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/IEC 2018
© IEEE 2018



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2018

© IEEE 2018

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO or IEEE at the respective address below or ISO's member body in the country of the requester.

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

© ISO/IEC 2018 – All rights reserved
© IEEE 2018 – All rights reserved

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

© ISO/IEC 2018 – All rights reserved
© IEEE 2018 – All rights reserved

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

© ISO/IEC 2018 – All rights reserved
© IEEE 2018 – All rights reserved

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.

© ISO/IEC 2018 – All rights reserved
© IEEE 2018 – All rights reserved

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.

© ISO/IEC 2018 – All rights reserved
© IEEE 2018 – All rights reserved

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.

© ISO/IEC 2018 – All rights reserved
© IEEE 2018 – All rights reserved

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.

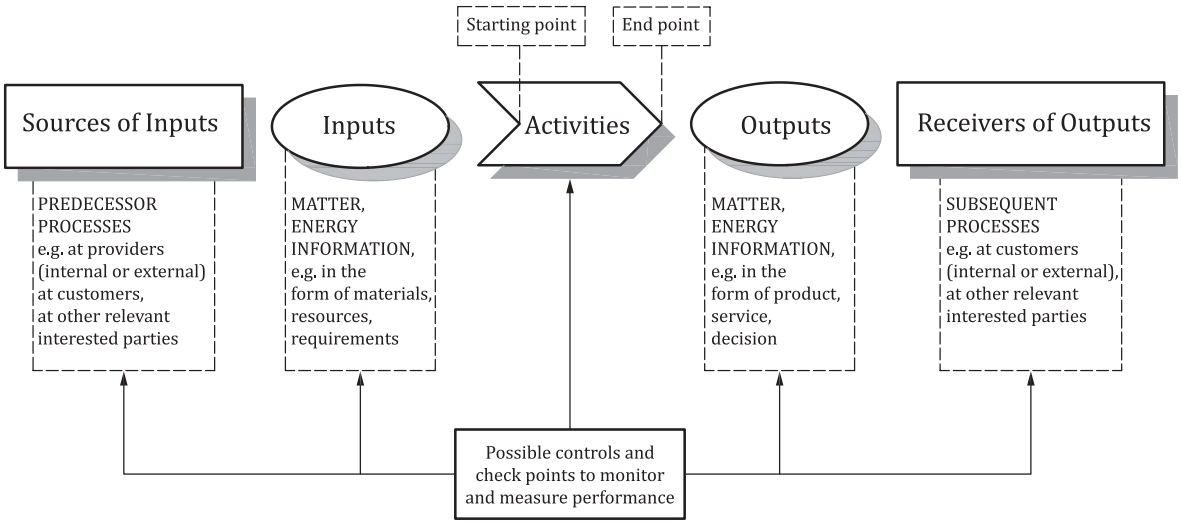
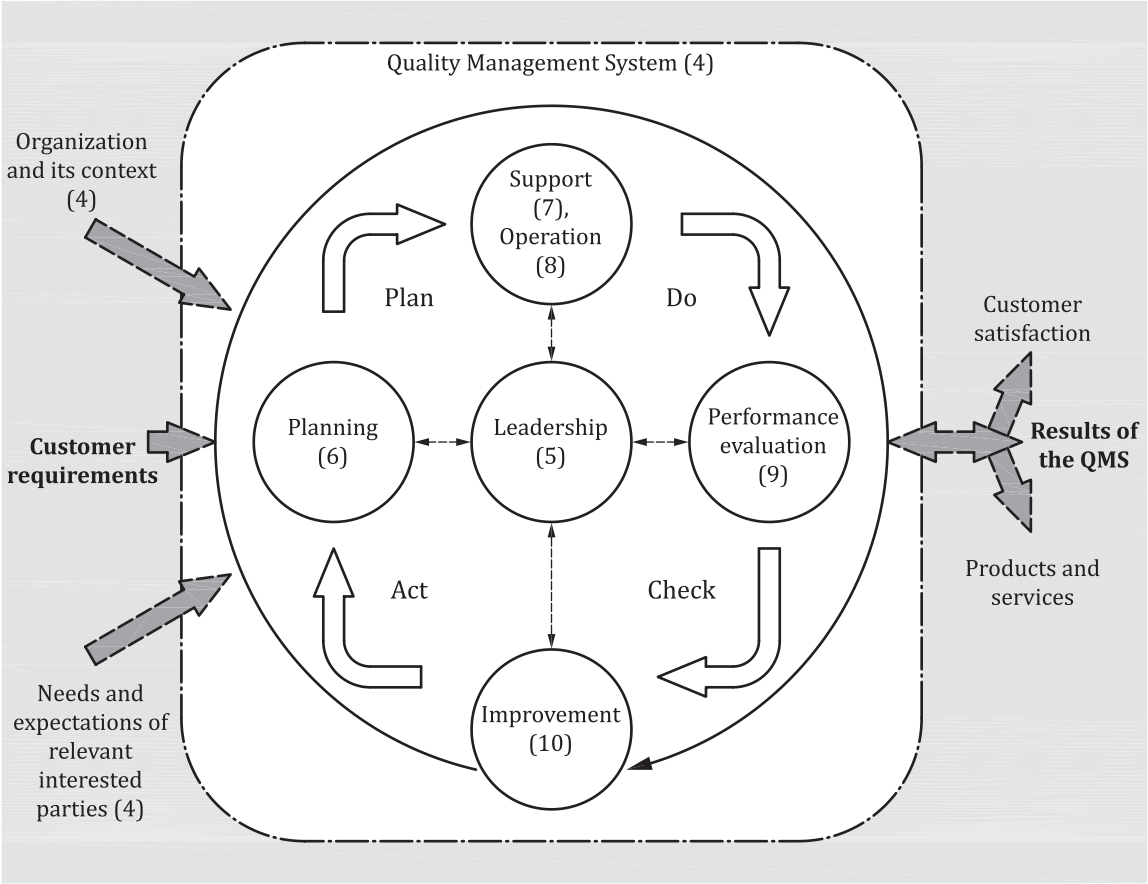


Figure 1 — Schematic representation of the elements of a single process

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.

© ISO/IEC 2018 – All rights reserved
© IEEE 2018 – All rights reserved



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.

© ISO/IEC 2018 – All rights reserved
© IEEE 2018 – All rights reserved

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

© ISO/IEC 2018 – All rights reserved
© IEEE 2018 – All rights reserved

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.

© ISO/IEC 2018 – All rights reserved
© IEEE 2018 – All rights reserved

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*

© ISO/IEC 2018 – All rights reserved
© IEEE 2018 – All rights reserved

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]

© ISO/IEC 2018 – All rights reserved
© IEEE 2018 – All rights reserved

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.

© ISO/IEC 2018 – All rights reserved
© IEEE 2018 – All rights reserved