PD ISO/TR 18128:2014

BSI Standards Publication

Information and documentation — Risk assessment for records processes and systems

bsi.

...making excellence a habit.™

Document Sharing Hub

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.

© The British Standards Institution 2014. Published by BSI Standards Limited 2014

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

Documents
Document Sharing Hub

Full document details: PD ISO/TR 18128:2014

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 — Evaluation du risque pour les processus et systèmes d'enregistrement

Reference number
ISO/TR 18128:2014(E)

Documents
Document Sharing Hub

© ISO 2014

Full document details: PD ISO/TR 18128:2014

COPYRIGHT PROTECTED DOCUMENT

© ISO 2014

All rights reserved. Unless otherwise specified, 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
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

© ISO 2014 – All rights reserved

Documents
Document Sharing Hub

Full document details: PD ISO/TR 18128:2014

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**

© ISO 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/TR 18128:2014

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*.

© ISO 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/TR 18128:2014

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.

© ISO 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/TR 18128:2014

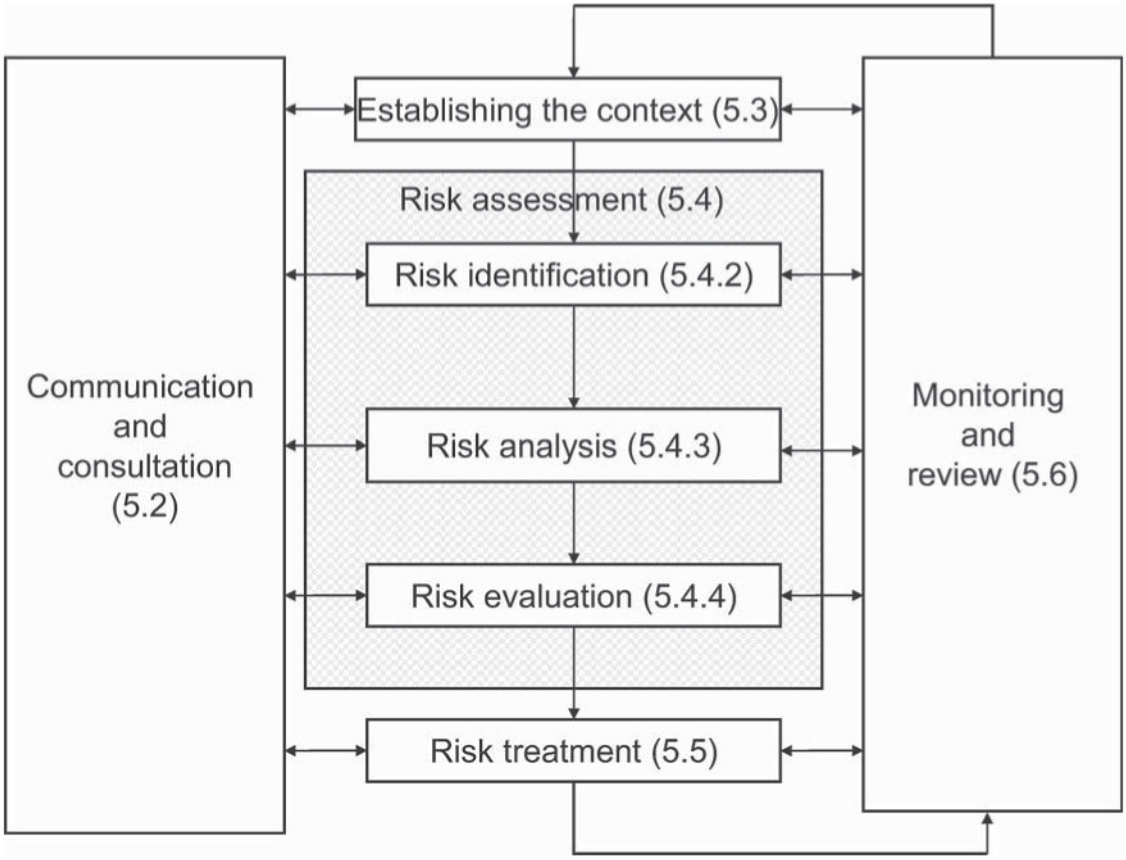

Figure 1 — Risk Management process

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

© ISO 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/TR 18128:2014

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*

© ISO 2014 – All rights reserved

Documents
Document Sharing Hub

Full document details: PD ISO/TR 18128:2014

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 30300, ISO Guide 73 and the following apply.

