INTERNATIONAL STANDARD

ISO/IEC 16085

IEEE Std 16085-2006

Second edition
2006-12-15

Systems and software engineering — Life cycle processes — Risk management

Ingénierie des systèmes et du logiciel — Processus du cycle de vie — Gestion des risques

Reference number
ISO/IEC 16085:2006(E)
IEEE
Std 16085-2006

ISO/IEC 16085:2006(E)
IEEE Std 16085:2006
(Revision of
IEEE Std 1540-2001)

Systems and software engineering — Life cycle processes — Risk management

Sponsor

Software & Systems Engineering Standards Committee
of the
IEEE Computer Society

ISO
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

Abstract: A process for the management of risk in the life cycle is defined. It can be added to the existing set of software life cycle processes defined by the ISO/IEC 12207 or ISO/IEC 15288 series of standards, or it can be used independently.

Keywords: integrity, risk, risk acceptance, risk analysis, risk management, risk treatment

Print: ISBN 0-7381-4968-3 SH95519
PDF: ISBN 0-7381-4969-1 SS95519

International Standard ISO/IEC 16085:2006(E)

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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

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

Attention is 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 16085 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 7, *Software and system engineering*.

International Organization for Standardization/International Electrotechnical Commission
Case postale 56 • CH-1211 Genève 20 • Switzerland

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. The IEEE develops its standards through a consensus development process, approved by the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and serve without compensation. While the IEEE administers the process and establishes rules to promote fairness in the consensus development process, the IEEE does not independently evaluate, test, or verify the accuracy of any of the information contained in its standards.

Use of an IEEE Standard is wholly voluntary. The IEEE disclaims liability for any personal injury, property or other damage, of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, or reliance upon this, or any other IEEE Standard document.

The IEEE does not warrant or represent the accuracy or content of the material contained herein, and expressly disclaims any express or implied warranty, including any implied warranty of merchantability or fitness for a specific purpose, or that the use of the material contained herein is free from patent infringement. IEEE Standards documents are supplied "**AS IS**."

The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE Standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard. Every IEEE Standard is subjected to review at least every five years for revision or reaffirmation. When a document is more than five years old and has not been reaffirmed, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE Standard.

In publishing and making this document available, the IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity. Nor is the IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing this, and any other IEEE Standards document, should rely upon the advice of a competent professional in determining the exercise of reasonable care in any given circumstances.

Interpretations: Occasionally questions may arise regarding the meaning of portions of standards as they relate to specific applications. When the need for interpretations is brought to the attention of IEEE, the Institute will initiate action to prepare appropriate responses. Since IEEE Standards represent a consensus of concerned interests, it is important to ensure that any interpretation has also received the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to interpretation requests except in those cases where the matter has previously received formal consideration. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position, explanation, or interpretation of the IEEE.

Comments for revision of IEEE Standards are welcome from any interested party, regardless of membership affiliation with IEEE. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Comments on standards and requests for interpretations should be addressed to:

Secretary, IEEE-SA Standards Board
445 Hoes Lane
Piscataway, NJ 08854
USA

NOTE—Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. The IEEE shall not be responsible for identifying patents for which a license may be required by an IEEE standard or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

IEEE Introduction

This introduction is not part of ISO/IEC/IEEE 16085:2006, Systems and software engineering — Life cycle processes — Risk management.

Risk management is a key discipline for making effective decisions and communicating the results within organizations. The purpose of risk management is to identify potential managerial and technical problems before they occur so that actions can be taken that reduce or eliminate the probability and/or impact of these problems should they occur. It is a critical tool for continuously determining the feasibility of project plans, for improving the search for and identification of potential problems that can affect life cycle activities and the quality and performance of products, and for improving the active management of projects.

This standard can be applied equally to systems and software. Annex D is specific to software and the ISO/IEC 12207 series of life cycle standards, in order to summarize where risk management is mentioned, in lieu of a specific risk management process.

Notice to users

Errata

Errata, if any, for this and all other standards can be accessed at the following URL: http://standards.ieee.org/reading/ieee/updates/errata/index.html. Users are encouraged to check this URL for errata periodically.

Interpretations

Current interpretations can be accessed at the following URL: http://standards.ieee.org/reading/ieee/interp/index.html.

Patents

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. The IEEE shall not be responsible for identifying patents or patent applications for which a license may be required to implement an IEEE standard or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

Participants

The following individuals participated in the development of this standard.

Robert N. Charette, *Chair*
Paul R. Croll
Cheryl Jones
Garry J. Roedler
James W. Moore

When the IEEE-SA Standards Board approved this standard, it had the following membership:

Steve M. Mills, *Chair*
Richard H. Hulett, *Vice Chair*
Don Wright, *Past Chair*
Judith Gorman, *Secretary*

Mark D. Bowman
Dennis B. Brophy
Joseph Bruder
Richard Cox
Bob Davis
Julian Forster*
Joanna N. Guenin
Mark S. Halpin
Raymond Hapeman

William B. Hopf
Lowell G. Johnson
Herman Koch
Joseph L. Koepfinger*
David J. Law
Daleep C. Mohla
Paul Nikolich

T. W. Olsen
Glenn Parsons
Ronald C. Petersen
Gary S. Robinson
Frank Stone
Malcolm V. Thaden
Richard L. Townsend
Joe D. Watson
Howard L. Wolfman

*Member Emeritus

Also included are the following nonvoting IEEE-SA Standards Board liaisons:

Satish K. Aggarwal, *NRC Representative*
Richard DeBlasio, *DOE Representative*
Alan H. Cookson, *NIST Representative*

Michael D. Fisher
IEEE Standards Project Editor

Contents

Systems and software engineering — Life cycle processes — Risk management

1. Overview

This standard prescribes a continuous process for risk management. Clause 1 provides an overview and describes the purpose, scope, and field of application, as well as prescribing the conformance criteria. Clause 2 lists the normative references; informative references are provided in Annex E. Clause 3 provides definitions. Clause 4 describes how risk management is applied to the life cycle. Clause 5 prescribes the requirements for a risk management process.

There are several informative annexes. Annex A, Annex B, and Annex C recommend content of three documents: Risk Management Plan, Risk Action Request, and Risk Treatment Plan. Annex D summarizes where risk management is mentioned in the ISO/IEC 12207 series of software life cycle process standards. An equivalent annex is not included for ISO/IEC 15288, the system life cycle process standard, since it includes a risk management process. Annex E, as previously mentioned, is an annotated bibliography of standards and other documents related to the material covered in this standard.

1.1 Scope

This standard describes a process for the management of risk during systems or software acquisition, supply, development, operations, and maintenance.

1.2 Purpose

The purpose of this standard is to provide suppliers, acquirers, developers, and managers with a single set of process requirements suitable for the management of a broad variety of risks. This standard does not provide detailed risk management techniques, but instead focuses on defining a process for risk management in which any of several techniques may be applied.

1.3 Field of application

This standard defines a process for the management of risk throughout the life cycle. This standard is suitable for adoption by an organization for application to all appropriate projects. This standard is useful for managing the risks associated with organizations dealing with system or software issues.

This standard may be applied in conjunction with the ISO/IEC 12207:1995 series of standards, ISO/IEC 15288, or applied independently.

1.3.1 Application with ISO/IEC 12207:1995 series

ISO/IEC 12207:1995 is currently the ISO's "umbrella" standard describing standard processes for the acquisition, supply, development, operations, and maintenance of software. The standard recognizes that actively managing risk is a key success factor in the management of a software project. ISO/IEC 12207:1995 mentions risk and risk management in several places, but did not provide a process for risk management (see Annex D). This risk management standard provides that process in a manner aligned with the risk management process definition provided by subsequent amendments to ISO/IEC 12207. This standard may be used for managing organizational-level risk or project-level risk, in any domain or life cycle phase, to support the perspectives of managers, participants, and other stakeholders.

In the life cycle process framework provided by ISO/IEC 12207:1995, risk management is an "organizational life cycle process." The activities and tasks in an organizational process are the responsibility of the organization using that process. The organization therefore ensures that this process has been established.

When used with ISO/IEC 12207:1995, this standard assumes that the other management and technical processes of ISO/IEC 12207 perform the treatment of risk. Appropriate relationships to those processes are described.

1.3.2 Application with ISO/IEC 15288:2002 series

ISO/IEC 15288:2002 includes a risk management process and mentions risk and risk management in several places. This standard may be used for managing organizational-level risk, enterprise-level risk, or project-level risk, in any domain or life cycle stage, to support the perspectives of managers, participants, and other stakeholders.

16085 is broadly compatible with the risk management process documented in ISO/IEC 15288:2002 and provides additional process information to aid planning and execution of risk management. When used with ISO/IEC 15288:2002, this standard assumes that the other management and technical processes of ISO/IEC 15288 perform the treatment of risk. The scope, purpose, field of application, and conformance requirements in Clause 1 can be interpreted for system life cycle application. The definitions (Clause 3), process information (Clause 5) and outlines for the risk management plan (Annex A), risk action request (Annex B), and risk treatment plan (Annex C) can be directly applied to the system life cycle.

