For the purposes of 8.4.1, free software (such as open source development tools) should be considered as purchased.

In developing, supplying, installing and maintaining software products, types of purchased products may include:

a) COTS software or shareware;

b) customized software and services;

c) subcontracted development (e.g. contract staff or outsourced full product development);

d) outsourced activities (e.g. testing, independent verification and validation, facilities management);

e) tools intended to assist in the development of software (e.g. design and development or configuration management tools, code analysers, debuggers, test analysers, generators, compilers);

f) computer and communications hardware;

g) key components (e.g. integrated circuits can be subject to change or to uncertain continued availability);

h) user and product documentation;

i) training courses and materials.

The type and extent of control to be exercised by the organization over a supplier of subcontracted design or development (e.g. joint projects) becomes especially important when selecting the supplier, because confidence in the relationship can be critical to the success of the development.

In developing, supplying, installing and maintaining software products, consideration about purchased products may require the organization to manage the risks associated with licensing, maintenance, help desk, and customer support services (such as concern for continued availability of support for purchased product as a result of later releases). One way of determining the capability of suppliers to provide an acceptable product may be by performing process assessment. Process assessment provides information for risk assessment and a view of maturity and capability level of the supplier's processes.

8.4.1.2 Purchased product control

Where the products listed in a) to i) above are purchased and intended to become part of the product, they should be controlled as components throughout the design and development. Contractual considerations should be addressed so that controls are in place for configuration management to be effective.

Care should be taken to check that contract staff have the specific skills and the levels of competence required, prior to being integrated as part of the project team.

Re-evaluation of suppliers' performance may be conducted by regular review and control during design and development as part of project management (see 8.3.4).

In some circumstances, the whole of ISO 9001:2015 may apply to the organization–supplier relationship.

The management of risk is often more critical in software development because of the nature of the product.

The supplier may be selected based upon the evaluation of the supplier's proposals and process capabilities, and other factors, such as analysis of a supplier's performance history, review of the responses to the supplier questionnaire, and review of software-related quality and verification plans.

NOTE For further information on assessing process capability of a supplier, see:

— ISO/IEC 33001, ISO/IEC TR 33014, ISO/IEC 33020, ISO/IEC TS 33053 and ISO/IEC TS 33073 for process assessment;

— ISO/IEC/IEEE 12207:2017, 6.1.1 includes the related acquisition process for selection and control of suppliers.

8.4.2 Type and extent of control

ISO 9001:2015, Quality management systems — Requirements

8.4.2 Type and extent of control

The organization shall ensure that externally provided processes, products and services do not adversely affect the organization's ability to consistently deliver conforming products and services to its customers.

The organization shall:

a) ensure that externally provided processes remain within the control of its quality management system;

b) define both the controls that it intends to apply to an external provider and those it intends to apply to the resulting output;

c) take into consideration:

1) the potential impact of the externally provided processes, products and services on the organization's ability to consistently meet customer and applicable statutory and regulatory requirements;

2) the effectiveness of the controls applied by the external provider;

d) determine the verification, or other activities, necessary to ensure that the externally provided processes, products and services meet requirements.

NOTE ISO/IEC/IEEE 12207 includes the related activities for control of suppliers [ISO/IEC/IEEE 12207:2017, 6.1.1.3 d)] and verification (ISO/IEC/IEEE 12207:2017, 6.4.9).

8.4.3 Information for external providers

ISO 9001:2015, Quality management systems — Requirements

8.4.3 Information for external providers

The organization shall ensure the adequacy of requirements prior to their communication to the external provider.

The organization shall communicate to external providers its requirements for:

a) the processes, products and services to be provided;

b) the approval of:

1) products and services;

2) methods, processes and equipment;

3) the release of products and services;

c) competence, including any required qualification of persons;

d) the external providers' interactions with the organization;

e) control and monitoring of the external providers' performance to be applied by the organization;

f) verification or validation activities that the organization, or its customer, intends to perform at the external providers' premises.

