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

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC/IEEE 16085:2021

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

© ISO/IEC 2021
© IEEE 2021

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC/IEEE 16085:2021

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

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

© ISO/IEC 2021 – All rights reserved
© IEEE 2021 – All rights reserved

Contents

Page

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC/IEEE 16085:2021

© ISO/IEC 2021 – All rights reserved
© IEEE 2021 – All rights reserved

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC/IEEE 16085:2021

© ISO/IEC 2021 – All rights reserved
© IEEE 2021 – All rights reserved

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.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC/IEEE 16085:2021

© ISO/IEC 2021 – All rights reserved
© IEEE 2021 – All rights reserved

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.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC/IEEE 16085:2021

© ISO/IEC 2021 – All rights reserved
© IEEE 2021 – All rights reserved

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.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC/IEEE 16085:2021

© ISO/IEC 2021 – All rights reserved
© IEEE 2021 – All rights reserved

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC/IEEE 16085:2021

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

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC/IEEE 16085:2021

© ISO/IEC 2021 – All rights reserved
© IEEE 2021 – All rights reserved

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.]

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC/IEEE 16085:2021

© ISO/IEC 2021 – All rights reserved
© IEEE 2021 – All rights reserved

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.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC/IEEE 16085:2021

© ISO/IEC 2021 – All rights reserved
© IEEE 2021 – All rights reserved

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]

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC/IEEE 16085:2021

© ISO/IEC 2021 – All rights reserved
© IEEE 2021 – All rights reserved

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.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC/IEEE 16085:2021

© ISO/IEC 2021 – All rights reserved
© IEEE 2021 – All rights reserved

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

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC/IEEE 16085:2021

© ISO/IEC 2021 – All rights reserved
© IEEE 2021 – All rights reserved

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

— ISO 31000

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC/IEEE 16085:2021

© ISO/IEC 2021 – All rights reserved
© IEEE 2021 – All rights reserved

— 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.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC/IEEE 16085:2021

© ISO/IEC 2021 – All rights reserved
© IEEE 2021 – All rights reserved

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.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC/IEEE 16085:2021

© ISO/IEC 2021 – All rights reserved
© IEEE 2021 – All rights reserved

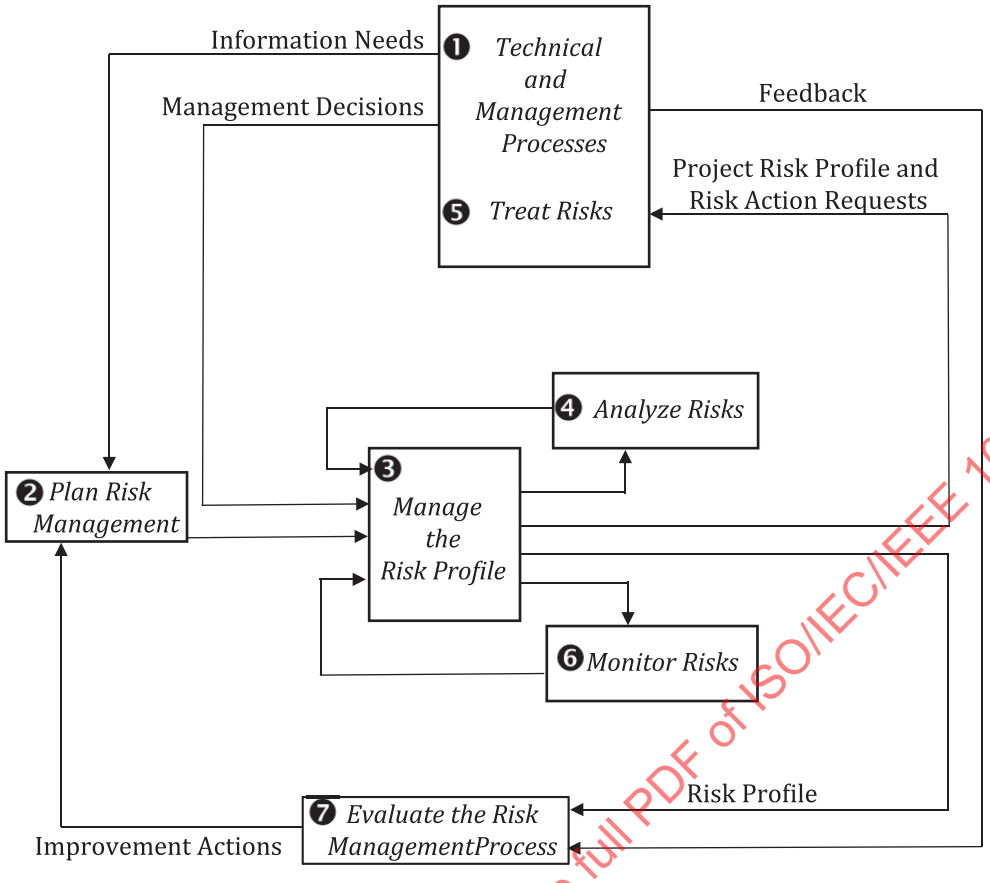

Figure 1 — Risk management process model

Managerial and technical processes involving the stakeholders define the information requirements (i.e., the information the stakeholders require to make informed decisions involving risks) that support the risk management process ❶. These information requirements are passed to both the "plan risk management" and the "manage the project risk profile" activities. In the "plan risk management" activity ❷, 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. Information created during this activity shall be documented in a risk management plan as described in 8.1.

In the "manage the risk profile" activity ❸, the current and historical risk management context and risk state information are captured. The risk profile includes the 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 risk profile information is continually updated and maintained through the "analyze risks" activity ❹, which identifies the risks, determines their probability and consequences, determines their risk exposures, and recommends 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 ❺. 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. Information created during this activity shall be documented in a risk treatment plan as described in 8.2.

All risks are continually monitored until they no longer need to be tracked, e.g. they are retired, during the "monitor risks" activity ❻. In addition, new risks and risk sources are sought out.

The risk management process is evaluated to improve its effectiveness. During the "evaluate the risk management process" activity ❼, information, including user and other feedback, is captured

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC/IEEE 16085:2021

© ISO/IEC 2021 – All rights reserved
© IEEE 2021 – All rights reserved

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 ❷.

The risk management process is applied continuously throughout the product life cycle and it is integrated with the other life cycle processes. 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 ❹, 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 process that goes from one phase to the next but is rather an iterative and incremental process that is implemented when necessary.

6.3 Outcomes

As a result of the successful implementation of the risk management process, the following outcomes shall be demonstrable:

a) Risks are identified.
b) Risks are analyzed.
c) Risk treatment options are identified, prioritized, and selected.
d) Appropriate treatment is implemented.
e) Risks are evaluated to assess changes in status and progress in treatment.

[ISO/IEC/IEEE 15288:2015 6.3.4.2 and ISO/IEC/IEEE 12207:2017 6.3.4.2]

6.4 Activities and tasks

6.4.1 General

The project shall implement the activities and tasks specified in 6.4.2 to 6.4.7 in accordance with applicable organization policies and procedures with respect to the Risk Management process.

6.4.2 Plan risk management

6.4.2.1 General

The plan risk management activity consists of the tasks specified in 6.4.2.2 and 6.4.2.3.

6.4.2.2 Define the risk management strategy

Organizations prepare for risk management by establishing and maintaining a strategy for identifying, analyzing, monitoring, treating, and communicating risks. The organization or project defines the purpose and scope of its risk management activities in the risk management strategy. The risk strategy includes a risk tolerance statement that articulates the project's attitude towards risk taking and influences all activities and tasks of the risk management process. The statement includes answers to questions such as: to what degree is the project willing to accept higher risk in exchange for more ambitious project objectives; and to what degree does the project rely on its already allocated resources to reduce the risk in achieving its objectives, as opposed to requesting more project resources for risk reduction?

