FINAL
DRAFT

# INTERNATIONAL STANDARD

# ISO/IEC/IEEE/FDIS 16085

ISO/IEC JTC **1**/SC **7**

Secretariat: BIS

Voting begins on:
**2020-09-21**

Voting terminates on:
**2020-11-16**

# Systems and software engineering — Life cycle processes — Risk management

*Ingénierie des systèmes et du logiciel — Processus du cycle de vie — Gestion des risques*

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

Reference number
ISO/IEC/IEEE/FDIS 16085:2020(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

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

Email: stds.ipr@ieee.org
Website: www.ieee.org

Published in Switzerland

# Contents

Page

# 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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the rules given in the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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.

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see https://patents.iec.c).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 7, *Systems and software engineering*, in cooperation with the Systems and Software Engineering Standards Committee of the IEEE Computer Society, under the Partner Standards Development Organization cooperation agreement between ISO and IEEE.

This edition cancels and replaces ISO/IEC 16085:2006, which has been technically revised.

The main changes compared to ISO/IEC 16085:2006 are as follows:

- Use common terminology, common process names, and common process structure with ISO/IEC/IEEE 15288:2015 and ISO/IEC/IEEE 12207:2017.
- Improve consistency with ISO 31000:2018, which provides generic principles, framework, and process for managing all forms of risk.
- Provide specialized guidance for performing risk management within the context of systems and software engineering projects.

This document is intended to be used in conjunction with ISO/IEC/IEEE 15288:2015, ISO/IEC/IEEE 12207:2017, ISO 31000 and IEC 31010, and is not a replacement.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

# Introduction

This document is an elaboration standard for the risk management process described in ISO/IEC/IEEE 15288 and ISO/IEC/IEEE 12207. This document provides requirements for the tasks and activities of the risk management process in Clause 6, consistent with these life cycle process International Standards. This document provides a definition of the content of the risk management plan (8.1) and risk treatment plan (8.2). This document also provides guidance for how risk management outcomes, activities, and tasks pertain to other processes.

This document prescribes a continuous process for risk management. Clause 1 provides an overview and the purpose, scope, and field of application. Clause 2 lists the normative references. Clause 3 provides terms and definitions. Clause 4 prescribes conformance criteria. Clause 5 describes key concepts and application with other International Standards. Clause 6 elaborates the risk management process as required by ISO/IEC/IEEE 15288 or ISO/IEC/IEEE 12207. Clause 6 also defines required purpose, outcomes, tasks, and activities of the risk management process for application to systems and software engineering projects in an integrated manner as described in Clause 7 and produces the information products described in Clause 8. Clause 7 suggests some typical risk areas, some typical opportunity areas, and some typical treatments for each life cycle process. Clause 8 prescribes the content for the risk management information items. The Bibliography lists informative references that are either referenced by this document or of interest to users of this document.

# Systems and software engineering — Life cycle processes — Risk management

## 1 Scope

### 1.1 Overview

This document:

- provides risk management elaborations for the processes described in ISO/IEC/IEEE 15288 and ISO/IEC/IEEE 12207,
- provides the users of ISO/IEC/IEEE 15288, ISO/IEC/IEEE 12207 and their associated elaboration standards with common terminology and specialized guidance for performing risk management within the context of systems and software engineering projects,
- specifies the required information items that are to be produced through the implementation of risk management process for claiming conformance, and
- specifies the required contents of the information items.

This document provides a universally applicable standard for practitioners responsible for managing risks associated with systems and software over their life cycle. This document is suitable for the management of all risks encountered in any organization or project appropriate to the systems or software projects regardless of context, type of industry, technologies utilized, or organizational structures involved.

This document does not provide detailed information about risk management practices, techniques, or tools which are widely available in other publications. Instead this document focuses on providing a comprehensive reference for integrating the large and wide variety of processes, practices, techniques, and tools encountered in systems and software engineering projects and other lifecycle activities into a unified approach for risk management, with the purpose of providing effective and efficient risk management while meeting the expectations and requirements of organization and project stakeholders.

### 1.2 Purpose

This document provides information on how to design, develop, implement, and continually improve risk management in a systems and software engineering project throughout its life cycle.

### 1.3 Field of application

This document is compatible with risk management as described in ISO/IEC/IEEE 15288 and ISO/IEC/IEEE 12207 and can also be applied in conjunction with ISO 31000. Depending on the scope and context of the systems or software engineering project of interest, there are a number of additional International Standards that can be applicable to the risk management effort including ISO 9001. This document is intended to provide additional information useful in implementing a system for integrated risk management for systems and software engineering projects. 5.2 discusses in more detail how this document can be applied with other standards.