Purchasing information for software may include, where applicable:

a) identification of the product ordered (such as product name, number, version, configuration);

b) requirements or the procedure to identify requirements where not fixed at the time of order;

c) standards to be applied (e.g. communications protocol, architectural specification, coding standards);

d) procedures and/or work instructions the supplier is instructed to follow;

e) description of the development environment (e.g. hardware, development tools, facilities);

f) description of the target environment (e.g. hardware, operating system);

g) requirements on personnel (e.g. prerequisite training, product knowledge).

The considerations covered in 8.2.2 may also be applied to subcontracts.

NOTE ISO/IEC/IEEE 12207 includes the related activities for agreeing with suppliers on requirements [ISO/IEC/IEEE 12207:2017, 6.1.1.3 c) 1)] and requirements specification (ISO/IEC/IEEE 12207:2017, 6.4.3).

8.5 Production and service provision

8.5.1 Control of production and service provision

ISO 9001:2015, Quality management systems — Requirements

8.5.1 Control of production and service provision

The organization shall implement production and service provision under controlled conditions.

Controlled conditions shall include, as applicable:

a) the availability of documented information that defines:

   1) the characteristics of the products to be produced, the services to be provided, or the activities to be performed;

   2) the results to be achieved;

b) the availability and use of suitable monitoring and measuring resources;

c) the implementation of monitoring and measurement activities at appropriate stages to verify that criteria for control of processes or outputs, and acceptance criteria for products and services, have been met;

d) the use of suitable infrastructure and environment for the operation of processes;

e) the appointment of competent persons, including any required qualification;

f) the validation, and periodic revalidation, of the ability to achieve planned results of the processes for production and service provision, where the resulting output cannot be verified by subsequent monitoring or measurement;

g) the implementation of actions to prevent human error;

h) the implementation of release, delivery and post-delivery activities.

8.5.1.1 Production and service provision in software

As stated in the guidance for design and development (see 8.3), a software development project should be organized according to a set of processes, which transform the requirements into a software product.

The "control of production and service provision" requirements specified in ISO 9001:2015, 8.5.1 can be interpreted for software products as:

a) in process control activities, e.g., procedures, coding guidelines, change management tools, modelling tools;

b) release activities, e.g. build, release, and replication;

c) delivery activities, e.g. delivery and installation;

d) post-delivery activities, e.g. operations, maintenance and customer support (these apply throughout the life of the product).

8.5.1.2 Build and release

Processes should be established for build, release, patching and replication of the software item(s). Build and release activities invoke configuration management (see 8.5.2).

The following provisions are appropriate to build and release:

a) identification of the software items that constitute each release, including associated build instructions;

b) identification of the types (or classes) of release, depending on the frequency and/or impact on the customer's operations and ability to implement changes at any point in time;

c) decision criteria and guidance to determine where localized temporary fixes or "patches" may be incorporated or where the release of a complete updated copy of the software product is necessary.

8.5.1.3 Replication

Where required, the organization should establish and perform replication, considering the following to ensure that replication is conducted correctly:

a) identification of the master and the copies, including format, variant and version;

b) the type of media for each software item and associated labelling;

c) the stipulation of required documentation such as manuals, user guides, licences and release notes, including identification and packaging;

d) controlling the environment under which the replication is effected for repeatability;

e) provision for ensuring correctness and completeness of the copies of the product.

8.5.1.4 Delivery

Delivery may be achieved by physical movement of media containing software or by electronic transmission.

The preservation of items during delivery is covered in 8.5.4.

8.5.1.5 Installation

Sometimes, customers or third parties conduct installation. In this case the role of the organization is to describe the steps the customer or third party needs to take to perform the installation. Sometimes, the installation is conducted by the organization. For the latter case, the following may apply:

a) the organization and customer should agree on their respective roles, responsibilities and obligations;

b) the need and extent of validation at each installation should be defined;

c) the need for installation instructions should be defined;

d) the need for configuration of the software and hardware for the specific installation should be defined;

e) the need for data capture and/or conversion and database population should be defined;

f) the acceptance procedure of each installation upon completion should be defined;

g) a schedule is needed;

h) access to customer's facilities and equipment should be arranged (e.g. security badges, passwords, escorts);

i) the availability of skilled personnel should be established;

j) the need to provide training associated with the specific intended use of the product during installation or as part of maintenance should be defined;

k) the need to perform backup and confirm recovery should be defined.

