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 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

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.

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.

This document focuses on using the results of process assessment to identify process-related risks and to determine the significance associated with application of the processes for a particular requirement or category of requirements. This can be performed to support risk mitigations, or to support decision making in acquisition scenarios.

NOTE 1 The particular requirement or the category of requirements can involve deploying an organization's processes for a new or an existing task, a contract, category of contracts, or an internal undertaking, a product or a service, or any other business requirement. The particular requirement or the category of requirements is defining the objective(s) for the process risk determination.

NOTE 2 Process risk determination does not address all aspects of risk, which can include strategic, organizational, financial, personnel and many other factors. The output from a process risk determination feeds into an organization's risk management process, but only with respect to process-related risk – as outlined in 6.6.

Determining process-related risks from process assessment results is based on mapping weaknesses to risks. Weaknesses are represented by process attribute ratings which differ from a full achievement. By comparing the achievement of process attribute ratings with a target process profile gaps can be identified which may give evidence to one or more specific risks.

The alignment of the underlying scope of the assessment to the particular requirement or category of requirements will impact the significance of the results of the process risk determination. When assessing processes with respect to a given process quality characteristic, ISO/IEC 33002 requires the identification of the process context as a part of the assessment scope. The process context describes the relations and dependencies between the application of a set of processes and their impact on a developed product, service or the organization developing it.

When aligning the assessment scope to the particular requirement or category of requirements, this should be done with respect to

— the impact of the selected processes to identified risks under investigation; and

— the comparability of the process context with the intended application of the processes for a particular requirement or category of requirements.

An assessment may be conducted specifically to determine process-related risks or may be selected from a pool of existing results.

In the first case, a target assessment scope including the process context should be defined as an input to the assessment. 6.3 provides guidance when defining a target assessment input.

In case the results are taken from a pool, special analysis should be performed to assure the significance of a selected assessment result as described in 6.8.

In any case, a target process profile of the desired extent of achievement of the process quality characteristic should be defined in relation to a given process context (for example, in relation to the development of a specific system). As described in 4.3.2, the target process quality level should be set up with respect to the existing particular requirements for the process risk determination thus matching the specific types of risks to be evaluated.

4.2 Process risk determination — purpose and outcomes

The purpose of process risk determination is to identify risks and to determine the significance of identified risks associated with application of the processes for a particular requirement or category of requirements.

As a result of successful implementation of process risk determination:

— objectives of the process risk determination are defined by identifying the particular requirement or category of requirements;

— types of risks to be evaluated appropriate to a particular requirement or category of requirements are identified, if applicable;

- target assessment input including the assessment scope and the process context is identified;
- target process profile in line with the target assessment input and appropriate to the objectives of the process risk determination is specified;
- process quality levels are determined according to the process context and the selected process profile;
- any gaps between target and assessed process quality characteristics are analysed;
- specific process-related types of risks are evaluated based on the gap analysis.

NOTE 1 The selected processes are chosen by the team as described in 5.2.2.

NOTE 2 The determination of process quality levels is generally carried out following a process assessment of the organization's implemented processes, as described in ISO/IEC 33002.

4.3 Significance of the process risk determination results

4.3.1 Impact of the assessment scope and the process context on the results of the process risk determination

When performing an assessment, the lack of achievement of process quality attributes for a selected process reference or process assessment model can give evidence for a specific risk or type of risk. Each risk type requires an appropriate assessment scope to be defined including a determined process context.

If an assessment is conducted specifically to determine process-related risks or if an assessment result is selected from a pool of existing results, the underlying assessment scope including the process context will impact the significance of the results.

To increase the significance of the results and conclusions, the process risk determination team may identify the type of risks to be addressed according to the particular requirement or category of requirements for the process risk determination. According to the identified type of risk, an appropriate target assessment scope should be set up, which is the base for defining the target assessment capability profile. Annex A provides a guideline on categorizing types of process-related risks.

The significance of the process risk determination results is further increased by defining specific assessment guidelines including criteria for collecting data and information collection as described in 6.5.

4.3.2 Categorizing process-related risks

The types of risks to be identified are defined by the objectives of the process risk determination and associated with application of the processes for a particular requirement or category of requirements.

To increase the level of significance of the process risk determination result, a specific type of risk may be identified after initializing the process risk determination to provide input for the sub-sequent steps. When identifying types of process-related risks, the risks may be grouped to categories for a particular requirement. This may be done by mapping identified risk root causes to deficits in the achievement of process quality attributes. Annex A shows an example of a categorization of types of process-related risk.

When focussing on a specific type of risk this has an impact on the definition of the target assessment input, the target process profile and the criteria for data and information collection.

4.3.3 Defining specific rating guidelines

Specific rating guidelines including the criteria for data and information collection may be set up by a community of interest to increase the significance and comparability of process risk determination results.

Refer to 6.5.4 for additional information.

5 Process risk determination process

5.1 Overview

Figure 1 illustrates the steps of process risk determination utilising a process assessment performed according to ISO/IEC 33002.

