



Nederlandse praktijkrichtlijn

NPR-ISO/IEC TR 33015 (en)

Information technology - Process assessment -
Guidance for process risk determination (ISO/IEC
TR 33015:2019,IDT)

Vervangt NEN-ISO/IEC 15504-4:2004;
NPR-ISO/IEC TS 15504-9:2011

ICS 35.080
augustus 2019

Als Nederlandse praktijkrichtlijn is aanvaard:

- ISO/IEC TR 33015:2019, IDT

Preview

Normcommissie 381007 'Software and systems engineering'



THIS PUBLICATION IS COPYRIGHT PROTECTED

DEZE PUBLICATIE IS AUTEURSRECHTELIJK BESCHERMD

Apart from exceptions provided by the law, nothing from this publication may be duplicated and/or published by means of photocopy, microfilm, storage in computer files or otherwise, which also applies to full or partial processing, without the written consent of the Royal Netherlands Standardization Institute.

The Royal Netherlands Standardization Institute shall, with the exclusion of any other beneficiary, collect payments owed by third parties for duplication and/or act in and out of law, where this authority is not transferred or falls by right to the Reproduction Rights Foundation.

Auteursrecht voorbehouden. Behoudens uitzondering door de wet gesteld mag zonder schriftelijke toestemming van het Koninklijk Nederlands Normalisatie-instituut niets uit deze uitgave worden verveelvoudigd en/of openbaar gemaakt door middel van fotokopie, microfilm, opslag in computerbestanden of anderszins, hetgeen ook van toepassing is op gehele of gedeeltelijke bewerking.

Het Koninklijk Nederlands Normalisatie-instituut is met uitsluiting van ieder ander gerechtigd de door derden verschuldigde vergoedingen voor verveelvoudiging te innen en/of daartoe in en buiten rechte op te treden, voor zover deze bevoegdheid niet is overgedragen c.q. rechtens toekomt aan de Stichting Reprorecht.

Although the utmost care has been taken with this publication, errors and omissions cannot be entirely excluded. The Royal Netherlands Standardization Institute and/or the members of the committees therefore accept no liability, not even for direct or indirect damage, occurring due to or in relation with the application of publications issued by the Royal Netherlands Standardization Institute.

Hoewel bij deze uitgave de uiterste zorg is nagestreefd, kunnen fouten en onvolledigheden niet geheel worden uitgesloten. Het Koninklijk Nederlands Normalisatie-instituut en/of de leden van de commissies aanvaarden derhalve geen enkele aansprakelijkheid, ook niet voor directe of indirecte schade, ontstaan door of verband houdend met toepassing van door het Koninklijk Nederlands Normalisatie-instituut gepubliceerde uitgaven.



©2019 Koninklijk Nederlands Normalisatie-instituut
Postbus 5059, 2600 GB Delft
Telefoon (015) 2 690 390, www.nen.nl

Copyright
Preview

**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*



Copyright
Preview



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

Bibliography 34

Copyright
Preview

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, *Systems 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.

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.

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.

Bestelformulier

Stuur naar:

NEN Standards Products & Services
t.a.v. afdeling Klantenservice
Antwoordnummer 10214
2600 WB Delft



NEN Standards Products & Services

Postbus 5059
2600 GB Delft

Vlinderweg 6
2623 AX Delft

T (015) 2 690 390
F (015) 2 690 271

www.nen.nl/normshop

Ja, ik bestel

__ ex. NPR-ISO/IEC TR 33015:2019 en

€ 125.90

Wilt u deze norm in PDF-formaat? Deze bestelt u eenvoudig via www.nen.nl/normshop

Gratis e-mailnieuwsbrieven

Wilt u op de hoogte blijven van de laatste ontwikkelingen op het gebied van normen, normalisatie en regelgeving? Neem dan een gratis abonnement op een van onze e-mailnieuwsbrieven. www.nen.nl/nieuwsbrieven

Gegevens

Bedrijf / Instelling

T.a.v. O M O V

E-mail

Klantnummer NEN

Uw ordernummer BTW nummer

Postbus / Adres

Postcode Plaats

Telefoon Fax

Factuuradres (indien dit afwijkt van bovenstaand adres)

Postbus / Adres

Postcode Plaats

Datum Handtekening

Retourneren

Fax: 015 2 690 271

E-mail: klantenservice@nen.nl

Post: NEN Standards Products & Services,

t.a.v. afdeling Klantenservice
Antwoordnummer 10214,
2600 WB Delft

(geen postzegel nodig).

Voorwaarden

- De prijzen zijn geldig tot 31 december 2018, tenzij anders aangegeven.
- Alle prijzen zijn excl. btw, verzend- en handelingskosten en onder voorbehoud bij o.m. ISO- en IEC-normen.
- Bestelt u via de normshop een pdf, dan betaalt u geen handeling en verzendkosten.
- Meer informatie: telefoon 015 2 690 391, dagelijks van 8.30 tot 17.00 uur.
- Wijzigingen en typfouten in teksten en prijsinformatie voorbehouden.
- U kunt onze algemene voorwaarden terugvinden op: www.nen.nl/leveringsvoorwaarden.