The introduction of a new software product or new software release at multiple user sites can require planning of implementation or rollout.

8.5.1.6 Post-delivery operations

A software-producing organization should consider the following post-delivery operations, as appropriate:

a) the need to set up a help desk to conduct telephone or other electronic communication with the customer(s);

b) arrangements, including network tools for ensuring continuity of support, such as disaster recovery, security and backup (see 7.1.3).

See also 8.5.5.

8.5.1.7 Maintenance

Maintenance of the software product that is requested by the customer for specific items, and a specific period of time, after initial delivery and installation, should be stipulated in the contract.

The organization should establish a process for performing maintenance activities and verifying them. Maintenance activities may also be performed on the development environment, tools and documentation. Maintenance should include the following, as appropriate:

a) scope of maintenance;

b) identification of the initial status of the maintained items;

c) support organization(s) and arrangements (see also 8.5.1.6);

d) maintenance activities including problem resolution, help desk support, hardware support and system monitoring to detect failure;

e) interface modifications that may be required when additions or changes are made to the hardware system, or components, controlled by the software;

f) configuration management, testing and quality assurance activities;

g) proposed release schedule;

h) how functional expansion and performance improvement will be carried out;

i) maintenance records and reports.

The records of the maintenance activities may be utilized for evaluation and enhancement of the software product and for improvement of the quality management system itself. When resolving problems, temporary fixes may be used to minimize downtime and permanent modifications carried out later.

For interface modifications and functional expansion, depending upon the scale of work, change control procedures should apply, or a new and separate development project should be initiated.

8.5.1.8 Validation of processes for product and service provision

The organization should consider what processes may be used to compensate for the inability to validate fully the product. Examples include the following:

a) a design and development review might consider how the design and development might fail in addition to the more normal check that the design and development will function correctly;

b) a program of failure mode and effect analyses that builds up a history of design and development failures and how they can be avoided.

Whatever methods are used, they should be commensurate with the risks and consequences of design and development failures.

NOTE ISO/IEC/IEEE 12207 includes the related technical processes for production and provision of services: Integration (ISO/IEC/IEEE 12207:2017, 6.4.8), Transition (ISO/IEC/IEEE 12207:2017, 6.4.10), Operation (ISO/IEC/IEEE 12207:2017, 6.4.12) and Maintenance (ISO/IEC/IEEE 12207:2017, 6.4.13).

8.5.2 Identification and traceability

ISO 9001:2015, Quality management systems — Requirements

8.5.2 Identification and traceability

The organization shall use suitable means to identify outputs when it is necessary to ensure the conformity of products and services.

The organization shall identify the status of outputs with respect to monitoring and measurement requirements throughout production and service provision.

The organization shall control the unique identification of the outputs when traceability is a requirement, and shall retain the documented information necessary to enable traceability.

8.5.2.1 Overview

For software, identification and traceability is commonly implemented through configuration management. Configuration management is a management discipline that applies technical and administrative direction to the design, development and support of configuration items, including software items. This discipline is also applicable to related documentation (see also 7.5.1) and hardware.

The degree of configuration management use is dependent on the project size, complexity and risk level.

One objective of configuration management is to provide full visibility of the product's present configuration and status. Another objective is that everyone working on the product at any time in its life cycle uses appropriate versions of items.

8.5.2.2 Traceability

Throughout the product life cycle, there should be a process to trace the components of the software item or product, from requirements through design, testing, release, operation and maintenance. Such tracing may vary in scope according to the requirements of the contract or marketplace, from being able to place a certain change request in a specific release, to recording the destination and usage of each variant of the product.