3.1 Terms specific to risk

3.1.1
risk
effect of uncertainty

Note 1 to entry: An effect is a deviation from the expected — positive or negative.

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: Risk is often characterized by reference to potential events (ISO Guide 73:2009, 3.5.1.3) and consequences (ISO Guide 73:2009, 3.6.1.3) or a combination of these.

Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood (ISO Guide 73, 3.6.1.1) of occurrence.

[SOURCE: ISO Guide 73:2009, definition 1.1]

3.2 Terms specific to records

3.2.1
records system
information system which captures, manages, and provides access to records through time

Note 1 to entry: This can include business applications or systems which create and maintain records.

[SOURCE: ISO 30300:2011, definition 3.4.4]

3.2.2
records processes
sets of activities by which records are created, controlled, used, kept and disposed of by the organization

4 Risk assessment criteria for the organization

4.1 Assessment of risk

Assessing risks for records processes and systems should be included, where it exists, in the organization's general risk management process. In this case, records professionals should take into account the organization's external and internal context and the context of the risk management process itself, including the following:

a) Roles and responsibilities: The role of records professionals in the assessment of risk related to records processes and systems should be specified.

b) Extent and scope of the risk assessment activities: Relationships with other risk assessment areas, such as information security, should be made explicit to avoid redundancy and conflicts and enable an integrated approach to risk assessment which includes records.

c) Methodology: The standard risk assessment methodology should be applied using the available risk assessment tools and reporting to the designated area or person.

d) Risk criteria: Where general risk criteria for the organization are established, risks related to records processes and systems should be assessed using these criteria.

© ISO 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/TR 18128:2014

Where the organization has not established a general risk management process, records professionals need to establish the risk criteria applying to records processes and systems prior to the assessment process.

4.2 Risk criteria

Criteria should be based on the legal requirements for the organization's jurisdiction and should include the following:

a) the nature and types of consequences to be included and how they will be measured;

b) the way in which probabilities are to be expressed;

c) how a level of risk will be determined;

d) the criteria by which it will be decided when a risk needs treatment;

e) the criteria for deciding when a risk is acceptable and/or tolerable;

f) whether and how combinations of risks will be taken into account.

Regarding the nature and types of consequences to be included in the risk assessment of records processes and systems, there is a general starting point which applies to all organizations. Records which are authentic, reliable, have integrity, and are useable for as long as they are required will support the needs of the organization. Risks are identified based on their potential to undermine those general characteristics of records which would make them fail to meet the purposes for which they are created.

For discussion of probability and frequency of events in risk assessment, see 6.2.

Criteria for evaluating risks, including the criteria by which it will be decided when a risk is acceptable or needs treatment, include the size and reach of the records systems in the organization, the number of users, and the use made of the system in the operations of the organization.

Similarly, criteria for evaluating risks affecting records processes should include the frequency of the process, how many systems it is used in, its relative importance in creating or managing records, the tracking of processes, and the potential for reversing or remedying adverse effects.

4.3 Assignment of priority

Generally, the organization shall determine which records are the core records of its operations and the level of significance attached to them. These are business decisions based on the advice of both records professionals and the business managers.

The priority assigned to individual records, their aggregations, records processes, or specific records systems can also be assessed in relation to responses to major disasters affecting all or many business operations. For example, first, certain records are needed in the immediate aftermath of a natural disaster, such as security contacts' addresses and phone numbers, building/facility entry records, contact details of disaster plan response teams, and insurance contacts and policy details. Second, the organization's business continuity planning should identify the functions which need to be restored first and the records needed to do so.

