ISO/~~DIS~~PRF 18128:~~2023(E)~~

ISO/TC 46/SC 11~~N~~

~~Date: 2023-02-20~~

Secretariat: SA

Date: 2024-02-04

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

iTeh Standards
(https://standards.iteh.ai)
Document Preview

PROOF

ISO/PRF 18128
https://standards.iteh.ai/catalog/standards/iso/bf6a8b70-8354-4a37-a513-499a3d6637db/iso-prf-18128

Edited DIS - MUST BE USED FOR FINAL DRAFT

Style Definition ...

Formatted: Font: 14 pt, Bold, English (United Kingdom)

Formatted: Left: 1.5 cm, Right: 1.5 cm, Section start: New page, Width: 21 cm, Height: 29.7 cm, Header distance from edge: 1.27 cm, Footer distance from edge: 1.27 cm

Formatted ...

Formatted: zzCover large

Formatted ...

Formatted: Space Before: 0 pt, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Formatted: Cover Title_A1, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

© ISO ~~2023~~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~~ISO's member body in the country of the requester.

ISO ~~Copyright Office~~ copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: + 41 22 749 01 11

~~Email: copyright@iso.org~~
E-mail: copyright@iso.org
Website: ~~www.iso.org~~www.iso.org

Published in Switzerland.

iTeh Standards
(https://standards.iteh.ai)
Document Preview

ISO/PRF 18128
https://standards.iteh.ai/catalog/standards/iso/bf6a8b70-8354-4a37-a513-499a3d6637db/iso-prf-18128

Formatted: HeaderCentered
Formatted: Font color: Auto, English (United Kingdom)
Formatted: Font color: Auto, English (United Kingdom)
Formatted: Font color: Auto, English (United Kingdom)
Formatted: Font color: Auto, English (United Kingdom)
Formatted: zzCopyright address
Formatted: Font color: Auto, English (United Kingdom)
Formatted: Font color: Auto, English (United Kingdom)
Formatted: zzCopyright address
Formatted: Font color: Auto, French (Switzerland)
Formatted: French (Switzerland)
Formatted: Font color: Auto, French (Switzerland)
Formatted: zzCopyright address
Formatted: Font color: Auto, French (Switzerland)
Formatted: Font color: Auto, English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: FooterPageRomanNumber

Formatted: HeaderCentered, Left

Contents ~~Page~~

Foreword vi
Introduction vii
1 Scope 1
2 Normative references 1
3 Terms and definitions 1
3.1 Terms specific to risk 1
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 6
5.5 Risk description 7
6 Uses of risk assessment techniques 8
7 Risk identification 8
7.1 General 8
7.2 Techniques for identifying risks 9
7.2.1 General 9
7.2.2 Checklist analysis for risk identification 9
8 Risk analysis 11
8.1 General 11
8.2 Techniques for analysing risks 11
8.2.1 General 11
8.2.2 Business impact analysis (BIA) 11
8.2.3 Human reliability analysis (HRA) 12
8.2.4 Bow tie analysis 13
9 Risk evaluation 15
9.1 General 15
9.2 Techniques for evaluating risk 15
9.2.1 As low as reasonably practicable (ALARP) 15

iTeh Standards
(https://standards.iteh.ai)
Document Preview
ISO/PRF 18128
https://standards.iteh.ai/catalog/standards/iso/4f6e8b70-8354-4a37-a513-99a3d6637db/iso-prf-18128

Formatted: FooterPageRomanNumber

~~© ISO 2023 – All rights reserved~~

© ISO 2024 – All rights reserved

Formatted: HeaderCentered

9.2.2 Reliability-centred maintenance (RCM) 16
9.2.3 Risk indices 18
9.2.4 Cost/benefit analysis 20
Annex A (informative) 23
Annex B (informative) Checklist of uncertainties 27
Bibliography 32