The risk management strategy at a minimum addresses the following:

— scope of risk management,

— sources of risk,

— risk criteria,

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC/IEEE 16085:2021

© ISO/IEC 2021 – All rights reserved
© IEEE 2021 – All rights reserved

— how risks are to be organized, categorized, compared, and consolidated,

— risk measures,

— parameters used for taking action including likelihood of occurrence, severity of consequence, and thresholds,

— definition of the rating scale for likelihood of occurrence and severity of consequence,

— treatment techniques, and

— how the organization will evaluate and improve its risk management process.

The risk management strategy shall be documented in a risk management plan. Organizations may develop their risk management strategy before starting a project, or early in the project, so that risks are proactively identified and managed.

NOTE This includes the risk management process of all supply chain suppliers and describes how risks from all suppliers will be raised to the next level(s) for incorporation in the project risk process.

6.4.2.3 Define and record the context of the risk management process

Define the context of the risk management process. The risk management context may include, but is not limited to:

— A list of stakeholders.

— A description from stakeholders' perspectives.

— Risk categories to be used. The risk categories may include technical, security, safety, quality, schedule, budget, resource, requirement, process, testing, competition, and supply chain disruption risks. Categories of risk that are perceived to be of special importance may be addressed separately. The risk categories include the relevant technical areas of the system. The risk categories facilitate identification of risks across the life cycle of the system.

— A description (perhaps by reference) of the technical and managerial objectives, assumptions, and constraints. For example, the project may be constrained from openly communicating some risk-related information to specific stakeholders.

— Any other relevant information that may influence the analysis or treatment of risk.

Document and baseline risk management context. The risk management context may be documented as a stand-alone document, in the risk management plan, in the risk profile, or other project documents.

6.4.3 Manage the risk profile

6.4.3.1 General

Manage the risk profile consists of the tasks specified in 6.4.3.2 to 6.4.3.4.

6.4.3.2 Define and record the risk thresholds and conditions

Risk thresholds define the level of exposure above which risks are addressed and below which risks may be accepted. Risk thresholds are defined for individual risks or combinations of risks. A risk threshold may be defined for the project as a whole or may be defined for groups of risks or individually depending on the characteristics of the project.

The risk threshold quantifies the risk tolerance with a more precise way so that organizations know when to accept, monitor, or treat risks. Risk thresholds are the levels of measured risk criteria that are acceptable without explicit review by the stakeholders. Risk thresholds are defined and when a measured risk criterion is below a value, above a value, or in a range of values, appropriate action is

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC/IEEE 16085:2021

© ISO/IEC 2021 – All rights reserved
© IEEE 2021 – All rights reserved

taken. When the risk criterion is below a certain value, it is accepted. When it is in a range of values, it is closely monitored to make sure that the value doesn't change. If it is above a value, the risk is treated.

6.4.3.3 Establish and maintain a risk profile

The risk profile creates a consistent current and historical view of the risks present on a project along with their treatment.

A risk profile includes:

— description of the risk,

— the risk's likely causes and events,

— possible consequences of the risk,

— the risk's severity of consequences,

— the risk's likelihood of occurrence,

— the risk's likelihood of detection should the risk become an issue,

— the risk's thresholds and conditions,

— the risk's current state,

— the risk's current treatment, or contingency strategy or plan, and

— the risk's history.

The risk profile is updated and baselined periodically. Updates may be made when there are changes in:

— the risk management context,

— a new risk is identified, or

— any change in an existing risk's information.

6.4.3.4 Periodically provide the relevant risk profile to stakeholders

Periodically communicate the risk profile or relevant risk profile (for example, a single risk or combination of risks) to stakeholders based upon their needs. Different stakeholders will need different subsets of the risks in the risk profile. The risk profile may be reviewed at project milestone or gate reviews. Periodically provide the relevant risk profile to stakeholders based upon their needs.

6.4.4 Analyze risks

6.4.4.1 General

Analyze risks consists of the tasks specified in 6.4.4.2 to 6.4.4.5.

6.4.4.2 Identify risks in the categories described in the risk management context

The risk identification task involves finding, recognizing, and describing risks that might affect the organization or project and prevent it from achieving its objectives.

Risks are identified from the categories identified in the risk management context. Use risk categories consistently for effective communication to stakeholders. Where possible, events, hazards, threats, or situations that can create risks are identified. Changes in the risk management context may cause additional risks. For example, changes in the assumptions may add or reduce risk. System or software anomalies, reports on measures, and other indicators are continuously reviewed as sources for risks.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC/IEEE 16085:2021

© ISO/IEC 2021 – All rights reserved
© IEEE 2021 – All rights reserved

For each risk, analyze it using combinations of risk-related measures. For example, when the risk may be anticipated to become a problem, consider analyzing the severity of consequences, likelihood of occurrence, and likelihood of detection should the risk become an issue. As a result of the analysis determine a priority. Consider sorting the risks by priority order.

ISO/IEC TR 33015 provides guidance on the identification of process related risks. This is done through process assessments.

All relevant risks should be identified. Stakeholders may consciously evaluate each identified risk and decide not to take action, which is deemed acceptance of the risk at the current state.

Related risks may be combined, and complex risks may be decomposed for ease of analysis, monitoring, and treatment.

Various approaches to identifying risks may be used including:

— risk questionnaires,

— taxonomies,

— brainstorming,

— scenario analysis,

— measurement analysis,

— identifying consequences and analyzing back to the risk (e.g. safety hazards),

— lessons learned from other projects, and

— other knowledge acquisition approaches.

Risks identified should be included in the risk profile. Thus, the risk profile is used to baseline risks.

Opportunities have the potential to provide benefits for the organization, system, or project. Each opportunity pursued can also have potential negative outcomes that detract from the expected benefit. Analysis of opportunities should include the risks associated with not pursuing an opportunity, as well as risks that arise if the opportunity is taken. In both cases, potential positive and negative outcomes should be considered.

NOTE IEEE 1044 provides useful information regarding software anomaly classification. IEEE 982.1 provides useful information regarding software measures related to dependability.

6.4.4.3 Estimate the likelihood of occurrence and consequences of each identified risk

The likelihoods of occurrence and severity consequences of each risk identified are estimated. Estimates may be made either quantitatively or qualitatively.

A qualitative risk analysis prioritizes the identified project risks using a pre-defined rating scale. Risks will be scored based on their probability or likelihood of occurring and the impact on project objectives should they occur. Probability and likelihood are commonly ranked on a numeric scale, which is defined by the organization. An example would be a one- to five-point scale, with five being the highest impact on project objectives – such as budget, schedule, or quality.

A quantitative risk analysis is a further analysis of the highest priority risks during which a numerical or quantitative rating is assigned in order to develop a probabilistic analysis of the project. A quantitative analysis quantifies the possible outcomes for the project and assesses the probability of achieving specific project objectives, provides a quantitative approach to making decisions when there is uncertainty, and defines realistic and achievable targets.

The stakeholders define which risks will be evaluated using qualitative methods and which will be evaluated using a quantitative scale.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC/IEEE 16085:2021

© ISO/IEC 2021 – All rights reserved
© IEEE 2021 – All rights reserved

Scale(s) for estimating risk likelihood of occurrence and severity of consequences should be used consistently. The descriptive and measurement uncertainty inherent in the scale used is described in the risk management plan. The units used are stated and consistent. When possible, capture the level of confidence in estimates of likelihood of occurrence or severity of consequences. If likelihood is expressed as a percentage, the denominator is the same in each case and is stated (for example, percentage of projects, percentage of contractors etc.). The population and time scale to which a likelihood applies should be consistent and stated.

