INTERNATIONAL STANDARD

ISO/IEC 90003

First edition
2004-02-15

Software engineering — Guidelines for the application of ISO 9001:2000 to computer software

Ingénierie du logiciel — Lignes directrices pour l'application de l'ISO 9001:2000 aux logiciels informatiques

Reference number
ISO/IEC 90003:2004(E)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

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

Published in Switzerland

Contents

Page

Foreword

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

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

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is 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.

ISO/IEC 90003 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 7, *Software and system engineering*.

This first edition of ISO/IEC 90003 cancels and replaces ISO 9000-3:1997, which has been updated for conformity with ISO 9001:2000. ISO 9000-3:1997 was under the responsibility of ISO/TC 176/SC 2.

Introduction

This International Standard provides guidance for organizations in the application of ISO 9001:2000 to the acquisition, supply, development, operation and maintenance of computer software.

It identifies the issues which 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 clause 8 of ISO 9001:2000 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.

Throughout ISO 9001:2000, "shall" is used to express a provision that is binding between two or more parties, "should" to express a recommendation among possibilities and "may" to indicate a course of action permissible within the limits of ISO 9001:2000. In this International Standard (ISO/IEC 90003), "should" and "may" have the same meaning as in ISO 9001:2000, i.e. "should" to express a recommendation among possibilities and "may" to indicate a course of action permissible within the limits of this International Standard.

Organizations with quality management systems for developing, operating or maintaining software based on this International Standard may choose to use processes from ISO/IEC 12207 and ISO/IEC 12207:1995/Amd.1:2002 to support or complement the ISO 9001:2000 process model. It should be noted that the quality management process defined in ISO/IEC 12207:1995/Amd.1:2002, F.3.1.4 is not consistent with the definition of quality management in ISO 9000, ISO 9001 and other ISO/TC 176 standards. The related paragraphs of ISO/IEC 12207:1995/Amd.1:2002 are referenced in each clause of this International Standard; however, they are not intended to imply requirements additional to those in ISO 9001:2000. Further guidance to the use of ISO/IEC 12207 may be found in ISO/IEC TR 15271. For additional guidance, frequent references are provided to the International Standards for software engineering defined by ISO/IEC JTC 1/SC 7 and in particular ISO/IEC 9126-1, ISO/IEC TR 9126-2, ISO/IEC TR 9126-3, ISO/IEC TR 9126-4, ISO/IEC 15939 and ISO/IEC 15504 (all parts). Where these references are specific to a clause or subclause of ISO 9001:2000 they appear after the guidance for that clause or subclause. Where they apply generally across the parts of a clause or subclause, the references are included at the end of the last part of the clause or subclause.

Where text has been quoted from ISO 9001:2000, that text is enclosed in a box, for ease of identification.

Software engineering — Guidelines for the application of ISO 9001:2000 to computer software

1 Scope

1.1 General

ISO 9001:2000, Quality management systems — Requirements

1.1 General

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

a) needs to demonstrate its ability to consistently provide product that meets customer and applicable regulatory requirements, and

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

NOTE In this International Standard, the term “product” applies only to the product intended for, or required by, a customer.

This International Standard provides guidance for organizations in the application of ISO 9001:2000 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 9001:2000.

Annex A (informative) provides a table pointing to additional guidance in the implementation of ISO 9001:2000 available in ISO/IEC JTC 1/SC 7 and ISO/TC 176 standards.

The guidelines provided in this International Standard are not intended to be used as assessment criteria in quality management system registration/certification.

1.2 Application

ISO 9001:2000, Quality management systems — Requirements

1.2 Application

All requirements of this International Standard are generic and are intended to be applicable to all organizations, regardless of type, size and product provided.

Where any requirement(s) of this International Standard cannot be applied due to the nature of an organization and its product, this can be considered for exclusion.

Where exclusions are made, claims of conformity to this International Standard are not acceptable unless these exclusions are limited to requirements within clause 7, and such exclusions do not affect the organization's ability, or responsibility, to provide product that meets customer and applicable regulatory requirements.

The application of this International Standard is appropriate to software that is

— part of a commercial contract with another organization,

— a product available for a market sector,

— used to support the processes of an organization,

— embedded in a hardware product, or

— 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 organization's quality management system should cover all aspects (software related and non-software related) of the business.

2 Normative references

ISO 9001:2000, Quality management systems — Requirements

2 Normative reference

The following normative document contains provisions which, through reference in this text, constitute provisions of this International Standard. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this International Standard are encouraged to investigate the possibility of applying the most recent edition of the normative document indicated below. For undated references, the latest edition of the normative document referred to applies. Members of ISO and IEC maintain registers of currently valid International Standards.

ISO 9000:2000, *Quality management systems — Fundamentals and vocabulary*.

3 Terms and definitions

ISO 9001:2000, Quality management systems — Requirements

3 Terms and definitions

For the purposes of this International Standard, the terms and definitions given in ISO 9000 apply.

The following terms, used in this edition of ISO 9001 to describe the supply chain, have been changed to reflect the vocabulary currently used:

supplier → **organization** → **customer**

The term "organization" replaces the term "supplier" used in ISO 9001:1994, and refers to the unit to which this International Standard applies. Also, the term "supplier" now replaces the term "subcontractor".

Throughout the text of this International Standard, wherever the term "product" occurs, it can also mean "service".

For the purposes of this document, the terms and definitions given in ISO 9001:2000, and certain terms (repeated here for convenience) given in ISO/IEC 12207 apply.

However, in the event of a conflict in terms and definitions, the terms and definitions specified in ISO 9000:2000 apply.

NOTE ISO/IEC 12207:1995 provides detailed provisions for seventeen software life cycle processes. ISO/IEC 12207:1995/Amd.1:2002 provides high-level provisions for many additional processes. This International Standard will make reference to terms defined in both.

3.1
activity
collection of related tasks

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

[ISO/IEC 12207:1995, definition 3.5]

3.3
configuration item
entity within a configuration that satisfies an end use function and that can be uniquely identified at a given reference point

[ISO/IEC 12207:1995, definition 3.6]

3.4
COTS
Commercial-Off-The-Shelf (acronym)
⟨software product⟩ available for purchase and use without the need to conduct development activities

3.5
development
software life cycle process that contains the activities of requirements analysis, design, coding, integration, testing, installation and support for acceptance of software products

3.6
life cycle model
framework containing the processes, activities, and tasks involved in the development, operation, and maintenance of a software product, spanning the life of the system from the definition of its requirements to the termination of its use

[ISO/IEC 12207:1995, definition 3.11]

NOTE The requirements of ISO 9001:2000 would apply to maintenance, only if contractually required, after acceptance of the product by the customer. However, generally the requirements do not apply to maintenance.

3.7
measure, verb
make a measurement

[ISO/IEC 14598-1:1999, definition 4.17]

3.8
measure, noun
variable to which a value is assigned as the result of measurement

[ISO/IEC 15939:2002, definition 3.14]

3.9
measurement
set of operations having the object of determining a value of a measure

[ISO/IEC 15939:2002, definition 3.17]

3.10

process

set of interrelated or interacting activities which transforms inputs into outputs

NOTE 1 Inputs to a process are generally outputs of other processes.

NOTE 2 Adapted from ISO 9000:2000, definition 3.4.1.

3.11

regression testing

testing required to determine that a change to a system component has not adversely affected functionality, reliability or performance and has not introduced additional defects

3.12

release

particular version of a configuration item that is made available for a specific purpose

EXAMPLE A test release.