1.3.3 Application independent of ISO/IEC series

This standard may be used independently of any particular systems or software life cycle process standard. When used in this manner, the standard applies additional provisions for the treatment of risk.

1.4 Conformance

An organization or project may claim conformance to this standard by implementing a process, demonstrating through plans and performance all of the requirements (specified as mandatory by the word shall) in the activities and tasks described in Clause 5.

Note that in those instances where this standard is applied independently of ISO/IEC 12207:1995 or ISO/IEC 15288:2002, an additional set of requirements for risk treatment is provided in 5.1.4.2.

1.5 Disclaimer

This standard establishes minimum requirements for a risk management process, activities and tasks. Implementing these requirements or the preparation of risk management plans or risk action requests according to this standard does not ensure an absence of risks. Conformance with this standard does not absolve any party from any social, moral, financial, or legal obligation.

2. Normative references

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

ISO/IEC 12207:1995, Information Technology — Software Life Cycle Processes.[1]

ISO/IEC 12207:1995/AMD.1:2002, Information Technology — Software Life Cycle Processes — Amendment 1.

ISO/IEC 12207:1995/AMD.2:2003, Information Technology — Software Life Cycle Processes — Amendment 2.

ISO/IEC 15026:1998, Information Technology — System and Software Integrity Levels.

ISO/IEC 15288: 2002, Systems Engineering — System life cycle processes

NOTES

1—ISO/IEC 12207:1995 is not needed if this standard is being applied independently of ISO/IEC 12207.

2—IEEE/EIA 12207.0-1996 may be used as a replacement for ISO/IEC 12207:1995.[2]

3—ISO/IEC 15288:2002 is not needed if this standard is being applied independently of ISO/IEC 15288.

3. Definitions

For the purposes of this document, the following terms and definitions apply. *The Authoritative Dictionary of IEEE Standard Terms* [B19] should be referenced for terms not defined in this clause.

3.1 consequence: An outcome of an event.

NOTES

1—There can be more than one consequence from one event.

2—Consequences can range from positive to negative. However, consequences are always negative for safety aspects.

3—Consequences can be expressed qualitatively or quantitatively.

[ISO Guide 73:2002, definition 3.1.2]

3.2 event: The occurrence of a particular set of circumstances.

[1]ISO/IEC publications are available from the ISO Central Secretariat, Case Postale 56, 1 rue de Varembé, CH-1211, Genève 20, Switzerland/Suisse (http://www.iso.ch/). ISO/IEC publications are also available in the United States from Global Engineering Documents, 15 Inverness Way East, Englewood, Colorado 80112, USA (http://global.ihs.com/). Electronic copies are available in the United States from the American National Standards Institute, 11 West 42nd Street, 13th Floor, New York, NY 10036, USA (http://www.ansi.org/).

[2] IEEE publications are available from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331, USA (http://standards.ieee.org/).

NOTES

1—The event can be certain or uncertain.

2—The event can be a single occurrence or a series of occurrences.

3—The probability associated with the event can be estimated for a given period of time.

[ISO Guide 73:2002, definition 3.1.4]

3.3 probability: The extent to which an event (3.1.4) is likely to occur

NOTES

1—ISO 3534-1:1993, definition 1.1, gives the mathematical definition of probability as "a real number in the scale 0 to 1 attached to a random event. It can be related to a long-run relative frequency of occurrence or to a degree of belief that an event will occur. For a high degree of belief, the probability is near 1."

2—Frequency rather than probability may be used in describing risk.

3—Degrees of belief about probability can be chosen as classes or ranks, such as

— rare/unlikely/moderate/likely/almost certain, or
— incredible/improbable/remote/occasional/probable/frequent.

[ISO Guide 73:2002, definition 3.1.3]

3.4 project risk profile: A project's current and historical risk-related information; a compendium or aggregate of all of the individual risk profiles in a project.

NOTE—The project risk profile information includes the risk management context, along with the chronological record of risks and their individual risk profiles, priority ordering, risk-related measures, treatment status, contingency plans, and risk action requests. A project risk profile consists of a collection of the risk profiles of all the individual risks, which in turn includes the current and historical risk states. See risk profile and risk state.

3.5 risk: The combination of the probability of an event and its consequence.

NOTES

1—The term "risk" is generally used only when there is at least the possibility of negative consequences.

2—In some situations, risk arises from the possibility of deviation from the expected outcome or event.

3—See ISO/IEC Guide 51 for issues related to safety.

[ISO Guide 73:2002, definition 3.1.1]

3.6 risk acceptance: The decision to accept a risk.

NOTES

1—The verb "to accept" is chosen to convey the idea that acceptance has its basic dictionary meaning.

2—Risk acceptance depends on risk criteria.

[ISO Guide 73:2002, definition 3.4.10]

3.7 risk action request: The recommended treatment alternatives and supporting information for one or more risks determined to be above a risk threshold.

3.8 risk category: A class or type of risk (e.g., technical, legal, organizational, safety, economic, engineering, cost, schedule).

NOTE—A risk category is a characterization of a source of risk. See source.

3.9 risk criteria: The terms of reference by which the significance of risk is assessed.

NOTE—Risk criteria can include associated cost and benefits, legal and statutory requirements, socio-economic and environmental aspects, the concerns of stakeholders, priorities and other inputs to the assessment.

[ISO Guide 73:2002, definition 3.1.6]

3.10 risk exposure: The potential loss presented to an individual, project, or organization by a risk; a function of the probability that the risk will occur and the magnitude of the consequences of its occurrence.

NOTE—Risk exposure is commonly defined as the product of a probability and the magnitude of a consequence, i.e., an expected value or expected exposure. This risk management standard takes a broader view that includes qualitative expressions of risk exposure.

3.11 risk management plan: A description of how the elements and resources of the risk management process will be implemented within an organization or project.

3.12 risk management process: A continuous process for systematically identifying, analyzing, treating, and monitoring risk throughout the life cycle of a product or service.

3.13 risk management system: set of elements of an organization's management system concerned with managing risk.

NOTES

1—Management system elements can include strategic planning, decision making, and other processes for dealing with risk.

2—The culture of an organization is reflected in its risk management system.

[ISO Guide 73:2002, definition 3.1.8]

3.14 risk profile: A chronological record of a risk's current and historical risk state information.

3.15 risk state: The current project risk information relating to an individual risk.

NOTE—The information concerning an individual risk may include the current description, causes, probability, consequences, estimation scales, confidence of the estimates, treatment, threshold, and an estimate of when the risk will reach its threshold.

3.16 risk threshold: A condition that triggers some stakeholder action.

NOTE—Different risk thresholds may be defined for each risk, risk category or combination of risks based upon differing risk criteria.

3.17 risk treatment: The process of selection and implementation of measures to modify risk.

NOTE

1—The term “risk treatment” is sometimes used for the measures themselves.

2—Risk treatment measures can include avoiding, optimizing, transferring or retaining risk.

[ISO Guide 73:2002, definition 3.4.1]

3.18 source: An item or activity having a potential for a consequence.

NOTE—In the context of safety, source is a hazard (refer to ISO/IEC Guide 51:1999).

[ISO Guide 73:2002, definition 3.1.5]

3.19 stakeholder: Any individual, group or organization that can affect, be affected by, or perceive itself to be affected by, a risk.

NOTES

1—The decision-maker is also a stakeholder.

2—The term “stakeholder” includes but has a broader meaning than interested party (which is defined in ISO 9000:2000).

[ISO Guide 73:2002, definition 3.2.1]

4. Application of this standard

To facilitate use with ISO/IEC 12207:1995 and ISO/IEC 15288, this standard is written using many of the same conventions for process descriptions. The risk management life cycle process discussed herein is divided into a set of activities; and the requirements of each activity are specified in a set of tasks. Second-level subclauses (x.1) denote processes, third-level subclauses (x.x.1) denote activities, and fourth-level subclauses (x.x.x.1) denote tasks.

This risk management standard supports the acquisition, supply, development, operation, and maintenance of products and services. Application of this standard does not require any particular life cycle process model.

Project-level risk management is most effective when used along with risk management processes operating at the organizational level. The processes, activities, and tasks of this risk management standard should be integrated with other organization risk management practices and systems. If the organizational risk management processes do not exist, this standard may be useful as a guide for building them.

Further, while application of the standard focuses on system and software risks, the process should be integrated and coordinated with an organization's problem management approaches, e.g., in the event that a contingency plan must be implemented. The risk treatment activity should be managed in the same manner as other project management activities.

Risk management is most effective when it is integrated with the measurement process. ISO/IEC 15939, defines a measurement process applicable to all engineering and management disciplines. The measurement process defined in ISO/IEC 15939 works in conjunction with the risk management activities and tasks defined in 16085 to help characterize and quantify risks.