Uncertainties in estimates used to make decisions should be analyzed so the level of confidence in estimates can be stated.

A single value for a severity of consequence or likelihood of occurrence may need to be ambiguously defined. (For example, an event may have a distribution of consequences or severities.) The likelihood of occurrence and severity of consequence will not produce a clearly defined level of risk. In that case, comparing thresholds is not possible. Instead, options include taking the mean, the most likely value of the distribution or a percentile value. The rationale for picking any one particular likelihood and severity pair should be stated and compatible with the definitions of the thresholds.

NOTE 1 Distributions relevant to risk can be highly skewed.

NOTE 2 IEC 31010 provides additional information on analyzing risk in these circumstances.

6.4.4.4 Evaluate each risk against its risk thresholds

Evaluate each risk against its risk thresholds and conditions and note if the risk does not meet its threshold.

Risks may be evaluated independently, in combination, or with their interactions with higher-level system or organizational risks. Evaluate combinations of risks against the project risk threshold so that the combination, while below their individual risk thresholds, does not unacceptably place the project as a whole at risk.

Different techniques may be used to evaluate the risks, such as decision trees, scenario planning, game theory, probabilistic analysis, fault-tree analysis, failure mode and effects analysis, and linear programming.

Highlight important risks based on considerations such as when the risk may become a problem, severity of consequence, legal concerns, and contractual concerns. These risks may need more urgent treatment, more careful monitoring or to be communicated to higher levels of management

Update each risk in the risk profile to record the result of the evaluation. Periodically, reevaluate all risks in the risk profile. As part of the reevaluation, evaluate the effectiveness of existing controls or mitigations.

NOTE IEEE 982.1 provides useful information regarding software measures related to dependability. ISO/IEC/IEEE 15939 provides a measurement process that can be used to help evaluate risks.

6.4.4.5 Define and record recommended treatment strategies and measures

For each risk that does not meet its threshold, define one or more risk treatment strategies. Some risk treatment strategies are:

— undertake further analysis to better understand the risk,

— reconsider the project objectives,

— do nothing further,

— maintain existing controls,

— involve the appropriate stakeholder(s) (in other words, escalate the risk),

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC/IEEE 16085:2021

© ISO/IEC 2021 – All rights reserved
© IEEE 2021 – All rights reserved

— treat the risk to reduce severity of consequences,

— treat the risk to reduce likelihood of occurrence,

— treat the risk to increase the likelihood of detection should the risk become an issue, and

— other risk treatment options. (See 6.4.5.2)

Define and recommend measures of the effectiveness of the treatment strategies and options.

Document and baseline the recommended risk treatment strategies and measures. Also, document the risk treatment strategies considered and why or why not they were recommended.

6.4.5 Treat risks

6.4.5.1 General

Treat risks consists of the tasks specified in 6.4.5.2 to 6.4.5.5.

6.4.5.2 Identify recommended alternatives for risk treatment

Risk treatments usually focuses on minimizing negative consequences and their likelihood but may include increasing potential positive effects and their likelihood as well.

> Risk treatment options are not necessarily mutually exclusive or appropriate in all circumstances. Options for treating risk can involve one or more of the following:
>
> — removing the risk source,
>
> — planning contingency actions for cases in which a risk is accepted,
>
> — taking or increasing the risk in order to pursue an opportunity,
>
> — sharing the risk (e.g. through contracts, buying insurance), and
>
> — retaining the risk by informed decision.
>
> [ISO 31000:2018, 6.5.2]

Risk treatment can also introduce new risks that need to be managed. Any newly identified risks should be evaluated, mitigated, recorded and kept under ongoing review.

Decision makers and other stakeholders should be aware of the nature and extent of the residual risk after risk treatment. The residual risk should be documented and subjected to monitoring, review, and, where appropriate, further treatment.

6.4.5.3 Implement risk treatment alternatives

Selecting the most appropriate risk treatment option(s) involves balancing the potential benefits derived in relation to the achievement of the objectives against the costs, effort, or disadvantages of implementation. Also, selected treatments are based on the priority of risks, considering the severity of the consequences, likelihood of occurrence, or any other factors and the extent to which they will reduce risk and improve regulatory and contractual compliance. Whenever a risk treatment alternative is recommended, stakeholders will determine if the risk is acceptable. If the stakeholders determine that actions should be taken to make a risk acceptable, then a risk treatment alternative will be implemented, supported by the necessary resources, and monitored and coordinated with other project activities.

Justification for risk treatment is broader than solely economic considerations and should take into account all of the organization's obligations, voluntary commitments, and stakeholder views. The

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC/IEEE 16085:2021

© ISO/IEC 2021 – All rights reserved
© IEEE 2021 – All rights reserved

selection of risk treatment options should be made in accordance with the project's objectives, risk criteria, and available resources.

When selecting risk treatment options, the organization should consider the values, perceptions, and potential involvement of stakeholders and the most appropriate ways to communicate and consult with them. Though equally effective, some risk treatments can be more acceptable to some stakeholders than to others.

Also, it is important that controls be put in place that are proportional to the risks. Risk analysis assists such a process by identifying those risks requiring attention by the management. Risk control actions should be prioritized by their potential benefits to selected stakeholders, such as the users, the customer, the organization, or the public.

6.4.5.4 Monitor high priority risks

The stakeholders may accept a risk even though it exceeds its risk threshold, e.g. if the treatment cost is too high, the timing is not suitable, or a lack of treatment resources exists. In this situation, the risk is considered a high priority and monitored continuously to determine if any future risk treatment actions are necessary.

> Risk treatments, even if carefully designed and implemented, might not produce the expected outcomes and could produce unintended consequences. Monitoring and review need to be an integral part of the risk treatment implementation to give assurance that the different forms of treatment become and remain effective.
>
> [ISO 31000:2018, 6.5.2]

The stakeholders may also ask for more information be provided to make a risk treatment decision, or they may suggest some other treatment approach.

6.4.5.5 Once a risk treatment is selected, coordinate management action

When treatments have been implemented, risk profiles should be modified to reflect any new or updated controls. It can be useful to record also why these controls are believed to be sufficient to save effort when risks are reviewed.

Effectiveness of internal control is determined by how much the risk will be either eliminated or reduced by the control measures proposed. The latter need to be measured in terms of potential economic effect if no action is taken, versus the cost of the action(s) proposed. Every response action has a related cost, and it is important that the treatment offers value for money in relation to the risk controlled by it. Therefore, it is important to put controls in place to monitor risk treatments and to get the appropriate approval prior to implementing the risk treatment.

Controls for treating risk can involve one or more of the following:

— Preventative controls limit undesirable outcomes. The more an undesirable outcome should be avoided, the more appropriate preventative controls should be considered.

— Corrective controls correct undesirable outcomes that have occurred and provide a way to achieve some recovery against loss or damage. Contingency planning is an important element of corrective control.

— Directive controls ensure that a particular outcome is achieved and are particularly important when avoiding an undesirable event – typically related to health and safety or to security.

— Detective controls identify occasions of occurrence of undesirable outcomes. Their effect is, by definition, "after the event" so they are only appropriate when the resulting loss or damage can be accepted.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC/IEEE 16085:2021

© ISO/IEC 2021 – All rights reserved
© IEEE 2021 – All rights reserved

6.4.6 Monitor risks

6.4.6.1 General

Monitor risks consists of the tasks specified in 6.4.6.2 to 6.4.6.4.