~~1. Scope 1~~
~~2. Normative references 1~~
~~3. Terms and definitions 2~~
~~3.1 Terms specific to risk 2~~
~~3.2 Terms specific to records 2~~
~~4. Core concepts 4~~
~~4.1. Issues and concerns about uncertainty 4~~
~~5. Determining scope, context and criteria 4~~
~~5.1 General 4~~
~~5.2 Defining the scope 5~~
~~5.3 External and internal context 5~~
~~5.3.1 External context 5~~
~~5.3.2 Internal context 6~~
~~5.4 Definition of records risk criteria 6~~
~~5.5 Risk description 7~~
~~6. Uses of risks assessment techniques 8~~
~~7. Risk identification 8~~
~~7.1 General 8~~
~~7.2 Techniques for identifying risks 9~~
~~7.2.1 Checklist analysis for risk identification 10~~
~~8. Risk analysis 11~~
~~8.1 General 11~~
~~8.2 Techniques for analysing risks 11~~
~~8.2.1 Business Impact Analysis (BIA) 12~~
~~8.2.2 Human Reliability Analysis (HRA) 13~~
~~8.2.3 Bow tie analysis 14~~
~~9. Risk evaluation 15~~
~~9.1. General 15~~
~~9.2. Techniques for evaluating risk 15~~
~~9.2.1. As low as reasonably practicable (ALARP) 15~~

iTeh Standards
(https://standards.iteh.ai)
Document Preview
ISO/PRF 18128
https://standards.iteh.ai/catalog/standards/iso/bf6a8b70-8354-4a37-a513-499a3d6637db/iso-prf-18128

Formatted: FooterPageRomanNumber

~~© ISO 2023 – All rights reserved~~

© ISO 2024 – All rights reserved

Edited DIS - MUST BE USED FOR FINAL DRAFT

Formatted: HeaderCentered, Left

~~9.2.2. Reliability-centred maintenance (RCM) 17~~
~~9.2.3. Risk indices 19~~
~~9.2.4. Cost/benefit analysis 21~~
~~Annex A 23~~
~~A.1 Introduction to categorization of techniques following IEC 31010: 2019 23~~
~~A.2 Application of categorization of techniques following IEC 31010: 2019 24~~
~~Annex B 26~~
~~B.1 Checklist of uncertainties 26~~
~~10. Bibliography 31~~

iTeh Standards
(https://standards.iteh.ai)
Document Preview

ISO/PRF 18128
https://standards.iteh.ai/catalog/standards/iso/bf6a8b70-8354-4a37-a513-499a3d6637db/iso-prf-18128

Formatted: FooterPageRomanNumber

~~© ISO 2023 – All rights reserved~~

© ISO 2024 – All rights reserved

Formatted: HeaderCentered

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.~~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~~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~~www.iso.org/members.html.

iTeh Standards
(https://standards.iteh.ai)
Document Preview
ISO/PRF 18128
https://standards.iteh.ai/catalog/standards/sist/99a3d6637db/iso-prf-18128

Formatted: FooterPageRomanNumber

~~© ISO 2023 – All rights reserved~~

© ISO 2024 – All rights reserved

Edited DIS - MUST BE USED FOR FINAL DRAFT

Formatted: HeaderCentered, Left

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)~~Figure 1) to apply to records risks, including information on relevant risk assessment tools and techniques. It covers the risk assessment components:

a) ~~a)~~ risk identification,

b) ~~b)~~ risk analysis, and

c) ~~c)~~ risk evaluation.

iTeh Standards
(https://standards.iteh.ai)
Document Preview
ISO/PRF 18128
https://standards.iteh.ai/catalog/standards/iso/bf6a8b70-8354-4a37-a513-499a3d6637db/iso-prf-18128