5. Risk management in the life cycle

The purpose of the risk management is to identify, analyze, treat and monitor risks continuously. As a result of successful implementation of risk management

a) The scope of risk management to be performed is determined.

b) Appropriate risk management strategies are defined and implemented.

c) Risks are identified as they develop and during the conduct of a project.

d) Risks are analyzed, and the priority in which to apply resources to treatment of these risks are determined.

e) Risk measures are defined, applied, and assessed to determine changes in the status of risk and the progress of the treatment activities.

f) Appropriate treatment is taken to correct or avoid the impact of risk based on its priority, probability, and consequence.

5.1 Risk management process

The risk management process is a continuous process for systematically addressing risk throughout the life cycle of a product or service.

This process consists of the following activities:

a) Plan and implement risk management
b) Manage the project risk profile
c) Perform risk analysis
d) Perform risk monitoring
e) Perform risk treatment
f) Evaluate the risk management process

The risk management process is illustrated in Figure 1. Note that the performance of risk treatment is assumed to be part of general technical and managerial processes.

The numbers in the discussion below refer to the appropriate box in Figure 1.

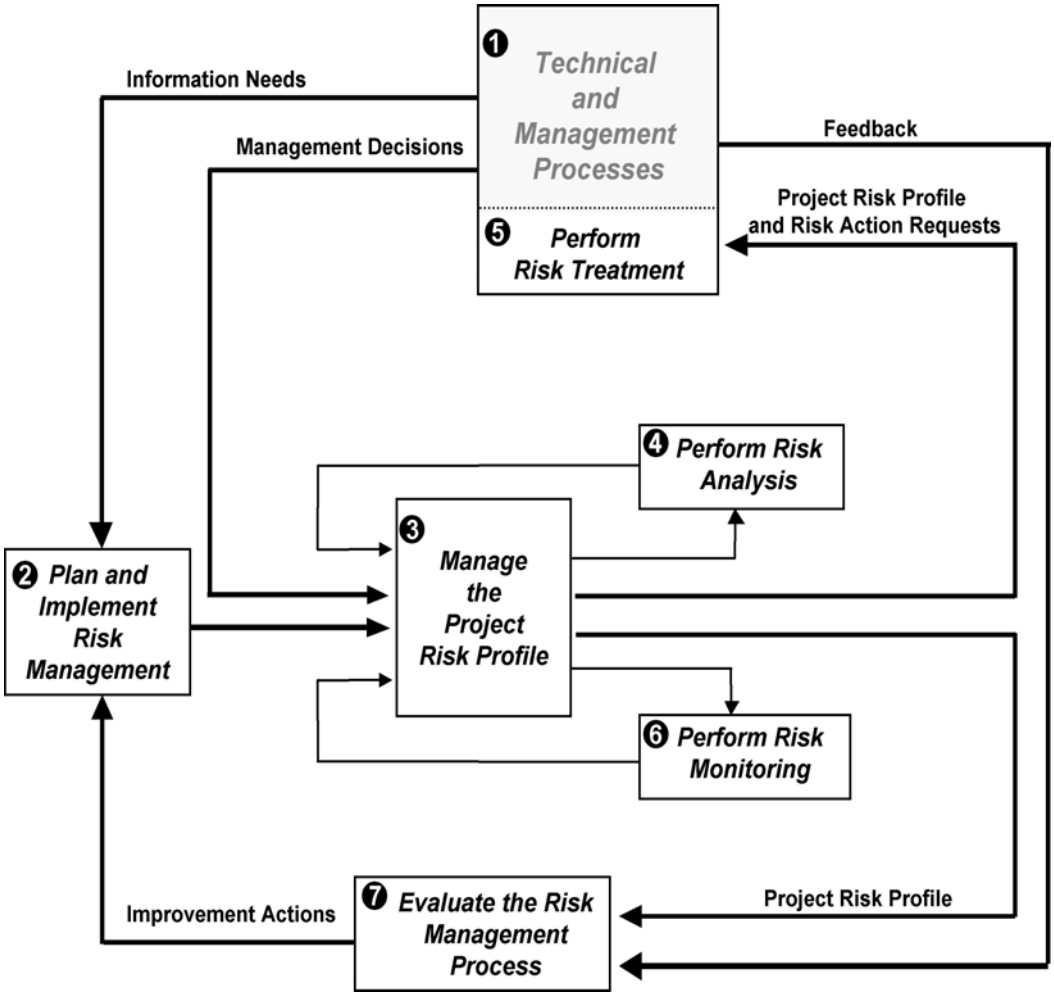

Figure 1—Risk management process model (informative)

Managerial and technical processes involving the stakeholders define the information requirements (i.e., the information the stakeholders require to make informed decisions involving risks) the risk management process must support❶. These information requirements are passed to both the "plan and implement risk management" and the "manage the project risk profile" activities. In the "plan and implement risk management" activity❷, the policies regarding the general guidelines under which risk management will be conducted, the procedures to be used, the specific techniques to be applied, and other matters relevant to risk planning are defined.

In the "manage the project risk profile" activity❸, the current and historical risk management context and risk state information are captured. The project risk profile includes the sum total of all the individual risk profiles (i.e., the current and historical risk information concerning an individual risk), which, in turn, includes all the risk states.

The project risk profile information is continually updated and maintained through the "perform risk analysis" activity❹, which identifies the risks, determines their probability and consequences, determines their risk exposures, and prepares risk action requests recommending treatment for risks determined to be above their risk threshold(s).

Treatment recommendations, along with the status of other risks and their treatment status, are sent to management for review❺. Management decides what risk treatment is implemented for any risk found to be unacceptable. Risk treatment plans are created for risks that require treatment. These plans are coordinated with other management plans and other ongoing activities.

All risks are continually monitored until they no longer need to be tracked, e.g., they are retired, during the "perform risk monitoring" activity❻. In addition, new risks and risk sources are sought out.

Periodic evaluation of the risk management process is required to ensure its effectiveness. During the "evaluate the risk management process" activity❼, information, including user and other feedback, is captured for improving the process or for improving the organization's or project's ability to manage risk. Improvements defined as a result of evaluation are implemented in the "plan and implement risk management" activity❷.

The risk management process is applied continuously throughout the product life cycle. However, activities and tasks of the risk management process interact with the individual risks in an iterative manner once the risk management process begins. For example, in the "perform risk analysis" activity❹, a risk may be re-estimated several times during the performance of risk evaluation due to an increase in knowledge about the risk gained during the evaluation task itself. The risk management process is not a "waterfall" process.

5.1.1 Plan and implement risk management

The purpose of the "plan and implement risk management" activity is to establish a risk management process. Where an organizational risk management process exists, the risk management process should be aligned to it. This activity shall establish who is to perform risk management, define the specific risk management process to be used, assign the resources required to implement the process, and define how risks and their treatment are to be communicated and coordinated among stakeholders.

This activity should be performed at the beginning of the project and repeated when information needs change. Information created during this activity shall be documented in a risk management plan such as that found in Annex A.

NOTE—IEEE Std 1058-1998 [B24] requires the documentation of a risk management plan in the software project management plan. AS/NZ Std 4360 [B2] provides a general framework for establishing and implementing a risk management system within an organization.

This activity consists of the tasks listed in 5.1.1.1 through 5.1.1.5.

5.1.1.1 Establish risk management policies

Risk management policies describing the guidelines under which risk management is to be performed shall be explicitly defined. The policies shall support gathering risk related information needed by the stakeholders. The policies should discuss how

a) Risk management is to be implemented, administered, and supported by management and staff
b) Ongoing commitment to risk management by stakeholders is to be obtained and maintained
c) The risk management process is to be coordinated among stakeholders
d) Orientation and training of personnel in the risk management process is to be conducted and what experience is required of personnel
e) Risk information, e.g., the project risk profile, is to be communicated and reviewed by stakeholders and how often
f) Resources are to be made available to treat risks

The policies should align with existing organizational risk management policies whenever feasible. A documented organizational risk management policy that defines the above may be referenced and only the specifics for a project need to be documented.

5.1.1.2 Establish the risk management process.

A description of the risk management process to be implemented shall be documented and promulgated. The description of the procedures that implement the risk management process should include

a) The frequency at which risks are to be reanalyzed and monitored
b) The type of risk analysis required (quantitative and/or qualitative)
c) The scales to be used to express risk probability and consequences and their descriptive and measurement uncertainty
d) The types of risk thresholds to be used
e) The types of measures used to track and monitor the state of the risks
f) How risks are to be prioritized for treatment
g) Which stakeholder(s) perspectives the risk management process supports
h) The risk sources and risk categories to be considered

During this task, risk management process, specific procedures, and techniques should be selected to match the project situation.

NOTE—IEC Guide 60300-3-9:1995 [B7] provides guidelines for the selection and utilization of commonly used risk analysis techniques. IEC Std 61508-7:2000 [B16] provides useful material related to measures and techniques related to safety.

The risk management process should align with existing organizational risk management processes whenever feasible. A documented organizational risk management process that defines the previous list may be referenced and only the specifics for a project need to be documented.

5.1.1.3 Establish responsibility

The parties responsible for performing risk management and their roles and responsibilities shall be explicitly identified. Parties shall be assigned responsibility for the risk management process within the organizational unit.