8.5.2.3 Configuration management process

The scope of configuration management should include the following:

a) planning of the process including defining activities, responsibilities and the tools to be procured;

b) identifying uniquely the name and versions of each configuration item and when they are to be brought under configuration control (configuration identification);

c) identifying the versions of each software item which together constitute a specific version of a complete product (baseline), including re-used software, libraries, and purchased and customer supplied software;

d) identifying the build status of software products under development, delivered or installed, for single or multiple environments, as appropriate;

e) controlling simultaneous updates of a given software item by two or more people working independently (configuration control);

f) providing coordination for the updating of multiple products in one or more locations as required;

g) identifying, tracking and reporting of the status of items, including all actions and changes resulting from a change request or problem, from initiation through to release (configuration status accounting);

h) providing configuration evaluation (status of verification and validation activities);

i) providing release management and control of delivery of the software product;

j) providing configuration audit results.

Control of documented information is in 7.5.3 and control of changes in 8.5.6 — both these subclauses are related to configuration management.

NOTE For further information, see the following:

— ISO 10007 (guidelines for Configuration Management);

— ISO/IEC/IEEE 12207:2017, 6.3.5 (Configuration Management process);

— the ISO/IEC 19770 series provides procedures and requirements for an IT asset management system.

8.5.3 Property belonging to customers or external providers

ISO 9001:2015, Quality management systems — Requirements

8.5.3 Property belonging to customers or external providers

The organization shall exercise care with property belonging to customers or external providers while it is under the organization's control or being used by the organization.

The organization shall identify, verify, protect and safeguard customers' or external providers' property provided for use or incorporation into the products and services.

When the property of a customer or external provider is lost, damaged or otherwise found to be unsuitable for use, the organization shall report this to the customer or external provider and retain documented information on what has occurred.

NOTE A customer's or external provider's property can include materials, components, tools and equipment, premises, intellectual property and personal data.

The organization may be required to acquire and include product and data supplied by the customer into the development process, such as:

1) software products including commercial software products supplied by the customer;
2) development tools;
3) development environments including network services;
4) test and operational data;
5) interface or other specifications;
6) hardware;
7) intellectual property, and confidential and proprietary information, including specifications.

In any maintenance agreement, consideration should be given to addressing:

a) required licensing and support, including subsequent revisions to the product;
b) limitations or constraints in re-use of the product in other projects.

The means by which updates to customer-supplied items are accepted and integrated should be defined.

The organization may apply the same kinds of verification activities to customer-supplied product as to purchased product. This includes requirements for records indicating which changes have been implemented and at what locations for multiple products and sites.

The methods for identifying the customer-supplied product should be part of configuration management for the product (see 8.5.2).

NOTE 1 The ISO/IEC 19770 series provides procedures and requirements for an IT asset management system.

NOTE 2 ISO 9001:2015 incorporates the care of the property belonging to external suppliers, for which the same requirements as those contemplated for the clients (term used in the ISO/IEC 19770 series), apply.

8.5.4 Preservation

ISO 9001:2015, Quality management systems — Requirements

8.5.4 Preservation

The organization shall preserve the outputs during production and service provision, to the extent necessary to ensure conformity to requirements.

NOTE Preservation can include identification, handling, contamination control, packaging, storage, transmission or transportation, and protection.

A software-producing organization should plan that its products are not altered from the point of production, through replication, handling and storage, to the point of delivery. Software information does not degrade; however, the media on which it is stored may be subject to deterioration, and appropriate precautions should be taken by the organization.

Delivery should provide for appropriate preventive action to protect the software product from damage.

In addition, an appropriate level of software virus checking and appropriate measures to protect product integrity are needed. Delivery of software may be achieved by physical movement of media containing software or by electronic transmission. The following should be considered, and appropriate actions taken when handling, packaging, storing or delivering software:

a) storing software items, maintaining versions of products in established baselines;

b) permitting the controlled access to and retrieval of the master and any copies, protecting them from unauthorized change or corruption;

c) protecting computer media, particularly with respect to computer viruses, electromagnetic and electrostatic environments;

d) providing for regular backup of software, including off-site storage for disaster recovery;

e) ensuring the timely copying of software to replacement media;

f) storing of software media in a protected environment, preventing deterioration and protecting from obsolescence;

g) the effects of using compression and decompression techniques (the reduction of the space taken on a data medium by encoding data, taking advantage of redundancy in the data);

h) the effects of using encryption and decryption techniques (the transformation of data into an unintelligible form for data security).