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

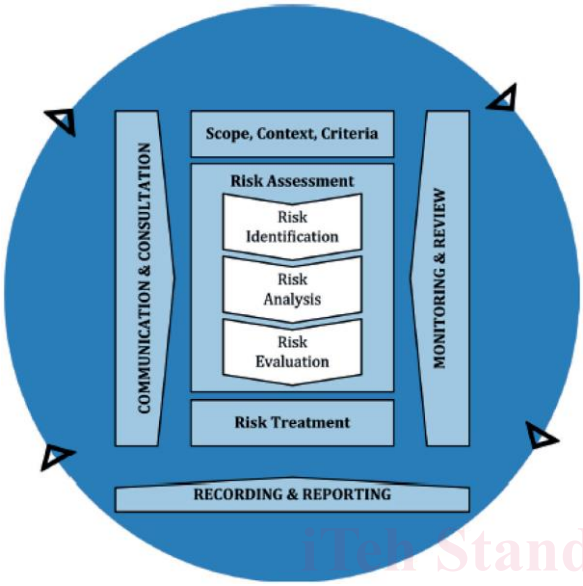
~~The~~This document does not deal with risk treatment. Once the assessment of records risks has been completed, the assessed risks are documented and communicated to the organization's risk management section. Response to the assessed risks should be undertaken as part of the organization's overall 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.

Formatted: FooterPageRomanNumber

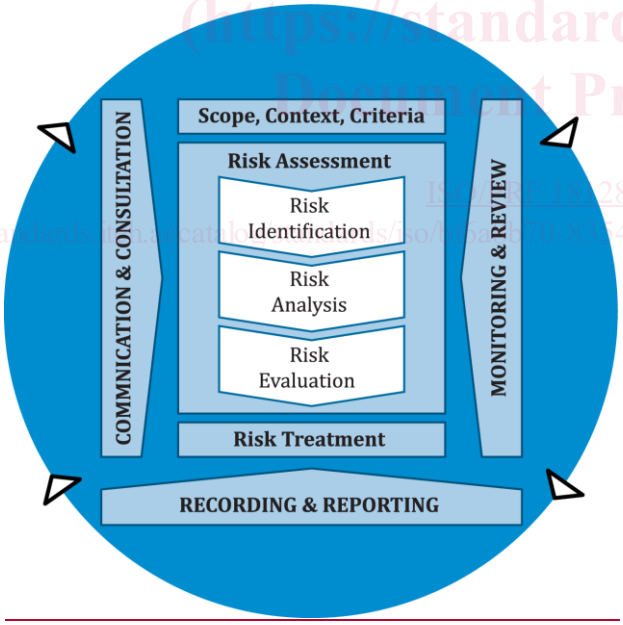
~~© ISO 2023 – All rights reserved~~

© ISO 2024 – All rights reserved

Formatted: HeaderCentered



iTeh Standards
(https://standards.iteh.ai)
Document Preview
ISO/PRF 18128
https://standards.iteh.ai/catalog/standards/iso/[illegible]-4a37-a513-499a3d6637db/iso-prf-18128



NOTE Source ISO 31000:2018, Figure 4

Formatted: FooterPageRomanNumber

~~© ISO 2023 – All rights reserved~~

© ISO 2024 – All rights reserved

Edited DIS - MUST BE USED FOR FINAL DRAFT

Formatted: HeaderCentered, Left

Figure 1 — Risk ~~Management~~management process

iTeh Standards
(https://standards.iteh.ai)
Document Preview

ISO/PRF 18128
https://standards.iteh.ai/catalog/standards/iso/bf6a8b70-8354-4a37-a513-499a3d6637db/iso-prf-18128

Formatted: FooterPageRomanNumber

~~© ISO 2023 – All rights reserved~~

© ISO 2024 – All rights reserved

iTeh Standards
(https://standards.iteh.ai)
Document Preview

ISO/PRF 18128
https://standards.iteh.ai/catalog/standards/iso/bf6a8b70-8354-4a37-a513-499a3d6637db/iso-prf-18128

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

1 Scope

The document:

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

b) ~~b)~~ provides techniques for analysing records risks;

c) ~~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 ~~address~~ directly address the mitigation of risks, as methods for these ~~will~~ 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~~:2020~~, Information and documentation — Records management — Core concepts and vocabulary