5.1.1.4 Assign resources

The responsible parties shall be provided with adequate resources to perform the risk management process.

5.1.1.5 Establish the risk management process evaluation

A description of the process for evaluating and improving the risk management process, along with how information will be captured for lessons learned, shall be provided. Any relevant lessons from prior use of the process should be incorporated into this implementation of the process.

5.1.2 Manage the project risk profile

The purpose of the "manage the project risk profile" activity is to create a consistent current and historical view of the risks present along with their treatment, so that the risks can be communicated fully and succinctly to relevant stakeholders. It includes the risk management context, the current risk state, and risk history.

The project risk profile shall be maintained throughout the life cycle.

This activity consists of the tasks listed in 5.1.2.1 through 5.1.2.4.

5.1.2.1 Define the risk management context

The context of the risk management process shall be defined and documented.

The definition of the risk management context shall include a description of one or more stakeholders' perspectives that the risk action request supports and one or more risk categories to be managed. Security, safety, or other categories of risk that are perceived to be of special importance may be addressed separately.

NOTE—IEEE Std 1228-1994 [B26], ISO Std 14791[B33], IEC Std 60300 series [B5]-[B7] and IEC Std 61508 series [B10]-[B16] may be used in conjunction with this standard to address risks related to safety.

The risk management context definition shall also include a description (perhaps by reference) of the technical and managerial

a) Objectives (e.g., what are the key technical, political or economic performance criteria that must be met for the project to be considered successful?)
b) Assumptions (e.g., what is considered outside the control of the project?)
c) Constraints (e.g., what limits have been placed on the project?)

Any other relevant information that may influence the analysis or treatment of risk (e.g., is the project able to openly communicate risk-related information, or is there a reason this is prohibited?) should also be included.

5.1.2.2 Establish risk thresholds

Risk thresholds, defining the conditions under which a level of risk may be accepted, shall be documented.

Risk thresholds are the maximum levels of measured risk criteria that are acceptable without explicit review by the stakeholders. Risk thresholds shall be defined for individual risks or combinations of risks. A risk threshold for the project as a whole should be defined. Risk thresholds should be derived for system and software from the system integrity levels in accordance with the provisions of ISO/IEC 15026:1998. Risk thresholds may also be defined for cost, schedule, technical, and other relevant consequences or exposure values.

Measures indicating when a risk is likely to exceed its risk threshold should be defined and documented in its risk state.

NOTE—IEEE Std 1012-1998 [B22] describes the use of integrity levels in planning verification and validation activities. ISO/IEC 15026:1998 [B38] discusses the use of system and software integrity levels. IEC 61508-5:1998 [B14] provides examples of methods for the determination of safety integrity levels. ISO/IEC 15939:2002 [B40] describes a measurement process that can be used to help characterize and quantify risks.

5.1.2.3 Establish and maintain the project risk profile

A project risk profile shall be established and maintained. A project risk profile includes the overall project risk information, the collection of the risk profiles of all the individual risks, which in turn includes the current and historical risk states. A project risk profile shall consist of, at a minimum,

a) The risk management context
b) A chronological record of each risk's state including their probability, consequences, and risk thresholds
c) The priority of each risk based on risk criteria supplied by the stakeholders
d) The risk action requests for risks along with the status of their treatment

The project risk profile should contain a detailed description of each risk, its causes, the estimation scales used, the risk-related measures used to evaluate status, contingency plans, and other risk-related information captured in the risk state.

The project risk profile shall be updated when there are changes in an individual risk's state, e.g., its description, exposure or treatment, changes occur to the risk management context, or a new risk is identified. Information should be captured in electronic form to ease its capture, communication, and assessment.

5.1.2.4 Communicate risk status

The project risk profile or relevant risk profile (e.g., a single or combination of risks) shall be communicated periodically to stakeholders based upon their needs. Risk status information should be made available as widely as possible to all the stakeholders.

5.1.3 Perform risk analysis

The purposes of the “perform risk analysis” activity are to

a) Identify the initiating events, hazards, threats, or situations that create risks
b) Estimate the probability of occurrence, the consequences for each risk, and the expected timing of the risk
c) Evaluate each risk or defined combination of risks against its applicable threshold, generate alternatives to treat risks above their risk thresholds, and make recommendations for treatment based on a priority order

Risk analysis shall be performed continuously throughout the life cycle.

The “perform risk analysis” activity consists of the tasks listed in 5.1.3.1 through 5.1.3.3.

5.1.3.1 Risk identification

Risks shall be identified in the categories included in the risk management context. Changes in the risk management context, e.g., additional risk due to changes in the assumptions, shall also be identified.

Various approaches to identifying risks should be used. These approaches may include the use of risk questionnaires, taxonomies, brainstorming, scenario analysis, lessons learned, and prototyping or other knowledge acquisition approaches. Repeatable identification processes may be used to aid in the capture of lessons learned. Where possible, events, hazards, threats, or situations that can create risks should be identified to aid future risk treatment. Risks not identified are implicitly accepted.

Risk categories should be used consistently for effective communication to stakeholders. Risks that are related may be combined for ease of analysis, monitoring, and treatment. System or software anomalies, reports on measures, and other indicators should be continuously reviewed as sources for risks.

NOTE—IEEE Std 1044-1993 [B23] provides useful information regarding anomaly classification. IEEE Std 982.1-1988 [B20] provides useful information regarding software measures related to reliability. ISO/IEC 15939 [B40] provides a measurement process that can be used to help identify and characterize risks.

5.1.3.2 Risk estimation

The probability of occurrence and consequences of each risk identified shall be estimated.

Estimates may be either quantitative or qualitative. The stakeholders should define which risks will be evaluated using a qualitative scale and which will be evaluated using a quantitative scale.

The scale(s) used for estimating risk probability and consequences shall be used consistently. The descriptive and measurement uncertainty inherent in the scale used should be described in the risk management plan. The level of confidence in a risk's estimate should be captured in its risk state.

5.1.3.3 Risk evaluation

Each risk shall be evaluated against its risk thresholds. Risks should be evaluated independently, in combination, and along with their interactions with system and enterprise risks. Risks should be evaluated against the project risk threshold to assure that a combination of risks, while below their individual thresholds, does not unacceptably place the project as a whole at risk. Different techniques may be used to evaluate the risks, such as decision trees, scenario planning, game theory, probabilistic analysis, and linear programming.

Risks shall be placed in a priority ordering-the ordering criteria determined by the stakeholders. Priority may be based upon when the risk is anticipated to become a problem, the risk exposure, risk-related measures, or some other consistent criteria.

Various treatment alternatives to addressing risk should be considered to reduce or eliminate risks. For each risk that is above its risk threshold, recommended treatment strategies such as eliminating the risk, reducing its probability of occurrence or severity of consequence, or accepting the risk shall be defined and documented in a risk action request such as that found in Annex B. Contingency plans should be developed for all risks above their thresholds. Measures indicating the effectiveness of the treatment alternatives shall also be defined. The risks, their recommended treatments, and measures of risk treatment effectiveness shall be communicated to the stakeholders for approval, rejection, or modification.

NOTE—IEEE Std 982.1-1988 [B20] provides information that may be useful in defining risk-related measures. IEC 60300-3-9:1995 [B7], IEC Std 60812:1985 [B8] and IEC Std 61025:1990 [B9] provide useful techniques to aid in risk evaluation. ISO/IEC 15939 [B40] provides a measurement process that can be used to help evaluate risks.

5.1.4 Perform risk treatment

The purposes of the “perform risk treatment” activity are to

a) Determine whether risks are acceptable to the stakeholders, and if not,

b) Initiate actions to reduce the risks to an acceptable level.

Risk treatment involves the selection, planning, monitoring, and controlling of actions to decrease risk exposure.

Stakeholders shall evaluate for treatment every risk that is above its risk threshold. Risk treatment shall be continuously performed as required (see section 5.1.4.1).

5.1.4.1 Selecting risk treatment

Stakeholders shall be provided recommended alternatives for risk treatment in risk action requests. Whenever a risk treatment alternative is recommended in a risk action request, an evaluation shall be made by the stakeholders to determine if the risk is acceptable. If the stakeholders determine that actions should be taken to make a risk acceptable, then a risk treatment alternative shall be implemented, supported by the necessary resources, and monitored and coordinated with other project activities.

The stakeholders may accept a risk even though it exceeds its risk threshold, e.g., if the treatment cost is too high, the timing isn't suitable, or a lack of treatment resources exists. In this situation, the risk shall be considered a high priority and monitored continuously to determine if any future risk treatment actions are necessary.

The stakeholders may also ask that more information upon which to make a risk treatment decision be provided in the risk action request or they may suggest some other treatment approach. If the stakeholders suggest treatment alternatives that are not in the risk action request, the risk action request shall be returned to the "perform risk analysis" activity for analysis of the suggested treatment alternatives. The risk action request shall then be resubmitted to the stakeholders for reevaluation.