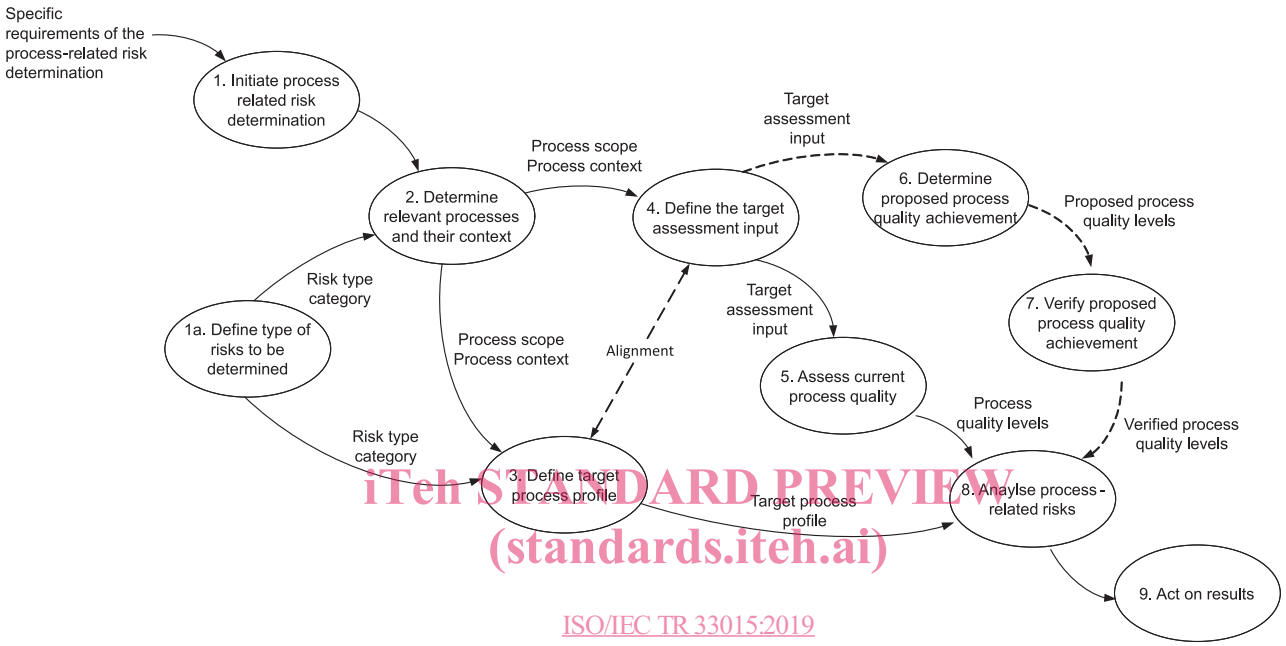

Figure 1 — Steps of process risk determination

The ovals in Figure 1 represent steps in the process, and the arrows represent information being passed between steps.

5.2 Activities of process risk determination

5.2.1 Step 1 – Initiate process risk determination

A process risk determination plan should be produced, approved by the sponsor, and used to monitor progress. The plan should include:

— the purpose of the process risk determination;

— the process assessment method to be used;

— the organizational scope i.e. the organizational unit whose processes are to be the subject of the process risk determination;

— the target process profile (inserted after it has been defined in step 3);

— key roles and responsibilities;

— resources;

— appropriate milestones, review points, and reporting mechanisms.

When carrying out the process risk determination as part of a supplier selection activity, the sponsor may decide either to disclose the target process profile to the potential suppliers, or not, as appropriate.

The sponsor may also invite the organizational unit to submit a statement of the process quality characteristics that it proposes to bring to bear in meeting the specified requirement.

The team may optionally perform a categorization to align the assessment scope to the particular requirement or category of requirements with respect to the impact of the selected processes to identified risks under investigation and the comparability of the process context with the intended application of the processes for a particular requirement or category of requirements.

Please refer to Annex A for additional guidance.

5.2.2 Step 2 – Identify relevant processes and the relevant process context

The team identifies relevant processes and associated process reference and assessment models.

The process context of the intended application of the processes for a particular requirement or category of requirements is identified.

Please refer to 6.3.3 to 6.3.5 for additional guidance.

5.2.3 Step 3 – Define target process profile

The team defines the target process profile, as described in 6.4.

The target process profile comprises a set of target process profiles that express the process quality which the team judges to be adequate, subject to an acceptable process-related risk, for meeting the specified requirement.

5.2.4 Step 4 – Define target assessment input

The target assessment input is prepared as described in 6.3.

A target assessment input is defined, which is either provided as an input for an assessment performed specifically to determine process-related risks or which is considered when selecting from a pool of existing assessment results.

The target assessment input should comprise as a minimum:

— the process quality characteristic and process measurement framework as described in 6.3.2;

— the process reference and assessment model as identified in step 2;

— the identified relevant processes and the relevant process context as defined in step 2 and in line with the target process profile as defined in step 3;

— the criteria for data and information collection as described in 6.5.3.