[ISO/IEC 12207:1995, definition 3.22]

NOTE The term “release” used in the ISO 9001:2000 text quoted in this International Standard is used in the context of the definition provided in ISO 9000:2000, 3.6.13, which is different from the ISO/IEC 12207 definition quoted above.

3.13

replication

copying a software product from one medium to another

3.14

software item

identifiable part of a software product

3.15

software product

set of computer programs, procedures, and possibly associated documentation and data

[ISO/IEC 12207:1995, definition 3.26]

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

NOTE 2 This is different from a product in ISO 9000[2].

NOTE 3 For the purposes of this International Standard, “software” is synonymous with “software product”.

3.16

software service

performance of activities, work, or duties connected with a software product, such as its development, maintenance and operation

[ISO/IEC 12207:1995, definition 3.27]

4 Quality management system

4.1 General requirements

ISO 9001:2000, Quality management systems — Requirements

4.1 General requirements

The organization shall establish, document, implement and maintain a quality management system and continually improve its effectiveness in accordance with the requirements of this International Standard.

The organization shall

a) identify the processes needed for the quality management system and their application throughout the organization (see 1.2),

b) determine the sequence and interaction of these processes,

c) determine criteria and methods needed to ensure that both the operation and control of these processes are effective,

d) ensure the availability of resources and information necessary to support the operation and monitoring of these processes,

e) monitor, measure and analyse these processes, and

f) implement actions necessary to achieve planned results and continual improvement of these processes.

These processes shall be managed by the organization in accordance with the requirements of this International Standard.

Where an organization chooses to outsource any process that affects product conformity with requirements, the organization shall ensure control over such processes. Control of such outsourced processes shall be identified within the quality management system.

NOTE Processes needed for the quality management system referred to above should include processes for management activities, provision of resources, product realization and measurement.

Guidance is provided for items a) and b) of ISO 9001:2000, 4.1, in relation to the organizational processes as follows (see 5.4.2, and 7.4.1 for additional guidance on outsourcing).

a) ***Process identification and application***

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

b) ***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. waterfall, incremental and evolutionary, and

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

NOTE For further information, see the following:

— ISO/IEC 12207[11] and ISO/IEC 12207:1995/Amd.1:2002[12] (software life cycle processes) which define a set of software life cycle processes that may be used for reference;

— ISO/IEC TR 15271:1998[21], Annex C (guide to ISO/IEC 12207) which provides guidance on how to use processes from ISO/IEC 12207 in different life cycles.

4.2 Documentation requirements

4.2.1 General

ISO 9001:2000, Quality management systems — Requirements

4.2.1 General

The quality management system documentation shall include

a) documented statements of a quality policy and quality objectives,

b) a quality manual,

c) documented procedures required by this International Standard,

d) documents needed by the organization to ensure the effective planning, operation and control of its processes, and

e) records required by this International Standard (see 4.2.4).

NOTE 1 Where the term “documented procedure” appears within this International Standard, this means that the procedure is established, documented, implemented and maintained.

NOTE 2 The extent of the quality management system documentation can differ from one organization to another due to

a) the size of organization and type of activities,

b) the complexity of processes and their interactions, and

c) the competence of personnel.

NOTE 3 The documentation can be in any form or type of medium.

Documents for the effective planning, operation, and control of processes for software [ISO 9001:2000, 4.2.1, item d)] may cover the following:

1) descriptions of processes, such as those identified in implementing 4.1;

2) descriptions of procedural instructions and/or templates used;

3) descriptions of life cycle models used, such as waterfall, incremental and evolutionary;

4) descriptions of tools, techniques, technologies, and methods such as those identified in implementing 4.1;

5) technical topics such as standards or guidance documents for coding, design and development, and testing.

NOTE For further information on document identification as part of configuration management, see 7.5.3.

4.2.2 Quality manual

ISO 9001:2000, Quality management systems — Requirements

4.2.2 Quality manual

The organization shall establish and maintain a quality manual that includes

a) the scope of the quality management system, including details of and justification for any exclusions (see 1.2),

b) the documented procedures established for the quality management system, or reference to them, and

c) a description of the interaction between the processes of the quality management system.

4.2.3 Control of documents

ISO 9001:2000, Quality management systems — Requirements

4.2.3 Control of documents

Documents required by the quality management system shall be controlled. Records are a special type of document and shall be controlled according to the requirements given in 4.2.4.

A documented procedure shall be established to define the controls needed

a) to approve documents for adequacy prior to issue,

b) to review and update as necessary and re-approve documents,

c) to ensure that changes and the current revision status of documents are identified,

d) to ensure that relevant versions of applicable documents are available at points of use,

e) to ensure that documents remain legible and readily identifiable,

f) to ensure that documents of external origin are identified and their distribution controlled, and

g) to prevent the unintended use of obsolete documents, and to apply suitable identification to them if they are retained for any purpose.

NOTE For further information on document control as part of configuration management, see 7.5.3.

4.2.4 Control of records

ISO 9001:2000, Quality management systems — Requirements

4.2.4 Control of records

Records shall be established and maintained to provide evidence of conformity to requirements and of the effective operation of the quality management system. Records shall remain legible, readily identifiable and retrievable. A documented procedure shall be established to define the controls needed for the identification, storage, protection, retrieval, retention time and disposition of records.

4.2.4.1 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, and

f) review and inspection records, such as those for design reviews, code inspections, and walk-throughs.

4.2.4.2 Evidence of effective operation

Examples of evidence of effective operation of the quality management system may include, but are not limited to

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, and

f) software release records.

4.2.4.3 Retention and disposition

When determining the retention periods for records, consideration should be given to statutory and regulatory requirements. 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.

NOTE For further general guidance related to ISO 9001:2000, 4.2, see ISO/IEC 12207:1995[11], 6.1, and ISO/IEC 12207:1995/Amd.1:2002[12], F.2.1 (documentation process).

5 Management responsibility

5.1 Management commitment

ISO 9001:2000, Quality management systems — Requirements

5.1 Management commitment

Top management shall provide evidence of its commitment to the development and implementation of the quality management system and continually improving its effectiveness by

a) communicating to the organization the importance of meeting customer as well as statutory and regulatory requirements,

b) establishing the quality policy,

c) ensuring that quality objectives are established,

d) conducting management reviews, and

e) ensuring the availability of resources.

5.2 Customer focus

ISO 9001:2000, Quality management systems — Requirements

5.2 Customer focus

Top management shall ensure that customer requirements are determined and are met with the aim of enhancing customer satisfaction (see 7.2.1 and 8.2.1).

5.3 Quality policy

ISO 9001:2000, Quality management systems — Requirements

5.3 Quality policy

Top management shall ensure that the quality policy

a) is appropriate to the purpose of the organization,

b) includes a commitment to comply with requirements and continually improve the effectiveness of the quality management system,

c) provides a framework for establishing and reviewing quality objectives,

d) is communicated and understood within the organization, and

e) is reviewed for continuing suitability.

5.4 Planning

5.4.1 Quality objectives

ISO 9001:2000, Quality management systems — Requirements

5.4.1 Quality objectives

Top management shall ensure that quality objectives, including those needed to meet requirements for product [see 7.1 a)], are established at relevant functions and levels within the organization. The quality objectives shall be measurable and consistent with the quality policy.

NOTE Information on attributes of software processes suitable for setting objectives may be found in ISO/IEC 15504-1[22]. ISO/IEC 15504 (all parts) may be used for assessing process capabilities and for setting objectives for improving process capabilities.