5.1.4.2 Risk treatment planning and implementation

This subclause has alternative provisions depending on whether this standard is being applied in conjunction with ISO/IEC 12207:1995 or ISO/IEC 15288:2002. If it is, the provisions of 5.1.4.2.1 apply. If not, the provisions of 5.1.4.2.2 apply.

5.1.4.2.1 Risk treatment with ISO/IEC 12207:1995 and ISO/IEC 15288:2002

This alternative subclause applies to all users of this standard who are applying it in conjunction with IEEE/ ISO/IEC 12207:1995 or ISO/IEC 15288:2002.

Once a risk treatment is selected, it shall receive the same management actions as problems do, in accordance with the execution and control activities in 7.1.3.3 of ISO/IEC 12207:1995 or 5.4.4.3 of ISO/IEC 15288: 2002.

5.1.4.2.2 Risk treatment independent of ISO/IEC 12207:1995 or ISO/IEC 15288:2002

This alternative subclause applies to all users of this standard who are applying it independently of IEEE/ ISO/IEC 12207:1995 or ISO/IEC 15288:2002.

When a risk treatment alternative has been accepted, the stakeholders shall define a detailed plan for treatment, such as that described in informative Annex C. How this plan is to be executed and resources provided and monitored for progress and success shall be established. A party shall be assigned responsibility for the success of each risk treatment.

The risk treatment plan shall be implemented and integrated in accordance with existing project plans and their management processes and activities.

Stakeholders should define contingency actions in event of the failure of a risk's treatment. Contingency actions may also be necessary for some risks that are deemed acceptable.

5.1.5 Perform risk monitoring

The purposes of the "perform risk monitoring" activity are to

a) Review and update the individual risk states and the risk management context
b) Assess the effectiveness of risk treatment
c) Seek out new risks and sources

5.1.5.1 Monitor risk

All risks shall be monitored throughout the life cycle for changes in their state using measures that will be recorded in the project risk profile. The risk management context shall also be monitored for changes and be documented in the project risk profile. Risks shall be placed in a monitoring priority order based on criteria supplied by the stakeholders (e.g., risk exposure, timing.). The monitoring priority should be reviewed periodically to verify that the priority ordering is still valid. High priority risks should be monitored frequently. Risks whose state has changed shall undergo risk evaluation. Evaluation should occur promptly after discovery.

5.1.5.2 Monitor risk treatment

Measures shall be implemented and monitored to evaluate the effectiveness of risk treatments. The cause of an ineffective treatment should be identified and remedied promptly. Criteria should be set by the stakeholders to determine when a risk no longer needs to be monitored for treatment effectiveness.

NOTE—ISO/IEC 15939 [B40] provides a measurement process that can be used to help monitor the impact of risk treatments.

5.1.5.3 Seek new risks

The system shall be continuously monitored for new risks and sources throughout its life cycle. New risks and sources shall be communicated to the stakeholders after risk analysis.

5.1.6 Evaluate the risk management process

The purposes of the "evaluate the risk management process" activity are to provide feedback to the stakeholders regarding

a) The quality of the risk management process
b) Areas where the risk management procedures, process, or policies should be improved
c) The identification of opportunities for modifying organizational risk management procedures, processes, or policies to better reduce or eliminate systemic risks

This activity consists of the tasks listed in 5.1.6.1 through 5.1.6.3.

5.1.6.1 Capture risk management information

Information about the risks identified, their sources, their causes, their treatment, and the success of the treatments selected shall be collected throughout the project's life cycle for purposes of improving the risk management process and generating lessons learned. The information captured may be useful to improving organizational risk management procedures, processes, or policies. Information may be captured in electronic form to ease its capture, communication, and assessment.

5.1.6.2 Assess and improve the risk management process

The risk management process shall be periodically reviewed for its effectiveness and efficiency. Opportunities for improving the project or organizational risk management systems and processes should be identified, including consideration of how the risks posed by the risk management process itself can be reduced or eliminated. Where applicable, the process should be improved, the organizational risk management systems and policies and process updated (if these exist), and the project risk management plan updated. The stakeholders shall determine the review period.

5.1.6.3 Generate lessons learned

Information on the risks identified, their treatment, and the success of the treatments shall be reviewed periodically by the stakeholders and other parties for purposes of identifying systemic project and organizational risks. Individual project lessons learned may be collected to aid in the identification of systemic risks. The stakeholders shall determine the review period.

5.2 Null Clause

This clause is intentionally left blank to conform to the numbering conventions of ISO/IEC 12207.

Annex A

(informative)

Risk management plan

A.1 Purpose

The purpose of the risk management plan is to define how the risk management activities are implemented and supported during a project. The risk management plan is a key output of the planning process, and serves as the mechanism for implementing risk management. The risk management plan would meet the intent of ISO/IEC 12207:1995, 5.2.4.5 item k), IEEE/EIA12207.1-1997, 6.11.3 item l) [B28], and ISO/IEC 15288:2002, 5.3.6.4 item a) that require the inclusion of risk management information or approach in the project management plan or other project documentation. A risk management plan that follows the outline below would also meet the intent of 4.5.4 of IEEE Std 1058-1998 [B24].

A.2 Risk management plan

The risk management process should result in a risk management plan that includes the sections shown in the outline below. If there is no information pertinent to a section or a required paragraph within a section, the management plan should contain the phrase, “This section is not applicable to this plan” below the section or paragraph heading, together with the appropriate reason for the omission. Additional information may be added if needed. Some of the risk management plan may appear in other documents. If so, reference to those documents should be made in the body of management plan.

The outline of the risk management plan is shown as follows:

1. Overview
    1.1 Date of Issue and Status
    1.2 Issuing Organization
    1.3 Approval Authority
    1.4 Updates
2. Scope

[Define the boundaries and limitations of risk on the project]

3. Reference Documents
4. Glossary
5. Risk Management Overview

[Describe the specifics of risk management for this project or organization's situation.]

6. Risk Management Policies

[Describe the guidelines by which risk management will be conducted.]

7. Risk Management Process Overview

8. Risk Management Responsibilities

[Define the parties responsible for performing risk management.]

9. Risk Management Organization

[Describe the function or organization assigned responsibility for risk management within the organizational unit.]

10. Risk Management Orientation and Training

11. Risk Management Costs and Schedules

12. Risk Management Process Description

[If there is an organizational risk management process that is being used for this project or situation, refer to it. If adaptation of the process is appropriate, describe the adaptations made. Describe the procedures that implement the risk management process. If no organizational process exists, describe the risk management process and procedures to be used for the project or situation.]

12.1 Risk Management Context

12.2 Risk Analysis

12.3 Risk Monitoring

12.4 Risk Treatment

[Describe how risks are to be treated. If a standard management process exists for handling deviations or problems, refer to this process. If risks require a separate risk treatment activity due to specific circumstance, describe this activity.]

13. Risk Management Process Evaluation

[Describe how this project or organization will gather and use measurement information to help improve the risk management process for the project and/or for the organization.]

13.1 Capturing Risk Information

13.2 Assessing the Risk Management Process

13.3 Generating Lessons Learned

14. Risk Communication

[Describe how risk management information will be coordinated and communicated among stakeholders and interested parties (i.e., those who are interested in the performance or success of the project or product, but not necessarily of the organization) such as what risks need reporting to which management level.]

14.1 Process Documentation and Reporting

14.2 Coordinating Risk Management with Stakeholders

14.3 Coordinating Risk Management with Interested Parties

15. Risk Management Plan Change Procedures and History

Annex B

(informative)

Risk action request

B.1 Purpose

The purpose of the risk action request is to provide a mechanism by which risk information can be captured and communicated to the stakeholders. The risk management process requires the creation of risk action requests for risks above their risk threshold.

B.2 Risk action request

The risk management process should result in risk action requests that include the information shown in the outline below. If there is no information pertinent to a section or a required paragraph within a section, the action request should contain the phrase, “This section is not applicable to this request” below the section or paragraph heading, together with the appropriate reason for the omission. Additional sections may be added if needed. Parts of the risk action request may appear in other documents. If so, reference to those documents should be made in the body of the action request.

The outline of the risk action request is shown as follows:

1. Date of Initiation

2. Scope

3. Subject

4. Request Originator

5. Risk Management Process Context

[This section may be provided once, and then referenced in subsequent action requests if no changes have occurred.]

5.1 Process Scope

5.2 Stakeholder Perspective

5.3 Risk Categories

5.4 Risk Thresholds

5.5 Project Objectives

5.6 Project Assumptions

5.7 Project Constraints

6. Risks

[This section may cover one risk or many, as the user chooses. Where all the information above applies to the whole set of risks, one action request may suffice. Where the information varies, each request may cover the risk or risks that share common information.]

6.1 Risk Description(s)

6.2 Risk Probability

6.3 Risk Consequences

6.4 Expected Timing of Risk

7. Risk Treatment Alternatives

7.1 Alternative Descriptions

7.2 Recommended Alternative(s)

7.3 Justifications

8. Risk Action Request Disposition

[Each request should be annotated as to whether it is accepted, rejected, or modified, and the rationale provided for whichever decision is taken.]

