*Recognized as an*
*American National Standard (ANSI)*

**IEEE Std 1540-2001**

# IEEE Standard for Software Life Cycle Processes—Risk Management

*Sponsor*

**Software Engineering Standards Committee**
**of the**
**IEEE Computer Society**

*Approved 17 March 2001*

**IEEE-SA Standards Board**

**Abstract:** *A process for the management of risk in the life cycle of software is defined. It can be added to the existing set of software life cycle processes defined by the IEEE/EIA 12207 series of standards, or it can be used independently.*
**Keywords:** *acceptability, integrity, risk, risk analysis, risk management, risk treatment*

---

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



*Print: ISBN 0-7381-2834-1 SH94925*
*PDF: ISBN 0-7381-2835-X SS94925*

**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.

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
P.O. Box 1331
Piscataway, NJ 08855-1331
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 is the sole entity that may authorize the use of certification marks, trademarks, or other designations to indicate compliance with the materials set forth herein.

# Introduction

(This introduction is not part of IEEE Std 1540-2001, IEEE Standard for Software Life Cycle Processes—Risk Management.)

Software risk management is a key discipline for making effective decisions and communicating the results within software 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 likelihood 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 software life cycle activities and the quality and performance of software products, and for improving the active management of software projects.

By successfully implementing this risk management standard

- Potential problems will be identified
- The likelihood and consequences of these risks will be understood
- The priority order in which risks should be addressed will be established
- Treatment alternatives appropriate for each potential problem above its risk threshold will be recommended
- Appropriate treatments will be selected for risks above their thresholds
- The effectiveness of each treatment will be monitored
- Information will be captured to improve risk management policies
- The risk management process and procedures will be regularly evaluated and improved

This software risk management standard supports the acquisition, supply, development, operation, and maintenance of software products and services. This standard is written for use in conjunction with existing organizational risk management processes, which are assumed to be processes similar to those described within this standard. This standard is written for those parties who are responsible in their organization for defining, planning, implementing, or supporting software risk management. The domain of use, the stage of the software life cycle a software project or product is in, and the specific characteristics of an organization will influence how the standard is applied in practice.

This standard defines a continuous software risk management process applicable to all software-related engineering and management disciplines. The risk management process itself is made up of several activities and tasks that function in an iterative manner. The process defines the minimum activities of a risk management process, the risk management information required and captured, and its use in managing risk. The risk management process defined in this standard can be adapted for use at an organization level or project level, for different types and sizes of projects, for projects in different life cycle phases, and to support diverse stakeholder perspectives. It is intended that the standard will be adapted by individual organizations and projects to meet their specific situations and needs. For this reason, this standard does not specify the use of any specific risk management techniques or associated organizational structures for implementing risk management. The standard implicitly supports, however, the use of tools and techniques that can make risk management a continuous process. Capturing and communicating risk-related information in electronic form to all parties involved in a project is encouraged.

The writers of this standard understand that many users may wish to apply it in conjunction with the IEEE/EIA 12207 series of software life cycle process standards. Therefore, the standard is designed so that it may be applied independently or with IEEE/EIA12207.

When applied independently, the standard provides a complete and self-contained description of a software risk management process that may be applied throughout the software life cycle.

When applied with IEEE/EIA 12207.0-1996, this risk management standard adds a process for managing risk to the existing set of software life cycle processes defined by the IEEE/EIA 12207 series. This means the standard assumes that the activities involved in the treatment of risk follow standard IEEE/EIA 12207.0-1996 management practices. Therefore, the treatment of risk will typically follow the same management actions as used when encountering problems as described in 7.1.3.3 of IEEE/EIA 12207.0-1996.

This standard is written from the viewpoint that software risk management is an integral part of software engineering technical and managerial processes and is not performed by a separate organizational element. If for some reason the treatment of risk is required to be performed by a separate organizational element, e.g., because of the size or nature of the software project, the magnitude or number of the risks involved, or IEEE/EIA 12207.0-1996 is not being followed, this standard can continue to be applied.