5.4.2 Quality management system planning

ISO 9001:2000, Quality management systems — Requirements

5.4.2 Quality management system planning

Top management shall ensure that

a) the planning of the quality management system is carried out in order to meet the requirements given in 4.1, as well as the quality objectives, and

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

Planning may occur at organizational and project/product 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 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 and training plans;

d) defining how software engineering methods are tailored for the organization's projects within the life cycle (see 1.2 Application);

e) identifying the tools and environment for software development, operations or maintenance;

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

g) identifying any software reuse (see also 7.5.4).

The organization's management representative should consider any change to a software life cycle model which may affect the quality management system and should ensure that such changes do not compromise any quality management system controls.

Software quality planning at the project/product level is discussed in 7.1.

5.5 Responsibility, authority and communication

5.5.1 Responsibility and authority

ISO 9001:2000, Quality management systems — Requirements

5.5.1 Responsibility and authority

Top management shall ensure that responsibilities and authorities are defined and communicated within the organization.

5.5.2 Management representative

ISO 9001:2000, Quality management systems — Requirements

5.5.2 Management representative

Top management shall appoint a member of management who, irrespective of other responsibilities, shall have responsibility and authority that includes

a) ensuring that processes needed for the quality management system are established, implemented and maintained,

b) reporting to top management on the performance of the quality management system and any need for improvement, and

c) ensuring the promotion of awareness of customer requirements throughout the organization.

NOTE The responsibility of a management representative can include liaison with external parties on matters relating to the quality management system.

For a software-producing organization, there is benefit if the management representative has had experience with software development.

5.5.3 Internal communication

ISO 9001:2000, Quality management systems — Requirements

5.5.3 Internal communication

Top management shall ensure that appropriate communication processes are established within the organization and that communication takes place regarding the effectiveness of the quality management system.

5.6 Management review

5.6.1 General

ISO 9001:2000, Quality management systems — Requirements

5.6.1 General

Top management shall review the organization's quality management system, at planned intervals, to ensure its continuing suitability, adequacy and effectiveness. This review shall include assessing opportunities for improvement and the need for changes to the quality management system, including the quality policy and quality objectives.

Records from management reviews shall be maintained (see 4.2.4).

5.6.2 Review input

ISO 9001:2000, Quality management systems — Requirements

5.6.2 Review input

The input to management review shall include information on

a) results of audits,

b) customer feedback,

c) process performance and product conformity,

d) status of preventive and corrective actions,

e) follow-up actions from previous management reviews,

f) changes that could affect the quality management system, and

g) recommendations for improvement.

Guidance is provided for ISO 9001:2000, 5.6.2, item c) as follows.

One way to measure process performance is to perform software process assessments (see 8.2.3). The outcomes of software process assessments should be considered as input to management reviews.

One way to measure product conformity is to perform software product evaluation (see 8.2.4). The outcomes of software product evaluation should be considered as input to management review.

5.6.3 Review output

ISO 9001:2000, Quality management systems — Requirements

5.6.3 Review output

The output from the management review shall include any decisions and actions related to

a) improvement of the effectiveness of the quality management system and its processes,

b) improvement of product related to customer requirements, and

c) resource needs.

6 Resource management

6.1 Provision of resources

ISO 9001:2000, Quality management systems — Requirements

6.1 Provision of resources

The organization shall determine and provide the resources needed

a) to implement and maintain the quality management system and continually improve its effectiveness, and

b) to enhance customer satisfaction by meeting customer requirements.

6.2 Human resources

6.2.1 General

ISO 9001:2000, Quality management systems — Requirements

6.2.1 General

Personnel performing work affecting product quality shall be competent on the basis of appropriate education, training, skills and experience.

NOTE For further information, see ISO/IEC 12207:1995/Amd.1:2002[12], F.3.4.1 (human resource management) and F.3.4.2 (training).

6.2.2 Competence, awareness and training

ISO 9001:2000, Quality management systems — Requirements

6.2.2 Competence, awareness and training

The organization shall

a) determine the necessary competence for personnel performing work affecting product quality,

b) provide training or take other actions to satisfy these needs,

c) evaluate the effectiveness of the actions taken,

d) ensure that its personnel are aware of the relevance and importance of their activities and how they contribute to the achievement of the quality objectives, and

e) maintain appropriate records of education, training, skills and experience (see 4.2.4).

The training needs should be determined considering the requirements notation, design methods, specific programming languages, tools, techniques and computer resources to be used in the development 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.

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

The form of training may not be necessarily 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, identifying areas of improvement in personal performance (among other areas for improvement).

6.3 Infrastructure

ISO 9001:2000, Quality management systems — Requirements

6.3 Infrastructure

The organization shall determine, provide and maintain the infrastructure needed to achieve conformity to product requirements. Infrastructure includes, as applicable

a) buildings, workspace and associated utilities,

b) process equipment (both hardware and software), and

c) supporting services (such as transport or communication).

The infrastructure should include hardware, software, tools and facilities for development, operation or maintenance of software.

The infrastructure may include software tools that support the design and development process including the following:

a) tools, such as for analysis, design and development, configuration management, testing, project management, documentation, code creation or generation;

b) application development and support environments;

c) knowledge management, intranet, extranet tools;

d) network tools, including security, backup, virus protection, firewall;

e) help desk and maintenance tools;

f) access controls;

g) software libraries;

h) operations 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 and design and development 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, as appropriate, to determine whether there is a need to improve and/or upgrade them.

NOTE For further information, see the following:

— ISO/IEC 12207:1995[11], 7.2 and ISO/IEC 12207:1995/Amd.1:2002[12], F.3.2 (infrastructure process);

— ISO/IEC 14598-2[14] (acquisition) and ISO/IEC 14598-3[15] (evaluation of a software product);

— ISO/IEC 14102[13].

6.4 Work environment

ISO 9001:2000, Quality management systems — Requirements

6.4 Work environment

The organization shall determine and manage the work environment needed to achieve conformity to product requirements.

7 Product realization

7.1 Planning of product realization

ISO 9001:2000, Quality management systems — Requirements

7.1 Planning of product realization

The organization shall plan and develop the processes needed for product realization. Planning of product realization shall be consistent with the requirements of the other processes of the quality management system (see 4.1).

In planning product realization, the organization shall determine the following, as appropriate:

a) quality objectives and requirements for the product;

b) the need to establish processes, documents, and provide resources specific to the product;

c) required verification, validation, monitoring, inspection and test activities specific to the product and the criteria for product acceptance;

d) records needed to provide evidence that the realization processes and resulting product meet requirements (see 4.2.4).

The output of this planning shall be in a form suitable for the organization's method of operations.

NOTE 1 A document specifying the processes of the quality management system (including the product realization processes) and the resources to be applied to a specific product, project or contract, can be referred to as a quality plan.

NOTE 2 The organization may also apply the requirements given in 7.3 to the development of product realization processes.

7.1.1 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 9001:2000 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. For products where failure may cause injury or danger to people, or damage or corruption of property or the environment, design and development of such software should ensure definition of specific design and development requirements that specify desired immunity from, and response to, potential failure conditions.

Software development 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 7.3.1). Software quality planning at the project/product level should result in a description of how specific products are to be developed, assessed or maintained.

7.1.2 Quality planning

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 re-visited 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.

NOTE 1 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.