6.4.6.2 Continually monitor the risk management context

Monitor the risks in the risk profile throughout the life cycle for changes in their state, especially, when the risk becomes an issue. Monitor for changes in the risk's severity, likelihood of occurrence, likelihood of detection, thresholds, conditions, and priority. Monitor high priority risks more frequently. Reevaluate changed risks (6.4.4.4).

Monitor any critical assumptions made during analysis because if these change, the risk may exceed its threshold.

Monitor the risk management context for changes. Document those changes as appropriate. Based on the changes, reevaluate the appropriate risks.

6.4.6.3 Implement and monitor measures to evaluate the effectiveness of risk treatments

Implement the treatment measures developed as part of the treatment strategies. Monitor and evaluate those measures. Identify and remedy the cause(s) of ineffective treatments promptly. If needed, identify a more effective risk treatment (See 6.4.5.2).

6.4.6.4 Continually monitor for the emergence of new risks and sources throughout the life cycle

Monitor the project continually for new risks and sources throughout its life cycle. Add new risks and sources identified to the risk profile. Analyze (6.4.4) and treat (6.4.5) the new risks promptly. Communicate new risks and sources to the stakeholders after risk analysis as part of the periodic communication of the risk profile. Communication of risks with a high priority may be expedited to the appropriate stakeholder.

6.4.7 Evaluate the risk management process

6.4.7.1 General

Evaluate the risk management process activity consists of the tasks specified in 6.4.7.2 to 6.4.7.4.

In ISO/IEC/IEEE 12207 and ISO/IEC/IEEE 15288, process evaluation is part of the Quality Assurance and Life Cycle Management processes. Process improvement is part of the Life Cycle Management process.

6.4.7.2 Analyze recurring issues, problems, and risks over time

Information about the risks identified, their sources, their causes, their treatment, and the success of the treatments selected is collected throughout the project's life cycle for purposes of improving the risk management process and generating lessons learned. Apply measures to the risk profiles data (for example, number of risks per some measure of project size or complexity, number of risks per category, treatment success versus expected, etc.). The information captured may be useful to improving organizational risk management strategy, procedures, processes, or policies.

6.4.7.3 Identify lessons learned

Periodically review the risk management process for its effectiveness and efficiency. Opportunities for improving the project or organizational risk management and processes are identified, including consideration of how the risks posed by the risk management process itself can be reduced or

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC/IEEE 16085:2021

© ISO/IEC 2021 – All rights reserved
© IEEE 2021 – All rights reserved

eliminated. Individual project lessons learned may be collected to aid in the identification of systemic risks. The stakeholders determine the review period.

6.4.7.4 Improve the risk management process

Information on the risks identified, their treatment, and the success of the treatments are reviewed periodically by the stakeholders and other parties for purposes of identifying systemic project and organizational risks. Where applicable, the process is improved, the organizational risk management and policies and process updated (if these exist), and the project risk management plan updated.

7 Risk management in life cycle processes

7.1 Overview

A primary goal of this document is to elaborate the risk management process described in ISO/IEC/IEEE 15288 and ISO/IEC/IEEE 12207. In this respect the focus of the application of ISO/IEC/IEEE 15288 and ISO/IEC/IEEE 12207 to this document involves the integration of risk management and "risk-based thinking" into all systems or software engineering life cycle processes. This is accomplished by identifying and analyzing the systems and software engineering life cycle processes used by the organization or project, and instituting policy, practices, procedures, techniques, and/or tools that help ensure appropriate risk management within those life cycle processes. Likewise, the aspects of systems and software engineering life cycle processes that support reduction in uncertainty and enhance risk management are integrated to form a holistic risk management approach.

Each life cycle process can be invoked, as required, at any time throughout the life cycle. The order that the processes are presented in this clause does not imply any prescriptive order in their use.

In 7.2 to 7.6, all the life cycle processes are presented in the order from ISO/IEC/IEEE 12207 and ISO/IEC/IEEE 15288. For each life cycle process there are three subclauses: typical risk areas, typical opportunity areas, and typical treatment. The content of these subclauses are examples, not an exhaustive list, and not a checklist.

7.2 Risk management in agreement processes

7.2.1 General

The two Agreement processes discussed in 7.2.2 and 7.2.3 specify the requirements for the establishment of agreements with organizational entities external and internal to the organization.

7.2.2 Acquisition process

7.2.2.1 Typical risk areas

Typical risks of the Acquisition process can include:

— lack of clarity of agreements;

— lack of feasibility in the parameters of agreement (e.g. infeasible cost, schedule, or outcomes);

— poor acquisition strategy;

— poor understanding of acceptance processes between the parties;

— acquirers that do not actively participate in their projects;

— acquirers not taking responsibilities for the definition of system requirements;

— acquirers not taking responsibilities for the definition of software requirements;

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC/IEEE 16085:2021

© ISO/IEC 2021 – All rights reserved
© IEEE 2021 – All rights reserved

— acquirers that make no effort to take accountability for requirements;

— features or functions are requested that are not in the established agreement;

— proceeding without stakeholder agreement on defined requirements;

— misunderstood requirements;

— failure to review and negotiate agreement details.

7.2.2.2 Typical opportunity areas

Typical opportunities of the Acquisition process can include:

— a strategy that reflects the nature of the product, the scope of activities, and the characteristics of the supplier(s);

— use of standard agreements;

— preferred supplier lists that are updated on a regular basis;

— suppliers to avoid lists that are updated on a regular basis.

7.2.2.3 Typical treatments

Typical treatments of the Acquisition process can include:

— detailed planning;

— understanding of the supplier marketplace and capabilities;

— early engagement with potential suppliers to understand the responsibilities, obligations, and concerns of each other;

— modifying acquisition plans and agreements based on feedback;

— the project management and purchasing departments of the acquirer comprehend what system and software development entails;

— the purchasing department and the information system department of the acquirer collaborate when defining requirements;

— the acquirer actively participates in the project while clarifying its role with the supplier;

— the supplier understands the requirements and confirm its understanding with the acquirer;

— the acquirer expresses all requirements in the most appropriate form such as documentation and mock-ups;

— the acquirer makes known to its entire organization that the organization decides and is responsible for the requirements;

— the supplier agreement or contract is multi-stage when the requirements are not fully defined.

7.2.3 Supply Process

7.2.3.1 Typical risk areas

Typical risks of the Supply process can include:

— the response to the acquirer's request is infeasible;

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC/IEEE 16085:2021

© ISO/IEC 2021 – All rights reserved
© IEEE 2021 – All rights reserved

— mismatch between acquirer's knowledge of needs versus supplier's knowledge of feasibility and cost drivers for solution;

— proceeding to the next step without agreement among stakeholders;

— agreements do not allow for change;

— incomplete requirements;

— not fully understanding the requirement as written;

— interpretation of terminology is different;

— supplier assumptions do not match acquirers.

7.2.3.2 Typical opportunity areas

Typical opportunities of the Supply process can include:

— identifying outcomes with additional benefits to the acquirer for little incremental cost;

— providing outcomes that result in high operability and maintainability.

7.2.3.3 Typical treatments

Typical treatments of the Supply process can include:

— performing detailed planning before agreements are established;

— engaging closely with acquirer to understand the scope;

— applying evolutionary approaches to delivery;

— engaging with potential suppliers and modify acquisition plans and agreements based on feedback;

— setting up agreements to allow for change;

— delivering a straightforward, clear proposal;

— examining the characteristics of the system or software of interest and apply a suitable development method, environment, and tools;

— performing a set of reviews from ISO/IEC/IEEE 24748-8.