NOTE For further general guidance related to ISO 9001:2015, 8.5.4, see the following:

— ISO/IEC 25010 for guidance on quality characteristics of software products;

— ISO/IEC 14764;

— ISO/IEC 26514;

— ISO/IEC/IEEE 12207:2017, 6.4.7.3 b) 5) and 6) includes the related tasks for preservation of output.

8.5.5 Post-delivery activities

ISO 9001:2015, Quality management systems — Requirements

8.5.5 Post-delivery activities

The organization shall meet requirements for post-delivery activities associated with the products and services.

In determining the extent of post-delivery activities that are required, the organization shall consider:

a) statutory and regulatory requirements;

b) the potential undesired consequences associated with its products and services;

c) the nature, use and intended lifetime of its products and services;

d) customer requirements;

e) customer feedback.

NOTE Post-delivery activities can include actions under warranty provisions, contractual obligations such as maintenance services, and supplementary services such as recycling or final disposal.

Specific guidance for software is already included in 8.5.1.5, 8.5.1.6 and 8.5.1.7.

NOTE ISO/IEC/IEEE 12207:2017, 6.4.13 includes the related post-delivery activities in the Maintenance process.

8.5.6 Control of changes

ISO 9001:2015, Quality management systems — Requirements

8.5.6 Control of changes

The organization shall review and control changes for production or service provision, to the extent necessary to ensure continuing conformity with requirements.

The organization shall retain documented information describing the results of the review of changes, the person(s) authorizing the change, and any necessary actions arising from the review.

In the software development environment, control of design and development changes is usually addressed as part of configuration management (see 8.5.2).

Changes to a software specification or component should maintain appropriate consistency between requirements, designs, code, tests specifications, user manuals and, where relevant, other additional items.

NOTE 1 For further information, see ISO/IEC/IEEE 12207:2017, 6.3, on Technical Management processes.

NOTE 2 For further general guidance related to ISO 9001:2015, 8.5.6, see the following:

— ISO/IEC 25051 for guidance on any procured COTS software products;

— ISO/IEC 26514 for design and development documentation guidance;

— ISO/IEC 19761, ISO/IEC 20926 and ISO/IEC 20968 for guidance on estimation of size methods;

— ISO/IEC/IEEE 12207:2017, 6.3.5 includes the related production change control activities as part of the CM process.

NOTE 3 According to ISO 9001:2015 change control applies to all stages of the production and service life cycle, which extends beyond design and development.

8.6 Release of products and services

ISO 9001:2015, Quality management systems — Requirements

8.6 Release of products and services

The organization shall implement planned arrangements, at appropriate stages, to verify that the product and service requirements have been met.

The release of products and services to the customer shall not proceed until the planned arrangements have been satisfactorily completed, unless otherwise approved by a relevant authority and, as applicable, by the customer.

The organization shall retain documented information on the release of products and services. The documented information shall include:

a) evidence of conformity with the acceptance criteria;

b) traceability to the person(s) authorizing the release.

An organization should monitor and measure the conformity of products to quality requirements by means such as review, verification and validation. Examples of product characteristics that may be monitored or measured include:

a) functionality;

b) maintainability;

c) efficiency;

d) portability;

e) usability;

f) reliability.

The issue (e.g., version, baseline) of software or product released should be recorded and be traceable back to specified requirements and related to low and high level tests. It should be possible to establish the level of software functionality in any given build or release and be able to provide valid test results.

NOTE For further information, see the following:

— Technical processes (ISO/IEC/IEEE 12207:2017, 6.4), which contains provisions for evaluation of software products during development and when completed and the Verification process (ISO/IEC/IEEE 12207:2017, 6.4.9) which is applicable before release of products and services to the customer. Controlled release of software is tracked through configuration management activities, [ISO/IEC/IEEE 12207:2017, 6.3.5.3 d)];

— ISO/IEC 25010;

— ISO/IEC 25040 and ISO/IEC 25041.