To facilitate use with IEEE/EIA 12207 series, the standard is written using the vocabulary and style of IEEE/EIA 12207.0-1996.

Finally, this standard supports the IEEE standards that involve the management of specific categories of risk, such as IEEE Std 1228-1994.

## Participants

At the time this standard was completed, the Software Risk Management Working Group had the following membership:

**Robert N. Charette,** *Chair*

| | | |
|---|---|---|
| Dennis Ahern | Richard E. Fairley | Patrick O'Brien |
| Rami Audi | Ron Higuera | Gerry Ourada |
| Robert Cohen | David Hulett | Frank Parolek |
| Timothy Coleman | Cheryl Jones | John Phippen |
| Edward Conrow | Alan Lacour | Garry Roedler |
| Paul R. Croll | Robert MacIver | Joyce A. Statz |
| Mallory Davis | John McGarry | Kenneth Stranc |
| Harpal Dhama | James Moore | Richard H. Thayer |
| Audrey Dorofee | Jerry A. Moore | Karen Valdez |

The following members of the balloting committee voted on this standard:

Edward A. Addy
Barbara K. Beauchamp
Leo Beltracchi
H. Ronald Berlack
Richard E. Biehl
Sandro Bologna
Juris Borzovs
Lawrence Catchpole
Keith Chan
Robert N. Charette
Keith Chow
Antonio M. Cicu
Rosemary Coleman
Paul R. Croll
Martin D'Souza
Gregory T. Daich
Bostjan K. Derganc
Perry R. DeWeese
Harpal Dhama
Dave Dikel
Audrey Dorofee
Carl Einar Dragstedt
Sherman Eagles
Franz D. Engelmann
William Eventoff
Jonathan H. Fairclough
Richard E. Fairley
John W. Fendrich
Jay Forster
John H. Fowler
Andrew Gabb
Julio Gonzalez-Sanz
L. M. Gunther
Jon D. Hagar
George F. Hayhoe
Rick Hefner
Mark Heinrich
Mark Henley
Debra Herrmann
Stan Hopkins
John W. Horch
George Jackelen
Frank V. Jorgensen
Vladan V. Jovanovic
Ronald J. Kohl
Thomas M. Kurihara
J. Dennis Lawrence
Karl Leung
Bob Lewis
Robert MacIver
Stan Magee
Harold Mains
Tomoo Matsubara
Ian R. McChesney
Patrick D. McCray
William McMullen
Denis C. Meredith
James W. Moore
Jerry A. Moore
Finnbarr P. Murphy
Gerald L. Ourada
Mark Paulk
Alexander J. Polack
Ann E. Reedy
Annette D. Reilly
Garry Roedler
Terence P. Rout
Andrew P. Sage
Helmut Sandmayr
Frederico Sousa Santos
Robert J. Schaaf
Hans Schaefer
David J. Schultz
Subrato Sensharma
Robert W. Shillato
Melford E. Smyre
Robert Spillers
Joyce A. Statz
Fred J. Strauss
Toru Takeshita
Richard H. Thayer
Douglas H. Thiele
Booker Thomas
Patricia Trellue
Leonard L. Tripp
Glenn D. Venables
Scott A. Whitmire
John M. Williams
Natalie C. Yopconka
Janusz Zalewski

When the IEEE-SA Standards Board approved this standard on 17 March 2001, it had the following membership:

**Donald N. Heirman,** *Chair*
**James T. Carlo,** *Vice Chair*
**Judith Gorman,** *Secretary*

Chuck Adams
Mark D. Bowman
Clyde R. Camp
Richard DeBlasio
Harold E. Epstein
H. Landis Floyd
Jay Forster*
Howard M. Frazier
James H. Gurney
Raymond Hapeman
Richard J. Holleman
Richard H. Hulett
Lowell G. Johnson
Joseph L. Koepfinger*
Peter H. Lips
Paul J. Menchini
Daleep C. Mohla
Robert F. Munzner
Ronald C. Petersen
Malcolm V. Thaden
Geoffrey O. Thompson
Akio Tojo
Howard L. Wolfman

*Member Emeritus

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

Satish K. Aggarwal, *NRC Representative*
Alan H. Cookson, *NIST Representative*
Donald R. Volzka, *TAB Representative*

Catherine Berger
*IEEE Standards Project Editor*

# Contents

# IEEE Standard for Software Life Cycle Processes—Risk Management

## 1. Overview

This standard prescribes a continuous process for software 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 may be applied to the software 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 IEEE/EIA 12207 series of software life cycle process standards. Annex E, as previously mentioned, is an annotated bibliography of standards and related documents mentioned in the text of this standard.