This document is applicable to:

- project teams which use ISO/IEC/IEEE 15288 and ISO/IEC/IEEE 12207 on projects dealing with man-made systems, software-intensive systems, software and hardware products, and services related to those systems and products, regardless of organization or project scope, product(s), methodology, size, or complexity;

- project teams performing risk management activities to aid in ensuring that their application of risk management conforms to ISO/IEC/IEEE 15288 and/or ISO/IEC/IEEE 12207;
- project teams using ISO/IEC/IEEE 15289 on projects dealing with human-made systems, software-intensive systems, software and hardware products, and services related to those systems and products, regardless of organization or project scope, product(s), methodology, size, or complexity; and
- project teams generating information items developed during the application of risk management processes to conform to ISO/IEC/IEEE 15289.

This document can be applied in conjunction with ISO 31000 and IEC 31010 to augment risk management performed within the context of ISO/IEC/IEEE 15288 and/or ISO/IEC/IEEE 12207.

## 2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document, (including any amendments) applies.

ISO/IEC/IEEE 12207:2017, *Systems and software engineering — Software life cycle processes*

ISO/IEC/IEEE 15288:2015, *Systems and software engineering — System life cycle processes*

## 3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO, IEC, and IEEE maintain terminological databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at https://www.iso.org/
- IEC Electropedia: available at http://www.electropedia.org/
- IEEE Standards Dictionary Online: available at: http://dictionary.ieee.org

NOTE Definitions for other system and software engineering terms typically can be found in ISO/IEC/IEEE 24765, available at www.computer.org/sevocab.

### 3.1
**consequence**

outcome of an event affecting one or more *stakeholders* (3.11)

Note 1 to entry: An event can lead to a range of consequences.

Note 2 to entry: A consequence can be certain or uncertain and can have positive or negative effects on *objectives* (3.3).

Note 3 to entry: Consequences can be expressed qualitatively or quantitatively.

Note 4 to entry: Initial consequences can escalate through follow-on effects.

[SOURCE: ISO Guide 73:2009, 3.6.1.3, modified — In the definition, "objectives" has been replaced by "one or more stakeholders"; the notes to entry have been reordered.]

**3.2**
**likelihood**
chance of something happening

Note 1 to entry: In *risk* (3.5) management terminology, the word “likelihood” is used to refer to the chance of something happening, whether defined, measured, or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period).

Note 2 to entry: The English term “likelihood” does not have a direct equivalent in some languages; instead, the equivalent of the term “probability” is often used. However, in English, “probability” is often narrowly interpreted as a mathematical term. Therefore, in risk management terminology, “likelihood” is used with the intent that it should have the same broad interpretation as the term “probability” has in many languages other than English.

[SOURCE: ISO Guide 73:2009, 3.6.1.1]

**3.3**
**objective**
result to be achieved

Note 1 to entry: An objective can be strategic, tactical, or operational.

Note 2 to entry: An objective can relate to different disciplines (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product, and process).

Note 3 to entry: An objective can be expressed in other ways, e.g. as an intended outcome, a purpose, an operational criterion, an objective related to *risk* (3.5) management, or by the use of other words with similar meaning (e.g. aim, goal, or target).

Note 4 to entry: Objectives related to risk management are set by the *organization* (3.4), consistent with the risk policy, to achieve specific results.

[SOURCE: ISO/IEC 19770-1:2017, 3.37, modified — In Note 3 to entry, "asset management objective" has been replaced by "objective related to risk management"; the original Note 4 to entry has been replaced by a new one.]

**3.4**
**organization**
person or group of people that has its own functions with responsibilities, authorities, and relationships to achieve its *objectives* (3.3)

Note 1 to entry: The concept of organization includes, but is not limited to sole-trader, company, corporation, firm, enterprise, authority, partnership, association, charity or institution, or part or combination thereof, whether incorporated or not, public or private.

[SOURCE: ISO 9000:2015, 3.2.1, modified — Note 2 to entry has been removed.]

**3.5**
**risk**
effect of uncertainty on *objectives* (3.3)

Note 1 to entry: An effect is a deviation from the expected — positive or negative. A positive effect is also known as an opportunity.

Note 2 to entry: Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product, and process).

Note 3 to entry: Risk is often characterized by reference to potential events and *consequences* (3.1), or a combination of these.

Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated *likelihood* (3.2) of occurrence.

