TECHNICAL REPORT

ISO/IEC TR 33015

First edition
2019-08

Information technology — Process assessment — Guidance for process risk determination

Technologies de l'information — Évaluation des processus — Recommandations pour la détermination des risques liés aux processus

Reference number
ISO/IEC TR 33015:2019(E)

© ISO/IEC 2019



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2019

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
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword ..... **v**

Introduction ..... **vi**

1 Scope **1**

2 Normative references **1**

3 Terms and definitions **1**

4 General introduction **1**
4.1 Determining process-related risk 1
4.2 Process risk determination — purpose and outcomes 2
4.3 Significance of the process risk determination results 3
4.3.1 Impact of the assessment scope and the process context on the results of the process risk determination 3
4.3.2 Categorizing process-related risks 3
4.3.3 Defining specific rating guidelines 3

5 Process risk determination process **4**
5.1 Overview 4
5.2 Activities of process risk determination 4
5.2.1 Step 1 – Initiate process risk determination 4
5.2.2 Step 2 – Identify relevant processes and the relevant process context 5
5.2.3 Step 3 – Define target process profile 5
5.2.4 Step 4 – Define target assessment input 5
5.2.5 Step 5 – Assess current process quality 5
5.2.6 Step 6 – Determine proposed process quality characteristic achievement 6
5.2.7 Step 7 – Verify proposed process quality characteristic achievement 6
5.2.8 Step 8 – Analyse process-related risk 7
5.2.9 Step 9 – Act on results 7

6 Guidance on process risk determination **7**
6.1 General 7
6.2 Initiating the process risk determination 7
6.3 Determining the target assessment input 8
6.3.1 General 8
6.3.2 Selecting the process quality characteristic and the process measurement framework 8
6.3.3 Selecting process reference model(s) 8
6.3.4 Selecting the process assessment model 8
6.3.5 Selecting the set of processes 8
6.3.6 Determining the process context 9
6.4 Defining target process profile 9
6.5 Guidelines for assessments used for process risk determination 12
6.5.1 General 12
6.5.2 Specific guidelines on determining the target assessment input 12
6.5.3 Specific criteria for data and information collection 12
6.5.4 Specific rating rules or recommendations 13
6.6 Evaluating process-related risk 13
6.6.1 Inferring process-related risk from assessment output 13
6.6.2 Analysing weaknesses 15
6.7 Using process risk determination for supplier selection 15
6.8 Comparability of assessment output analysis 15

Annex A (informative) **Categorizing types of process-related risks** **17**

Annex B (informative) **Analysing process-related risks** **21**

Annex C (informative) **Target process profiles** **27**

© ISO/IEC 2019 – All rights reserved

Bibliography **34**

 © ISO/IEC 2019 – 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).

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 http://patents.iec.ch).

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/TC JTC1, *Information technology*, Subcommittee SC 7, *System and software engineering*.

This first edition cancels and replaces ISO/IEC TR 15504-4:2004 and ISO/IEC TR 15504-9:2011, which have been technically revised.

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.

© ISO/IEC 2019 – All rights reserved

Introduction

This document is part of a set of International Standards ISO/IEC 33001 – ISO/IEC 33099, termed the ISO/IEC 330xx family, designed to provide a consistent and coherent framework for the assessment of process quality characteristics, based on objective evidence resulting from implementation of the processes. The framework for assessment covers processes employed in the development, maintenance, and use of systems across the information technology domain and those employed in the design, transition, delivery, and improvement of services. Results of assessment can be applied for improving process performance, or for identifying and addressing risks associated with application of processes.

This document provides guidance on the application of the results of process assessment for process risk determination. The guidance covers:

— Initiating process risk determination

— Identifying relevant processes and the relevant process context

— Defining target process profile

— Defining target assessment input

— Assessing current process quality

— Determining proposed process quality characteristic achievement

— Verifying proposed process quality characteristic achievement

— Analysing process-related risk

— Acting on results

This document is primarily addressed to the stakeholders of the process risk determination, members of the process risk determination team and other people, such as lead assessors or assessment team members, who need guidance on performing a process risk determination based on conformant process assessments. It will also be of value to developers of process assessment methods and tools supporting process assessment as well as members of assessed organizations.

The set of International Standards ISO/IEC 33001 – ISO/IEC 33099 defines the requirements and resources needed for process assessment. The overall architecture and content is described in ISO/IEC 33001.

This document assumes familiarity with the normative parts of the ISO/IEC 330xx family of standards.

Several International Standards in the ISO/IEC 330xx family of standards for process assessment are intended to replace and extend parts of the ISO/IEC 15504 series. ISO/IEC 33001:2015, Annex A provides a detailed record of the relationship between the ISO/IEC 330xx family and the ISO/IEC 15504 series.

© ISO/IEC 2019 – All rights reserved

Information technology — Process assessment — Guidance for process risk determination

1 Scope

This document provides guidance on the application of the results of a process assessment for process risk determination.

The guidance provided does not presume specific organizational structures, management philosophies, life cycle models or development methods. In relation to process risk determination, this guidance is applicable within any customer–supplier relationship, and to any organization wishing to perform a process risk determination of its processes.

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 33001, *Information technology — Process assessment — Concepts and terminology*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 33001 and the following apply.

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

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

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

3.1
process risk determination
systematic assessment and analysis of selected processes against a target process profile, carried out with the aim of identifying process-related risks to meet a particular specified requirement

3.2
process-related risk
risk resulting from weaknesses in the performance, management, or deployment of a process

4 General introduction

4.1 Determining process-related risk

The purpose of process assessment is to understand the state of the processes implemented by an organizational unit.

Results of a process assessment can be applied for improving process performance, or for identifying and addressing process-related risks associated with the application of processes.

Guidance on using process assessment as part of a complete framework and method for process improvement as part of a continual improvement activity is provided in ISO/IEC 33014.

© ISO/IEC 2019 – All rights reserved