### 1.1 Scope

This standard describes a process for the management of risk during software acquisition, supply, development, operations, and maintenance. It is intended that both technical and managerial personnel throughout an organization apply this standard.

### 1.2 Purpose

The purpose of this standard is to provide software 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 software life cycle. It is suitable for adoption by an organization for application to all appropriate projects or for use in an individual project. Although the standard is written for the management of risk in software projects, it may also be useful for the management of both system-level and organization-level risks.

This standard is written so that it may be applied in conjunction with the IEEE/EIA 12207 series of standards or applied independently.

### 1.3.1 Application with IEEE/EIA 12207 series

IEEE/EIA 12207.0-1996 is currently the IEEE'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. The IEEE/EIA 12207 series mentions risk and risk management in several places, but does not provide a process for risk management (see Annex D). This risk management standard provides that process. 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 IEEE/EIA 12207.0-1996, 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 the process exists and functions.

When used with IEEE/EIA 12207.0-1996, this standard assumes that the other management and technical processes of IEEE/EIA 12207 perform the treatment of risk. Appropriate relationships to those processes are described.

### 1.3.2 Application independently of IEEE/EIA series

This standard may be used independently of any particular 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.

In those instances where this standard is applied independently of IEEE/EIA 12207.0-1996, 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 software risk management process, activities and tasks. Implementing these requirements or the preparation of software risk management plans or software risk action requests according to this standard does not ensure an absence of software related or other risks. Conformance with this standard does not absolve any party from any social, moral, financial, or legal obligation.

# 2. References

This clause lists the other standards that must be available in order to apply correctly this standard.

This standard shall be used in conjunction with the following publications:

IEEE/EIA 12207.0-1996, IEEE/EIA Standard—Industry Implementation of International Standard ISO/IEC 12207:1995, Standard for Information Technology—Software Life Cycle Processes.[1]

[1]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/).

 

IEEE Std 610.12-1990, IEEE Standard Glossary of Software Engineering Terminology.

ISO/IEC 15026:1998, Information Technology—System and Software Integrity Levels.[2]

NOTES

1—IEEE/EIA 12207.0-1996 is not needed if this standard is being applied independently of IEEE/EIA 12207.
2—ISO/IEC 12207-1995 may be used as a replacement for IEEE/EIA 12207.0-1996.

## 3. Definitions

For the purposes of this standard, the following terms and definitions apply. The Authoritative Dictionary of IEEE Standard Terms [B1][3] and IEEE Std 610.12-1990 should be referenced for terms not defined in this clause.

**3.1 acceptability:** The exposure to loss (financial or otherwise) that an organization is willing to tolerate from a risk.

NOTE—Risk acceptability may apply to an individual risk or to a collection of risks, such as the totality of risks confronting a project or enterprise. Acceptability may differ for different categories of risk and may depend on the cost of treatment or other factors.

**3.2 consequence:** An outcome of an event, hazard, threat or situation.

NOTE—The outcome may be a loss or a gain and may be expressed qualitatively or quantitatively.

**3.3 likelihood:** A quantitative or qualitative expression of the chances that an event will occur.

NOTE—Quantitative expressions may include numerical scales or probabilities.

**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 likelihood of an event, hazard, threat, or situation occurring and its undesirable consequences; a potential problem.

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

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

[2]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/).

[3]The numbers in brackets correspond to those of the bibliography in Annex E.

**3.8 risk exposure:** The potential loss presented to an individual, project, or organization by a risk; a function of the likelihood 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 software risk management standard takes a broader view that includes qualitative expressions of risk exposure.

