PD ISO/TR 18128:2014

BSI Standards Publication

Information and documentation — Risk assessment for records processes and systems

bsi.

...making excellence a habit.™

National foreword

This Published Document is the UK implementation of ISO/TR 18128:2014.

The UK participation in its preparation was entrusted to Technical Committee IDT/2/17, Archives/records management.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

ISBN 978 0 580 78296 1

ICS 01.140.20

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 March 2014.

Amendments issued since publication

Date	Text affected

PD ISO/TR 18128:2014

TECHNICAL REPORT

ISO/TR 18128

First edition
2014-03-15

Information and documentation — Risk assessment for records processes and systems

Information et documentation — Évaluation du risque pour les processus et systèmes d'enregistrement

Reference number
ISO/TR 18128:2014(E)

Published in Switzerland

Contents

Page

Foreword ..... **iv**
Introduction ..... **v**
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 Risk assessment criteria for the organization **2**
4.1 Assessment of risk 2
4.2 Risk criteria 3
4.3 Assignment of priority 3
5 Risk identification **3**
5.1 General 3
5.2 Context: External factors 5
5.3 Context: Internal factors 6
5.4 Records systems 8
5.5 Records processes 11
6 Analysing identified risks **12**
6.1 General 12
6.2 Likelihood analysis and probability estimation 13
7 Evaluating risks **15**
7.1 General 15
7.2 Evaluating impact of adverse events 16
7.3 Evaluating the risk 16
8 Communicating the identified risks **17**
Annex A (informative) **Example of a documented risk entry in a risk register** **19**
Annex B (informative) **Example: checklists for identifying areas of uncertainty** **20**
Annex C (informative) **Guide to using controls from ISO/IEC 27001, Annex A** **27**
Bibliography **37**

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 documents 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 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).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/TC 46, *Information and documentation*, Subcommittee SC 11, *Archives/records management*.

Introduction

All organizations identify and manage the risks to their functioning successfully. Identifying and managing the risks to records processes and systems is the responsibility of the organization's records professional.

This Technical Report is intended to help records professionals and people who have responsibility for records in their organization to assess the risks related to records processes and systems.

NOTE System means any business application which creates and stores records.

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 or not create records in response to general business risk 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 Technical Report 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 and control of the records.

The consequence of risk events to records processes and systems is 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 Technical Report provides guidance and examples based on the general risk management process established in ISO 31000 (see Figure 1) to apply to risks related to records processes and systems. It covers

a) risk identification,

b) risk analysis, and

c) risk evaluation.

The results of the analysis of risk to records processes and systems should be incorporated into the organization's general risk management framework. As a result, the organization will have better control of its records and their quality for business purposes.

Clause 5 provides a comprehensive list of areas of uncertainty related to records processes and systems as a guide for risk identification.

Clause 6 provides guidance to determining the consequences and probabilities of identified risk events, taking into account the presence (or not) and the effectiveness of any existing controls.

Clause 7 provides guidance to determining the significance of the level and type of risks identified.

The report does not deal with risk treatment. Once the assessment of risks related to records processes and systems has been completed, the assessed risks are documented and communicated to the organization's risk management section. Response to the assessed risks is 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.

