TECHNICAL REPORT

ISO/IEC TR 7052

First edition
2023-09

Software engineering — Controlling frequently occurring risks during development and maintenance of custom software

Ingéniérie du logiciel — Contrôle des risques fréquents au cours du développement et de la maintenance d'un logiciel sur mesure

Reference number
ISO/IEC TR 7052:2023(E)

© ISO/IEC 2023



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2023

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 at the address below or ISO's member body in the country of the requester.

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

Published in Switzerland

© ISO/IEC 2023 – All rights reserved

Contents

Page

Foreword ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Abbreviated terms ... **11**
5 Explanatory note on terms ... **11**
5.1 The term risk ... 11
5.2 The term control ... 11
6 Risks ... **12**
6.1 General ... 12
6.2 Product-related risks ... 13
6.2.1 General ... 13
6.2.2 Risk 01: The quality of the software is reduced because of modifications to it ... 13
6.2.3 Risk 02: The quality of the software is reduced because of modifications to the environment in which it runs ... 13
6.3 Project-related risks ... 14
6.3.1 General ... 14
6.3.2 Risk 03: Planned functionality is not completed on time because of underestimation of the amount of work involved ... 14
6.3.3 Risk 04: The product is not delivered on time and within budget because the scope is changed ... 14
6.3.4 Risk 05: The software does not meet the requirements laid down because the team does not have the required expertise ... 15
6.3.5 Risk 06: The product does not offer the right functionality because of inadequate management of the work ... 15
6.3.6 Risk 07: The product lacks the right non-functional properties because functional requirements were given too much priority ... 16
6.3.7 Risk 08: Misunderstandings occur because the communication between stakeholders is poor ... 16
6.3.8 Risk 09: Custom software does not (demonstrably) meet obligations because development, use and maintenance were not sufficiently auditable ... 17
6.3.9 Risk 10: The product is not delivered on time because a great deal of time was needed to set up for software development ... 17
7 Controls ... **18**
7.1 General ... 18
7.2 Project-related controls ... 18
7.2.1 General ... 18
7.2.2 Project preparation ... 19
7.2.3 Project execution ... 23
7.2.4 Completion of development and/or maintenance ... 27
7.3 Organization-related controls ... 28
7.3.1 Control 16: Supporting teams with specialist knowledge and tools ... 28
7.3.2 Control 17: Continuous risk management ... 29
Annex A (informative) **Overview of risks and controls** ... **31**
Annex B (informative) **Assessment tool** ... **33**
Bibliography ... **35**

© ISO/IEC 2023 – 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 document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 7, *Software and systems engineering*.

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 and www.iec.ch/national-committees.

© ISO/IEC 2023 – All rights reserved

Introduction

Information and communication technology (ICT) projects run many risks. ICT projects often have to contend with delay, budget overruns, and an end result of low quality.

ICT projects in which custom software is developed and/or maintained often run extra risks, on top of the risks that are part and parcel of ICT projects in general[31]. This seems to be caused by the sheer size and complexity of such custom software projects, and by a failure to mitigate the risks inherent to software development in general, despite the fact that they are well known, and that there are suitable controls for their management.

This document describes controls for some of the risks inherent in custom software development. The purpose of this document is that during the development of custom software stakeholders can avail themselves of a collection of suitable controls. The controls included are common of themselves, making this collection of controls a logical starting point for assuring the quality of custom software development. Controls were selected for inclusion based on the experience and opinion of the subject matter experts contributing to this document.

Two target groups are important when mitigating risks during the development of custom software:

a) the software development acquirers and suppliers;

b) the end users and maintainers of the software developed.

This document details risks and controls specific to custom software development. Risk management in the context of software development is covered in ISO/IEC/IEEE 12207 and its elaboration standard ISO/IEC/IEEE 16085. Generic risk management is covered by ISO 31000 and its related standards.

This document is based on NPR 5326 developed by Royal Netherlands Standardization Institute Foundation (NEN, https://www.nen.nl/).

© ISO/IEC 2023 – All rights reserved

Software engineering — Controlling frequently occurring risks during development and maintenance of custom software

1 Scope

This document:

— describes frequently occurring risks during development and maintenance of custom software;

— describes possible controls for frequently occurring risks;

— describes the related:

  — activities, facilities and roles typically used for these controls;

  — properties of products and processes;

  — standards, measurements, testing and assessment of the properties of products and processes.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

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

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
acceptance test-driven development
ATDD
development method where team members with various backgrounds [*developers* (3.18), testers and business analysts] jointly write the acceptance tests prior to development of the relevant functionality

Note 1 to entry: Although the name of the method, acceptance test-driven development, suggests that ATDD is a specialization of *test-driven development* (3.46) (TDD), this is not the case. Rather, TDD focuses on driving development by writing *unit tests* (3.48) first and ATDD focuses on driving development by writing acceptance tests first.

[SOURCE: NEN NPR 5326:2019, 3.1, modified —Added note 1 to entry.]

3.2
acquirer
stakeholder that acquires or procures a product or service from a *supplier* (3.44)

Note 1 to entry: Other terms commonly used for an acquirer are buyer, customer, owner, purchaser or internal/organizational sponsor.

[SOURCE: ISO/IEC/IEEE 12207:2017, 3.1.1]

© ISO/IEC 2023 – All rights reserved