NOTE 2 ISO/IEC 12207[11] and ISO/IEC 12207:1995/Amd.1:2002[12] include quality planning and development planning as a single planning activity leading to the creation of project management plan(s). A mapping table is provided in Annex B, to show how the items in 7.1.1 and 7.3.1 are satisfied by the related items in ISO/IEC 12207:1995, 5.2.4.5, 5.3.1.4 and 6.3.1.3.

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

a) inclusion of, or reference to, the plans for development (see 7.3.1);

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 manual and any stated exclusions (ISO 9001:2000, 1.2);

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 8.2.4);

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 7.3.4, 7.3.5 and 7.3.6);

h) configuration management procedures to be carried out (see 7.5.3);

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 4.2.4);

m) change management, such as for resources, timescale 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 to reduce the possible occurrence of unintended omissions and errors.

NOTE 3 For further general guidance related to ISO 9001:2000, 7.1, see the following:

— ISO/IEC 12207:1995[11], 5.2.4 (planning), 5.3.1 (development process implementation), and 6.1 to 6.8, and ISO/IEC 12207:1995/Amd.1:2002[12], F.2 (supporting life cycle processes);

— ISO/IEC 9126-1:2001[5];

— ISO/IEC 14598-2[14];

— ISO/IEC TR 15846:1998[27], 6.2 (planning of configuration management);

— ISO/IEC TR 16326:1999[30], 6.2.2 (planning of project management).

7.2 Customer-related processes

7.2.1 Determination of requirements related to the product

ISO 9001:2000, Quality management systems — Requirements

7.2.1 Determination of requirements related to the product

The organization shall determine

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 specified or intended use, where known,

c) statutory and regulatory requirements related to the product, and

d) any additional requirements determined by the organization.

7.2.1.1 Customer-related requirements [ISO 9001:2000, 7.2.1, items a) and b)]

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 these circumstances.

Specific actions may include:

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

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

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

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

b) the development of the requirements in close co-operation 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;

c) the obtention of the customer's approval of the requirements;

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

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.

The requirements may need to 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 obligations. Some of these characteristics may be mission and/or safety critical.

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.

The requirements should be expressed in clear and unambiguous terms that facilitate validation during product acceptance. Requirements should be traceable throughout the development life cycle (see 7.5.3)

7.2.1.2 Additional requirements determined by the organization [ISO 9001:2000, 7.2.1, item d)]

NOTE 1 For further information on 7.2.1.1, see the following:

— ISO/IEC 12207:1995[11], 5.3.2 to 5.3.4 (development process) and ISO/IEC 12207:1995/Amd.1:2002[12], F.1.3.1 (requirements elicitation), F.1.3.2 (systems requirements analysis) and F.1.3.4 (software requirements analysis);

— ISO/IEC 9126-1:2001[5];

— ISO/IEC 15026:1998[20].

NOTE 2 For further information on 7.2.1.2, see ISO/IEC 12119:1994[10].

7.2.2 Review of requirements related to the product

ISO 9001:2000, Quality management systems — Requirements

7.2.2 Review of requirements related to the product

The organization shall review the requirements related to the product. This review shall be conducted prior to the organization's commitment to supply a product to the customer (e.g. submission of tenders, acceptance of contracts or orders, acceptance of changes to contracts or orders) and shall ensure that

a) product requirements are defined,

b) contract or order requirements differing from those previously expressed are resolved, and

c) the organization has the ability to meet the defined requirements.

Records of the results of the review and actions arising from the review shall be maintained (see 4.2.4).

Where the customer provides no documented statement of requirement, the customer requirements shall be confirmed by the organization before acceptance.

Where product requirements are changed, the organization shall ensure that relevant documents are amended and that relevant personnel are made aware of the changed 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 or advertising material.

7.2.2.1 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:

a) 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);

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

c) 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;

d) the operating system or hardware platform;

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

f) replication and distribution requirements;

g) 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;

h) management issues:

   1) risk management should be addressed (see also 7.2.2.2);

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

   3) scheduling of progress, technical reviews and outputs;

4) installation, maintenance and support requirements;

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

i) 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.

7.2.2.2 Risks

The following risks may be included when reviewing requirements related to the product:

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.

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.

7.2.2.3 Customer representative

The customer may have responsibilities under the contract. Particular issues may include the need for the customer to co-operate 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) organizing access to end-users, where appropriate.

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

NOTE For further information on requirements review see ISO/IEC 12207:1995[11], 5.2.1 (supply process — initiation), 5.2.6 (supply process — review and evaluation), 6.4.2.1 (contract verification), and 6.6 (joint review process). For further information on risk management see ISO/IEC 12207:1995/Amd.1:2002[12], F.3.1.5 (risk management).

7.2.3 Customer communication

ISO 9001:2000, Quality management systems — Requirements

7.2.3 Customer communication

The organization shall determine and implement effective arrangements for communicating with customers in relation to

a) product information,

b) enquiries, contracts or order handling, including amendments, and

c) customer feedback, including customer complaints.

7.2.3.1 General

For computer software, the method of communication may vary depending on the type of contractual 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.

7.2.3.2 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:

a) ***product information***, including

   1) development plans,

   2) conformance of outputs, such as design and development documents, to the customer's agreed requirements,

   3) demonstrations of outputs of the development processes, such as prototypes, and

   4) acceptance test results;

b) ***enquiries, contracts and amendments***, including

   1) the progress of activities concerning the eventual users of the system under development, such as deployment and training,

   2) the progress of software development work undertaken by the organization,

   3) the progress of agreed activities being undertaken by the customer,

   4) the processing of risk management issues, problems and change control items, and

   5) the methods by which the customer will be advised of current or planned future changes.

7.2.3.3 Customer communication during operations and maintenance

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

a) ***product information***, including

   1) online help, user manuals describing the product and its use,

   2) descriptions of new releases and upgrades, and

   3) product web sites;

b) ***enquiries, contracts and amendments***, including

1) progress on product or service delivery, and/or maintenance activities, and

2) processing service or product risks, issues and change requests;

c) ***customer feedback***, including

1) help desk arrangements and effectiveness,

2) progress on customer complaints processing, and

3) surveys, user groups, conferences.

NOTE For further information, see the following:

— ISO/IEC 12207:1995[11], 6.6 (joint reviews process), 5.2.5 (supply process — execution and control), 5.2.6 (supply process — review and evaluation) and 5.2.7 (supply process — delivery and completion), and ISO/IEC 12207:1995/Amd.1:2002[12], F.1.4.2 (customer support).

— ISO/IEC 14764:1999[19] (software maintenance), 6.8.1 (maintainability and the development process), 7.3.3 (guidelines for a maintenance plan) and 8.2 (problem and modification) to 8.2.3 (controls).

7.3 Design and development

7.3.1 Design and development planning

ISO 9001:2000, Quality management systems — Requirements

7.3.1 Design and development planning

The organization shall plan and control the design and development of product.

During the design and development planning, the organization shall determine

a) the design and development stages,

b) the review, verification and validation that are appropriate to each design and development stage, and

c) the responsibilities and authorities for design and development.

The organization shall manage the interfaces between different groups involved in design and development to ensure effective communication and clear assignment of responsibility.

Planning output shall be updated, as appropriate, as the design and development progresses.

7.3.1.1 Design and development planning

Design and development should be carried out in a disciplined manner to prevent or minimize the occurrence of problems. This approach reduces dependence on verification and validation as the sole methods for identifying problems. The organization should therefore ensure that the software products are developed in compliance with specified requirements and in accordance with design and development planning and/or quality planning (see 7.1 for quality planning).