Special attention should be paid to where a combination of risks applies to records identified as core operational.

5 Risk identification

5.1 General

Identification of risks is structured under the following categories: context, systems, and processes involved in creating and controlling the records of the organization.

© ISO 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/TR 18128:2014

The external context of the organization refers to the political and societal, the macro-economic and technological, and the physical and environmental factors beyond its control, which have an impact on its operations and are taken into account when determining its records requirements. The external context includes the external stakeholders, who or which have a particular interest in the organization's operations.

The organization also has an internal context which is the internal factors not controlled by the records professional(s) responsible for the records processes and systems. The internal context includes factors such as the structure and finances of the organization, the technology it deploys, the resourcing of activities (people and budgets), and the organization's culture, all of which influence the policies and practices for managing records.

Potential events with uncertain effects can be external or internal to the organization.

Uncertain effects caused by change in the external context can differ according to the perspective of the different levels of the organization (see Figure 2). It is also recognized that all change presents opportunities which can be positive in effect.

Figure 2 — The multiple layers of context of an organization's records and records processes

The purpose of risk identification is to identify what can happen or what situations can exist that could affect the capacity of records to support the needs of the organization.

The risk identification process includes identifying the causes and source of the risk, events, situations, or circumstances which could have a material impact upon the organization's objectives and the nature of that impact. There are numerous methods for risk identification. See IEC 31010, Annex B for a comparison of major methods.

Identified risks should be documented in a risk register, either in one specific to records or in the organization's risk register. See the example given in Annex A.

NOTE Annex B is an example of a checklist based on the structure of Clause 5 which can be used in an organization to identify risks to records processes and systems systematically.

© ISO 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/TR 18128:2014

5.2 Context: External factors

5.2.1 Areas of uncertainty: Changes in political-societal context

Changes in the political and societal climate, nationally and internationally, can affect public attitudes to governments' and corporate behaviour. This can bring about legal and regulatory change, which impacts the organization's operations and, consequently, its records requirements.

Examples of areas of changing public attitudes which can affect records requirements are national security, access to government and corporate information, privacy, intellectual property rights, and corporate reporting responsibilities. More generally, examples of areas of uncertainty include the following:

a) legal and regulatory changes affecting the organization's records requirements;

a) changes in government policies affecting the organization's records, records processes, and systems;

b) new standards or codes of practice that affect the organization's records, records processes, and systems;

c) changing demand for records services;

d) changing stakeholders' expectations;

e) changes to reputation of, or trust in, the organization's ability to deliver its services.

5.2.2 Areas of uncertainty: Macro-economic and technological environment

Changes in the macro-economic, business, and industrial environment and in information technology have high impact on competition and customer demand. Change can be gradual and continuous, or punctuated by crises, but also constitutes an area of uncertainty which can offer positive opportunities.

Examples of areas of uncertainty arising from such changes to the macro-economic and business environment include the following:

a) changes in ownership and/or revenues of the organization which affect management priorities including managing records;

b) changes in the objectives, functions, and operations of the organization, changing records requirements;

c) increased activity from regulators, increasing external demands for records;

d) increased litigation, increasing demands for records;

e) introduction and adoption of new technologies across society;

EXAMPLES Spread of social media to business use; use of mobile computing devices for business.

f) changes in the market or client base of the organization.

These changes will be reflected in organizational changes which are discussed below (see 5.3.1).

5.2.3 Areas of uncertainty: Physical environment and infrastructure

The possibility of large-scale, natural or man-made disasters affecting the general operations of the organization is a major area of uncertainty requiring identification and assessment. The potential damage of such disasters include direct impact on the records and their storage and the less direct

© ISO 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/TR 18128:2014

impact of loss of services upon which the organization depends, for example, water and power supply and other services. Areas of uncertainty include the following:

a) regional or local destructive or disruptive environmental phenomena such as earthquake, hurricane/cyclone, tsunami, flood, fire, major storms, or prolonged drought;

b) the potential for acts of war or terrorism to cause major structural damage or disruption to service supply to premises or vicinity of the organization;

c) other disruption to the organization's power, water, waste management, information technology, transport services, or other core utilities and services.

