INTERNATIONAL STANDARD

ISO/IEC 16085

IEEE Std 1540-2001

First edition
2004-10-01

Information technology — Software life cycle processes — Risk management

Technologies de l'information — Processus du cycle de vie du logiciel — Gestion des risques

Reference number
ISO/IEC 16085:2004(E)
IEEE Std 1540-2001

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

International Standard ISO/IEC 16085:2004(E)
IEEE Std 1540™-2001

Information technology — Software life cycle processes — Risk management

Sponsor

Software Engineering Standards Committee
of the
IEEE Computer Society

Approved 17 March 2001

IEEE-SA Standards Board

Adopted as an International Standard by the International Organization for Standardization and by the International Electrotechnical Commission

IEEE

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 0-7381-4102-X SH95262
PDF: ISBN 0-7381-4103-8 SS95262

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. 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 IEEE (as IEEE Std 1540-2001) and was adopted, under a special “fast-track procedure”, by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, in parallel with its approval by national bodies of ISO and IEC.

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.

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*

Judith Gorman, *Secretary*

Mark D. Bowman
Chuck Adams
Clyde R. Camp
James T. Carlo
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

Information technology — 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]

