

Systems and software engineering — Life cycle processes — Risk management

ICS 35.080

National foreword

This British Standard was published by BSI. It is the UK implementation of ISO/IEC 16085:2006. It supersedes BS ISO/IEC 16085:2004 which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/15, Software and systems engineering.

A list of organizations represented on IST/15 can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 January 2007

© BSI 2007

ISBN 978-0-580-49977-7

Amendments issued since publication

Amd. No.	Date	Comments

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*



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

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

Contents

1. Overview 1

1.1 Scope 1

1.2 Purpose 1

1.3 Field of application 2

1.4 Conformance 2

1.5 Disclaimer 3

2. Normative references 3

3. Definitions 3

4. Application of this standard 6

5. Risk management in the life cycle 6

5.1 Risk management process 6

5.2 Null Clause 15

Annex A (informative) Risk management plan 16

Annex B (informative) Risk action request 19

Annex C (informative) Risk treatment plan 21

Annex D (informative) Application of risk management in the software life cycle 23

Annex E (informative) Annotated bibliography 30

Systems and software engineering — Life cycle processes — Risk management

1. Overview

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

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

1.1 Scope

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

1.2 Purpose

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

1.3 Field of application

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

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

1.3.1 Application with ISO/IEC 12207:1995 series

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

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

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

1.3.2 Application with ISO/IEC 15288:2002 series

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

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

1.3.3 Application independent of ISO/IEC series

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

1.4 Conformance

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

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

1.5 Disclaimer

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

2. Normative references

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

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

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

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

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

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

NOTES

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

2—IEEE/EIA 12207.0-1996 may be used as a replacement for ISO/IEC 12207:1995.²

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

3. Definitions

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

3.1 consequence: An outcome of an event.

NOTES

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

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

3—Consequences can be expressed qualitatively or quantitatively.

[ISO Guide 73:2002, definition 3.1.2]

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

¹ISO/IEC publications are available from the ISO Central Secretariat, Case Postale 56, 1 rue de Varembe, 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/>).

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

NOTES

- 1—The event can be certain or uncertain.
- 2—The event can be a single occurrence or a series of occurrences.
- 3—The probability associated with the event can be estimated for a given period of time.

[ISO Guide 73:2002, definition 3.1.4]

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

NOTES

- 1—ISO 3534-1:1993, definition 1.1, gives the mathematical definition of probability as “a real number in the scale 0 to 1 attached to a random event. It can be related to a long-run relative frequency of occurrence or to a degree of belief that an event will occur. For a high degree of belief, the probability is near 1.”
- 2—Frequency rather than probability may be used in describing risk.
- 3—Degrees of belief about probability can be chosen as classes or ranks, such as
 - rare/unlikely/moderate/likely/almost certain, or
 - incredible/improbable/remote/occasional/probable/frequent.

[ISO Guide 73:2002, definition 3.1.3]

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

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

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

NOTES

- 1—The term “risk” is generally used only when there is at least the possibility of negative consequences.
- 2—In some situations, risk arises from the possibility of deviation from the expected outcome or event.
- 3—See ISO/IEC Guide 51 for issues related to safety.

[ISO Guide 73:2002, definition 3.1.1]

3.6 risk acceptance: The decision to accept a risk.

NOTES

- 1—The verb “to accept” is chosen to convey the idea that acceptance has its basic dictionary meaning.
- 2—Risk acceptance depends on risk criteria.

[ISO Guide 73:2002, definition 3.4.10]

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

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

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

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

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

[ISO Guide 73:2002, definition 3.1.6]

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

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

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

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

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

NOTES

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

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

[ISO Guide 73:2002, definition 3.1.8]

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

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

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

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

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

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

NOTE

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

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

[ISO Guide 73:2002, definition 3.4.1]

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

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

[ISO Guide 73:2002, definition 3.1.5]

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

NOTES

1—The decision-maker is also a stakeholder.

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

[ISO Guide 73:2002, definition 3.2.1]

4. Application of this standard

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

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

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

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

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

5. Risk management in the life cycle

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

- a) The scope of risk management to be performed is determined.
- b) Appropriate risk management strategies are defined and implemented.
- c) Risks are identified as they develop and during the conduct of a project.
- d) Risks are analyzed, and the priority in which to apply resources to treatment of these risks are determined.
- e) Risk measures are defined, applied, and assessed to determine changes in the status of risk and the progress of the treatment activities.
- f) Appropriate treatment is taken to correct or avoid the impact of risk based on its priority, probability, and consequence.