7.3 Risk management in organizational project-enabling processes

7.3.1 General

The six organizational project-enabling processes discussed in 7.3.2 to 7.3.7 help ensure the organization's capability to acquire and supply products or services through the initiation, support and control of projects. These processes provide resources and infrastructure necessary to support projects and help ensure the satisfaction of organizational objectives and established agreements. These six processes are not intended to be a comprehensive set of business processes that enable strategic management of the organization's business.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC/IEEE 16085:2021

© ISO/IEC 2021 – All rights reserved
© IEEE 2021 – All rights reserved

7.3.2 Life cycle model management process

7.3.2.1 Typical risk areas

Typical risks of the Life Cycle Model Management process can include:

— the organization's life cycle processes, good by themselves, do not work together well enough, putting the value of the organization's systems and software engineering project results at risk (e.g. low productivity numbers against benchmarks; improper root cause analysis; too many risks materializing in spite of each individual process being de-risked; no sense that risk management integration has improved predictability);

— building silos, overlaps, and sub-optimization;

— processes are intertwined to a degree that observers and practitioners find the processes hard to unwind; risk management therefore also addresses an organization's life cycle processes as a whole;

— mismatch of lifecycle model to problem space.

7.3.2.2 Typical opportunity areas

Typical opportunities of the Life Cycle Model Management process can include:

— ability to adapt the model(s) as the lifecycle and knowledge of problem space and potential solutions increases over time;

— potential to create lifecycle models that explicitly try to improve knowledge of problem space and potential solutions over time.

7.3.2.3 Typical treatments

Typical treatments of the Life Cycle Model Management process can include:

— early processes in life cycle explicitly designed to treat risk (e.g. evolutionary approaches).

7.3.3 Infrastructure management process

7.3.3.1 Typical risk areas

Typical risks of the Infrastructure Management process can include:

— the infrastructure will not meet project needs, since the project either ignored the infrastructure or poorly specified the infrastructure requirements;

— timing of infrastructure availability is inappropriate.

7.3.3.2 Typical opportunity areas

Typical opportunities of the Infrastructure Management process can include:

— manage infrastructure elements as systems in their own right.

7.3.3.3 Typical treatments

Typical treatments of the Infrastructure Management process can include:

— identify requirements for infrastructure elements and interfaces, dependencies, and assumptions with development and other lifecycle processes, and system products.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC/IEEE 16085:2021

© ISO/IEC 2021 – All rights reserved
© IEEE 2021 – All rights reserved

7.3.4 Portfolio management process

7.3.4.1 Typical risk areas

Typical risks of the Portfolio Management process can include:

— projects are mismatched, misaligned in time, or overlap in scope;

— realizing that a project may not be viable.

7.3.4.2 Typical opportunity areas

Typical opportunities of the Portfolio Management process can include:

— harmonizing and streamlining projects;

— managing interdependencies between related projects.

7.3.4.3 Typical treatments

Typical treatments of the Portfolio Management process can include:

— identifying dependencies;

— maintaining resources to track and address changes as they occur.

7.3.5 Human resource management process

7.3.5.1 Typical risk areas

Typical risks of the Human Resource Management process can include:

— inadequate skills;

— insufficient resources;

— inadequate training;

— insufficient or outdated knowledge and skills inventory.

7.3.5.2 Typical opportunity areas

Typical opportunities of the Human Resource Management process can include:

— training existing staff;

— using external resources;

— using technology readily available in the marketplace.

7.3.5.3 Typical treatments

Typical treatments of the Human Resource Management process can include:

— understanding base skills and needed skills for current and future projects;

— developing training plans to address knowledge and skill gaps.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC/IEEE 16085:2021

© ISO/IEC 2021 – All rights reserved
© IEEE 2021 – All rights reserved

7.3.6 Quality management process

7.3.6.1 Typical risk areas

Typical risks of the Quality Management process can include:

— the "access or evaluate quality management" activity is often not done well; specifically, often there is little or no history of quality assurance evaluation results;

— establishing quality management procedures that are so burdensome for the project so that the effects schedule, resources, and costs are not commensurate with the value of the project;

— not listening to the management of the project teams or not implementing their suggestions;

— overly complex assurance processes may defeat their intent;

— helping assure the quality process and procedures are sufficient for the project;

— the existing quality management process has not changed based on lessons identified on other projects;

— lack of independence for quality management personnel.

In a multi-location development organization, creating and maintaining a quality management system which does not consider:

— the differences in national or organization culture;

— the differences in the resources available in each location especially people, management, or tools;

— the size and complexity of the project being supported.

7.3.6.2 Typical opportunity areas

Typical opportunities of the Quality Management process can include:

— matching effort of assurance resources to consequence of failure;

— streamlining activities and developing work aids to make process more effective and efficient;

— matching effort, knowledge and skills of assurance resources to the project specifics, likelihood of occurrence, and severity consequences of failure of the risks.

7.3.6.3 Typical treatments

Typical treatments of the Quality Management process can include:

— training everyone in organization to understand their responsibility in quality management;

— ensuring the quality process and procedures are complete and appropriate for the project.

7.3.7 Knowledge management process

7.3.7.1 Typical risk areas

Typical risks of the Knowledge Management process can include:

— incomplete or inaccurate inventory of organizational knowledge and skills;

— lack of knowledge needs for the present and future;

— understanding how to capture tacit knowledge such as intuitive skills.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC/IEEE 16085:2021

© ISO/IEC 2021 – All rights reserved
© IEEE 2021 – All rights reserved

7.3.7.2 Typical opportunity areas

Typical opportunities of the Knowledge Management process can include:

— leveraging knowledge from external resources;

— leveraging knowledge of individuals and share across the organization.

7.3.7.3 Typical treatments

Typical treatments of the Knowledge Management process can include:

— implementing processes and activities that will store, grow, and share knowledge.

7.4 Risk management in technical management processes

7.4.1 General

The eight technical management processes discussed in 7.4.2 to 7.4.9 are used to establish and evolve plans, to execute the plans, to assess actual achievement and progress against the plans and to control execution through to fulfilment. Individual technical management processes may be invoked at any time in the life cycle and at any level in a hierarchy of projects, as required by plans or unforeseen events. The technical management processes are applied with a level of rigor and formality that depends on the complexity, historical information, and uncertainty of the project.

7.4.2 Project planning process

7.4.2.1 Typical risk areas

Typical risks of the Project Planning process can include:

— insufficient or incorrect identification of project scope, objectives, and constraints;

— inconsistent or changing scope of the project;

— inadequate definition and maintenance of project structure including life cycle models, work breakdown structure, and processes;

— insufficient subject matter experts in the requirements, design, development, verification, or validation activities;

— insufficient or incorrect development method, environment and tools;

— unintended consequences and additional uncertainties related to repeated changes in scope, objectives and constraints, and excessive unanticipated re-planning and rework;

— using a rough estimate written in the early phase through the whole lifecycle without reviews;

— inappropriate level of detail;

— invalid assumptions;

— estimations that lack rationale;

— estimations that lack proper scope;

— insufficient focus on the development of the operational system;

— lack of consideration of sustainment of system.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC/IEEE 16085:2021

© ISO/IEC 2021 – All rights reserved
© IEEE 2021 – All rights reserved

7.4.2.2 Typical opportunity areas

Typical opportunities of the Project Planning process can include:

— opportunities to increase the likelihood of reaching or exceeding project objectives and targets related to customer expectations;

— early development of a project plan that includes insights, information, and priorities for success obtained through the risk management process may produce more desirable outcomes that align with stakeholder needs and requirements;

— early utilization of data and analyses to more quickly and efficiently develop and maintain the project plan.

