International Standard

ISO 18128

Information and documentation — Records risks — Risk assessment for records management

First edition
2024-03

Reference number
ISO 18128:2024(en)

© ISO 2024



COPYRIGHT PROTECTED DOCUMENT

© ISO 2024

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

Contents

Page

Foreword ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
3.1 Terms specific to risk ... 2
3.2 Terms specific to records ... 2
4 Core concepts ... **3**
4.1 Issues and concerns about uncertainty ... 3
5 Determining scope, context and criteria ... **4**
5.1 General ... 4
5.2 Defining the scope ... 4
5.3 External and internal context ... 5
5.3.1 General ... 5
5.3.2 External context ... 5
5.3.3 Internal context ... 5
5.4 Definition of records risk criteria ... 5
5.5 Risk description ... 6
6 Uses of risk assessment techniques ... **7**
7 Risk identification ... **7**
7.1 General ... 7
7.2 Techniques for identifying risks ... 8
7.2.1 General ... 8
7.2.2 Checklist analysis for risk identification ... 9
8 Risk analysis ... **9**
8.1 General ... 9
8.2 Techniques for analysing risks ... 10
8.2.1 General ... 10
8.2.2 Business impact analysis (BIA) ... 10
8.2.3 Human reliability analysis (HRA) ... 11
8.2.4 Bow tie analysis ... 12
9 Risk evaluation ... **13**
9.1 General ... 13
9.2 Techniques for evaluating risk ... 13
9.2.1 As low as reasonably practicable (ALARP) ... 13
9.2.2 Reliability-centred maintenance (RCM) ... 14
9.2.3 Risk indices ... 16
9.2.4 Cost/benefit analysis ... 18
Annex A (informative) **Categorization of techniques following IEC 31010** ... **20**
Annex B (informative) **Checklist of uncertainties** ... **22**
Bibliography ... **26**

© ISO 2024 – All rights reserved

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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 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).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes 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 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. ISO 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.

This document was prepared by Technical Committee ISO/TC 46, *Information and documentation*, Subcommittee SC 11, *Archives/records management*.

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 2024 – All rights reserved

Introduction

Successful organizations identify and manage all their business risks. Identifying and managing the risks to records processes, controls and systems (records risks) is the responsibility of the organization's records professionals.

This document is intended to help records professionals and people who have responsibility for records in their organization to assess records risks.

This is distinct from the task of identifying and assessing the organization's business risks to which creating and keeping adequate records is one strategic response. The decisions to create records or not in response to general business risks are business decisions, which should be informed by the analysis of the organization's records requirements undertaken by records professionals together with business managers. The premise of this document is that the organization has created records of its business activities to meet operational and other purposes and has established at least minimal mechanisms for the systematic management of the records.

The consequence of records risk events can be the loss of, or damage to, records, which are therefore no longer useable, reliable, authentic, complete, or unaltered, and therefore can fail to meet the organization's purposes.

The document provides guidance and examples based on the general risk management process established in ISO 31000 (see Figure 1) to apply to records risks, including information on relevant risk assessment tools and techniques. It covers the risk assessment components:

a) risk identification,

b) risk analysis, and

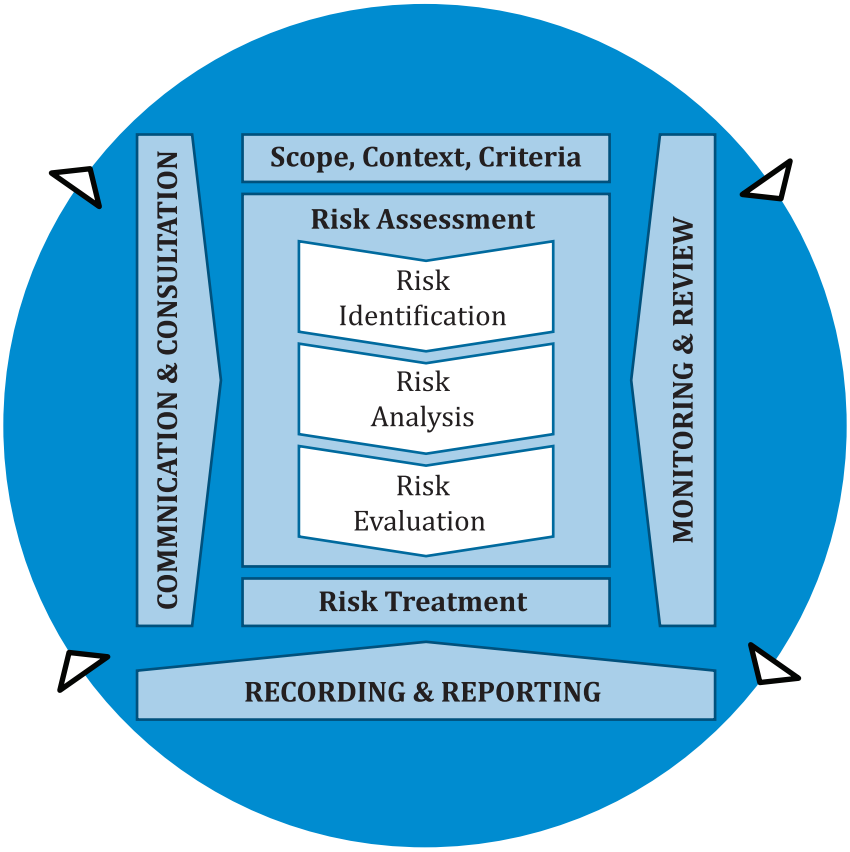
c) risk evaluation.

This document introduces and explains selected techniques from IEC 31010 that are applicable in a records management environment (see Table A.2 for the list of techniques).

The results of the assessment of records risk should be incorporated into the organization's general risk management framework. Consequently, the organization will have better control of its records and their quality for business purposes.

This document does not deal with risk treatment. Once the assessment of records risks has been completed, the assessed risks are documented and communicated to the organization's risk management section. Response to the assessed risks should be undertaken as part of the organization's overall risk management program. The priority assigned by the records professional to the assessed risks is provided to inform the organization's decisions about managing those risks.

© ISO 2024 – All rights reserved



NOTE Source ISO 31000:2018, Figure 4

Figure 1 — Risk management process

© ISO 2024 – All rights reserved

Information and documentation — Records risks — Risk assessment for records management

1 Scope

The document:

a) provides methods for identifying and documenting risks related to records, records processes, controls and systems (records risks);

b) provides techniques for analysing records risks;

c) provides guidelines for conducting an evaluation of records risks.

This document intends to assist organizations in assessing records risks so they can ensure records continue to meet identified business needs as long as required.

This document can be used by all organizations regardless of size, nature of their activities, or complexity of their functions and structure.

This document does not directly address the mitigation of risks, as methods for these vary from organization to organization.

It can be used by records professionals or people who have responsibility for records and records processes, controls and/or systems in their organizations, and by auditors or managers who have responsibility for risk management programs in their organizations.

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 30300, *Information and documentation — Records management — Core concepts and vocabulary*

ISO 31000, *Risk management — Guidelines*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 30300, ISO 31000 and the following 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/

© ISO 2024 – All rights reserved