5.2.4 Areas of uncertainty: External security threats

Risk identification shall include hostile external security threats with the potential impacts ranging from damage to premises or service supply to unauthorised access to systems including records systems. Examples of external security threats include the following:

a) unauthorised external intrusion/access into records systems and unauthorised changes to records;

b) unidentified security compromise or exploitation of vulnerability that is not monitored and leads to information degradation;

EXAMPLE Use of spyware or malware and vulnerability from unpatched software security breaches or weaknesses.

c) physical intrusion into records storage or IT hardware space;

d) denial of services or other intentional attack on Internet services;

e) physical vandalism;

f) loss of third-party services on which the records systems are dependent.

NOTE Risk assessment is an integral element of the implementation of ISO/IEC 27000 series of International Standards for information security. They provide extensive coverage of areas of uncertainty related to information security.

5.3 Context: Internal factors

5.3.1 Areas of uncertainty: Organizational change

Management decisions affecting the organization such as amalgamations, take-overs, and other acquisitions, restructuring, downsizing, outsourcing, or the reverse, off-shoring of services constitute a significant area of uncertainty in the internal context of the organization. These decisions will affect the records processes and systems, for example,

a) change of ownership of records and records systems and consequent transfer of records to and from the organization,

b) change of ownership of records and records systems resulting in forced migration of records or amalgamations of systems,

c) access arrangements to records systems for continuing right of access to records, following transfers and migrations,

d) inheritance of responsibility for records and records systems without adequate documentation,

e) loss of personnel or corporate memory affecting knowledge, of current records and systems, including knowledge of procedures to retrieve and use them, and of older records inherited through organizational change,

© ISO 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/TR 18128:2014

f) abandonment of records and records systems, especially legacy systems, where no responsibility is assigned,

g) change of terms within third-party service contracts,

h) new internal policies or modified existing ones within the organization that affect the records systems and processes,

i) policies and procedures which have not been reviewed and updated, and are no longer applicable, or are inconsistent or contradictory following organizational change,

j) changes in organization's personnel that can affect responsibility for records,

k) changes in personnel policy, training budget, and opportunities that affect the capacity of people who are responsible for records, and

l) disaster recovery plan is not updated which can affect records in the event of a disaster.

5.3.2 Areas of uncertainty: Technological change

Introduction of new technologies and systems are opportunities for improvement but also constitute areas of uncertainty with potential for adverse effects. The areas of uncertainty include the following:

a) technological changes that affect interoperability between systems that create or control records;

b) compatibility with existing platforms and systems;

c) planning and implementation of migration of records;

d) reconfiguration of responsibilities and controls of records processes;

e) effectiveness of implementation of change;

EXAMPLE Adequacy of planning and management of project to implement new platform or software.

f) extent to which the existing policies cover new technologies that the organization has adopted;

EXAMPLE Using cloud services, social media, RFID, GPS.

g) capacity of system administrators and developers deploying new technologies to understand the implications of those technologies for records requirements, at the project stage and in implementation;

EXAMPLE Use of collaborative software or wiki environments for development of new systems which cannot capture the project records and system documentation adequately.

h) capacity of existing technical infrastructure to meet new requirements resulting from organization's or records systems' technological development.

5.3.3 Areas of uncertainty: Resources — People and competencies

The organization is dependent on competent staff to deliver all its operations including the records processes and systems. The records professional or people who have responsibility for records management assesses areas of uncertainty including the following:

a) number of personnel to create and control records and to design and maintain records systems;

b) awareness of records policies and processes;

c) engagement of top management in support for records management;

d) awareness of risks related to records processes and systems and ability of top management to make decisions on appropriate mitigation;

© ISO 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/TR 18128:2014