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

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

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

**3.12 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, likelihood, consequences, estimation scales, confidence of the estimates, treatment, threshold, and an estimate of when the risk will reach its threshold.

**3.13 risk threshold:** The criteria (e.g., a level of risk exposure) against which stakeholders evaluate a risk.

NOTE—Different risk thresholds may be defined for each risk, risk category or combination of risks. Exceeding a risk threshold is a condition that triggers some stakeholder action. *See* **acceptability.**

**3.14 risk treatment:** The process of selecting and implementing risk control options.

**3.15 stakeholder:** A person or group that has an interest in the management of risk.

## 4. Application of this standard

To facilitate use with IEEE/EIA 12207.0-1996, 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.

In the life cycle process framework provided by IEEE/EIA 12207.0, risk management is an "organizational life cycle process." The activities and tasks in an organizational life cycle process are the responsibility of the organization using that process. The organization ensures that the process exists and functions.

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

Software risk management is most effective when used along with organizational risk management processes. 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 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.

## 5. Risk management in the software life cycle

The purpose of the risk management is to identify and mitigate the risks continuously. As a result of successful implementation of risk management

a) The scope of risk management to be performed will be determined.
b) Appropriate risk management strategies will be defined and implemented.
c) Risks will be identified in a strategy and as they develop during the conduct of the project.
d) The risks will be analyzed, and the priority in which to apply resources to monitor these risks will be determined.
e) Risk measures will be defined, applied, and assessed to determine changes in the status of risk and the progress of the monitoring activities.
f) Appropriate action will be taken to reduce or avoid the impact of risk.

### 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.

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 so forth, 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.

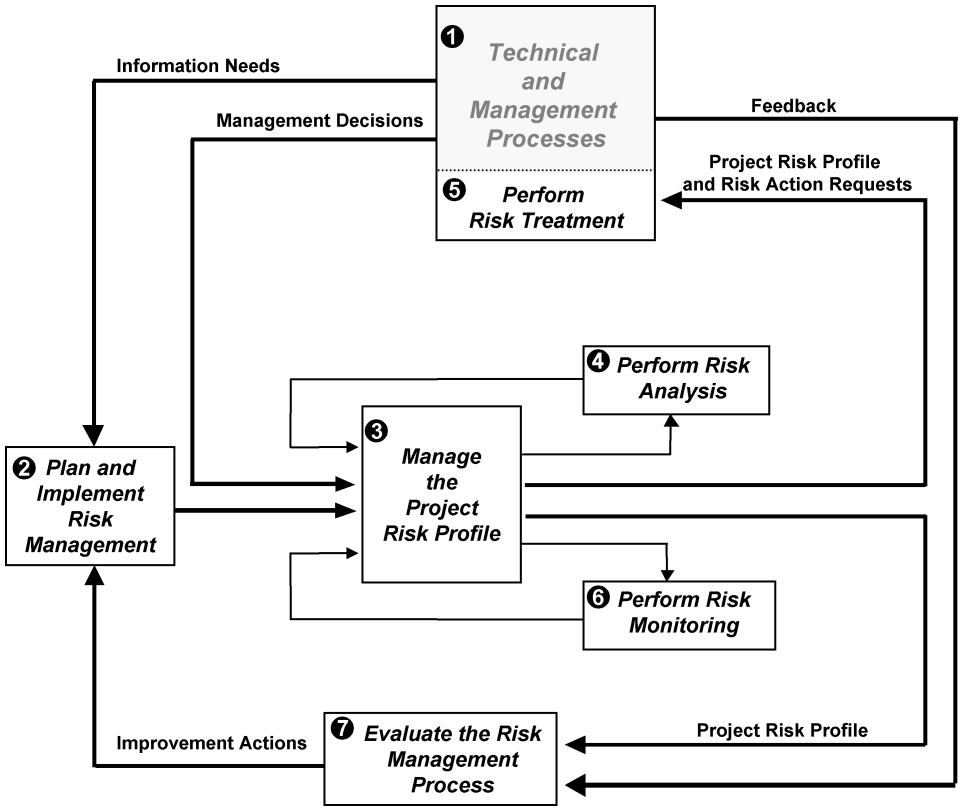


**Figure 1—Risk management process model (informative)**

The project risk profile information is continually updated and maintained through the "perform risk analysis" activity❹, which identifies the risks, determines their likelihood 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 during the "perform risk monitoring" activity❻. In addition, new risks 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 software 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 software risk management process. Where an organizational risk management process exists, the software 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. 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 [B7] requires the documentation of a risk management plan in the software project management plan.

