



BSI Standards Publication

Systems and software engineering — Life cycle processes — Risk management

National foreword

This British Standard is the UK implementation of ISO/IEC/IEEE 16085:2021. It supersedes BS ISO/IEC 16085:2006, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/15/-/3, Life cycle management.

A list of organizations represented on this committee can be obtained on request to its committee manager.

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

© The British Standards Institution 2021
Published by BSI Standards Limited 2021

ISBN 978 0 539 00198 3

ICS 35.080

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 2021.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------

INTERNATIONAL
STANDARD

ISO/IEC/
IEEE
16085

First edition
2021-01

Systems and software engineering — Life cycle processes — Risk management

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



Reference number
ISO/IEC/IEEE 16085:2021(E)

Documents
© ISO/IEC 2021
© IEEE 2021



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2021

© IEEE 2021

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
Email: copyright@iso.org
Website: 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
Website: www.ieee.org

Contents

Page

Foreword	v
Introduction	vii
1 Scope	1
1.1 Overview	1
1.2 Purpose	1
1.3 Field of application	1
2 Normative references	2
3 Terms and definitions	2
4 Conformance	5
4.1 Intended usage	5
4.2 Conformance to information items	5
4.3 Conformance to process	5
4.4 Full conformance	5
5 Key concepts and application	5
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 General	7
5.2.2 Application with ISO/IEC/IEEE 15288 or ISO/IEC/IEEE 12207	8
5.2.3 Application with ISO 31000	8
5.2.4 Application with ISO 9001	8
5.2.5 Application with other ISO, IEC, ISO/IEC, and ISO/IEC/IEEE standards	9
6 Risk management process	9
6.1 Purpose	9
6.2 Process	9
6.3 Outcomes	11
6.4 Activities and tasks	11
6.4.1 General	11
6.4.2 Plan risk management	11
6.4.3 Manage the risk profile	12
6.4.4 Analyze risks	13
6.4.5 Treat risks	16
6.4.6 Monitor risks	18
6.4.7 Evaluate the risk management process	18
7 Risk management in life cycle processes	19
7.1 Overview	19
7.2 Risk management in agreement processes	19
7.2.1 General	19
7.2.2 Acquisition process	19
7.2.3 Supply Process	20
7.3 Risk management in organizational project-enabling processes	21
7.3.1 General	21
7.3.2 Life cycle model management process	22
7.3.3 Infrastructure management process	22
7.3.4 Portfolio management process	23
7.3.5 Human resource management process	23

7.3.6	Quality management process.....	24
7.3.7	Knowledge management process.....	24
7.4	Risk management in technical management processes.....	25
7.4.1	General.....	25
7.4.2	Project planning process.....	25
7.4.3	Project assessment and control process.....	26
7.4.4	Decision management process.....	27
7.4.5	Risk management process.....	27
7.4.6	Configuration management process.....	28
7.4.7	Information management process.....	29
7.4.8	Measurement process.....	30
7.4.9	Quality assurance process.....	30
7.5	Risk management in technical processes.....	31
7.5.1	General.....	31
7.5.2	Business or mission analysis process.....	31
7.5.3	Stakeholder needs and requirements definition process.....	32
7.5.4	System/Software requirements definition process.....	33
7.5.5	Architecture definition process.....	34
7.5.6	Design definition process.....	35
7.5.7	System analysis process.....	35
7.5.8	Implementation process.....	36
7.5.9	Integration process.....	37
7.5.10	Verification process.....	37
7.5.11	Transition process.....	38
7.5.12	Validation process.....	39
7.5.13	Operation process.....	39
7.5.14	Maintenance process.....	40
7.5.15	Disposal process.....	41
7.6	Tailoring process.....	41
7.6.1	Typical risk areas.....	41
7.6.2	Typical opportunity areas.....	42
7.6.3	Typical treatments.....	42
8	Information items.....	42
8.1	Risk management plan.....	42
8.1.1	Purpose.....	42
8.1.2	Risk management plan outline.....	42
8.2	Risk treatment plan.....	44
8.2.1	Purpose.....	44
8.2.2	Risk treatment plan outline.....	44
	Bibliography.....	46
	IEEE Notices and Abstract.....	48

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.

5.1.3 Systems and software

It is a fundamental premise of this document that software always exists in the context of a system. Since software does not operate without hardware, the processor upon which the software is executed can be considered as part of the system. Alternatively, hardware or services hosting the software system and handling communications with other systems can also be viewed as enabling systems or external systems in the operating environment.

[ISO/IEC/IEEE 12207:2017 5.2.1]

5.1.4 Uncertainty and its relationship to risk

Risk and uncertainty are related. Higher levels of uncertainty inherent in large complex systems and software engineering projects require commensurate levels of risk management.

