

Australian/New Zealand Standard™

**Information technology—Systems and
software engineering—Life cycle
processes—Risk management**



AS/NZS ISO/IEC 16085:2007

This Joint Australian/New Zealand Standard was prepared by Joint Technical Committee IT-015, Software and Systems Engineering. It was approved on behalf of the Council of Standards Australia on 19 February 2007 and on behalf of the Council of Standards New Zealand on 16 March 2007.
This Standard was published on 28 March 2007.

The following are represented on Committee IT-015:

Australian Computer Society
Australian Electrical and Electronic Manufacturers Association
Australian Society of Technical Communications
Australian Software Metrics Association
Engineers Australia/ACTS Joint Board in Software Engineering
Griffith University
National Association of Testing Authorities Australia
National ICT Australia
New Zealand Organisation for Quality
Software Quality Association, ACT
Software Quality Association, NSW
Systems Engineering Society of Australia
The University of Queensland
University of Auckland, NZ
University of South Australia
University of Technology, Sydney
Vendor Interests, NZ

Keeping Standards up-to-date

Standards are living documents which reflect progress in science, technology and systems. To maintain their currency, all Standards are periodically reviewed, and new editions are published. Between editions, amendments may be issued. Standards may also be withdrawn. It is important that readers assure themselves they are using a current Standard, which should include any amendments which may have been published since the Standard was purchased.

Detailed information about joint Australian/New Zealand Standards can be found by visiting the Standards Web Shop at www.standards.com.au or Standards New Zealand web site at www.standards.co.nz and looking up the relevant Standard in the on-line catalogue.

Alternatively, both organizations publish an annual printed Catalogue with full details of all current Standards. For more frequent listings or notification of revisions, amendments and withdrawals, Standards Australia and Standards New Zealand offer a number of update options. For information about these services, users should contact their respective national Standards organization.

We also welcome suggestions for improvement in our Standards, and especially encourage readers to notify us immediately of any apparent inaccuracies or ambiguities. Please address your comments to the Chief Executive of either Standards Australia or Standards New Zealand at the address shown on the back cover.

This Standard was issued in draft form for comment as DR 06667.

Australian/New Zealand Standard™

Information technology—Systems and software engineering—Life cycle processes—Risk management

First published as AS/NZS ISO/IEC 16085:2007.

COPYRIGHT

© Standards Australia/Standards New Zealand

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher.

Jointly published by Standards Australia, GPO Box 476, Sydney, NSW 2001 and Standards New Zealand, Private Bag 2439, Wellington 6020

ISBN 0 7337 8143 8

PREFACE

This Standard was prepared by the Joint Standards Australia/Standards New Zealand Committee IT-015, Software and Systems Engineering.

The objective of this Standard is to provide software users (technical and managerial personnel) with a process for the management of risk during software acquisition, supply, development, operations, and maintenance.

This Standard is identical with, and has been reproduced from ISO/IEC 16085:2006, *Information technology—Systems and software engineering—Life cycle processes—Risk management*.

As this Standard is reproduced from an international standard, the following applies:

- (a) Its number appears on the cover and title page while the international standard number appears only on the cover.
- (b) In the source text ‘this standard’ should read ‘this Australian/New Zealand Standard’.
- (c) A full point substitutes for a comma when referring to a decimal marker.

References to International Standards should be replaced by references to Australian or Australian/New Zealand Standards, as follows:

<i>Reference to International Standard</i>	<i>Australian/New Zealand Standard</i>
ISO/IEC	AS/NZS ISO/IEC
12207 Information technology—Software life cycle processes	12207 Information technology—Software life cycle processes
15026 Information technology—System and software integrity levels	15026 Information technology—System and software integrity levels
15288 Systems engineering—System life cycle processes	15288 Systems engineering—System life cycle processes

The term ‘informative’ has been used in this Standard to define the application of the appendix to which it applies. An ‘informative’ appendix is only for information and guidance.

CONTENTS

	<i>Page</i>
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

AUSTRALIAN/NEW ZEALAND STANDARD

Information technology—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.

