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)

COPYRIGHT PROTECTED DOCUMENT

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

Contents

Page

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.

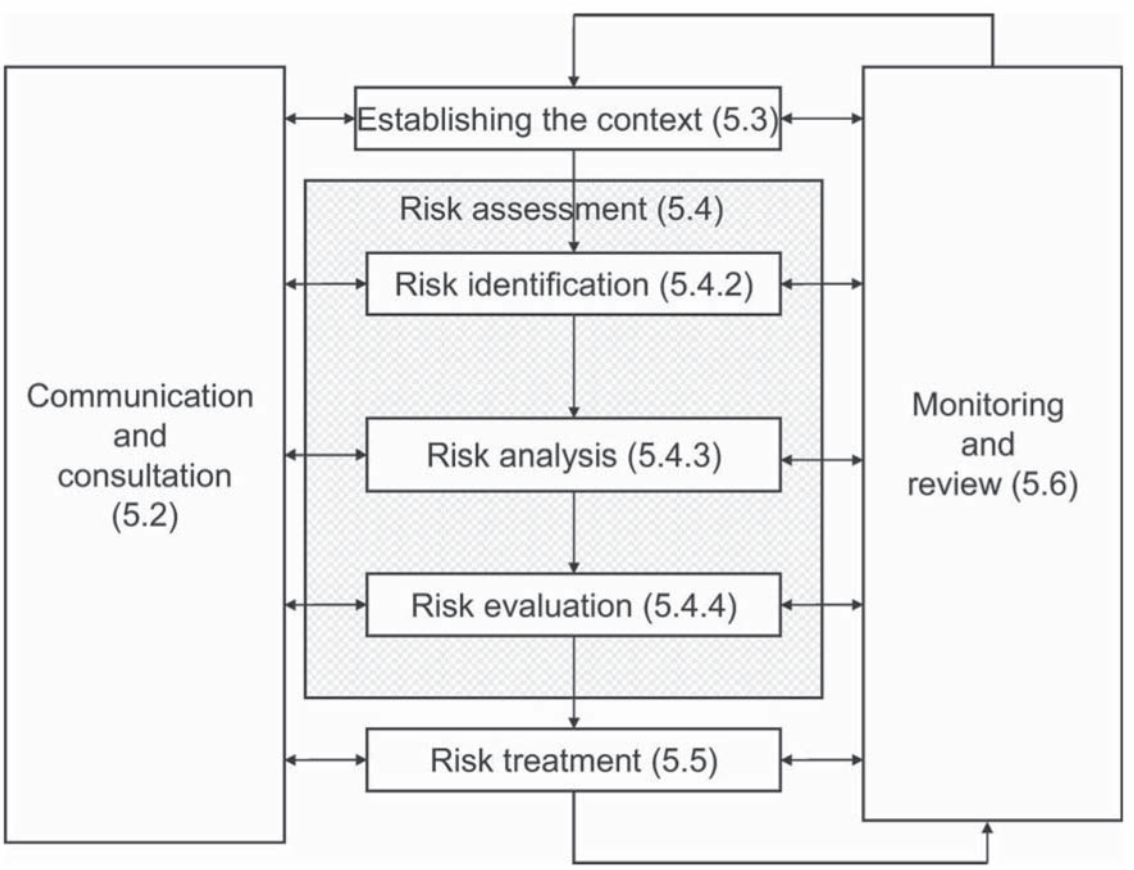

Figure 1 — Risk Management process

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*

ISO Guide 73:2009, *Risk management — 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.

[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.

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.

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.

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

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,

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;

e) management of the relationship between the administrative responsibilities for the records systems and the viewpoints of operational users;

f) adequacy of the competencies to create and control records of personnel;

g) loss of key personnel with vital skills and in-depth organizational knowledge or history;

h) deterioration of skill levels of personnel;

i) adequacy of means to evaluate effectiveness or suitability of personnel.

5.3.4 Areas of uncertainty: Resources — Finances and materials

The funding and material resources available to manage the record processes and systems adequately are affected by both the external, economic, and business environment and by the level of support for records management in the organization. Areas of uncertainty include the following:

a) adequacy of financial resources to meet commitments and goals of records management;

b) adequacy of financial resources to purchase, upgrade, or maintain adequate systems.

5.4 Records systems

When assessing the impact of risk on the systems which create or control records, the design of the systems, the issues of maintenance, sustainability, continuity, interoperability, and security should be taken into account. The systems used by the organization change over time according to the economic circumstances, changes in its activities and personnel, and changes in its size and structure. It is critical that top management is adequately informed about risk to records systems and takes responsibility for the organizational response.

NOTE 1 All references to systems in this section can be understood as references to records systems in 3.2.1.