NOTE 1 ISO/IEC 12207:1995[11] and ISO/IEC 12207:1995/Amd.1:2002[12] include quality planning and development planning as a single planning activity leading to the creation of project management plan(s). A mapping table is provided in Annex B, to show how the items in 7.1.1 and 7.3.1 are satisfied by the related items in ISO/IEC 12207:1995[11], 5.2.4.5, 5.3.1.4 and 6.3.1.3.

NOTE 2 Some items in the following list have been included in the quality planning list in 7.1.2. These are noted in square brackets.

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

a) 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:

   1) activities to be carried out;

   2) required inputs to each activity;

   3) required outputs from each activity;

   4) verification required for each activity output [as 7.1.2 g) – see also 7.3.5];

   5) management and supporting activities to be carried out;

   6) required team training [as 7.1.2 k)];

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

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

d) organizational and technical interfaces between different individuals or groups, such as sub-project teams, suppliers, partners, users, customer representatives, quality assurance representative (see 7.3.1.4);

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

f) the schedule identifying:

   1) the stages of the project [see also 7.1.2 j)];

   2) the work breakdown structure;

   3) the associated resources and timing;

   4) the associated dependencies;

   5) the milestones;

   6) verification and validation activities [as 7.1.2 g)];

g) the identification of:

   1) standards, rules, practices and conventions, methodology, life cycle model, statutory and regulatory requirements [as 7.1.2 d) and e)];

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

   3) facilities, hardware and software for development;

   4) configuration management practices [as 7.1.2 h)];

   5) method of controlling nonconforming software products;

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

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

   8) methods of control for virus protection;

   9) security controls;

h) the identification of related planning (including planning of the system) addressing topics such as quality (see 7.1), risk management, configuration management, supplier management, integration, testing (see 7.3.6), release management, installation, training, migration, maintenance, re-use, communication and measurement;

i) documentation control including document/record archive and distribution.

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.

NOTE 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.

7.3.1.2 Review, verification and validation

The review, verification and validation for software design and development are covered in 7.3.4 to 7.3.6. In software operations and maintenance, they may be covered in service level agreements or maintenance procedures.

7.3.1.3 Responsibilities and authorities

There is no specific guidance.

7.3.1.4 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 ensure that appropriate capacity and training are available to achieve committed service levels.

NOTE 1 For further information on design and development planning see ISO/IEC 12207:1995[11], 5.2.4 (planning) and 5.3.1 (development process implementation).

NOTE 2 For further information on software project management see ISO/IEC TR 16326:1999[30], 6.2.2 (planning).

7.3.2 Design and development inputs

ISO 9001:2000, Quality management systems — Requirements

7.3.2 Design and development inputs

Inputs relating to product requirements shall be determined and records maintained (see 4.2.4). These inputs shall include

a) functional and performance requirements,

b) applicable statutory and regulatory requirements,

c) where applicable, information derived from previous similar designs, and

d) other requirements essential for design and development.

These inputs shall be reviewed for adequacy. Requirements shall be complete, unambiguous and not in conflict with each other.

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.

For guidance on ISO 9001:2000, 7.3.2 items a), b) and d), see 7.2.1.

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, and

h) omissions of key performance measures.

NOTE For further information see ISO/IEC 9126-1:2001[5] for software quality requirements as software quality characteristics.

7.3.3 Design and development outputs

ISO 9001:2000, Quality management systems — Requirements

7.3.3 Design and development outputs

The outputs of design and development shall be provided in a form that enables verification against the design and development input and shall be approved prior to release.

Design and development outputs shall

a) meet the input requirements for design and development,

b) provide appropriate information for purchasing, production and for service provision,

c) contain or reference product acceptance criteria, and

d) specify the characteristics of the product that are essential for its safe and proper use.

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, and

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.

Tools should be validated for their specific intended use (see 7.3.6 and 7.6).

NOTE For further information, see ISO/IEC 12207:1995[11], 5.3.5 to 5.3.7 (design and testing).

7.3.4 Design and development review

ISO 9001:2000, Quality management systems — Requirements

7.3.4 Design and development review

At suitable stages, systematic reviews of design and development shall be performed in accordance with planned arrangements (see 7.3.1)

a) to evaluate the ability of the results of design and development to meet requirements, and

b) to identify any problems and propose necessary actions.

Participants in such reviews shall include representatives of functions concerned with the design and development stage(s) being reviewed. Records of the results of the reviews and any necessary actions shall be maintained (see 4.2.4).

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 8.3). 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.

NOTE 1 ISO/IEC 12207:1995[11] and ISO/IEC 12207:1995/Amd.1:2002[12] treat project management and technical reviews as separate activities. A mapping table is provided in Annex B to show how the related items in the following list are satisfied in ISO/IEC 12207:1995[11], 6.6.

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

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.

NOTE 2 For further information, see the following:

— ISO/IEC 12207:1995[11], 5.3.4.2, 5.3.5.6 and 5.3.6.7 (requirements and design evaluations) and 6.6.3 (technical reviews), and ISO/IEC 12207:1995/Amd.1:2002[12], F.2.6 (joint reviews);

— ISO/IEC TR 15271:1998[21], Annex A (quality processes and evaluation requirements).

7.3.5 Design and development verification

ISO 9001:2000, Quality management systems — Requirements

7.3.5 Design and development verification

Verification shall be performed in accordance with planned arrangements (see 7.3.1) to ensure that the design and development outputs have met the design and development input requirements. Records of the results of the verification and any necessary actions shall be maintained (see 4.2.4).

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.

NOTE For further information, see ISO/IEC 12207:1995[11], 5.3 (development) and 6.4 (verification), and ISO/IEC 12207:1995/Amd.1:2002[12], F.1.3 (development) and F.2.4 (verification).

7.3.6 Design and development validation

ISO 9001:2000, Quality management systems — Requirements

7.3.6 Design and development validation

Design and development validation shall be performed in accordance with planned arrangements (see 7.3.1) to ensure that the resulting product is capable of meeting the requirements for the specified application or intended use, where known. Wherever practicable, validation shall be completed prior to the delivery or implementation of the product. Records of the results of validation and any necessary actions shall be maintained (see 4.2.4).

7.3.6.1 Validation

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

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 may not be possible, or feasible, to validate fully the software product by measurement and monitoring. An example may 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.

7.3.6.2 Testing

Validation may often be performed by testing. 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 testing for software includes 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 and analysis of results as well as problem and change management.

NOTE For further information, see the following:

— ISO/IEC 12207:1995[11], 5.3 (development) and 6.5 (validation), and ISO/IEC 12207:1995/Amd.1:2002[12], F.1.3 (development) and F.2.5 (validation);

— ISO/IEC 14598-3[15] and ISO/IEC 14598-5[17].

7.3.7 Control of design and development changes

ISO 9001:2000, Quality management systems — Requirements

7.3.7 Control of design and development changes

Design and development changes shall be identified and records maintained. The changes shall be reviewed, verified and validated, as appropriate, and approved before implementation. The review of design and development changes shall include evaluation of the effect of the changes on constituent parts and product already delivered.

Records of the results of the review of changes and any necessary actions shall be maintained (see 4.2.4).

In the software development environment, control of design and development changes is usually addressed as part of configuration management (see 7.5.3).

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 12207:1995[11], 5.5.2, 5.5.3 (modifications), 6.1 and 6.2 (configuration management), and ISO/IEC 12207:1995/Amd.1:2002[12], F.2.1 (documentation) and F.2.2 (configuration management).

