

# DRAFT INTERNATIONAL STANDARD

## ISO/IEC/IEEE/DIS 16085

ISO/IEC JTC 1/SC 7

Secretariat: **BIS**

Voting begins on:  
**2020-03-17**

Voting terminates on:  
**2020-06-09**

---

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

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

ICS: 35.080

**iTeh STANDARD PREVIEW**  
(standards.iteh.ai)  
Full standard:  
<https://standards.iteh.ai/catalog/standards/sist/7df2e52d-0a70-4ee7-a28b-137450e3a009/iso-iec-ieee-dis-16085>

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

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.

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.

This document is circulated as received from the committee secretariat.



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

© ISO/IEC 2020  
© IEEE 2020

**iTeh STANDARD PREVIEW**  
(standards.iteh.ai)  
Full standard:  
<https://standards.iteh.ai/catalog/standards/sist/7df2e52d-0a70-4ee7-a28b-137450e3a009/iso-iec-ieee-dis-16085>



**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2020

© IEEE 2020

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO or IEEE at the respective address below or ISO's member body in the country of the requester.

ISO copyright office  
CP 401 • Ch. de Blandonnet 8  
CH-1214 Vernier, Geneva  
Phone: +41 22 749 01 11  
Fax: +41 22 749 09 47  
Email: [copyright@iso.org](mailto:copyright@iso.org)  
Website: [www.iso.org](http://www.iso.org)

Published in Switzerland

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

Email: [stds.ipr@ieee.org](mailto:stds.ipr@ieee.org)  
Website: [www.ieee.org](http://www.ieee.org)

# Contents

Page

<b>Foreword</b>	<b>v</b>
<b>Introduction</b>	<b>vii</b>
<b>1 Overview</b>	<b>1</b>
1.1 Scope	1
1.2 Purpose	1
1.3 Field of application	1
<b>2 Normative references</b>	<b>2</b>
<b>3 Terms and definitions</b>	<b>2</b>
<b>4 Conformance</b>	<b>5</b>
4.1 Intended Usage	5
4.2 Conformance to information items	5
4.3 Conformance to process	5
4.4 Full conformance	5
<b>5 Key concepts and application</b>	<b>5</b>
5.1 Key concepts	5
5.1.1 Risk and opportunity	5
5.1.2 Project and organizational specific terminology	5
5.1.3 Systems and software	6
5.1.4 Uncertainty and its relationship to risk	6
5.1.5 Complexity and its relationship to risk	6
5.1.6 Risk management above the project level	6
5.1.7 Purpose and principles for risk management	6
5.2 Application	7
5.2.1 Application with ISO/IEC/IEEE 15288 or ISO/IEC/IEEE 12207	8
5.2.2 Application with ISO 31000	8
5.2.3 Application with ISO 9001	8
5.2.4 Application with other ISO, IEC, ISO/IEC, and ISO/IEC/IEEE standards	9
<b>6 Risk management process</b>	<b>9</b>
6.1 Purpose	9
6.2 Process	9
6.3 Outcomes	11
6.4 Activities and tasks	11
6.4.1 Plan risk management	11
6.4.2 Manage the risk profile	12
6.4.3 Analyze risks	13
6.4.4 Treat risks	16
6.4.5 Monitor risks	18
6.4.6 Evaluate the Risk Management process	18
<b>7 Risk management in life cycle processes</b>	<b>19</b>
7.1 Overview	19
7.2 Risk management in agreement processes	19
7.2.1 Acquisition Process	19
7.2.2 Supply Process	21
7.3 Risk management in organizational project-enabling processes	21
7.3.1 Life cycle model management process	22
7.3.2 Infrastructure management process	22
7.3.3 Portfolio management process	23
7.3.4 Human resource management process	24
7.3.5 Quality management process	24
7.3.6 Knowledge management process	25
7.4 Risk management in technical management processes	26
7.4.1 Project planning process	26

7.4.2	Project assessment and control process .....	27
7.4.3	Decision management process .....	28
7.4.4	Risk management process .....	29
7.4.5	Configuration management process .....	29
7.4.6	Information management process .....	31
7.4.7	Measurement process .....	31
7.4.8	Quality assurance process .....	32
7.5	Risk management in technical processes .....	33
7.5.1	Business or mission analysis process .....	33
7.5.2	Stakeholder needs and requirements definition process .....	34
7.5.3	System/Software requirements definition process .....	35
7.5.4	Architecture definition process .....	36
7.5.5	Design definition process .....	37
7.5.6	System analysis process .....	38
7.5.7	Implementation process .....	39
7.5.8	Integration process .....	39
7.5.9	Verification process .....	40
7.5.10	Transition process .....	41
7.5.11	Validation process .....	42
7.5.12	Operation process .....	43
7.5.13	Maintenance process .....	43
7.5.14	Disposal process .....	44
7.6	Tailoring .....	45
7.6.1	.....	45
<b>8</b>	<b>Information items .....</b>	<b>46</b>
8.1	Risk management plan .....	46
8.1.1	Purpose .....	46
8.1.2	Risk management plan outline .....	46
8.2	Risk treatment plan .....	47
8.2.1	Purpose .....	47
8.2.2	Risk treatment plan outline .....	48
	<b>Bibliography .....</b>	<b>49</b>

## 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.

IEEE (Institute for Electrical and Electronics Engineers) 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.