Annex C

(informative)

Risk treatment plan

C.1 Purpose

The purpose of the risk treatment plan is to define how risks that are found unacceptable are to be treated. The risk treatment plan serves as the mechanism for implementing a selected recommended alternative defined within a risk action request.

C.2 Risk treatment plan

After a recommended treatment alternative described within the risk action request has been selected, a risk treatment plan should be developed that includes the sections shown in the outline below. Some of the information for the treatment plan may appear within the risk action request. If so, references to the risk action request should be made in the body of treatment plan in the pertinent sections. If there is no information pertinent to a section, the treatment plan should contain the phrase, “This section is not applicable to this plan” below the section or paragraph heading, together with the appropriate reason for the omission. Additional information may be added to the plan if needed.

To reduce the necessity to develop an individual risk treatment plan for each individual risk, risk treatment plans may be defined for dealing with risks sharing pertinent characteristics.

The outline of the risk treatment plan is shown as follows:

1. Overview

1.1 Date of Issue and Status

1.2 Issuing Authority

1.3 Approval Authority

1.4 Updates

2. Scope

3. Reference Documents

4. Glossary

5. Planned Risk Treatment Activities and Tasks

[Describe the specifics of the risk treatment selected for a risk or combination of risks found to be unacceptable. Describe any difficulties that may be found in implementing the treatment.]

6. Treatment Schedule

7. Treatment Resources and their Allocation

8. Responsibilities and Authority

[Describe who is responsible for ensuring that the treatment is being implemented and their authority.]

9. Treatment Control Measures

[Define the measures that will be used to evaluate the effectiveness of the risk treatment.]

10. Treatment Cost

11. Interfaces among Parties Involved

[Describe any coordination among stakeholders or with the project's master plan that must occur for the treatment to be properly implemented.]

12. Environment/Infrastructure

[Describe any environmental or infrastructure requirements or impacts, e.g., safety or security impacts that the treatment may have.]

13. Risk Treatment Plan Change Procedures and History

Annex D

(informative)

Application of risk management in the software life cycle

This annex lists references to risk in ISO/IEC 12207:1995 as well as in the IEEE/EIA 12207 series. Subclause D.1 lists references to the ISO/IEC standard and subclause D.2 lists references to the IEEE standards.

D.1 Application of risk management in the ISO/IEC 12207 series

References to "risk" and "risk management" are made throughout ISO/IEC 12207 series of standards including amendments 1 and 2. Those references are paraphrased here for convenience.

D.1.1 General

Annex F of ISO/IEC 12207:1995/Amd.1:2002 (E), provides information regarding risk management. Application of this standard is consistent with the information presented in that annex.

Annex H of ISO/IEC 12207:1995/Amd.1:2002 (E), provides information regarding risk management. Application of this standard is consistent with the information presented in that annex.

D.1.2 Acquisition process

[ISO/IEC 12207:1995, 5.1.1.6] When considering the various options for acquisition-such as off-the-shelf, developed, etc.-the acquirer should include risk in the criteria.

[ISO/IEC 12207:1995, 5.1.1.8] An acquisition plan should contain a description of risk and risk management methods.

[ISO/IEC 12207:1995/Amd.1:2002 (E), H.1.2] The purpose of the Acquisition Strategy process is to ensure the products to be acquired will comply with the mission, goals and objectives of the business and to provide the basis for planning all aspects of the acquisition project…As a result of successful implementation of the process:… 5) the business risks, financial, technical and resource implications for differing or alternative approaches or solutions will be identified.

D.1.3 Supply process

[ISO/IEC 12207:1995, 5.2.4.4] The supplier shall consider the options for developing the software product or supplying the software service-such as developed, off-the-shelf, etc.-against an analysis of risks associated with each option.

[ISO/IEC 12207:1995, 5.2.4.5] The supplier shall develop and document project management plan(s). Items to be considered in the plan include but are not limited to ... k) Risk management; that is management of the areas of the project that involve potential technical, cost, and schedule risks.

D.1.4 Operation process

[ISO/IEC 12207:1995/Amd.1:2002 (E), F.1.4.1] As a result of successful implementation of Operational use: 1) operational risks for the product introduction and operation are identified and monitored.

D.1.5 Verification process

[ISO/IEC 12207:1995, 6.4.1.1] A determination shall be made if the project warrants a verification effort and the degree of organizational independence of that effort needed. The project requirements shall be analyzed for criticality. Criticality may be gauged in terms of ... b) the maturity of and risks associated with the software technology to be used.

D.1.6 Joint review process

[ISO/IEC 12207:1995, 6.6.2.1] Project status shall be evaluated relative to the applicable project plans, schedules, standards, and guidelines. The outcome of the review should be discussed between the two parties and should provide for ... d) Evaluating and managing the risk issues that may jeopardize the success of the project.

[ISO/IEC 12207:1995, 7.1.2.1] The manager shall prepare the plans for execution of the process. The plans associated with the execution of the process shall contain descriptions of the associated activities and tasks and identification of the software products that will be provided. These plans shall include, but are not limited to … f) Quantification of risks associated with the tasks or the process itself.

D.1.7 Management process

[ISO/IEC 12207:1995/Amd.1:2002 (E), F.3.1] The Management Process includes purposes and outcomes for the following sub-processes: … Risk Management …

[ISO/IEC 12207:1995/Amd.1:2002 (E), F.3.1.5] The purpose of Risk management is to identify, manage and mitigate the risks continuously, at both the organizational and project level. As a result of successful implementation of Risk management: 1) the scope of the risk management to be performed is determined; 2) appropriate risk management strategies are defined and implemented; 3) risks to the project are identified in the project's risk management strategy, and as they develop during the conduct of the project; 4) the risks are analyzed and the priority in which to apply resources to monitor these risks are determined; 5) risk monitoring techniques are selected to determine the change in the risk status and the progress of the monitoring activities; and 6) appropriate action is taken to correct or avoid the impact of risk.

[ISO/IEC 12207:1995/Amd.2:2003 (E), F.3.1.5] The purpose of risk management is to identify, analyze, treat and monitor the risks continuously. As a result of successful implementation of risk management: 1) the scope of risk management to be performed is determined; 2) appropriate risk management strategies are defined and implemented; 3) risks are identified as they develop and during the conduct of the project; 4) risks are analyzed, and the priority in which to apply resources to treatment of these risks is determined; 5) risk measures are defined, applied, and assessed to determine changes in the status of risk and the progress of the treatment activities; and 6) appropriate treatment is taken to correct or avoid the impact of risk based on its priority, probability, and consequence or other defined risk threshold.

D.1.8 Tailoring process

[ISO/IEC 12207:1995, Annex A] Risk is a factor to be considered in tailoring the standard.

D.1.9 Supporting life cycle processes

[ISO/IEC 12207:1995/Amd.1:2002 (E), G.1.1, 6.9.2.2] In association with the developer the usability specialist will: … d) Assess risk to stakeholders and users.

D.1.10 Financial Requirements

[ISO/IEC 12207:1995/Amd.1:2002 (E), H.1.6] The purpose of the Financial Requirements process is to specify the requirements to prepare the infrastructure for an effective financial management of the acquisition project… As a result of successful implementation of the process: 1) financial management, risks and costs to the acquirer will be established.

D.1.11 Project Requirements

[ISO/IEC 12207:1995/Amd.1:2002 (E), H.1.7] The purpose of the Project Requirements process is to specify the requirements to ensure the acquisition project are performed with adequate planning, staffing, directing, organizing and control over project tasks and activities… As a result of successful implementation of the process: … 6) risks associated with project lifecycle and with suppliers will be identified.

D.1.12 Contract Agreement

[ISO/IEC 12207:1995/Amd.1:2002 (E), H.1.11] The purpose of the Contract Agreement process is to negotiate and approve a contract / agreement that clearly and unambiguously specifies the expectations, responsibilities, work products / deliverables and liabilities of both the supplier(s) and the acquirer… As a result of successful implementation of the process: … 2) mechanisms for monitoring the capability and performance of the supplier(s) and for mitigation of identified risks are reviewed and considered for inclusion in the contract conditions.

D.1.13 Supplier Relationships

[ISO/IEC 12207:1995/Amd.1:2002 (E), H.1.15] The purpose of the Supplier Relationships process is to improve acquirer-supplier relationships in terms of quality of services and value for money so as to gain a better understanding of the needs of both parties… As a result of successful implementation of the process: … 4) potential benefits of improved relationships and reciprocal risks of no change will be identified.

[ISO/IEC 12207:1995/Amd.1:2002 (E), H.2.1.3, 5.1.8.3] As part of the defining policies for the management supplier relationships… c) potential benefits of improved relationships and reciprocal risks of no change will be identified.

D.1.14 User Relationships

[ISO/IEC 12207:1995/Amd.1:2002 (E), H.1.15] The purpose of the User Relationships process is to improve

acquirer-user relationships in terms of quality of services and value for money so as to gain a better understanding of the needs of both parties… As a result of successful implementation of the process: … 3) potential benefits of improved relationships and reciprocal risks of no change will be identified.