NOTE 2 When identifying risks relating to systems in organizations which have implemented ISO/IEC 27001 controls, records professionals should take into account how these controls can mitigate risks in some areas. In organizations where ISO/IEC 27001 has not been implemented, its controls can be used as a source for mitigation actions. Annex C is a table that links the examples of areas of uncertainty relating to records systems and ISO/IEC 27001 controls.

5.4.1 Areas of uncertainty: System design

System design and configuration is critical to record creation and longevity. It intersects with the risk identification for records processes. Adequate documentation of the system configuration is the foundation for addressing other areas of risk at the system level but also for the system's processes.

NOTE See 5.5 for records processes in systems.

Based on contemporary experience, identification of risks in system design, especially in the digital context, includes the following:

a) definition of records so the system creates and manages records adequate to the system's purposes;

EXAMPLE All records elements in a transactional database are identified and managed so transactions can be retrieved or re-created.

b) adequate identification of retention requirements;

EXAMPLE Retention periods and "triggers" for disposition action are specified in the record elements.

c) identification and documentation of all necessary records processes to be managed by the system;

d) effectiveness of design of the records systems appropriate to organization's employees and technology;

e) negotiation of dependence on vendor support;

f) access to vendor documentation.

5.4.2 Areas of uncertainty: Maintenance

Maintenance of the records systems refers primarily to the technological platform and systems support aspects which are affected by structural change in the organization, implementation of new systems, technological change, and competence and reliability of the technical support.

Areas of uncertainty include the following:

a) changes in business and operating systems affecting records systems;

b) skill level of system administrators and their understanding of requirements for managing records in systems;

c) reliability of systems suppliers and their ability to maintain and keep the systems technologically up to date;

d) adequacy of documentation of procedures for operational maintenance;

e) adequacy of technical documentation of the systems;

f) adequacy of documented back-up procedures for the records systems;

g) adequacy of restoration from backups.

5.4.3 Areas of uncertainty: Sustainability and Continuity

The sustainability of the records systems depends on the monitoring of change in the external and internal context of the organization so the records systems are updated to respond to changes in needs.

Continuity planning for records systems takes into account the organization's planning for business continuity. In the absence of a business continuity plan for the organization, the records professional assesses the records systems to establish priority and procedures for restoration following a disruption to service.

Areas of uncertainty include the following:

a) change in external and internal context affecting the organization's records requirements;

b) adequacy of quality assurance monitoring to identify changes in records requirements;

c) adequacy of assessment of actual costs of implementation and maintenance of the records systems including human resources;

d) adequacy of identification and documentation of records systems;

e) maintenance and accessibility of system specifications and documentation;

f) adequacy of documentation of decisions taken in the implementation of records systems available to all users who need them;

g) ability of a records system to maintain the usability of records;

h) capacity to import records from legacy or other business systems;

i) migration of records to a new records system due to either change in records requirements or in technology;

j) changes to other systems upon which the records system is dependent;

k) ability of cloud-based systems to export records when required and to re-integrate them into the organization's systems;

l) adequacy of a records system's event history, including its retention for the life of the system and management of dependence on other systems, to ensure it remains meaningful over time;

EXAMPLE Maintenance of documentation of unique identifiers used in event history for users or business units.

m) ability of records systems to support business continuity by providing access to records in the event of a disaster;

n) contingency planning for disruptions of service.

5.4.4 Areas of uncertainty: Interoperability

Records systems have dependencies on and relationships with other systems which can be points of vulnerability.

Areas of uncertainty include the following:

a) adequacy of identification and specification of interoperability required between records systems and other business systems;

b) dependency of records systems on data sources external to the records system and capacity to exchange data with or link or refer to data in these systems (e.g. cloud, other external storage services);

c) compatibility of standards or specifications for the exchange of records or interoperability between systems;

d) the effectiveness of system interoperability after changes or technological upgrades to either or both of the integrated systems;

e) management of metadata relating to record controls between systems to sustain usability and meaning of the records.

5.4.5 Areas of uncertainty: Security

Risk assessment of security of records systems can be conducted using the ISO/IEC 27000 series of standards and applied as part of the organization's information security management system, where available. National information system security standards or requirements can also be applicable to records systems.

ISO/IEC 27005, Annexes B to D, include examples of uncertainty areas that apply to any information system. Uncertainties more specific to records systems also include the following:

a) adequacy of the organization's security policy with respect to records, records processes, and systems;

b) ability to enforce and protect access rules and permissions related to records, records processes, and systems;

c) policy and controls for third parties working on behalf of the organization that affects the storage, access and control of records, and records systems.

5.5 Records processes

Risk identification focuses on the creation of the records (or record elements) and control processes for managing the records and the records systems.