7.4.2.3 Typical treatments

Typical treatments of the Project Planning process can include:

— using a continuous estimation process that will be updated with changing project information;

— revising project monitoring to add more frequent progress reviews;

— tracking schedule performance in sufficient detail to support recovery;

— adding a quality assurance review to assure requirements, plans, and overall business objectives are reviewed as defined in the project plan;

— establishing rules for updating the cost estimates especially when requirements are evolving;

— using historical data where possible to make estimates;

— planning for and including the activities required to transition the system from the supplier to the acquirer;

— clearly identifying and documenting the scope of work and functional and non-functional requirements in all appropriate plans, agreements, and contracts;

— estimating and planning for the operation and maintenance phase of the system;

— estimating and planning for the system life cycle costs.

7.4.3 Project assessment and control process

7.4.3.1 Typical risk areas

Typical risks of the Project Assessment and Control process can include:

— incomplete or inaccurate business needs and requirements;

— incomplete or inaccurate assessment results;

— vague plans;

— inappropriate reviews;

— unclear review goals;

— periodic reviews not held or period between reviews is insufficient to control processes (for example, one per year is probably not enough for most programs);

— significant deviations and variations are not detected;

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC/IEEE 16085:2021

© ISO/IEC 2021 – All rights reserved
© IEEE 2021 – All rights reserved

— projects that consume excessive resources and are over budget, late, or lacking acceptable quality deliverables.

7.4.3.2 Typical opportunity areas

Typical opportunities of the Project Assessment and Control process can include:

— pre-determining periodically and at major events when an assessment is most beneficial.

7.4.3.3 Typical treatments

Typical treatments of the Project Assessment and Control process can include:

— reevaluating assessment and planning activities to include lessons learned;

— deviations and variations from processes and plans are reviewed and addressed.

7.4.4 Decision management process

7.4.4.1 Typical risk areas

Typical risks of the Decision Management process can include:

— decision making approach has not been agreed upon and approved by all stakeholders;

— timely decisions are not made;

— decisions are not based on accurate information;

— all relevant stakeholders are not included in the decision making.

7.4.4.2 Typical opportunity areas

Typical opportunities of the Decision Management process can include:

— tailoring decision-making and supporting analysis based on consequences and risk.

7.4.4.3 Typical treatments

Typical treatments of the Decision Management process can include:

— effort and background research/analysis to inform decision needs to be commensurate with the potential consequence of the wrong decision;

— verifying that all decisions that involve cost and schedule risk of a certain impact exercise the appropriate decision-making processes;

— clarifying all stakeholders understand the agreement process and the rules for approval, and act in accordance with them.

7.4.5 Risk management process

7.4.5.1 General

NOTE The Risk Management process is described in detail in Clause 6.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC/IEEE 16085:2021

© ISO/IEC 2021 – All rights reserved
© IEEE 2021 – All rights reserved

7.4.5.2 Typical risk areas

Typical risks of the Risk Management process can include:

— inappropriate or insufficient risk categories;

— inappropriate or insufficient risk thresholds;

— the focus is only on projects and not the organization, products, and services;

— all critical risks are not identified;

— risk likelihood of occurrence or consequence are estimated incorrectly.

7.4.5.3 Typical opportunity areas

Typical opportunities of the Risk Management process can include:

— risk management and risk-based thinking pervades all activities at all levels in the organization;

— risks are captured and managed from all activities at all levels in the organization.

7.4.5.4 Typical treatments

Typical treatments of the Risk Management process can include:

— standardizing risk management process across the organization;

— collecting and analyzing risk metrics such as likelihood of occurrence and consequence;

— verifying that all stakeholders have participated and agree with the stakeholder agreement.

7.4.6 Configuration management process

7.4.6.1 Typical risk areas

Typical risks of the Configuration Management (CM) process can include:

— planned baselines are not clearly defined when the project starts;

— baselines are not established, reproducible, or maintained;

— controlled items are not identified;

— current status of development or individual product instances is unknown;

— baselines are not reviewed for integrity;

— teams work to different baselines without knowing which one is correct or without clear management direction to do so;

— baselines are unclear;

— variation and change are not explicitly managed;

— all required items are not included in the CM process;

— complete inventory of system and software components is not available when needed;

— users circumvent the process and fail to update items when changed;

— suppliers are not made aware of changes;

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC/IEEE 16085:2021

© ISO/IEC 2021 – All rights reserved
© IEEE 2021 – All rights reserved

— CM controls do not protect the integrity of items maintained in the CM libraries;

— changes to baselines are made without understanding the impact of the change on other aspects of the program (e.g. cost, schedule, affected products, interfaces);

— consistency issues when using multiple CM systems.

7.4.6.2 Typical opportunity areas

Typical opportunities of the Configuration Management process can include:

— tailoring CM practices to the type of product and associated risks (e.g. the level of CM for workstations in an office environment versus flight systems of aircraft is very different);

— documenting repeatable CM process;

— integrating CM with related processes, such as Supply and Maintenance.

7.4.6.3 Typical treatments

Typical treatments of the Configuration Management process can include:

— automating configuration management practices;

— documenting and disseminating the plan(s) for configuration management to the stakeholders for concurrence;

— developing plans which include the definition of the planned controlled items, when they are to be controlled, process for making changes, and baselines to be established;

— automating integration of the different CM tools used across a program;

— implementing periodic configuration reviews and audits;

— discussing and communicating changes to the baseline with all relevant stakeholders.

7.4.7 Information management process

7.4.7.1 Typical risk areas

Typical risks of the Information Management process can include:

— not appropriately communicating and disseminating the purpose of the project and project documents to all relevant stakeholders;

— information is inconsistent, incorrect, or misleading;

— the form of the information is inappropriate.

7.4.7.2 Typical opportunity areas

Typical opportunities of the Information Management process can include:

— improving the efficiency of information storage and retrieval;

— simplifying information capture;

— increasing the timeliness of reports and dashboards.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC/IEEE 16085:2021

© ISO/IEC 2021 – All rights reserved
© IEEE 2021 – All rights reserved

7.4.7.3 Typical treatments

Typical treatments of the Information Management process can include:

— streamlining information management policies and procedures;

— developing the information management system with a clear understanding of its policy and purpose;

— establishing consistent information formats and delivery media;

— automating content management;

— testing or evaluating the usability of information products.

7.4.8 Measurement process

7.4.8.1 Typical risk areas

Typical risks of the Measurement process can include:

— measuring everything;

— not making key measurements;

— lack of what is measured;

— inconsistent measurement within and between projects;

— measurement is used inappropriately (e.g. used to measure personnel's performance).

7.4.8.2 Typical opportunity areas

Typical opportunities of the Measurement process can include:

— tailoring measures to provide insight into specific risks.

7.4.8.3 Typical treatments

Typical treatments of the Measurement process can include:

— using methodology based on project and organization specific issues and risks;

— supplementing the ISO/IEC/IEEE 12207 and ISO/IEC/IEEE 15288 Measurement process with other measurement processes and standards such as ISO/IEC/IEEE 15939;

— measuring only items that are actionable with the resources available;

— sharing reports based on the measures with all appropriate stakeholders.

7.4.9 Quality assurance process

7.4.9.1 Typical risk areas

Typical risks of the Quality Assurance process can include:

— if there are multiple test teams, the risk of not checking each team's testing and reporting;

— performing quality assurance on all activities in the process;

— failure to identify processes and procedures that should have been applied to the project;

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC/IEEE 16085:2021

© ISO/IEC 2021 – All rights reserved
© IEEE 2021 – All rights reserved

— failure to identify project non-compliance with procedures.

7.4.9.2 Typical opportunity areas

Typical opportunities of the Quality Assurance process can include:

— eliminating the low value quality assurance activities;

— maximizing quality assurance efforts between and among similar projects in the organization.