ISO 31000~~:2018~~, 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~~https://www.iso.org/obp

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

3.1 Terms specific to risk

3.1.1
risk
effect of uncertainty on objectives

~~© ISO 2023 – All rights reserved~~

iTeh Standards (https://standards.iteh.ai) Document Preview

Formatted: Font: Not Bold

Formatted: Main Title 1, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Formatted: Numbered + Level: 1 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0 cm + Indent at: 0 cm, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers, Tab stops: Not at 0.7 cm + 1.4 cm + 2.1 cm + 2.8 cm + 3.5 cm + 4.2 cm + 4.9 cm + 5.6 cm + 6.3 cm + 7 cm

Formatted: Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Formatted: Default Paragraph Font

Formatted: Adjust space between Latin and Asian text, Adjust space between Asian text and numbers, Tab stops: Not at 0.7 cm + 1.4 cm + 2.1 cm + 2.8 cm + 3.5 cm + 4.2 cm + 4.9 cm + 5.6 cm + 6.3 cm + 7 cm

Formatted: Default Paragraph Font

Formatted: Default Paragraph Font

Formatted: Default Paragraph Font

Formatted: Default Paragraph Font

Formatted: Default Paragraph Font

Formatted: Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Formatted: Default Paragraph Font

Formatted: Default Paragraph Font

Formatted: Default Paragraph Font

Formatted: Default Paragraph Font

Formatted: English (United Kingdom)

Formatted: Font: Cambria, 11 pt, English (United Kingdom)

Formatted: English (United Kingdom)

Formatted: English (United Kingdom)

Formatted: English (United Kingdom)

Formatted: Adjust space between Latin and Asian text, Adjust space between Asian text and numbers, Tab stops: Not at 0.71 cm

Formatted: Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Formatted: HeaderCentered

Note 1 to entry: An effect is a deviation from the expected. It can be positive, negative or both, and can address, create or result in opportunities and threats.

Note 2 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

Note 3 to entry: Objectives can have different aspects and categories, and can be applied at different levels.

Note 4 to entry: Risk is usually expressed in terms of risk sources, potential events, their consequences and their likelihood.

Note 5 to entry: In the high level structure's core terms and definitions for management systems stated in ISO/IEC Directives, Part 1:2019, Annex L , the definition of risk and the Notes to entry are slightly different.

[SOURCE: ISO 30300:2020, ~~definition~~ 3.1.26]

3.1.2
risk management
coordinated activities to direct and control an organization with regards to risk

[SOURCE: ISO 31000:2018, ~~definition~~ 3.2]

3.2 Terms specific to records

3.2.1
authoritative record
~~*record* (3.2.2)~~*record* (3.2.2) which possess the characteristics of authenticity, reliability, integrity and useability

[SOURCE: ISO 30300:2020, ~~definition~~ 3.2.3]

3.2.2
record
information created or received and maintained as evidence and as an asset by an organization, in pursuit of legal obligations or in the course of conducting business

Note 1 to entry: to entry; Records are normally used in plural.

Note 2 to entry: In a management system standard (MSS) implementation, the records created to conduct and direct the management system and to document its implementation are called documented information.

[SOURCE: ISO 30300:2020, ~~definition~~ 3.2.10]

3.2.3
records control
instrument for helping in the conduct of *records processes* ~~(3.2.5)~~(3.2.5)

EXAMPLE Examples of records controls include metadata schemas for records, business classification schemes, access and permission rules, and disposition authorities.

[SOURCE: ISO 30300:2020, ~~definition~~ 3.5.6]

Formatted: FooterPageRomanNumber

~~© ISO 2023 – All rights reserved~~

© ISO 2024 – All rights reserved

Edited DIS - MUST BE USED FOR FINAL DRAFT

iTeh Standards (https://standards.iteh.ai) Document Preview

ISO/PRF 18128

https://standards.iteh.ai/catalog/standards/iso/bf6a8b70-8354-4a37-a513-499a3d6637db/iso-prf-18128