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 accomplished
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 estimate risk likelihood 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 categories to be considered

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

The risk management process should align to 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 software’s 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 risk management context definition 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. Software security, safety, or other categories of software risk that are perceived to be of special importance may be addressed separately.

NOTE—IEEE Std 1228-1994 [B5] may be used in conjunction with this standard to address risks related to software 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 criteria by which the acceptability of a risk must be determined shall be defined and documented in the risk state of each risk.

Risk thresholds are the maximum levels of measured 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 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 [B4] describes the use of integrity levels in planning verification and validation activities. ISO/IEC 15026:1998 discusses the use of software integrity levels.

#### 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 likelihoods, consequences, and risk thresholds
c) The priority ordering of each risk based on criteria supplied by the stakeholders
d) The risk action requests for risks along with the status of their treatment

The 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 likelihood 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 software's 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. Software anomalies, reports on software measures, and other indicators should be continuously reviewed as sources for risks.

NOTE—IEEE Std 1044-1993 [B6] provides useful information regarding anomaly classification. IEEE Std 982.1-1988 [B2] provides useful information regarding software measures related to reliability.

#### 5.1.3.2 Risk estimation

The likelihood 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 likelihood 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 likelihood 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 [B2] provides information that may be useful in defining risk-related measures.

 

### 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.

#### 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 IEEE/EIA 12207.0-1996. 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 IEEE/EIA 12207.0-1996

This alternative subclause applies to all users of this standard who are applying it in conjunction with IEEE/EIA 12207.0-1996.

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 IEEE/EIA 12207.0-1996.

##### 5.1.4.2.2 Risk treatment independent of IEEE/EIA 12207.0-1996

This alternative subclause applies to all users of this standard who are applying it independently of IEEE/EIA 12207.0-1996.

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 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

#### 5.1.5.1 Monitor risk

All risks shall be continuously monitored 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.). 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.

#### 5.1.5.3 Seek new risks

The project shall be continuously monitored for new risks throughout the software's life cycle. New risks 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 causes, their treatment, and the success of the treatments selected shall be collected throughout the software 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 processes should be identified. Where applicable, the process should be improved, the organizational risk management 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.

# 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 software risk management. The risk management plan would meet the intent of IEEE/EIA 12207.0-1996, 5.2.4.5 item k) and IEEE/EIA12207.1-1997, 6.11.3 item l) [B8] that require the inclusion of risk management information in the project management plan. A risk management plan that follows the outline below would also meet the intent of 4.5.4 of IEEE Std 1058-1998 [B7].

## 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, 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 Likelihood

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 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.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 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.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.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.5 Operation process

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

## D.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.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.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.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.10 Tailoring process

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

## D.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 tradeoffs 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] IEEE 100, *The Authoritative Dictionary of the IEEE Standards Terms*, Seventh Edition.

[B2] IEEE Std 982.1-1988, IEEE Standard Dictionary of Measures to Produce Reliable Software.

[B3] 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.*

[B4] 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.*

[B5] 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.*

[B6] IEEE Std 1044-1993, IEEE Standard Classification for Software Anomalies.

*Risk considerations may be useful in classifying anomalies.*

[B7] 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.*

[B8] 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.*

[B9] 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.*

[B10] ISO/TMB DGUIDE 73:2001, Draft Guide on Risk management—Vocabulary—Guidelines for use in standards.

*The terminology used in this standard is consistent with the vocabulary recorded in the draft ISO Guide under preparation by the ISO Technical Management Board. It is expected that this terminology will be widely implemented in ISO and other standards.*