[ISO/IEC 12207:1995/Amd.1:2002 (E), H.2.1.4, 5.1.9.2] As part of the defining policies to manage user relationships… b) potential benefits of improved relationships and reciprocal risks of no change will be identified.

D.2 Application of risk management in the IEEE/EIA 12207 series

References to "risk" and "risk management" are made throughout IEEE/EIA 12207 series of standards. Those references are paraphrased here for convenience.

D.2.1 General

Annex L of IEEE/EIA 12207.2-1997 provides information regarding risk management. Application of this standard is consistent with the information presented in that annex.

[IEEE/EIA 12207.1-1997, 4.2.4, Guidance] Management life cycle data should contain content regarding "management and technical risks."

[IEEE/EIA 12207.1, 5.2.2] Any plan should include or reference information regarding risks.

D.2.2 Acquisition process

[IEEE/EIA 12207.0-1996, 5.1.1.6] When considering the various options for acquisition-such as off-the-shelf, developed, etc.-the acquirer should include risk in the criteria.

[IEEE/EIA 12207.0-1996, 5.1.1.8] An acquisition plan should contain a description of risk and risk management methods.

[IEEE/EIA 12207.2-1997, 5.1.1.8, Guidance] The acquisition plan should establish a software measurement program that, among other goals, aids in managing cost, schedule, and technical risk.

[IEEE/EIA 12207.1-1997, 6.1.3] The acquisition plan should include risks considered as well as methods to manage the risks.

[IEEE/EIA 12207.2-1997, 5.1.3.5, Guidance] The investigation of the impact of changes to the contract should include all potential significant risks.

[IEEE/EIA 12207.2-1997, 5.1.4.2, Guidance] Arrangements should be established to ensure both the acquirer and the supplier cooperate to provide necessary information and work together to resolve problems and risks.

D.2.3 Supply process

[IEEE/EIA 12207.0-1996, 5.2.4.4] The supplier shall consider the options for developing the software product or supplying the software service-such as developed, off-the-shelf, etc.-against an analysis of risks associated with each option.

[IEEE/EIA 12207.0-1996, 5.2.4.5] The supplier shall develop and document project management plan(s). Items to be considered in the plan include but are not limited to ... k) Risk management; that is management of the areas of the project that involve potential technical, cost, and schedule risks.

[IEEE/EIA 12207.2-1997, 5.2.4.5 k), Guidance] Refers to IEEE/EIA 12207.2-1997, Annex L, for information on risk management.

[IEEE/EIA 12207.1-1997, 6.11.3] The Project Management Plan should include risk management.

[IEEE/EIA 12207.2-1997, 5.2.5.3 a), Guidance] Recommends including risk management in the activities to be monitored by the supplier throughout the contracted life cycle.

D.2.4 Development process

[IEEE/EIA 12207.2-1997, 5.3.1.4, Guidance] Planning for development describes the approach (methods/procedures/tools) to applicable activities and tasks of the development process, covers all applicable clauses regarding development, and identifies applicable risks/uncertainties regarding those activities and tasks and describes plans for dealing with them.

[IEEE/EIA 12207.2-1997] Figure I.2 of IEEE/EIA 12207.2-1997 depicts a sample risk analysis for determining an appropriate development strategy.

[IEEE/EIA 12207.1-1997, 6.26.3] The System Requirements Specification should provide constraints on computer resources consistent “with the degree of risk identified.”

D.2.5 Operation process

[IEEE/EIA 12207.0-1996, G.11] The objectives for operation process include ... a) Identify and mitigate operational risks.

D.2.6 Verification process

[IEEE/EIA 12207.0-1996, 6.4.1.1] A determination shall be made if the project warrants a verification effort and the degree of organizational independence of that effort needed. The project requirements shall be analyzed for criticality. Criticality may be gauged in terms of ... b) the maturity of and risks associated with the software technology to be used.

D.2.7 Joint review process

[IEEE/EIA 12207.2-1997, 6.6.1.3 Guidance] Risk items should be included in joint reviews.

[IEEE/EIA 12207.0-1996, 6.6.2.1] Project status shall be evaluated relative to the applicable project plans, schedules, standards, and guidelines. The outcome of the review should be discussed between the two parties and should provide for ... d) Evaluating and managing the risk issues that may jeopardize the success of the project.

[IEEE/EIA 12207.2-1997, 6.6.2.1 Guidance] In addition to contractually required reviews (see Guidance for 5.1.2.3 and Guidance 2 for 5.2.4.5), the supplier, including the developer, maintainer, or operator, as applicable, may propose additional joint management reviews. The supplier and other applicable parties should plan and take part in such additional reviews at locations and dates proposed by the supplier and approved by the acquirer. Candidate joint management reviews are identified in Annex G of IEEE/EIA 12207.2-1997. These reviews should be attended by persons with authority to make cost and schedule decisions and may have the following objectives:... c) Arrive at agreed-upon mitigation strategies for near-term and long-term risks that could not be resolved at joint technical reviews; and d) Identify and resolve management-level issues and risks not raised at joint technical reviews.

[IEEE/EIA 12207.2-1997, 6.6.3.1 Guidance] The supplier, including the developer and/or the maintainer and/or the operator, as applicable, should plan and take part in joint technical reviews at locations and dates proposed by the supplier and approved by the acquirer. These reviews should be attended by persons with technical knowledge of the software products to be reviewed. Support process disciplines (e.g., quality assurance, configuration management, verification, validation) should provide input to or be present at joint reviews. The reviews should focus on in-process and final software products, rather than materials generated especially for the review. The reviews may have the following objectives:… c) Arrive at agreed-upon mitigation strategies for identified risks, within the authority of those present; and d) Identify risks and issues to be raised at joint management reviews.

D.2.8 Problem resolution process

[IEEE/EIA 12207.2-1997, Figure J.2] The figure suggests that impact on risk is a criterion for labeling problem reports.

D.2.9 Management process

[IEEE/EIA 12207.0-1996, G.10] Objectives for the Management process include ... k) Determine the scope of risk management to be performed for the project ... l) Identify risks to the project as they develop ... m)

Analyze risks and determine the priority in which to apply resources to mitigate those risks ... n) Define, implement, and assess appropriate risk mitigation strategies...o) Define, apply, and assess risk metrics to measure the change in the risk state and the progress of the mitigation activities.

[IEEE/EIA 12207.0-1996, 7.1.2.1] The manager shall prepare the plans for execution of the process. The plans associated with the execution of the process shall contain descriptions of the associated activities and tasks and identification of the software products that will be provided. These plans shall include, but are not limited to … f) Quantification of risks associated with the tasks or the process itself.

D.2.10 Tailoring process

[IEEE/EIA 12207.0-1996, Annex A] Risk is a factor to be considered in tailoring the standard.

D.2.11 Miscellaneous

[IEEE/EIA 12207.2-1997, F.2] Examples of candidate criteria that may be used in evaluating reusable software products include, but are not limited to ... i) technical, cost, and schedule risks and trade-offs in using the software product.

[IEEE/EIA 12207.2-1997, H.1] In defining issues for software measurement, consider risks, problems, and uncertainties.

Annex E

(informative)

Annotated bibliography

[B1] ANSI/EIA 632, Processes for Engineering a System

This standard provides the process requirements for engineering systems. It includes a risk management process to reduce the effects of uncertain events that may result in changes to quality, cost, schedule or technical characteristics.

[B2] AS/NZS 4360:1999 Australian / New Zealand Standard for Risk Management

AS/NZ standard 4360 provides a general framework for establishing and implementing a risk management system within an organization. It is aimed at improving safety, quality and business performance in an organization. The material in this standard is useful in providing a larger context in which IEEE standard 1540 would operate.

[B3] BS-6079-3:2000 Project Management. Guide to the Management of Business Related Project Risk. BSI, 2000.

This British management standard gives guidance on the identification and control of business related risks encountered when undertaking projects. It is applicable to a wide spectrum of project organizations operating in the industrial, commercial and public or voluntary sectors. It is written for project sponsors and project managers, either or both of whom are almost always responsible to higher levels of authority for one or more projects of various types and sizes. It is intended that its application will be proportional to the circumstances and needs of the particular organization.

[B4] CAN/CSA-850-97, Risk Management Guideline for Decision-Makers. CSA, 1997.

This Canadian guideline is intended to assist decision- makers in effectively managing all types of risk issues, including injury or damage to health, property, the environment, or something else of value. This Guideline describes a process for acquiring, analyzing, evaluating, and communicating information that is necessary for decision-making. This Guideline provides a description of the major components of the risk management decision process, and their relationship to each other, in a step-by-step process.

[B5] IEC 60300-1:1993, Dependability Management, Part 1: Dependability programme management

IEC standard 60300-1 provides information on dependability assurance which addresses the reliability performance and maintainability performance of a product as well as the performance of maintenance support provided by the customer (and/or the supplier).

[B6] IEC 60300-2:1995, Dependability Management, Part 2: Dependability programme elements and tasks

IEC 60300-2 standard offers various techniques that may be useful in understanding product risks as part of an analysis, prediction or design review when performing dependability assurance.