5.1 Risk management process

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

This process consists of the following activities:

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

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

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

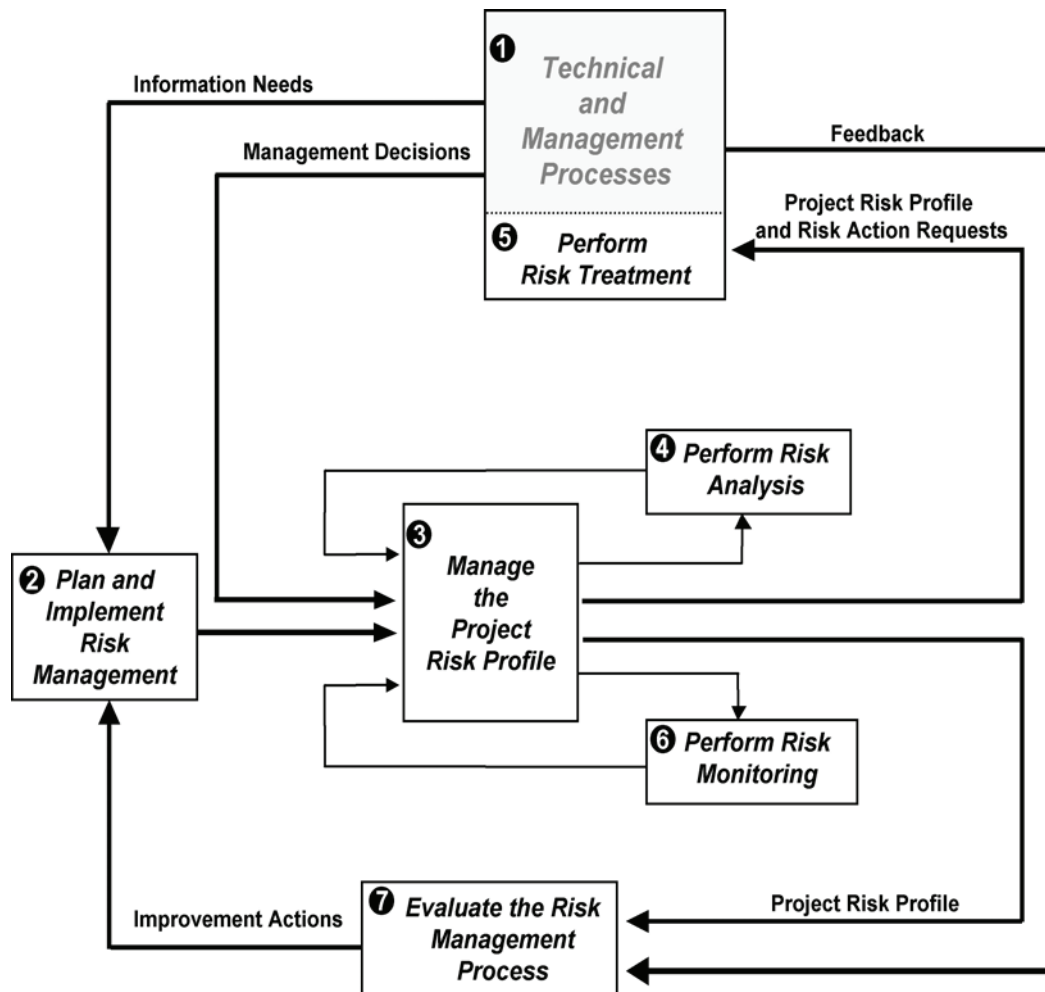


Figure 1—Risk management process model (informative)

Managerial and technical processes involving the stakeholders define the information requirements (i.e., the information the stakeholders require to make informed decisions involving risks) the risk management process must support^①. 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” activity^②, the policies regarding the general guidelines under which risk management will be conducted, the procedures to be used, the specific techniques to be applied, and other matters relevant to risk planning are defined.

In the “manage the project risk profile” activity^③, the current and historical risk management context and risk state information are captured. The project risk profile includes the sum total of all the individual risk profiles (i.e., the current and historical risk information concerning an individual risk), which, in turn, includes all the risk states.

The project risk profile information is continually updated and maintained through the “perform risk analysis” activity^④, which identifies the risks, determines their probability and consequences, determines their risk exposures, and prepares risk action requests recommending treatment for risks determined to be above their risk threshold(s).

Treatment recommendations, along with the status of other risks and their treatment status, are sent to management for review^⑤. Management decides what risk treatment is implemented for any risk found to be unacceptable. Risk treatment plans are created for risks that require treatment. These plans are coordinated with other management plans and other ongoing activities.

All risks are continually monitored until they no longer need to be tracked, e.g., they are retired, during the “perform risk monitoring” activity^⑥. In addition, new risks and risk sources are sought out.

Periodic evaluation of the risk management process is required to ensure its effectiveness. During the “evaluate the risk management process” activity^⑦, 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” activity^②.

The risk management process is applied continuously throughout the product life cycle. However, activities and tasks of the risk management process interact with the individual risks in an iterative manner once the risk management process begins. For example, in the “perform risk analysis” activity^④, a risk may be re-estimated several times during the performance of risk evaluation due to an increase in knowledge about the risk gained during the evaluation task itself. The risk management process is not a “waterfall” process.

5.1.1 Plan and implement risk management

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

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

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

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