Riskanalys för processer och system som hanterar verksamhetsinformation (ISO/TR 18128:2014, IDT)

Information and documentation – Risk assessment for records processes and systems (ISO/TR 18128:2014, IDT)
Standarder får världen att fungera

SIS (Swedish Standards Institute) är en fristående ideell förening med medlemmar från både privat och offentlig sektor. Vi är en del av det europeiska och globala nätverk som utarbetar internationella standarder. Standarder är dokumenterad kunskap utvecklad av framstående aktörer inom industri, näringsliv och samhälle och befrämjar handel över gränser, bidrar till att processer och produkter blir säkrare samt effektiverar din verksamhet.

Delta och påverka
Som medlem i SIS har du möjlighet att påverka framtida standarder inom ditt område på nationell, europeisk och global nivå. Du får samtidigt tillgång till tidig information om utvecklingen inom din bransch.

Ta del av det färdiga arbetet

Utveckla din kompetens och lyckas bättre i ditt arbete

Vill du veta mer om SIS eller hur standarder kan effektivisera din verksamhet är du välkommen in på www.sis.se eller ta kontakt med oss på tel 08-555 523 00.

Standards make the world go round

SIS (Swedish Standards Institute) is an independent non-profit organisation with members from both the private and public sectors. We are part of the European and global network that draws up international standards. Standards consist of documented knowledge developed by prominent actors within the industry, business world and society. They promote cross-border trade, they help to make processes and products safer and they streamline your organisation.

Take part and have influence
As a member of SIS you will have the possibility to participate in standardization activities on national, European and global level. The membership in SIS will give you the opportunity to influence future standards and gain access to early stage information about developments within your field.

Get to know the finished work
We offer our customers everything in connection with standards and their application. You can purchase all the publications you need from us - everything from individual standards, technical reports and standard packages through to manuals and online services. Our web service e-nav gives you access to an easy-to-navigate library where all standards that are relevant to your company are available. Standards and manuals are sources of knowledge. We sell them.

Increase understanding and improve perception
With SIS you can undergo either shared or in-house training in the content and application of standards. Thanks to our proximity to international development and ISO you receive the right knowledge at the right time, direct from the source. With our knowledge about the potential of standards, we assist our customers in creating tangible benefit and profitability in their organisations.

If you want to know more about SIS, or how standards can streamline your organisation, please visit www.sis.se or contact us on phone +46 (0)8-555 523 00

Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Foreword</td>
<td></td>
<td>iv</td>
</tr>
<tr>
<td>Introduction</td>
<td></td>
<td>v</td>
</tr>
<tr>
<td>1</td>
<td>Scope</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>Normative references</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>Terms and definitions</td>
<td>2</td>
</tr>
<tr>
<td>3.1</td>
<td>Terms specific to risk</td>
<td>2</td>
</tr>
<tr>
<td>3.2</td>
<td>Terms specific to records</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>Risk assessment criteria for the organization</td>
<td>2</td>
</tr>
<tr>
<td>4.1</td>
<td>Assessment of risk</td>
<td>2</td>
</tr>
<tr>
<td>4.2</td>
<td>Risk criteria</td>
<td>3</td>
</tr>
<tr>
<td>4.3</td>
<td>Assignment of priority</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>Risk identification</td>
<td>3</td>
</tr>
<tr>
<td>5.1</td>
<td>General</td>
<td>3</td>
</tr>
<tr>
<td>5.2</td>
<td>Context: External factors</td>
<td>5</td>
</tr>
<tr>
<td>5.3</td>
<td>Context: Internal factors</td>
<td>6</td>
</tr>
<tr>
<td>5.4</td>
<td>Records systems</td>
<td>8</td>
</tr>
<tr>
<td>5.5</td>
<td>Records processes</td>
<td>11</td>
</tr>
<tr>
<td>6</td>
<td>Analysing identified risks</td>
<td>12</td>
</tr>
<tr>
<td>6.1</td>
<td>General</td>
<td>12</td>
</tr>
<tr>
<td>6.2</td>
<td>Likelihood analysis and probability estimation</td>
<td>13</td>
</tr>
<tr>
<td>7</td>
<td>Evaluating risks</td>
<td>15</td>
</tr>
<tr>
<td>7.1</td>
<td>General</td>
<td>15</td>
</tr>
<tr>
<td>7.2</td>
<td>Evaluating impact of adverse events</td>
<td>16</td>
</tr>
<tr>
<td>7.3</td>
<td>Evaluating the risk</td>
<td>16</td>
</tr>
<tr>
<td>8</td>
<td>Communicating the identified risks</td>
<td>17</td>
</tr>
<tr>
<td>Annex A (informative)</td>
<td>Example of a documented risk entry in a risk register</td>
<td>19</td>
</tr>
<tr>
<td>Annex B (informative)</td>
<td>Example: checklists for identifying areas of uncertainty</td>
<td>20</td>
</tr>
<tr>
<td>Bibliography</td>
<td></td>
<td>37</td>
</tr>
</tbody>
</table>
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.
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

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.


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.


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.
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.