[B7] IEC 60300-3-9:1995, Dependability Management, Part 3: Application Guide — Section 9: Risk analysis of technological systems

IEC guide 60300-3-9 provides guidelines for the selection and utilization of commonly used risk analysis techniques. The guide may be helpful in determining which techniques are most applicable when performing general risk analysis.

[B8] IEC 60812:1985 Analysis techniques for system reliability — Procedures for failure mode and effects analysis (FEMA)

IEC standard 60812 provides guidance on how to perform Failure Mode and Effects Analysis (FMEA) and Failure Mode, Effects and Criticality Analysis (FMECA). This material is important in safety or other critical risk analyses.

[B9] IEC 61025:1990 Fault Tree Analysis (FTA)

IEC standard 61025 provides in-depth guidance on how to perform Fault Tree Analysis (FTA). This material is important in safety or other critical risk analyses.

[B10] IEC 61508-1:1998 Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 1: General requirements

IEC standard 61508-1 provides a generic approach for all safety life cycle activities for systems comprised of electrical and/or electronic and/or programmable electronic components (electrical/electronic/programmable electronic systems (E/E/PESs)) that are used to perform safety functions.

[B11] IEC 61508-2:2000 Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems

IEC standard 61508-2 specifies how to refine the information developed in accordance with IEC 61508-1, with the exception of devices utilizing software, which is specified in IEC 61508-3.

[B12] IEC 61508-3:1998 Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 3: Software Requirements

IEC standard 61508-3 applies to any software forming part of a safety-related system or used to develop a safety-related system within the scope of IEC 61508-1 and IEC 61508-2. This standard provides material useful in looking at software risks related to products.

[B13] IEC 61508-4:1998 Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 4: Definitions and abbreviations

IEC standard 61508-4 presents the definitions of the terms used in conjunction with IEC 61508.

[B14] IEC 61508-5:1998 Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 5: Examples of methods for the determination of safety integrity levels

IEC standard 61508-5 provides many useful examples for helping specify safety integrity levels. Specification of integrity levels can help define risk acceptability or threshold levels in a risk analysis.

[B15] IEC 61508-6:2000 Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3

IEC standard 61508-6 presents the guidelines for using standards IEC 61508-2 and IEC 61508-3.

[B16] IEC 61508-7:2000 Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 7: Overview of techniques and measures

IEC 61508-7 contains an overview of the various safety techniques and measures that are relevant to implementing IEC 61508-2 and IEC 61508-3.

[B17] IEC 61713:2000, Software dependability through the software life-cycle processes — Application guide

IEC application guide 61713 identifies software life-cycle process activities that will aid in achieving dependable software (i.e. software that reliably performs according to requirements). The material in this guide may be useful in identifying sources of risk.

[B18] IEC 62198:2001 Project risk management — Application guidelines

IEC 62198 provides a process for managing risks in a systematic and consistent manner. It is aimed at decision-makers, including project managers, risk managers and business managers.

[B19] IEEE 100, The Authoritative Dictionary of the IEEE Standards Terms, Seventh Edition.

[B20] IEEE Std 982.1-1988, IEEE Standard Dictionary of Measures to Produce Reliable Software.

[B21] IEEE Std 982.2-1988, IEEE Guide for the Use of IEEE Standard Dictionary of Measures to Produce Reliable Software.

Some of the measures described in IEEE Std 982.1 and IEEE Std 982.2 are appropriate for use in risk management.

[B22] IEEE Std 1012-1998, IEEE Standard for Software Verification and Validation Plans.

IEEE Std 1012-1998 uses integrity levels to determine appropriate verification and validation activities. It would be appropriate to determine these integrity levels in the baseline risk model.

[B23] IEEE Std 1044-1993, IEEE Standard Classification for Software Anomalies.

Risk considerations may be useful in classifying anomalies.

[B24] IEEE Std 1058-1998, IEEE Standard for Software Project Management Plans-Content Map to IEEE/EIA 12207.1.

IEEE Std 1058-1998 requires the specification of a risk management plan for identifying, analyzing and prioritizing project risk factors, as well as the procedures for contingency planning, risk monitoring, and changes in risk status.

[B25] IEEE Std 1220-1998, IEEE Standard for the Application and Management of the Systems Engineering Process

This standard provides activities for managing the Systems Engineering Process. Risk Management requirements are integrated throughout.

[B26] IEEE Std 1228-1994, IEEE Standard for Software Safety Plans.

IEEE Std 1228-1994 contains material useful in the management of software that is part of a system with safety requirements.

[B27] IEEE Std 1490:2003, IEEE Guide Adoption of PMI Standard — A Guide to the Project Management Body of Knowledge 2004

The purpose of this document is to identify and describe a subset of the Project Management Body of Knowledge that is generally accepted. Generally accepted means that the knowledge and practices described are applicable to most projects most of the time, and that there is widespread consensus about their value and usefulness. It does not mean that the knowledge and practices should be applied uniformly to all projects without considering whether they are appropriate. There is a section in the Project Management Body of Knowledge on risk management.

[B28] IEEE/EIA 12207.1-1997, IEEE/EIA Guide-Industry Implementation of International Standard ISO/IEC 12207:1995, Standard for Information Technology-Software Life Cycle Processes-Life Cycle Data.

This document suggests information items for recording the data produced by the processes of IEEE/EIA 12207.0-1996.

[B29] IEEE/EIA 12207.2-1997, IEEE/EIA Guide-Industry Implementation of International Standard ISO/IEC 12207:1995, Standard for Information Technology-Software Life Cycle Processes-Implementation Considerations.

This document provides supplementary guidance for IEEE/EIA 12207.0-1996.

[B30] ISO 3534-1:1993 Statistics — Vocabulary and symbols — Part 1: Probability and general statistical terms

ISO standard 3534-1:1993 defines 204 probability and general statistical terms.

[B31] ISO 9000:2000, Quality Management Systems — Fundamentals and Vocabulary

This standard provides the overall concepts and vocabulary used throughout the ISO 9000 family of standards on quality management systems.

[B32] ISO 10006:2003 Quality management systems. Guidelines for quality management in projects.

This document gives guidance on the application of quality management in projects. It is not a guide to "project management" itself, but rather guidance on quality in project management processes.

[B33] ISO 14971:2000 — Medical devices — Application of risk management to medical devices

ISO 14971 contains material on risk management for medical device systems with safety requirements.

[B34] ISO/IEC Guide 51:1999 Safety aspects — Guidelines for their inclusion in standards

ISO/IEC Guide 51 provides standards writers with guidelines for the inclusion of safety aspects in standards. It is applicable to any safety aspect related to people, property or the environment, or a combination of one or more of these (e.g. people only; people and property; people, property and the environment).

[B35] ISO/IEC Guide 73:2002, Guide on Risk management-Vocabulary-Guidelines for use in standards.

The terminology used in this standard is consistent with the vocabulary recorded in this ISO Guide.

[B36] ISO/IEC TR 19760:2004 Systems Engineering — A Guide for the Application of ISO/IEC 15288 System Life Cycle Processes

ISO/IEC TR 19760 provides guidance in Table C.12, Risk Management Process, for the implementation of the risk management process in ISO/IEC 15288. Additionally, there are several other references of the usage of risk management in conjunction with the processes.

[B37] ISO/IEC 12207:1995, Information Technology-Software Life Cycle Processes. ISO/IEC 12207:1995/AMD.1:2002, Information Technology-Software Life Cycle Processes — Amendment 1. ISO/IEC 12207:1995/AMD.2, Information Technology-Software Life Cycle Processes — Amendment 2.

The 1995 standard provides activities and tasks for 17 processes involved in the life cycle of a software product or service. The two amendments provide statements of purpose and outcomes for a larger number of processes.

[B38] ISO/IEC 15026:1998 Information technology — System and software integrity levels

ISO/IEC standard 15026 defines the concepts associated with integrity levels, i.e., a denotation of a range of values of a property of an item necessary to maintain system risks within tolerable limits. The standard also defines the processes for determining integrity levels and software integrity requirements, and places requirements on each process. The material in this standard can help define risk acceptability or threshold levels in a risk analysis

[B39] ISO/IEC 15288:2002 Systems Engineering — System life cycle processes

ISO/IEC standard 15288 calls for a risk management process to reduce the effects of uncertain events that may result in changes to quality, cost, schedule or technical characteristics.

[B40] ISO/IEC 15939: 2002, Software Engineering — Software Measurement Process

This standard defines a measurement process applicable to all engineering and management disciplines. The measurement process defined in ISO/IEC 15939 works in conjunction with the risk management activities and tasks defined in 16085 to help characterize and quantify risks.

[B41] JIS Q 2001:2001 Guidelines for development and implementation of risk management system.

This Japanese industrial standard provides principles and elements for the establishment of a risk management system. These principles and elements are applicable to any types of organizations, and to any kinds of risks. This Standard is not intended for use as a certification criterion.

ICS 35.080

Price based on 34 pages