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

PDF disclaimer

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

Adobe is a trademark of Adobe Systems Incorporated.

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

ISO
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

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

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

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

Head of Sales, Marketing &
Information Services
IEC Central Office
3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland
Tel:+41 22 919 02 11
Fax: +41 22 919 03 00
E-mail: info@iec.ch

Institute of Electrical and
Electronics Engineers
Standards Association
Manager, Standards
Intellectual Property
445 Hoes Lane
Piscataway, NJ 08854
E-mail: stds.ipr@ieee.org
Web: www.ieee.org

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.

Authorization to photocopy portions of any individual standard for internal or personal use is granted by the Institute of Electrical and Electronics Engineers, Inc., provided that the appropriate fee is paid to Copyright Clearance Center. To arrange for payment of licensing fee, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

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.

[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/).