NOTE 2 For further general guidance related to ISO 9001:2000, 7.3, see the following:

— ISO/IEC 12207:1995/Amd.1:2002[12], F.1.3.4 (software requirements analysis) and F.1.3.5 (software design);

— ISO/IEC 12119:1994[10] for guidance on any procured COTS software products;

— ISO/IEC 6592:2000[1] for design and development documentation guidance;

— ISO/IEC 19761[31], ISO/IEC 20926[32] and ISO/IEC 20968[33] for guidance on estimation of size methods;

— ISO/IEC TR 14759[18] for guidance on prototype categorization and examples of use;

— ISO/IEC 15910[28] for software user documentation process.

7.4 Purchasing

7.4.1 Purchasing process

ISO 9001:2000, Quality management systems — Requirements

7.4.1 Purchasing process

The organization shall ensure that purchased product conforms to specified purchase requirements. The type and extent of control applied to the supplier and the purchased product shall be dependent upon the effect of the purchased product on subsequent product realization or the final product.

The organization shall evaluate and select suppliers based on their ability to supply product in accordance with the organization's requirements. Criteria for selection, evaluation and re-evaluation shall be established. Records of the results of evaluations and any necessary actions arising from the evaluation shall be maintained (see 4.2.4).

7.4.1.1 Purchased products

For the purposes of 7.4.1, 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 may 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 exercized 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 may 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.

7.4.1.2 Purchased product control

Where the products listed in 7.4.1.1 a) to i) 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 to ensure that such controls are in place to ensure configuration management is effective.

Care should be taken to ensure 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 7.3.1).

In some circumstances, the whole of ISO 9001:2000 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 1 For further information, see ISO/IEC 12207:1995[11], 5.1 (acquisition process), and ISO/IEC 12207:1995/Amd.1:2002[12], F.1.1 (acquisition process).

NOTE 2 For further information on assessing process capability of a supplier, see ISO/IEC 15504-3[24].

7.4.2 Purchasing information

ISO 9001:2000, Quality management systems — Requirements

7.4.2 Purchasing information

Purchasing information shall describe the product to be purchased, including where appropriate

a) requirements for approval of product, procedures, processes and equipment,

b) requirements for qualification of personnel, and

c) quality management system requirements.

The organization shall ensure the adequacy of specified purchase requirements prior to their communication to the supplier.

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), and

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

The considerations covered in 7.2.2 may also be applied to subcontracts.

NOTE For further information, see ISO/IEC 12207:1995[11], 5.1.2 [request-for-proposal (-tender) preparation], and ISO/IEC 12207:1995/Amd.1:2002[12], F.1.1.1 (acquisition preparation).

7.4.3 Verification of purchased product

ISO 9001:2000, Quality management systems — Requirements

7.4.3 Verification of purchased product

The organization shall establish and implement the inspection or other activities necessary for ensuring that purchased product meets specified purchase requirements.

Where the organization or its customer intends to perform verification at the supplier's premises, the organization shall state the intended verification arrangements and method of product release in the purchasing information.

This verification can apply to the acceptance testing of purchased software used in development. Much of such software is impossible to verify thoroughly because of its extensive functionality. The organization is entitled to assume a degree of suitability but should conduct acceptance testing and ensure the availability of adequate support.

Where part of the software development has been subcontracted, or where the purchase of associated hardware and software is involved, the organization may need to determine the methods by which verification, validation and acceptance of the subcontracted work will be achieved. Where software developed under subcontract has to be integrated with software developed by the organization itself, other considerations may include the methods and tools used in the development. Inspection by the organization itself, and possibly by the customer, may be necessary. The general considerations for testing apply (see 8.2.4).

The organization may be required to acquire and include software products, including data or services such as contract staff, supplied by a third party. The organization should verify product and services upon receipt, taking

into account the requirements of the contract. The methods to verify the product may need to be defined as part of the purchasing requirements (such as acceptance testing). The guidance on verification and validation provided in 7.3.5 and 7.3.6 should be considered. For contract staffing, consideration should be given to the education, training, skills and experience of such staff, in such topics as programming language, development tools and system management.

When purchasing or obtaining data, careful consideration should be given to the format, medium, volume, source and content of data obtained (e.g. test data obtained from a third party). Data protection regulatory requirements may be relevant in some cases (e.g. privacy).

When purchasing software products, consideration should be given to the format and medium on which it is supplied to ensure operational requirements have been met. The functional and performance requirements of the product should be tested before use to ensure that the product performs as specified. The product may also need to be validated against the needs of the final product it is required to satisfy.

Since it may not always be possible to test the product at the point of receipt, it is important to ensure that it is tested before use or incorporation into the final product. Such tests may need to be conducted at the supplier's premises. When on the organization's premises, consideration should be given to ensuring that appropriate measures are in place to segregate the product until certainty about its integrity can be determined (e.g. virus infections).

Records of qualification and training records may be used to assist with verification of contract staff.

NOTE 1 For further information, see ISO/IEC 12207:1995[11], 5.1.5, and ISO/IEC 12207:1995/Amd.1:2002[12], F.1.1.4 (acquisition — customer acceptance).

NOTE 2 For further general guidance related to ISO 9001:2000, 7.4, see the following:

— ISO/IEC 9126-1:2001[5] for guidance on quality characteristics appropriate to purchasing software product;

— ISO/IEC 14598-4[16];

— ISO/IEC 19761[31], ISO/IEC 20926[32] and ISO/IEC 20968[33] for guidance on estimation of size methods.

7.5 Production and service provision

7.5.1 Control of production and service provision

ISO 9001:2000, Quality management systems — Requirements

7.5.1 Control of production and service provision

The organization shall plan and carry out production and service provision under controlled conditions. Controlled conditions shall include, as applicable

a) the availability of information that describes the characteristics of the product,

b) the availability of work instructions, as necessary,

c) the use of suitable equipment,

d) the availability and use of monitoring and measuring devices,

e) the implementation of monitoring and measurement, and

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

7.5.1.1 Production and service provision in software

As stated in the guidance for design and development (see 7.3), 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 9001:2000, 7.5.1 is equivalent for software products to

a) release activities, e.g. build, release, and replication,

b) delivery activities, e.g. delivery and installation, and

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

7.5.1.2 Build and release

Processes should be set up for build, release and replication of the software item(s). Build and release invoke configuration management (see 7.5.3, *identification and traceability*).

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 may be incorporated or release of a complete updated copy of the software product is necessary.

7.5.1.3 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 to ensure repeatability;

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

7.5.1.4 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 7.5.5.

7.5.1.5 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.

7.5.1.6 Operations

A software-producing organization should plan and control operations, including

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

b) arrangements for ensuring continuity of support, such as disaster recovery, security and backup (see 6.3).

7.5.1.7 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 7.5.1.6);

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.

NOTE For further information, see ISO/IEC 12207:1995[11], 5.3.12 (software installation), 5.4.4 (user support), 5.5 (maintenance process), 6.6.3 (process assurance) and 6.8 (problem resolution process), and ISO/IEC 12207:1995/Amd.1:2002[12], F.1.3.11 (software installation), F.1.4.2 (customer support), F.1.5 (maintenance process) and F.2.8 (problem resolution process).

7.5.2 Validation of processes for production and service provision

ISO 9001:2000, Quality management systems — Requirements

7.5.2 Validation of processes for production and service provision

The organization shall validate any processes for production and service provision where the resulting output cannot be verified by subsequent monitoring or measurement. This includes any processes where deficiencies become apparent only after the product is in use or the service has been delivered.

Validation shall demonstrate the ability of these processes to achieve planned results.