NOTE It is assumed that the records professional refers to ISO 15489-1, ISO/TR 15489-2, ISO 23081-1, ISO 23081-2, and ISO/TR 23081-3 for guidance on design of records and records processes.

5.5.1 Areas of uncertainty: Records design

The areas of uncertainty in the design processes are the following:

a) business activities are adequately analysed to identify records requirements;

b) gathering of records requirements is comprehensive for each business process, including needs of all interested parties;

c) adequacy of design of the records (e.g. identification of content and definition of metadata for identity, description, use, event history, and event planning) meets the records requirements;

d) naming and classification schema adequate for their purpose.

5.5.2 Areas of uncertainty: Records creation and records system implementation

The areas of uncertainty in the creation and implementation processes are the following:

a) points of creation or capture of all records elements are appropriate (timely, integrated, complete) to the business process and records system(s);

b) effectiveness of integration of records creation and control processes with the business processes where appropriate;

c) responsibilities of the record creators and the agents (if different) in the business transactions are adequately defined and documented;

d) allocation of responsibilities for capturing the organization's records from external environments meets the requirements;

e) metadata specifications are adequately documented and maintained;

f) processes for managing and recording access to records are appropriately documented and monitored.

5.5.3 Areas of uncertainty: Metadata

The areas of uncertainty in the metadata management processes are the following:

a) metadata technical specifications for documentation of records and records processes are accessible;

b) management of specifications enables updating as required.

5.5.4 Areas of uncertainty: Use of records and records systems

The areas of uncertainty in the access and use processes are the following:

a) consistency and timeliness of retrieval or access to records as required;

b) adequacy of management of user permissions for all records processes;

c) management of breaches of security or other access controls;

d) maintenance of records of who has accessed or modified records over time;

e) adequacy of training of personnel who use the processes;

f) compliance with the procedures.

5.5.4.1 Areas of uncertainty: Maintaining useability

The areas of uncertainty in the maintenance processes are the following:

a) maintenance of meaningfulness of records metadata over time, especially dependence on data from, or links to, external systems;

b) adequacy of record processes to preserve the authenticity and reliability of records over time;

c) maintenance of accessibility of records over time;

d) management of use of encryption of records for transmission;

e) adequacy of management of versions of records over time;

f) adequacy of retention of event history of records, to support meaningfulness of records over time;

g) software (including format changes) and hardware obsolescence issues relating to both records processes and systems.

EXAMPLE Older versions of digital records might not be accessible via current applications or versions of applications.

5.5.5 Areas of uncertainty: Disposition of records

The areas of uncertainty in the disposition processes are the following:

a) disposition of records implemented as designed and authorized;

b) disposition procedures include provision for holding records past their nominated retention period if required;

EXAMPLE Records required for legal proceedings or sought under Freedom of Information past their date of disposition.

c) disposition implementation is documented;

d) destruction is appropriately authorized and documented;

e) testing undertaken as to whether forensic recovery is possible from the discarded hardware and/or storage device.

EXAMPLE Adequacy of reformatting of hard drives of computers and printer-copiers, or storage devices such as memory sticks, to erase all records.

6 Analysing identified risks

6.1 General

Risk is analysed by determining its potential consequences and the likelihood of the risk's being realized.

In the case of records processes and systems, the consequences are identified according to the area of uncertainty and scaled according to the risk criteria established for the organization as outlined in Clause 4.

Existing controls and their effectiveness and efficiency should also be taken into account.

6.2 Likelihood analysis and probability estimation

Likelihood is the probability (or frequency) that the risk event will occur. The likelihood of the identified risks' being realized is analysed according to the nature of the area of uncertainty and the data available over a period of time sufficient to support a credible estimate.

Each risk has to be assessed in respect of the combination of the likelihood of something happening and the consequences which arise if it does actually happen.

Probabilities can be expressed in different ways, but normally are related to the level of risk. Qualitative methods can combine consequence, probability, and level of risk by significance levels such as "high", "medium", and "low".

Semiquantitative methods use numerical rating scales for consequence and probability and combine them to produce a level of risk using a formula. Scales can be linear or logarithmic or have some other relationship; formulae used can also vary.

Purely quantitative methods, which use numerical values for consequences and their probabilities, can be used where (statistical) performance data for records processes and systems are available for a substantial period of time.

Scaling the frequency of the event along the time axis can be appropriate for records processes and systems. An example of how probability can be scaled is shown in Table 1.