Note 5 to entry: Uncertainty is the state, even partial, of deficiency of information related to understanding or knowledge of an event, its consequence, or likelihood.

[SOURCE: ISO Guide 73:2009, 1.1, modified — In Note 1 to entry, the last sentence has been added.]

### 3.6
**risk criteria**
terms of reference against which the significance of a *risk* (3.5) is evaluated

Note 1 to entry: Risk criteria are based on organizational *objectives* (3.3), and external and internal context.

Note 2 to entry: Risk criteria can be derived from standards, laws, policies, and other requirements.

[SOURCE: ISO Guide 73:2009, 3.3.1.3]

### 3.7
**risk exposure**
potential loss presented to an individual, project, or *organization* (3.4) by a *risk* (3.5)

Note 1 to entry: Risk exposure is commonly defined as the product of a probability and the magnitude of a *consequence* (3.1), that is, an expected value or expected exposure."

### 3.8
**risk profile**
description of any set of *risks* (3.5)

Note 1 to entry: The set of risks can contain those that relate to the whole *organization* (3.4), part of the organization, or as otherwise defined.

Note 2 to entry: The phrase "as otherwise defined" includes one or more projects.

[SOURCE: ISO Guide 73:2009, 3.8.2.5, modified — Note 2 to entry has been added.]

### 3.9
**risk threshold**
measure of the level of uncertainty or the level of impact at which a *stakeholder* (3.11) may have a specific interest

Note 1 to entry: Different risk thresholds can be defined for each risk, risk category or combination of risks, based on differing *risk criteria* (3.6). Below that risk threshold, the *organization* (3.4) will accept the *risk* (3.5). Above that risk threshold, the organization will not tolerate the risk;

### 3.10
**risk tolerance**
degree, amount, or volume of *risk* (3.5) that an *organization* (3.4) or individual will withstand

[SOURCE: ISO/IEC/IEEE 24765:2017, 3.3543]

### 3.11
**stakeholder**
individual or *organization* (3.4) having a right, share, claim, or interest in a system or in its possession of characteristics that meet their needs and expectations

EXAMPLE End users, end user organizations, supporters, developers, producers, trainers, maintainers, disposers, acquirers, supplier organizations and regulatory bodies.

Note 1 to entry: Some stakeholders can have interests that oppose each other or oppose the system.

[SOURCE: ISO/IEC/IEEE 12207:2017, 3.1.59]

# 4 Conformance

## 4.1 Intended usage

This document provides a definition of the content of the risk management plan (8.1) and risk treatment plan (8.2). It also provides requirements for the tasks and activities of the risk management process in Clause 6, consistent with the requirements of ISO/IEC/IEEE 15288 and ISO/IEC/IEEE 12207. Users of this document can claim conformance to the process provisions or to the information item provisions, or both.

NOTE Requirements of this document are marked by the use of the verb “shall”. Recommendations are marked by the use of the verb “should". Permissions are marked by the use of the verb “may”.

## 4.2 Conformance to information items

A claim of conformance to information items to this document is equivalent to claiming conformance to the information item content requirements cited in Clause 8.

## 4.3 Conformance to process

A claim of conformance to the process provisions of this document implies claiming conformance to the risk management process from ISO/IEC/IEEE 15288 and ISO/IEC/IEEE 12207 as elaborated in Clause 6.

## 4.4 Full conformance

A claim of full conformance to this document is equivalent to claiming conformance to the information item content requirements cited in Clause 8 and the risk management process of ISO/IEC/IEEE 15288 and ISO/IEC/IEEE 12207 elaborated in Clause 6.

# 5 Key concepts and application

## 5.1 Key concepts

### 5.1.1 Risk and opportunity

In Clause 3, risk is defined as the “effect of uncertainty on objectives.” Risks can be either positive or negative because an effect is a deviation from the expected and therefore can be positive or negative. When the effect is positive, it is often considered an opportunity. Opportunity is used if there is a positive effect from uncertainty.

However, in common usage, risk generally means a negative effect. This document uses this more common interpretation of risk where there is a negative effect. Therefore, treatments will commonly be mitigations. The management and treatment of both risks and opportunities may or may not use the same process or stakeholders. Risks, threats, and opportunities should be understood and managed so as to maximize benefits and minimize negatives.

### 5.1.2 Project and organizational specific terminology

The precise language used by a specific systems or software engineering project can vary depending on organizational factors and context and may not be fully consistent with the definitions used by this document. In this situation, the project risk management plan should identify, analyze, and address the inconsistencies between the organization’s terminology and the terminology in this document.