The organization shall establish arrangements for these processes including, as applicable

a) defined criteria for review and approval of the processes,

b) approval of equipment and qualification of personnel,

c) use of specific methods and procedures,

d) requirements for records (see 4.2.4), and

e) revalidation.

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.

7.5.3 Identification and traceability

ISO 9001:2000, Quality management systems — Requirements

7.5.3 Identification and traceability

Where appropriate, the organization shall identify the product by suitable means throughout product realization.

The organization shall identify the product status with respect to monitoring and measurement requirements.

Where traceability is a requirement, the organization shall control and record the unique identification of the product (see 4.2.4).

NOTE In some industry sectors, configuration management is a means by which identification and traceability are maintained.

7.5.3.1 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 4.2.3) 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.

7.5.3.2 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 delivery.

7.5.3.3 Traceability

Throughout the product life cycle, there should be a process to trace the components of the software item or product. 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.

NOTE For further information, see the following:

— ISO 10007[9] (guidelines for configuration management);

— ISO/IEC 12207:1995[11], 6.2, and ISO/IEC 12207:1995/Amd.1:2002[12], F.2.2 (configuration management process);

— ISO/IEC TR 15846:1998[27] (software life cycle processes — configuration management), Clauses 7 to 12.

7.5.4 Customer property

ISO 9001:2000, Quality management systems — Requirements

7.5.4 Customer property

The organization shall exercise care with customer property while it is under the organization's control or being used by the organization. The organization shall identify, verify, protect and safeguard customer property provided for use or incorporation into the product. If any customer property is lost, damaged or otherwise found to be unsuitable for use, this shall be reported to the customer and records maintained (see 4.2.4).

NOTE Customer property can include intellectual property.

The organization may be required to acquire and include product and data supplied by the customer, e.g.

a) software products including commercial software products supplied by the customer,

b) development tools,

c) development environments including network services,

d) test and operational data,

e) interface or other specifications,

f) hardware, and

g) intellectual property, and confidential and proprietary information, including specifications.

In any maintenance agreement consideration should be given to addressing

— required licensing and support, including subsequent revisions to the product, and

— 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 7.5.3).

7.5.5 Preservation of product

ISO 9001:2000, Quality management systems — Requirements

7.5.5 Preservation of product

The organization shall preserve the conformity of product during internal processing and delivery to the intended destination. This preservation shall include identification, handling, packaging, storage and protection. Preservation shall also apply to the constituent parts of a product.

A software-producing organization should ensure 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 9001:2000, 7.5, see the following:

— ISO/IEC 9126-1:2001[5] for guidance on quality characteristics of software products;

— ISO/IEC TR 15846:1998[27];

— ISO/IEC 14764:1999[19];

— ISO/IEC 15910:1999[28].

7.6 Control of monitoring and measuring devices

ISO 9001:2000, Quality management systems — Requirements

7.6 Control of monitoring and measuring devices

The organization shall determine the monitoring and measurement to be undertaken and the monitoring and measuring devices needed to provide evidence of conformity of product to determined requirements (see 7.2.1).

The organization shall establish processes to ensure that monitoring and measurement can be carried out and are carried out in a manner that is consistent with the monitoring and measurement requirements.

Where necessary to ensure valid results, measuring equipment shall

a) be calibrated or verified at specified intervals, or prior to use, against measurement standards traceable to international or national measurement standards; where no such standards exist, the basis used for calibration or verification shall be recorded;

b) be adjusted or re-adjusted as necessary;

c) be identified to enable the calibration status to be determined;

d) be safeguarded from adjustments that would invalidate the measurement result;

e) be protected from damage and deterioration during handling, maintenance and storage.

In addition, the organization shall assess and record the validity of the previous measuring results when the equipment is found not to conform to requirements. The organization shall take appropriate action on the equipment and any product affected. Records of the results of calibration and verification shall be maintained (see 4.2.4).

When used in the monitoring and measurement of specified requirements, the ability of computer software to satisfy the intended application shall be confirmed. This shall be undertaken prior to initial use and reconfirmed as necessary.

NOTE See ISO 10012-1 and ISO 10012-2 for guidance.

Calibration is a technique that often has been perceived as not directly applicable to software. However, it may be applicable to hardware and tools used to test and validate the software. Consequently, items a) to e) in ISO 9001:2000, 7.6, 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 may be placed under configuration management prior to use.

Although “adjusted or re-adjusted as necessary” [ISO 9001:2000, 7.6, item b)] is not applicable to software, there may be a need to verify periodically that software used in measuring devices has not changed, due to exposure to harsh environments, such as viruses or electromagnetic fields.

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 simulation, collecting performance, resource utilization and coverage information),

c) computer hardware, and

d) instrumentation interfacing to the computer hardware.

The organization should control measuring and monitoring devices by means of a configuration management system (see 7.5.3).

8 Measurement, analysis and improvement

8.1 General

ISO 9001:2000, Quality management systems — Requirements

8.1 General

The organization shall plan and implement the monitoring, measurement, analysis and improvement processes needed

a) to demonstrate conformity of the product,

b) to ensure conformity of the quality management system, and

c) to continually improve the effectiveness of the quality management system.

This shall include determination of applicable methods, including statistical techniques, and the extent of their use.

The purpose of the software measurement process is to collect, analyse and report data relating to the products developed and processes implemented within the organizational unit, to support effective management of the processes, and to demonstrate objectively the quality of the products.

The monitoring, measurement, analysis and improvement processes should be identified as part of quality planning (see 7.1.2).

NOTE For further information, see the following:

— ISO/IEC 12207:1995[11], 7.3, and ISO/IEC 12207:1995/Amd.1:2002[12], F.3.3 (improvement process);

— ISO/IEC 15939:2002[29], Clause 5 (software measurement process);

— ISO/IEC 15504-1[22];

— ISO/IEC TR 9126-2[6] and ISO/IEC TR 9126-3[7] (product quality — internal and external metrics);

— ISO/IEC 14598-2[14] (software product evaluation — planning and management).

8.2 Monitoring and measurement

8.2.1 Customer satisfaction

ISO 9001:2000, Quality management systems — Requirements

8.2.1 Customer satisfaction

As one of the measurements of the performance of the quality management system, the organization shall monitor information relating to customer perception as to whether the organization has met customer requirements. The methods for obtaining and using this information shall be determined.

The organization's process for requesting, measuring and monitoring feedback of customer satisfaction should provide information on a continual or 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, and

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

NOTE For further information, see ISO/IEC TR 9126-4[8] (product quality — quality-in-use metrics).

8.2.2 Internal audit

ISO 9001:2000, Quality management systems — Requirements

8.2.2 Internal audit

The organization shall conduct internal audits at planned intervals to determine whether the quality management system

a) conforms to the planned arrangements (see 7.1), to the requirements of this International Standard and to the quality management system requirements established by the organization, and

b) is effectively implemented and maintained.

An audit programme shall be planned, taking into consideration the status and importance of the processes and areas to be audited, as well as the results of previous audits. The audit criteria, scope, frequency and methods shall be defined. Selection of auditors and conduct of audits shall ensure objectivity and impartiality of the audit process. Auditors shall not audit their own work.

The responsibilities and requirements for planning and conducting audits, and for reporting results and maintaining records (see 4.2.4) shall be defined in a documented procedure.

The management responsible for the area being audited shall ensure that actions are taken without undue delay to eliminate detected nonconformities and their causes. Follow-up activities shall include the verification of the actions taken and the reporting of verification results (see 8.5.2).