The target assessment input may also comprise specific rating rules or recommendations as described in 6.5.4.

Please refer to 6.3 for additional guidance.

5.2.5 Step 5 – Assess current process quality

The team may invite the organizational unit to perform an ISO/IEC 33002 conformant self-assessment based on the defined target assessment input and provide the results to the team.

Alternatively, the team may decide to initiate an independent process assessment, bearing in mind the nature, cost and importance of the specified requirement.

In either case, the output from the assessment of current process quality characteristic achievement will take the form of a set of process profiles as defined in ISO/IEC 33002.

Please refer to 6.5 for additional guidance.

5.2.6 Step 6 – Determine proposed process quality characteristic achievement

If invited to do so, the organizational unit may optionally submit to the team a statement of the process quality characteristic achievement that it proposes to bring to bear in meeting the specified requirement. The proposed process quality characteristic achievement should be based on one or more process assessments which:

— satisfy the requirements of ISO/IEC 33002;

— are a true representation of the organizational unit's current process quality characteristics with respect to the given target assessment input;

— may been produced specifically for the process risk determination, or generated during a recent self-assessment, or produced following a recent independent assessment.

A key feature of ISO/IEC 33002 is that process assessment outputs are re-useable. Many organizational units will have a repository of process assessment outputs generated as part of a process improvement programme. If a number of suitable process assessments are available, then the organizational unit may use the outputs as the basis of a proposed process quality characteristic achievement. If not, then the organization may carry out a self-assessment in accordance with the requirements of ISO/IEC 33002.

Please refer to 6.8 for additional guidance.

5.2.7 Step 7 – Verify proposed process quality characteristic achievement

If the organizational unit has submitted a statement of the process profile that it proposes to bring to bear in meeting the specified requirement, then the team should review the proposed process profile to establish how much credibility it merits, and decides what further action is needed to establish confidence in it. This will typically involve:

— checking that the proposed process profile is based on one or more conformant process assessments;

— checking the credibility of any improved process quality characteristic achievement by reviewing it against the defined target assessment input;

— checking the topicality of the assessment result.

NOTE Since detailed information about the underlying assessment (e.g. the list of collected evidence or the assessment plan) can be unavailable to the team, the verification can be supported by self-declaration of the providing organizational unit.

The sponsor may accept the proposed profile or decide to initiate an appropriate degree of independent process assessment. This may involve a sample of selected processes, or a comprehensive independent assessment of all processes specified in the target process profile. Having carried out the verification assessment, the team will be able to compare this output with the organization's proposed process quality characteristic achievement and derive a profile to be used for subsequent risk analysis.

If the process risk determination involves a number of competing suppliers, then the sponsor may wish to verify each supplier's proposed process profile by using an independent assessment team, the same assessment method and the same conformant process assessment model. This should not only provide the sponsor with greater confidence in the consistency with which each supplier is assessed, but also provide the suppliers with greater confidence in the fairness of the selection process.

If several organizational units – i.e. subcontractors, partners in a joint venture, or distinct divisions of an organization - will be involved in meeting a specified requirement, then the proposed process profile will comprise contributions from each of the organizational units.

Please refer to 6.6.2, 6.7 and 6.8 for additional guidance.

5.2.8 Step 8 – Analyse process-related risk

Process-related risk is assessed from the *probability* of a particular problem occurring, and from its potential *consequence*, should it occur as outlined in 6.6.

The chosen process risk determination method should contain a defined approach to analysing risk. A possible approach is outlined in Annex A.

5.2.9 Step 9 – Act on results

If the process risk determination has been carried out to determine the suitability of another organization's processes for a particular contract or category of contracts, then the sponsor will wish to take into account the assessment of process-related risk not only in making contract award decisions, but also when establishing contractual commitments related to ongoing risk management activities.

If the process risk determination has been carried out by an organization to determine the process quality characteristic achievement of its own processes for a particular requirement or category of requirements, then the sponsor may wish to initiate a process improvement programme to address any process-related risk issues identified.

6 Guidance on process risk determination

6.1 General

This clause provides guidance on issues specific to process risk determination.

6.2 Initiating the process risk determination

The process risk determination is based on the results of process assessments.

As described in 4.1 the objectives for the process risk determination are defined by a particular requirement or category of requirements. These requirements are determined and defined by the sponsor in line with the organization’s business goals.

ISO/IEC 33002 requires that any process assessment identify the assessment sponsor and possible assessment constraints. The sponsor for process risk determination may be, but is not generally, the same as the assessment sponsor. Especially when the process risk determination is performed in the context of supplier selection, the results might be requested by a customer organization represented by a sponsor from a pool of assessments available at the supplier which have been performed under the responsibility of different assessment sponsors.

The sponsor first decides whether or not to carry out a process risk determination.

The process risk determination should be implemented as a project in its own right, with defined project management, budget, milestones, and accountability. In short, the project should be managed according to a project management process, aligned to the process assessment model being used.

The sponsor should set up a process risk determination team to initialize the process-related risk determination, to determine the target assessment input and the target process profile, and to evaluate the process-related risks.