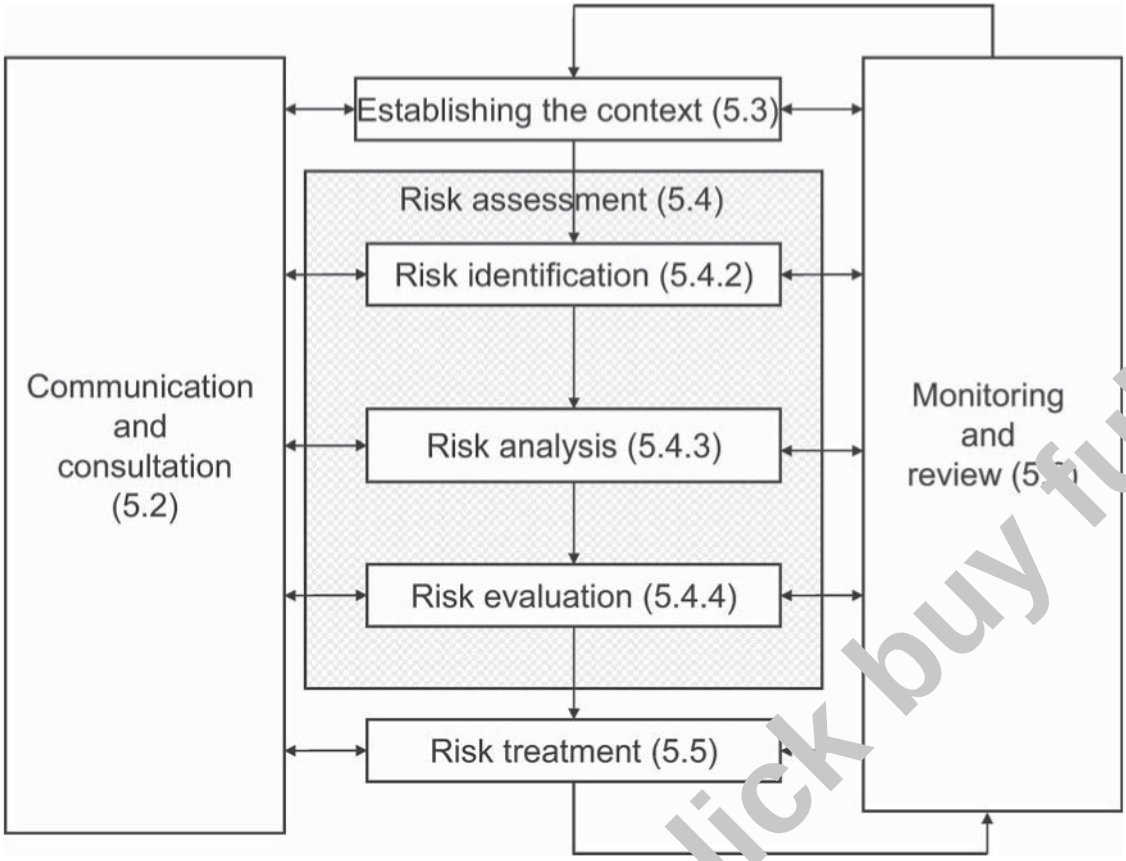

Figure 1 — Risk Management process

NOTE Figure 1 from ISO 31000:2009. Numbering refers to text of ISO 31000.

TECHNICAL REPORT **ISO/TR 18128:2014(E)**

Information and documentation — Risk assessment for records processes and systems

1 Scope

This Technical Report intends to assist organizations in assessing risks to records processes and systems so they can ensure records continue to meet identified business needs as long as required.

The report

a) establishes a method of analysis for identifying risks related to records processes and systems,

b) provides a method of analysing the potential effects of adverse events on records processes and systems,

c) provides guidelines for conducting an assessment of risks related to records processes and systems, and

d) provides guidelines for documenting identified and assessed risks in preparation for mitigation.

This Technical Report does not address the general risks to an organization's operations which can be mitigated by creating records.

This Technical Report can be used by all organizations regardless of size, nature of their activities, or complexity of their functions and structure. These factors, and the regulatory regime in which the organization operates which prescribes the creation and control of its records, are taken into account when identifying and assessing risk related to records and records systems.

Defining an organization or identifying its boundaries should take into account the complex structures and partnerships and contractual arrangements for outsourcing services and supply chains which are a common feature of contemporary government and corporate entities. Identifying the boundaries of the organization is the initial step in defining the scope of the project of risk assessment related to records.

This Technical Report does not address directly the mitigation of risks as methods for these will vary from organization to organization.

The Technical Report can be used by records professionals or people who have responsibility for records in their organizations and by auditors or managers who have responsibility for risk management programs in their organizations.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 30300:2011, *Information and documentation — Management systems for records — Fundamentals and vocabulary*

ISO Guide 73:2009, *Risk management — Vocabulary*

