INTERNATIONAL STANDARD

ISO/IEC/IEEE 16085

First edition
2021-01

Systems and software engineering — Life cycle processes — Risk management

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

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

COPYRIGHT PROTECTED DOCUMENT

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

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

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

Published in Switzerland

Contents

Page

Foreword ..... **v**

Introduction ..... **vii**

1 Scope **1**
1.1 Overview 1
1.2 Purpose 1
1.3 Field of application 1

2 Normative references **2**

3 Terms and definitions **2**

4 Conformance **5**
4.1 Intended usage 5
4.2 Conformance to information items 5
4.3 Conformance to process 5
4.4 Full conformance 5

5 Key concepts and application **5**
5.1 Key concepts 5
5.1.1 Risk and opportunity 5
5.1.2 Project and organizational specific terminology 5
5.1.3 Systems and software 6
5.1.4 Uncertainty and its relationship to risk 6
5.1.5 Complexity and its relationship to risk 6
5.1.6 Risk management above the project level 6
5.1.7 Purpose and principles for risk management 6
5.2 Application 7
5.2.1 General 7
5.2.2 Application with ISO/IEC/IEEE 15288 or ISO/IEC/IEEE 12207 8
5.2.3 Application with ISO 31000 8
5.2.4 Application with ISO 9001 8
5.2.5 Application with other ISO, IEC, ISO/IEC, and ISO/IEC/IEEE standards 9

6 Risk management process **9**
6.1 Purpose 9
6.2 Process 9
6.3 Outcomes 11
6.4 Activities and tasks 11
6.4.1 General 11
6.4.2 Plan risk management 11
6.4.3 Manage the risk profile 12
6.4.4 Analyze risks 13
6.4.5 Treat risks 16
6.4.6 Monitor risks 18
6.4.7 Evaluate the risk management process 18

7 Risk management in life cycle processes **19**
7.1 Overview 19
7.2 Risk management in agreement processes 19
7.2.1 General 19
7.2.2 Acquisition process 19
7.2.3 Supply Process 20
7.3 Risk management in organizational project-enabling processes 21
7.3.1 General 21
7.3.2 Life cycle model management process 22
7.3.3 Infrastructure management process 22
7.3.4 Portfolio management process 23
7.3.5 Human resource management process 23

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

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

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

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. The IEEE develops its standards through a consensus development process, approved by the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and serve without compensation. While the IEEE administers the process and establishes rules to promote fairness in the consensus development process, the IEEE does not independently evaluate, test, or verify the accuracy of any of the information contained in its standards.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see https://patents.iec.c).

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

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

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

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

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

— Use common terminology, common process names, and common process structure with ISO/IEC/IEEE 15288:2015 and ISO/IEC/IEEE 12207:2017.

— Improve consistency with ISO 31000:2018, which provides generic principles, framework, and process for managing all forms of risk.

— Provide specialized guidance for performing risk management within the context of systems and software engineering projects.

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

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

Introduction

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

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