BS ISO/IEC/IEEE 90003:2018

BSI Standards Publication

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

Documents
Document Sharing Hub

Full document details: BS ISO/IEC/IEEE 90003:2018

National foreword

This British Standard is the UK implementation of ISO/IEC/IEEE 90003:2018. It supersedes BS ISO/IEC 90003:2014, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/15, Software and systems engineering.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2018
Published by BSI Standards Limited 2018

ISBN 978 0 580 51180 6

ICS 03.100.70; 03.120.10; 35.080

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 November 2018.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS ISO/IEC/IEEE 90003:2018

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

Documents
Document Sharing Hub

Full document details: BS ISO/IEC/IEEE 90003:2018

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

Documents
Document Sharing Hub

Full document details: BS ISO/IEC/IEEE 90003:2018

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

AVA Documents
Document Sharing Hub
Full document details: BS ISO/IEC/IEEE 90003:2018

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
Documents Document Sharing Hub
Full document details: BS ISO/IEC/IEEE 90003:2018

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

Documents
Document Sharing Hub
Full document details: BS ISO/IEC/IEEE 90003:2018

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
Documents Document Sharing Hub
Full document details: BS ISO/IEC/IEEE 90003:2018

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

Documents
Document Sharing Hub
Full document details: BS ISO/IEC/IEEE 90003:2018

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.

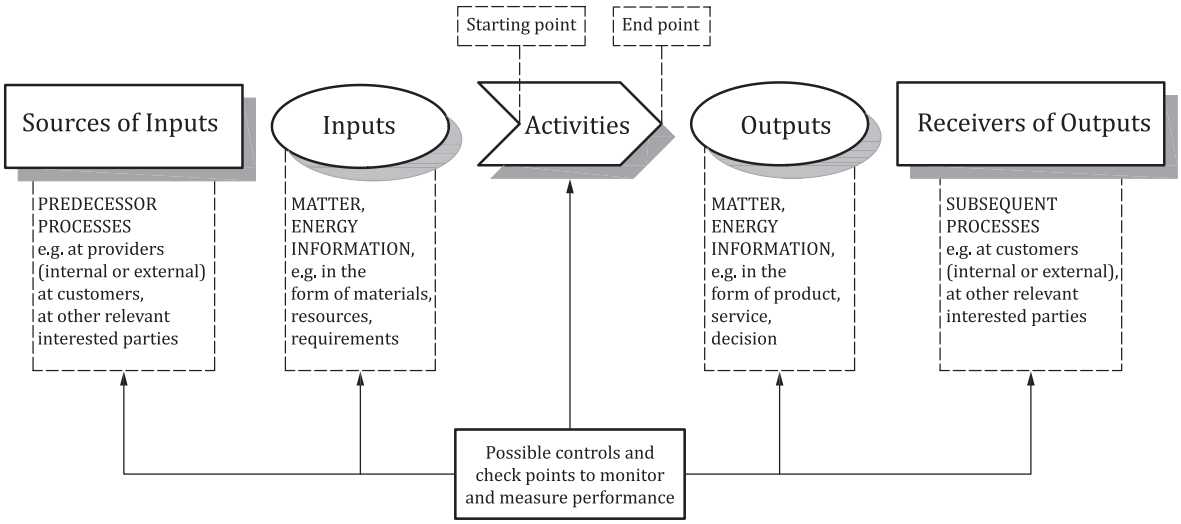
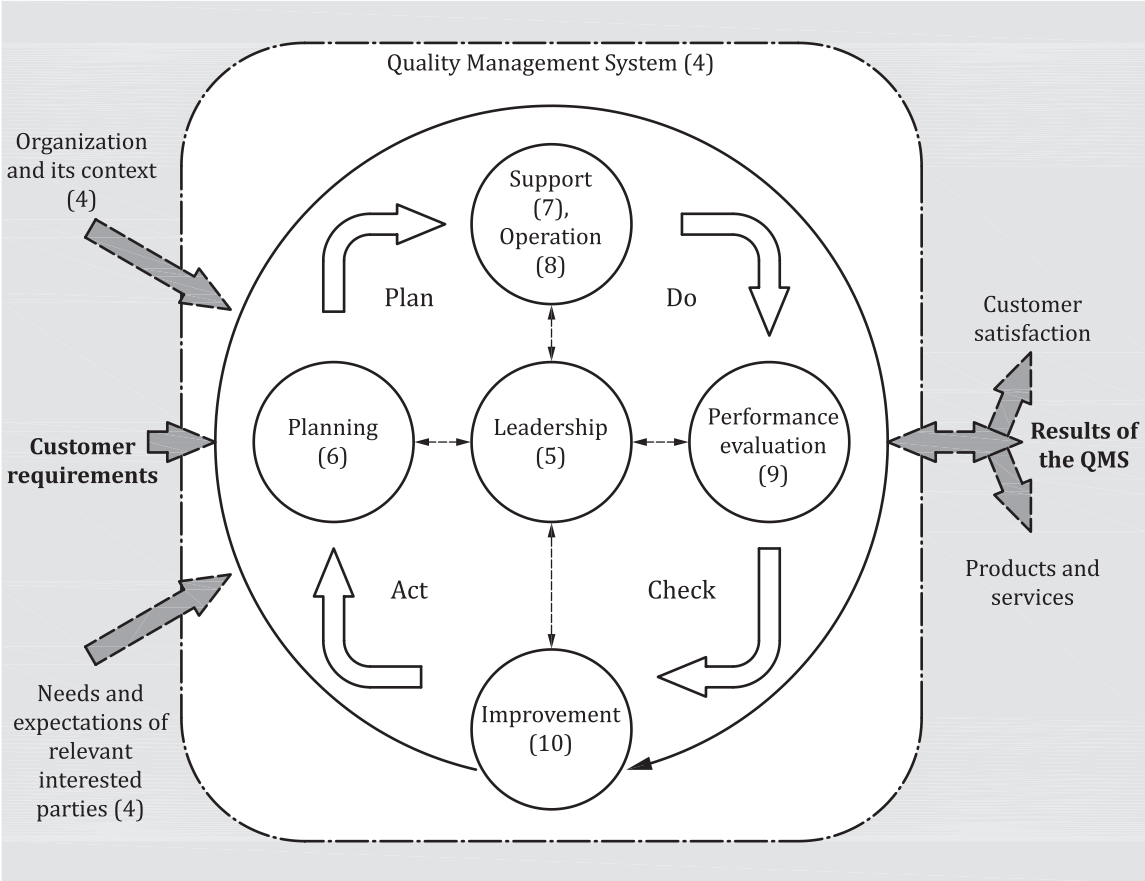