The systems and software engineering life cycle processes provide a structure that directly addresses uncertainty by defining, clarifying, communicating, and gaining consensus regarding not only the system-of-interest being realized, but also the processes, activities, resources, and individual roles and responsibilities utilized for its realization.

By integrating risk management with systems and software engineering life cycle processes, risks and uncertainties can be more efficiently and effectively identified, analyzed, and treated.

5.1.5 Complexity and its relationship to risk

Systems which are more complex typically have greater uncertainty. Catastrophic events often result not from a single cause but from interconnected risk factors and cascading failures. Each risk factor taken in isolation might not cause a disaster, but risk factors working in synergy can. Complex, interconnected systems generate many, sometimes unexpected or counterintuitive vulnerabilities. Where a small, localized, single event can trigger cascading failures, then a small, localized, single intervention can also provide a mitigation. In these situations, to adequately perform risk management requires a deep understanding of how the behaviour of a complex system or system of systems emerges from its many constituent parts. Therefore, it is prudent to integrate risk management with the systems and software engineering life cycle processes to more efficiently and effectively manage system complexities and their associated risks.

5.1.6 Risk management above the project level

This document emphasizes risk management at the project level using the ISO/IEC/IEEE 12207 or ISO/IEC/IEEE 15288 processes. ISO 31000 provides material for organizations which are implementing risk management at both the organizational and project level. Because external organizational risks can affect the project, both a project and organizational perspective should be considered when performing risk management.

5.1.7 Purpose and principles for risk management

Integrating risk management with all organizational processes improves the performance of risk management while gaining efficiencies.

ISO 31000 applies to all industries and sectors. Its purpose and basic principle are the creation and protection of value. It is applicable at all levels in any type of organization. In the field of systems and software engineering, the framework for the creation of value is set by ISO/IEC/IEEE 15288 and ISO/IEC/IEEE 12207, the core standards in their field. Within the framework defined by ISO/IEC/IEEE 15288 and ISO/IEC/IEEE 12207, this document's purpose and basic principle are the protection of systems and software engineering value. When the possibility of harm or hazard exists, risk management prioritizes focus on the reduction of the negative outcomes.

These principles derived from ISO 31000 provide guidance on the characteristics of efficient and effective risk management, communicating risk management's value, and explaining risk management's

intention and purpose. These principles are the foundation for managing risk and should be considered when establishing an organization's or project's risk management framework and processes. The principles described below better enable a project, at all levels, to manage the effects of uncertainty on its objectives:

- Integrated: Risk management is an integral part of all organizational activities.
- Structured and comprehensive: A structured and comprehensive approach to risk management that addresses all areas of the organization and project contributes to consistent and comparable results.
- Customized: The risk management framework and processes are customized and proportionate to the organization's external and internal context, as well as being related to its objectives.
- Inclusive: Appropriate and timely involvement of stakeholders enables their knowledge, views and perceptions to be considered. This results in improved awareness and informed risk management.
- Dynamic: Risks can emerge, change, or disappear as an organization's external and internal context changes. Risk management anticipates, detects, acknowledges, and responds to those changes and events in an appropriate and timely manner.
- Best available information: The inputs to risk management are based on historical and current information, as well as on future expectations. Risk management explicitly takes into account any limitations and uncertainties associated with such information and expectations. Information should be timely, clear, and available to relevant stakeholders.
- Human and cultural factors: Human behaviour and culture significantly influence all aspects of risk management at each level and stage.
- Continual improvement: Risk management is continually improved through learning, experience, and review/analysis of appropriate measurements.

5.2 Application

5.2.1 General

This document describes an integrated approach for implementing, performing, and continually improving risk management as applied to systems or software engineering projects. The concepts, methods, and application instructions described in this document are intended to be applied in conjunction with other risk management practices and systems, and with other standards, processes, and practices applicable to systems and software engineering projects and programs.

Risk management is most effective when performed as an integral part of all organizational processes. The risk management process covers all aspects of organizational and project work, the project outcome ("the realized system"), and the environment in which the realized system will operate. However, the risk management process is also applicable in cases where the user is only concerned about one or more selected aspects of the work, the outcome, or the environment. For example, the risk management process is applicable in a case where the user's concern is limited to the data security aspect of the realized system. Systems and software engineering projects can utilize a number of ISO, IEC, ISO/IEC, and ISO/IEC/IEEE International Standards. This document is an elaboration for the following International Standards which define risk management processes:

- ISO/IEC/IEEE 15288
- ISO/IEC/IEEE 12207

This document can be used in conjunction with the following International Standards which discuss risk management:

- ISO 31000

— ISO 9001

Additional International Standards can apply based on the unique scope and context of a particular systems or software engineering project. Additionally, depending on conformance requirements and flexibility for tailoring and/or applying various International Standards independently, a variety of application scenarios may be available to the systems or software engineering project. The application of this document in conjunction with or independent of other International Standards is determined as appropriate for the systems or software engineering project of interest.