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 editorial rules of the ISO/IEC Directives, Part 2 (see [www.iso.org/directives](http://www.iso.org/directives)).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO 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](http://www.iso.org/patents)).

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

For an explanation on 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 the following URL: [www.iso.org/iso/foreword.html](http://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 IEEE Computer Society Systems and Software Engineering Standards Committee, under the Partner Standards Development Organization cooperation agreement between ISO and IEEE. The main task of ISO/IEC JTC 1 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.

This third edition cancels and replaces the second edition (ISO/IEC/IEEE 16085:2006), which has been technically revised. This revision was started because of:

- revisions of ISO/IEC/IEEE 15288:2015 and ISO/IEC/IEEE 12207:2017. The purpose of these revisions is to use common terminology, use common process names, where applicable, common process structure, and evolve towards the harmonization of the standards while allowing backward compatibility; and
- creation and revision of ISO 31000 series. This includes ISO 31000:2018 *Risk Management – Guidelines* which provides generic principles, framework, and process for managing all forms of risk.

This document was developed with the following goals:

- provide 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.

**iTeh STANDARD PREVIEW**  
(standards.iteh.ai)  
Full standard:  
<https://standards.iteh.ai/catalog/standards/sist/7df2e52d-0a70-4ee7-a28b-137450e3a009/iso-iec-ieee-dis-16085>

## Introduction

This document is an elaboration standard for the risk management process described in ISO/IEC/IEEE 15288:2015 *Systems and Software Engineering – System life cycle processes* and ISO/IEC/IEEE 12207:2017 *Systems and Software Engineering – Software life cycle processes*. This document provides normative 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 normative 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 15288:2015 or ISO/IEC/IEEE 12207:2017. [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. There is a Bibliography which lists informative references that are either referenced by this document or of interest to users of this document.

iTeh STANDARD PREVIEW  
(standards.iteh.ai)  
Full standard:  
<https://standards.iteh.ai/catalog/standards/sist/16085-2020/iso-iec-ieee-dis-16085-2020>  
0a70-4ee7-a28b-137450e3a009/iso-iec-ieee-dis-16085-2020

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

Full standard:  
<https://standards.iteh.ai/catalog/standards/sist/7df2e52d-0a70-4ee7-a28b-137450e3a009/iso-iec-ieee-dis-16085>



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

## 1 Overview

### 1.1 Scope

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

- provides risk management elaborations for the processes described in ISO/IEC/IEEE 15288:2015 and ISO/IEC/IEEE 12207:2017,
- 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 may 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 may be applicable to the risk management effort including ISO 9001:2015. This document is intended to provide additional information useful in implementing a system for integrated risk management for systems and software engineering projects. [Clause 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 15288:2015 and ISO/IEC/IEEE 12207:2017 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 15288:2015 and/or ISO/IEC/IEEE 12207:2017,
- 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 15289.

This document may 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:

- IEC Electropedia: available at <http://www.electropedia.org/>
- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEEE Standards Dictionary Online: available at <https://ieeexplore.ieee.org/browse/standards/dictionary>

NOTE Definitions for other system and software engineering terms typically can be found in ISO/IEC/IEEE 24765, available at [www.computer.org/sevocab](http://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 -- term cross-references updated]

**3.2****likelihood**

chance of something happening

Note 1 to entry: In risk 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 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, consistent with the risk policy, to achieve specific results.

[SOURCE: ISO/IEC 19770-1:2017, 3.37, modified -- Note 3 to entry: removed reference to asset management and made editorial revisions. Original Note 4 to entry replaced.]

**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 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, 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 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/IEC/IEEE 12207:2017 and ISO/IEC/IEEE 15288:2015]

### 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, 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, 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, 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]

### 3.9

#### **risk threshold**

1. measure of the level of uncertainty or the level of impact at which a *stakeholder* (3.11) may have a specific interest. Below that risk threshold, the organization will accept the *risk* (3.5). Above that risk threshold, the organization will not tolerate the *risk* (3.5); 2. condition that triggers some *stakeholder* (3.11) action

Note 1 to entry: Different risk thresholds can be defined for each risk, risk category or combination of risks, based on differing risk criteria.

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

### 3.10

#### **risk tolerance**

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

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

### 3.11

#### **stakeholder**

individual or organization 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 and ISO/IEC/IEEE 15288:2015 ]

## 4 Conformance

### 4.1 Intended Usage

This document provides a normative definition of the content of the Risk Management Plan (8.1) and Risk Treatment Plan (8.2). It also provides normative requirements for the tasks and activities of the risk management process in [clause 6](#), consistent with the requirements of ISO/IEC/IEEE 15288:2015 and ISO/IEC/IEEE 12207:2017. 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 15288:2015 and ISO/IEC/IEEE 12207:2017 as elaborated in [clause 6](#) of this document.

### 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 15288:2015 and ISO/IEC/IEEE 12207:2017 elaborated in [clause 6](#) of this document.

## 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 as defined 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 definition 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, it is important that the project risk management plan identifies, analyzes, and addresses the inconsistencies between the organization’s terminology and the terminology in this document.