7.4.9.3 Typical treatments

Typical treatments of the Quality Assurance process can include:

— early engagement with the project to understand what project activities contain the biggest risk;

— helping ensure that all projects adhere to the applicable required policies, plans, procedures, and instructions;

— defining and documenting the agreed quality assurance process to be used on the project;

— analysis of non-compliances to determine trends that are used to reduce variation and improve quality.

7.5 Risk management in technical processes

7.5.1 General

The fourteen technical processes discussed in 7.5.2 to 7.5.15 are used to transform the needs of stakeholders into a product or service. They describe technical actions throughout the life cycle. Individual technical processes may be invoked at any time in the life cycle and at any level in a hierarchy of projects.

7.5.2 Business or mission analysis process

7.5.2.1 Typical risk areas

Typical risks of the Business or Mission Analysis process can include:

— lack of organizational and project business strategy;

— unclear problem definition or boundaries;

— lack of understanding of the total cost of the system.

7.5.2.2 Typical opportunity areas

Typical opportunities of the Business or Mission Analysis process can include:

— identifying new product lines and products;

— analyzing impacts of new technologies and reaching underserved stakeholders.

7.5.2.3 Typical treatments

Typical treatments of the Business or Mission Analysis process can include:

— establishing systematic strategic planning;

— comparing the organization's situation to similar or competing organizations;

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC/IEEE 16085:2021

© ISO/IEC 2021 – All rights reserved
© IEEE 2021 – All rights reserved

— tracking the predictive accuracy of previous long-range plans including assessments for impacts on environments and peoples' health, as well as business or mission performance;

— understanding the root cause of deviation from the business or mission problem or opportunity.

7.5.3 Stakeholder needs and requirements definition process

7.5.3.1 Typical risk areas

Typical risks of the Stakeholder Needs and Requirements Definition process can include:

— insufficient or incorrect identification of stakeholders;

— stakeholder requirements that do not satisfy the business requirements;

— established stakeholder requirements that are ignored during later lifecycle stages;

— unidentified and unresolved conflicts and inconsistencies in stakeholder needs and requirements;

— level of abstraction/detail too high or low (i.e., mismatched to problem space and purpose of requirements in acquisition or supply process);

— inadequate identification and definition of stakeholder needs and requirements;

— inadequate communication and understanding of stakeholder needs and requirements;

— unidentified and unresolved conflicts and inconsistencies in stakeholder needs and requirements;

— suppliers and other stakeholders are not included when defining requirements;

— lack of operational requirements;

— unrealistic requirements.

7.5.3.2 Typical opportunity areas

Typical opportunities of the Stakeholder Needs and Requirements Definition process can include:

— understanding the genuine business/mission benefits;

— development of a stakeholder needs and requirements definition strategy inclusive of insights gained through the risk management process;

— identification of previously undefined stakeholder needs and requirements, particularly those necessary to treat critical risks identified by the risk management process;

— utilization of the full set of risk management data and analyses to better, and more quickly and efficiently, strategize, define, and resolve conflicts and inconsistencies.

7.5.3.3 Typical treatments

Typical treatments of the Stakeholder Needs and Requirements Definition process can include:

— establishing communication and consultation;

— integrating risk management resources into stakeholder needs and requirements;

— communicating and consulting with the various stakeholders and stakeholder groups with the goal of understanding their respective needs and requirements from a risk (and opportunity management) perspective and ensuring that assessment and treatment of risks is performed adequately;

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC/IEEE 16085:2021

© ISO/IEC 2021 – All rights reserved
© IEEE 2021 – All rights reserved

— the supplier and acquirer agree that the requirements documents will be the basis whenever a question arises as to what is needed.

7.5.4 System/Software requirements definition process

7.5.4.1 General

NOTE The process name used here is from ISO/IEC/IEEE 12207. In ISO/IEC/IEEE 15288, this is the "System requirements definition process".

7.5.4.2 Typical risk areas

Typical risks of the System/Software Requirements Definition process can include:

— stakeholders needs and requirements are insufficiently or inaccurately captured;

— postponing requirement definitions that are critical to project success;

— requirements are too vague and can be interpreted in different ways;

— established software/system requirements are ignored;

— everyone measures the non-quantified requirements differently;

— system/software requirements do not satisfy the stakeholder requirements or business requirements;

— requirements go beyond the stakeholder needs and business requirements;

— system/software requirements contain the phrase "just the same as the present"; the term "same" is interpreted correctly only if it is about existing, discrete, tangible objects such as software programs;

— sudden growth in requirements;

— interfaces with other systems and with humans are not understood or defined;

— different priorities and weights of requirements are not shared with all stakeholders;

— requirements are not able to be verified and validated;

— there is a significant amount of requirements rework as project progresses ("scope creep").

7.5.4.3 Typical opportunity areas

Typical opportunities of the System/Software Requirements Definition process can include:

— capturing needs and requirements from stakeholders;

— stakeholders review requirements;

— prioritizing requirements;

— enhancing the requirements process to effectively and efficiently address changing requirements;

— analyzing the present system to derive requirements;

— validating the requirements form the viewpoint of the business;

— involving stakeholders in requirements change process.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC/IEEE 16085:2021

© ISO/IEC 2021 – All rights reserved
© IEEE 2021 – All rights reserved

7.5.4.4 Typical treatments

Typical treatments of the System/Software Requirements Definition process can include:

— using an iterative requirements process if requirements are incomplete;

— allowing sufficient time for requirements to be elicited and defined;

— informing suppliers if the requirements are incomplete;

— selecting a development approach that will allow requirements to evolve throughout the project;

— stakeholders will take measure to reduce risks caused by missing requirements;

— clearly stating the upgrades needed to the existing system to avoid confusion;

— the acquirer makes good use of the supplier's skill and experience at the requirements definition phase;

— when questions arise among the stakeholders, using the latest requirements baseline to provide answers;

— quantifying requirements as much as possible with the assistance of the stakeholders as needed;

— prioritizing requirements.

7.5.5 Architecture definition process

7.5.5.1 Typical risk areas

Typical risks of the Architecture Definition process can include:

— solution is incomplete and does not meet all the requirements;

— incomplete properties and relationships;

— multiple system configurations that cause architectural complexity;

— architecture inadvertently constrains future direction or growth of the system;

— interfaces with other systems and with humans are not incorporated into architecture;

— interfaces are not defined correctly.

7.5.5.2 Typical opportunity areas

Typical opportunities of the Architecture Definition process can include:

— optimizing the system attributes;

— modifying the architecture to simplify the design.

7.5.5.3 Typical treatments

Typical treatments of the Architecture Definition process can include:

— using architecture design language;

— using a defined architecture framework;

— documenting intended use of architecture;

— evaluating the architecture and applying the findings.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC/IEEE 16085:2021

© ISO/IEC 2021 – All rights reserved
© IEEE 2021 – All rights reserved

NOTE For architecture evaluation, ISO/IEC/IEEE 42030 can be applied.

7.5.6 Design definition process

7.5.6.1 Typical risk areas

Typical risks of the Design Definition process can include:

— incomplete design;

— unclear or incomplete specification of requirements;

— rushing through the design process;

— not addressing non-functional requirements;

— compromising on the design to meet resource constraints;

— complex design that exceeds the needs of the requirements and architecture;

— not addressing all functional requirements;

— lack of design documentation to support maintenance;

— design not maintained current with requirements;

— reducing functionality to compensate for cost and schedule overruns.

7.5.6.2 Typical opportunity areas

Typical opportunities of the Design Definition process can include:

— reuse of design elements;

— refactoring the architecture and design to address changes in requirements;

— simplifying the design by identifying unnecessary operations or insufficient procedures;

— designing good human interface.

7.5.6.3 Typical treatments

Typical treatments of the Design Definition process can include:

— consistent use of design patterns, models, and tools;

— checking design elements for traceability to requirements;

— stakeholders review of design definition;

— tracking of requirements traceability to and from (bi-directional) the requirements.