5.2.2 Application with ISO/IEC/IEEE 15288 or ISO/IEC/IEEE 12207

ISO/IEC/IEEE 15288 and ISO/IEC/IEEE 12207 establish a common framework of required process purposes and outcomes. Each also includes required activities and tasks to fulfil those processes. They define a set of processes and associated terminology from an engineering viewpoint.

The process framework defined in ISO/IEC/IEEE 15288 and ISO/IEC/IEEE 12207 includes risk management as one of the life cycle processes within the framework. This document is designed to be compatible with risk management as defined in ISO/IEC/IEEE 15288 and ISO/IEC/IEEE 12207. This document serves to:

- facilitate the implementation of a systems engineering project risk management process conforming to ISO/IEC/IEEE 15288 and ISO/IEC/IEEE 12207;
- facilitate the implementation of a project risk management process for organizations and projects conforming to ISO/IEC/IEEE 15288, and ISO/IEC/IEEE 12207 and ISO 31000 (and/or other International Standards);
- integrate or establish more effective interfaces between the systems engineering risk management process and other risk management processes, including project risk management, enterprise risk management, product-specific risk management, health and safety safety-related risk management, and information security-related risk management.

5.2.3 Application with ISO 31000

ISO 31000 provides principles, framework and a process for managing risk. It can be used by any organization regardless of its size, activity, or sector. ISO 31000 is intended to help organizations increase the likelihood of achieving objectives, improve the identification of opportunities and threats and effectively allocate and use resources for risk treatment. However, ISO 31000 cannot be used for certification purposes, nor does it provide guidance for internal or external audit programs. It does, however, provide guidance for establishing both a risk management framework and risk management process which may be subject to audit under management system programs, such as ISO 9001 or ISO/IEC 27001.

With respect to this document, ISO 31000 provides overarching understanding and guidance for the design, implementation, and continual improvement of a risk management framework for systems and software engineering projects. The concepts, methods, and application instructions contained in this document are intended to facilitate the tailored application of ISO 31000 specifically for the systems or software engineering project under consideration.

5.2.4 Application with ISO 9001

ISO 9001 provides the requirements for implementing quality management systems. It makes it explicit that risk-based thinking should be applied throughout the quality management system. Risk-based thinking helps to ensure that risk management is applied and integrated holistically with other life cycle processes in a disciplined approach that allows efficient and effective implementation to address both positive and negative events. This document describes such a disciplined approach.

5.2.5 Application with other ISO, IEC, ISO/IEC, and ISO/IEC/IEEE standards

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. For example, the types of International Standards could include:

- Additional International Standards related to project, program and other organizational system management such as ISO 21500.
- International Standards applicable to the specific industry, technologies, or activities that are part of the scope of the systems or software engineering project. In particular those that relate to the performance of risk management, functional safety, and security practices applicable to specific industries and for specific types of products or equipment. For example, ISO 14971, ISO 13485, and ISO 17666.
- International Standards that support risk management, including those regarding practices, analysis, tools, and techniques for risk, safety, security, and dependability (e.g. risk assessment, hazard analysis, fault tree analysis, reliability prediction, measurement process, etc.) such as IEC 31010 and ISO/IEC TR 33015. IEC 31010 discusses the challenges of assessing risk in various situations and several ways a value for level of risk can be obtained. The techniques described in IEC 31010 may be used when there is a need to identify risk or when a more in depth understanding of the risks and opportunities are needed.

Applicable additional International Standards can be identified as part of the systems or software project stakeholder needs and expectations, and system requirements definition processes.

6 Risk management process

6.1 Purpose

The purpose of the risk management process is to identify, analyze, treat and monitor risks continually. The risk management process is a continual process for systematically addressing risk throughout the life cycle of a system, product, or service. It can be applied to risks related to the acquisition, development, maintenance, or operation of a system.

[ISO/IEC/IEEE 15288:2015 6.3.4.1 and ISO/IEC/IEEE 12207:2017 6.3.4.1 with editorial modifications]

6.2 Process

The Life Cycle Model Management process of ISO/IEC/IEEE 12207 and ISO/IEC/IEEE 15288 contains an activity to establish a risk management process for the organization performing the project of interest.

In the course of a project, risk handling may impact everyone in the organization and therefore risk management is everyone's business. Whatever project action is taken, big or small, or whatever project situation is encountered, people should ask the question, and the organization should answer, whether the action has consequences that could adversely affect the project work, the project outcome, or the environment in which the system or software will be implemented.

The risk management process described in this clause is applicable when the potential of an adverse impact or positive opportunity is strong enough that it would put at risk any explicit project, organizational, system, or software objectives.

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 corresponding boxes in [Figure 1](#).