8.7 Control of nonconforming outputs

8.7.1 Identification and control of nonconforming outputs

ISO 9001:2015, Quality management systems — Requirements

8.7.1 The organization shall ensure that outputs that do not conform to their requirements are identified and controlled to prevent their unintended use or delivery.

The organization shall take appropriate action based on the nature of the nonconformity and its effect on the conformity of products and services. This shall also apply to nonconforming products and services detected after delivery of products, during or after the provision of services.

The organization shall deal with nonconforming outputs in one or more of the following ways:

a) correction;

b) segregation, containment, return or suspension of provision of products and services;

c) informing the customer;

d) obtaining authorization for acceptance under concession.

Conformity to the requirements shall be verified when nonconforming outputs are corrected.

In software development, segregation of nonconforming items may be effected by transferring the item out of a production or testing environment, into a separate environment. In the case of embedded software it may become necessary to segregate the nonconforming item (hardware) which contains the nonconforming software.

The supplier should identify at what points control and recording of nonconforming product is required.

Where a software item manifests a defect during development or maintenance, the investigation and resolution of such defects should be controlled and recorded.

Configuration management may be invoked to implement part of or the whole of this requirement.

Attention should be paid to the following aspects in the disposition of nonconformities:

a) any discovered problems and their possible impacts on any other parts of the software should be noted and those responsible notified so the problems can be tracked until they are resolved;

b) areas impacted by any modifications should be identified and re-tested, and the method for determining the scope of re-testing should be identified in a documented procedure;

c) the priority of the nonconformities should be established.

With software, repair or rework to achieve fulfilment of specified requirements creates a new software version. In software development, disposition of nonconforming product may be achieved by:

a) repair or rework (i.e. to fix defects) to meet the requirement;

b) acceptance with or without repair by concession;

c) treatment as a conforming product after the amendment of requirements;

d) rejection.

For software, as part of testing, problems, defects or bugs may be identified, recorded and resolved. The process for this is normally implemented through a software tool.

NOTE For further information, see the following:

— The Configuration Management process (ISO/IEC/IEEE 12207:2017, 6.3.5), the QA process (ISO/IEC/IEEE 12207:2017, 6.3.8), which is responsible for oversight of incident resolution and treatment of problems. All technical processes include responsibility for correction of errors and defects, particularly the Maintenance process (ISO/IEC/IEEE 12207:2017, 6.4.13);

— ISO/IEC 25051 and ISO/IEC 14102 for guidelines for the evaluation and selection of CASE tools.

8.7.2 Retaining documented information for nonconforming outputs

ISO 9001:2015, Quality management systems — Requirements

8.7.2 The organization shall retain documented information that:

a) describes the nonconformity;

b) describes the actions taken;

c) describes any concessions obtained;

d) identifies the authority deciding the action in respect of the nonconformity.

For software the documented information is usually held in a computer tool.

NOTE ISO/IEC/IEEE 12207 includes the QA process which is responsible for retention of data regarding treatment of nonconformities (incidents and problems), see ISO/IEC/IEEE 12207:2017, 6.3.8.3 d) and e).

9 Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

9.1.1 General

ISO 9001:2015, Quality management systems — Requirements

9.1.1 General

The organization shall determine:

a) what needs to be monitored and measured;

b) the methods for monitoring, measurement, analysis and evaluation needed to ensure valid results;

c) when the monitoring and measuring shall be performed;

d) when the results from monitoring and measurement shall be analysed and evaluated.

The organization shall evaluate the performance and the effectiveness of the quality management system.

The organization shall retain appropriate documented information as evidence of the results.

The monitoring, measurement, analysis and improvement processes should be identified as part of quality planning (see 6.2). Otherwise it should take place during the project life cycle or the software development life cycle.

Organizations normally measure some aspects of their processes in order to monitor, manage and assess them. Some organizations also conduct process capability assessment in a formal way. The most frequent measures include:

a) the planned and actual duration of a process activity;

b) the planned and actual cost of a process activity;

c) the planned quality levels and progressive measures of the selected quality characteristics.