NOTE See ISO 10011-1, ISO 10011-2 and ISO 10011-3 for guidance.

When software organizations separate their work into projects, audit planning should define a selection of projects and assess both the compliance of their project quality planning to the organization's quality management system and the compliance of the project to the project quality planning. This selection should ensure coverage of all stages and all processes.

This may necessitate auditing various projects at different stages of their product development life cycle, or auditing a single project as it progresses through various stages. Where the intended project changes its timescale, the internal audit schedule may be reviewed, either to change the timing of the audit or to consider a different project.

NOTE For further information, see ISO/IEC 12207:1995[11], 6.3 (quality assurance process) and 6.7 (audit process), and ISO/IEC 12207:1995/Amd.1:2002[12], F.2.3 (quality assurance process) and F.2.7 (audit process).

8.2.3 Monitoring and measurement of processes

ISO 9001:2000, Quality management systems — Requirements

8.2.3 Monitoring and measurement of processes

The organization shall apply suitable methods for monitoring and, where applicable, measurement of the quality management system processes. These methods shall demonstrate the ability of the processes to achieve planned results. When planned results are not achieved, correction and corrective action shall be taken, as appropriate, to ensure conformity of the product.

Organizations normally measure some aspects of their processes in order to monitor, manage and assess them. 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, and

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

NOTE 1 For further information, see ISO/IEC 12207:1995[11], 7.3.2 (process assessment) and 7.3.3 (process improvement), and ISO/IEC 12207:1995/Amd.1:2002[12], F.3.3.2 (process assessment).

NOTE 2 For guidance on conducting software process assessment, see ISO/IEC 15504-1[22], and that on performing an assessment, see ISO/IEC 15504-2[23].

See also ISO/IEC 15939:2002[29], Clause 5 (software measurement process).

8.2.4 Monitoring and measurement of product

ISO 9001:2000, Quality management systems — Requirements

8.2.4 Monitoring and measurement of product

The organization shall monitor and measure the characteristics of the product to verify that product requirements have been met. This shall be carried out at appropriate stages of the product realization process in accordance with the planned arrangements (see 7.1).

Evidence of conformity with the acceptance criteria shall be maintained. Records shall indicate the person(s) authorizing release of product (see 4.2.4).

Product release and service delivery shall not proceed until the planned arrangements (see 7.1) have been satisfactorily completed, unless otherwise approved by a relevant authority and, where applicable, by the customer.

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, and

f) reliability.

NOTE For further information, see the following:

— ISO/IEC 12207:1995[11], 5.3, and ISO/IEC 12207:1995/Amd.1:2002[12], F.1.3 (development process), which contains provisions for evaluation of software products during development and when completed;

— ISO/IEC 9126-1:2001[5];

— ISO/IEC 14598-3[15] and ISO/IEC 14598-5[17] (software product evaluation — process for developers and evaluators).

8.3 Control of nonconforming product

ISO 9001:2000, Quality management systems — Requirements

8.3 Control of nonconforming product

The organization shall ensure that product which does not conform to product requirements is identified and controlled to prevent its unintended use or delivery. The controls and related responsibilities and authorities for dealing with nonconforming product shall be defined in a documented procedure.

The organization shall deal with nonconforming product by one or more of the following ways:

a) by taking action to eliminate the detected nonconformity;

b) by authorizing its use, release or acceptance under concession by a relevant authority and, where applicable, by the customer;

c) by taking action to preclude its original intended use or application.

Records of the nature of nonconformities and any subsequent actions taken, including concessions obtained, shall be maintained (see 4.2.4).

When nonconforming product is corrected it shall be subject to re-verification to demonstrate conformity to the requirements.

When nonconforming product is detected after delivery or use has started, the organization shall take action appropriate to the effects, or potential effects, of the nonconformity.

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, and

d) rejection.

NOTE For further information, see the following:

— ISO/IEC 12207:1995[11], 6.2 (configuration management process) and 6.8 (problem resolution process), and ISO/IEC 12207:1995/Amd.1:2002[12], F.2.2 (configuration management process) and F.2.8 (problem resolution process);

— ISO/IEC 12119:1994[10];

— ISO/IEC TR 15846:1998[27].

8.4 Analysis of data

ISO 9001:2000, Quality management systems — Requirements

8.4 Analysis of data

The organization shall determine, collect and analyse appropriate data to demonstrate the suitability and effectiveness of the quality management system and to evaluate where continual improvement of the effectiveness of the quality management system can be made. This shall include data generated as a result of monitoring and measurement and from other relevant sources.

The analysis of data shall provide information relating to

a) customer satisfaction (see 8.2.1),

b) conformity to product requirements (see 7.2.1),

c) characteristics and trends of processes and products including opportunities for preventive action, and

d) suppliers.

Examples of “analysis of data” 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 15939:2002[29], 5.4 (software measurement process — evaluate results);

— ISO/IEC 19761[31], ISO/IEC 20926[32] and ISO/IEC 20968[33].

8.5 Improvement

8.5.1 Continual improvement

ISO 9001:2000, Quality management systems — Requirements

8.5.1 Continual improvement

The organization shall continually improve the effectiveness of the quality management system through the use of the quality policy, quality objectives, audit results, analysis of data, corrective and preventive actions and management review.

A strategic approach to process improvement may be achieved by establishing an improvement process. This can be applied to any or all of the software life cycle processes and involves process establishment, process assessment and process improvement.

NOTE For further information, see the following:

— ISO/IEC 12207:1995[11], 7.3, and ISO/IEC 12207:1995/Amd.1:2002[12], F.3.3 (improvement process);

— ISO/IEC 15504 (all parts) (software process assessment).

8.5.2 Corrective action

ISO 9001:2000, Quality management systems — Requirements

8.5.2 Corrective action

The organization shall take action to eliminate the cause of nonconformities in order to prevent recurrence. Corrective actions shall be appropriate to the effects of the nonconformities encountered.

A documented procedure shall be established to define requirements for

a) reviewing nonconformities (including customer complaints),

b) determining the causes of nonconformities,

c) evaluating the need for action to ensure that nonconformities do not recur,

d) determining and implementing action needed,

e) records of the results of action taken (see 4.2.4), and

f) reviewing corrective action taken.

Where corrective action directly affects the software products, configuration management may be invoked to manage the changes. Management should review corrective actions that involve changes to the software life cycle processes. An organization's procedures for corrective action should take into account the requirement to prevent recurrence.

NOTE For further information, see ISO/IEC 12207:1995[11], 6.8, and ISO/IEC 12207:1995/Amd.1:2002[12], F.2.8 (problem resolution process).

8.5.3 Preventive action

ISO 9001:2000, Quality management systems — Requirements

8.5.3 Preventive action

The organization shall determine action to eliminate the causes of potential nonconformities in order to prevent their occurrence. Preventive actions shall be appropriate to the effects of the potential problems.

A documented procedure shall be established to define requirements for

a) determining potential nonconformities and their causes,

b) evaluating the need for action to prevent occurrence of nonconformities,

c) determining and implementing action needed,

d) records of results of action taken (see 4.2.4), and

e) reviewing preventive action taken.

Process assessment may be useful in the gathering of data to anticipate problems (see 8.2.3).

NOTE For further general guidance related to ISO 9001:2000, 8.5, see the following:

— ISO/IEC 12207:1995[11], 7.3.2 (process assessment), and ISO/IEC 12207:1995/Amd.1:2002[12], F.3.3.2 (process assessment);

— ISO/IEC 15504-2[23].