7.5.7 System analysis process

7.5.7.1 General

NOTE The System Analysis process can be employed for a system, a software system, or any element.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC/IEEE 16085:2021

© ISO/IEC 2021 – All rights reserved
© IEEE 2021 – All rights reserved

7.5.7.2 Typical risk areas

Typical risks of the System Analysis process can include:

— only examining a subset of systems critical to the project;

— improperly quantified assumptions based on inadequate input;

— use of biased algorithms;

— differences between simulated time scale(s) and actual real time.

7.5.7.3 Typical opportunity areas

Typical opportunities of the System Analysis process can include:

— reuse;

— identifying the most critical systems and performing a detailed evaluation and analysis;

— identifying overly complex design or system elements which can be simplified;

— incorporating the use of non-developed items such as commercial off the shelf (COTS) or open source software.

7.5.7.4 Typical treatments

Typical treatments of the System Analysis process can include:

— reviewing analysis process for system information and data to confirm it is being implemented consistently.

7.5.8 Implementation process

7.5.8.1 General

For software systems, the purpose of the Implementation process is to realize a software system element.

7.5.8.2 Typical risk areas

Typical risks of the Implementation process can include:

— implementation begins before development, verification, and integration activities are sufficiently complete.

7.5.8.3 Typical opportunity areas

Typical opportunities of the Implementation process can include:

— an iterative or incremental approach is used to minimize the risk.

7.5.8.4 Typical treatments

Typical treatments of the Implementation process can include:

— conducting data analysis, visualizing the current processes, and prioritizing the problems and solutions;

— quantifying the implementation of the process;

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC/IEEE 16085:2021

© ISO/IEC 2021 – All rights reserved
© IEEE 2021 – All rights reserved

— defining a communication approach for implementation;

— completing reviews of the appropriate outputs of upstream processes before using as an input to the Implementation process for the corresponding component.

7.5.9 Integration process

7.5.9.1 Typical risk areas

Typical risks of the Integration process can include:

— not finding problems earlier when they are easier to fix;

— missing requirements and interfaces;

— incomplete or inadequate integration activities;

— lack of supporting infrastructure for integration;

— lack of structured integration process;

— system components including software are not tested as planned before being moved to integration.

7.5.9.2 Typical opportunity areas

Typical opportunities of the Integration process can include:

— leveraging activities with verification and validation process;

— early integration confirms key system end-end threads.

7.5.9.3 Typical treatments

Typical treatments of the Integration process can include:

— planning the sequence of integration;

— progressively testing partial system configurations;

— planning for rework an expected level of integration issues, based on the characteristics of the processes;

— designing facilities and infrastructure to support the expected integration processes and schedule expectations;

— instrumenting the system to allow efficient integration;

— where possible, starting integration activities early in the lifecycle.

7.5.10 Verification process

7.5.10.1 Typical risk areas

Typical risks of the Verification process can include:

— lack of updated requirements;

— verification activities are not using the current requirements;

— verification activities are not being performed with a consistent and relevant set of work products (requirements, architecture, design, prototype, and test cases);

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC/IEEE 16085:2021

© ISO/IEC 2021 – All rights reserved
© IEEE 2021 – All rights reserved

— poor management of identified issues;

— verification only occurs during testing;

— reviews are not performed during early stages of the lifecycle.

7.5.10.2 Typical opportunity areas

Typical opportunities of the Verification process can include:

— improved analysis and review of techniques and strategies;

— performing review based on measures of complexity;

— improved testing techniques and strategies such as risk-based testing;

— Use of automation.

7.5.10.3 Typical treatments

Typical treatments of the Verification process can include:

— quantifying the verification process and performing analyses;

— regularly reviewing verification activities.

7.5.11 Transition process

7.5.11.1 Typical risk areas

Typical risks of the Transition process can include:

— complex interactions between integration, verification and validation, transition, and acceptance processes are poorly defined or planned;

— transition takes too long resulting in delay of organizational operations;

— loss or corruption of data during transition;

— incomplete configuration is transitioned, missing some components;

— no possibility to roll back in the event of transition failure;

— users are unable or unwilling to work with the new system;

— interfaces with external systems are inactivated.

7.5.11.2 Typical opportunity areas

Typical opportunities of the Transition process can include:

— integration, verification and validation, transition, and acceptance processes are integrated and well planned;

— inefficient and costly processes are eliminated or automated;

— seldom-used data is archived;

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC/IEEE 16085:2021

© ISO/IEC 2021 – All rights reserved
© IEEE 2021 – All rights reserved

7.5.11.3 Typical treatments

Typical treatments of the Transition process can include:

— clear arrangements and responsibilities for transition are established in acquisition and supply agreements;

— preparing detailed transition and recovery plans;

— rehearsing system backup and restore, transition activities and data migrations;

— performing pilot site or incremental transitions where feasible;

— using change management and user training to familiarize users with transitioned systems;

— increasing user support and problem management support immediately following transition.

7.5.12 Validation process

7.5.12.1 Typical risk areas

Typical risks of the Validation process can include:

— validation environment is not available;

— validation is only performed in the later lifecycle stages of a project;

— validation is not performed before and after transition;

— sufficient time is not scheduled for validation activities prior to system installation;

— factory acceptance test or qualification tests are not conducted due to schedule constraints;

— accelerated aging testing time for validation is shortened from actual lifetime of the system.

7.5.12.2 Typical opportunity areas

Typical opportunities of the Validation process can include:

— leveraging validation activities and environments used on other projects;

— performing validation activities early and often;

— using a validation test environment as similar as possible to the expected operating environment.

7.5.12.3 Typical treatments

Typical treatments of the Validation process can include:

— improved traceability between stakeholder needs and requirements and risks;

— performing validation in an environment similar to the intended operating conditions.

7.5.13 Operation process

7.5.13.1 Typical risk areas

Typical risks of the Operation process can include:

— poor system usability;

— failure to achieve business/mission outcomes;

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC/IEEE 16085:2021

© ISO/IEC 2021 – All rights reserved
© IEEE 2021 – All rights reserved

— system used outside its planned design envelope;

— not simulating operations early enough in the project;

— operational service is interrupted or compromised due to disaster, loss of power, security attacks, or insufficient capacity;

— time lag (also known as latency) between remote operation and actual system activation resulting from effect of various operating conditions.

7.5.13.2 Typical opportunity areas

Typical opportunities of the Operation process can include:

— human intervention and manual monitoring processes are automated;

— hardware- and software-independent processes are virtualized;

— technology advances are implemented into the operational environment;

— development-operations cooperation improves timeliness and value of system improvements.

7.5.13.3 Typical treatments

Typical treatments of the Operation process can include:

— early operator involvement;

— well-documented operating envelope;

— virtualizing systems;

— implementing integrated CM, problem management, incident management, and security management tools;

— developing and rehearsing disaster recovery plans.

7.5.14 Maintenance process

7.5.14.1 Typical risk areas

Typical risks of the Maintenance process can include:

— system is not designed for efficient maintenance;

— maintenance does not maintain alignment with architectural intent;

— maintenance needs and requirements are not considered early in the project;

— poorly documented system impedes problem analysis;

— extended system lifespan reduces skilled maintenance sources.

7.5.14.2 Typical opportunity areas

Typical opportunities of the Maintenance process can include:

— use of techniques such as reliability-centered maintenance;

— use of agile and incremental techniques (perfective maintenance) for continuing system improvements and adaptation to new technologies.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC/IEEE 16085:2021

© ISO/IEC 2021 – All rights reserved
© IEEE 2021 – All rights reserved