NOTE 1 For further information, see the following:

— ISO/IEC/IEEE 15939;

— ISO/IEC 33001, ISO/IEC TR 33014, ISO/IEC 33020, ISO/IEC TS 33053 and ISO/IEC TS 33073 for process assessment, including process capability assessment model for quality management in ISO/IEC TS 33073;

— ISO/IEC 25001.

NOTE 2 The quality assurance process of ISO/IEC/IEEE 12207 includes measurement activities as part of QA strategy [ISO/IEC/IEEE 12207:2017, 6.3.8.3 a) 1) v)]. The Measurement process (ISO/IEC/IEEE 12207:2017, 6.3.7) includes detailed activities and tasks. Measurement analysis is also performed through the Project assessment and control process [ISO/IEC/IEEE 12207:2017, 6.3.2.3 b) 9)].

9.1.2 Customer satisfaction

ISO 9001:2015, Quality management systems — Requirements

9.1.2 Customer satisfaction

The organization shall monitor customers' perceptions of the degree to which their needs and expectations have been fulfilled. The organization shall determine the methods for obtaining, monitoring and reviewing this information.

NOTE Examples of monitoring customer perceptions can include customer surveys, customer feedback on delivered products and services, meetings with customers, market-share analysis, compliments, warranty claims and dealer reports.

The organization's process for requesting, measuring and monitoring feedback of customer satisfaction should provide information on a periodic basis as appropriate. For software consider, for example:

a) analysis of help desk calls relating to both product quality and service performance;

b) quality-in-use metrics derived from customer direct and indirect feedback;

c) other quality metrics based on use of the product;

d) number of software releases needed to fix problems, after initial delivery.

NOTE For further information, see:

— ISO/IEC 25010 (product quality — quality-metrics, ISO/IEC 25001, ISO/IEC 25040, ISO/IEC 25041 and ISO/IEC 25051 may also be helpful).

— The quality management process in ISO/IEC/IEEE 12207:2017, 6.2.5.3 b) 2) includes monitoring of customer satisfaction.

9.1.3 Analysis and evaluation

ISO 9001:2015, Quality management systems — Requirements

9.1.3 Analysis and evaluation

The organization shall analyse and evaluate appropriate data and information arising from monitoring and measurement.

The results of analysis shall be used to evaluate:

a) conformity of products and services;

b) the degree of customer satisfaction;

c) the performance and effectiveness of the quality management system;

d) if planning has been implemented effectively;

e) the effectiveness of actions taken to address risks and opportunities;

f) the performance of external providers;

g) the need for improvements to the quality management system.

NOTE Methods to analyse data can include statistical techniques.

Examples of "analysis and evaluation" for software may include problem reports from various levels of testing and issues identified in reviews or walkthroughs.

NOTE For further information, see the following:

— ISO/IEC/IEEE 15939:2017, 4.4 (software measurement process — evaluate results).

— ISO/IEC 19761, ISO/IEC 20926 and ISO/IEC 20968.

— The systems analysis process of ISO/IEC/IEEE 12207:2017, 6.4.6, is applicable. The Measurement process [ISO/IEC/IEEE 12207:2017, 6.3.7 b) 1)] includes detailed activities and tasks for analysis as integrated into every technical process. Measurement analysis is also performed through the Project assessment and control process [ISO/IEC/IEEE 12207:2017, 6.3.2.3 b) 9)].

9.2 Internal audit

9.2.1 Conducting audits

ISO 9001:2015, Quality management systems — Requirements

9.2.1 The organization shall conduct internal audits at planned intervals to provide information on whether the quality management system:

a) conforms to:

1) the organization's own requirements for its quality management system;

2) the requirements of this International Standard;

b) is effectively implemented and maintained.

Personnel responsible for conducting internal audits should have the appropriate level of competency (in software development, testing, operations or maintenance — as appropriate) and attained recognised approvals or qualifications to conduct formal internal audits.