Figure 1 — Schematic representation of the elements of a single process

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
Documents Document Sharing Hub
Full document details: BS ISO/IEC/IEEE 90003:2018



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

Documents
Document Sharing Hub
Full document details: BS ISO/IEC/IEEE 90003:2018

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

Documents
Document Sharing Hub
Full document details: BS ISO/IEC/IEEE 90003:2018

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

Documents
Document Sharing Hub
Full document details: BS ISO/IEC/IEEE 90003:2018

Documents
Document Sharing Hub

Full document details: BS ISO/IEC/IEEE 90003:2018

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

Documents
Document Sharing Hub
Full document details: BS ISO/IEC/IEEE 90003:2018

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
Documents Document Sharing Hub
Full document details: BS ISO/IEC/IEEE 90003:2018

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

Documents
Document Sharing Hub
Full document details: BS ISO/IEC/IEEE 90003:2018

— 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.

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

Documents
Document Sharing Hub

Full document details: BS ISO/IEC/IEEE 90003:2018

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.

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

Documents
Document Sharing Hub
Full document details: BS ISO/IEC/IEEE 90003:2018

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);

© ISO/IEC 2018 – All rights reserved
© IEEE 2018 – All rights reserved
Documents Document Sharing Hub
Full document details: BS ISO/IEC/IEEE 90003:2018

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.

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

Documents
Document Sharing Hub
Full document details: BS ISO/IEC/IEEE 90003:2018

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.

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

Documents
Document Sharing Hub

Full document details: BS ISO/IEC/IEEE 90003:2018

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.

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

Documents
Document Sharing Hub
Full document details: BS ISO/IEC/IEEE 90003:2018

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.

© ISO/IEC 2018 – All rights reserved
© IEEE 2018 – All rights reserved
Documents Document Sharing Hub
Full document details: BS ISO/IEC/IEEE 90003:2018

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.

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

Documents
Document Sharing Hub
Full document details: BS ISO/IEC/IEEE 90003:2018

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.

© ISO/IEC 2018 – All rights reserved
© IEEE 2018 – All rights reserved
Documents Document Sharing Hub
Full document details: BS ISO/IEC/IEEE 90003:2018

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.

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

Documents
Document Sharing Hub
Full document details: BS ISO/IEC/IEEE 90003:2018