Table 1 — Example of scaling probability

Probability Score	Interpretation
1	Rare probability, occurs once every 10 years or less
2	Low probability, occurs once every 3 years or less
3	Medium probability, occurs once a year
4	High probability, occurs more than once every month

6.2.1 Context: External factors

Assessing the likelihood of risk events – in the political and societal, macro-economic and business, and physical, environment – draws on historical and current information of the following categories:

a) changes of government or administrations;

b) statistical and other reporting of macro-economic and business data;

c) patterns of political and societal change in the national and/or international environment which are influential in the organization's geographical location;

d) rate of technological change and associated rate of societal adoption;

e) extreme weather or other adverse physical events including infrastructure disruption.

There can be very low frequency or no historical instances of extreme weather events (e.g. hurricanes) or adverse physical events (e.g. fires or widespread power failure) but it cannot be assumed these events cannot occur. Given the disastrous impact of such events, risk assessment shall include the possibility.

6.2.2 Context: Internal factors

Assessing the likelihood of risk events in changes to the structure and activities of the organization and its use of technology and resources is based on information about its recent history in the following categories:

a) changes in top management (including privatisation, amalgamations, and take-overs) and consequent changes;

b) the organization's own pattern of responses to external changes such as regulatory change, technological development, and the financial climate;

c) competencies of personnel and internal training regime;

d) turnover of personnel.

This history of recent changes should be placed in the context of the nature of the organization's activities, its size, and its own culture.

EXAMPLE Organizations with a strong focus on commercial competition or a history of early adoption of new technology are more likely to implement new technology than a not-for-profit service organization whose clientele are the elderly or socially disadvantaged. Change in funding can be a more likely factor forcing internal change in not-for-profit organizations. Assessing the likely rate of internal changes is based on information which is specific to the organization.

6.2.3 Systems

Assessing the likelihood of risk events in the area of systems is based on information collected about security, continuity, resourcing, interoperability, and maintenance (all of which identify anomalies, errors of execution, on-going issues, and problems to be used for establishing or estimating frequency).

The issues of security of the records systems and their interoperability and general resourcing are addressed and documented at the design and review stage, while continuity planning is an aspect of the organization's general business risk management program.

The processes involved in designing systems can be vulnerable to risk events which can affect the records processes of the system. This should be taken into account when assessing the likelihood of risk events at the system design stage.

Analysis of the records generated by the maintenance procedures should provide a sound basis for assessing the likelihood of adverse events. Maintenance of the system embraces both the technological and procedural aspects.

Information from quality control monitoring to identify non-conformities in the maintenance procedures should be analysed to assess frequency of occurrence and identify any patterns which can emerge. Such patterns of non-conformity should be analysed against the design specifications of the system.

Audit logs and similar records of security or access restriction breaches should be similarly analysed to identify any emerging pattern and assess frequency and their causes. Records which certify that back-ups for computerised systems have been taken in accordance with design specifications should provide information indicating any vulnerabilities and frequency of occurrence.

The assessment of the likelihood of adverse events in relation to the systems should take into account the priority assigned to the different records systems.

6.2.4 Processes

The processes of established records systems experience incremental change through pragmatic responses to anomalies or unforeseen minor events which can accumulate over time in the absence of conscious review and documented amendment. The accumulation of incremental changes in records processes constitutes as significant an area of uncertainty as external, major, adverse events. The

likelihood of divergence from the design specifications is assessed from the analysis of non-conformities and anomalous changes authorized in special circumstances.

Assessing the likelihood of risk events in the area of records processes is based on information accumulated from the use of the records and of the records controls and instruments such as the classification schemes or disposition authorities.

Relevant information sources include the following:

a) statistics of records created and used;

b) records of non-conformities from quality control monitoring;

c) records of changes to metadata schema;

d) records of disposition authority use;

e) records of access restriction changes and breaches.

A gap analysis of the information accumulated can be used to identify areas of activity of the organization where records creation is not meeting identified requirements, changed requirements, or new areas of activity.

Gap analysis and records of non-conformities should provide a basis for identifying any pattern of change to which the records system(s) has not responded adequately, indicating vulnerabilities.

7 Evaluating risks

7.1 General

The purpose of risk evaluation is to assist in making decisions, based on the outcomes of risk analysis, about which risks need treatment and the priority for treatment implementation.

Risk evaluation involves comparing the level of risk found during the analysis process with risk criteria established when the context was considered. Based on this comparison, the need for treatment can be considered.

The scale of consequence of adverse events and the adequacy of existing controls can be put together with a probability table to help identify the risks which should be the focus of actions, measures, or treatment.

Decisions can include the following:

a) whether a risk needs treatment;

b) priorities for treatment;

c) whether an activity should be undertaken;

d) which of a number of options should be adopted.

Evaluating the risk in relation to the likelihood and the adverse consequences should give due weight to the possible impact of rare or unprecedented occurrences if the impact is judged to be widespread and severe to the point of catastrophe. Likewise, the impact of an accumulation of minor breaches or non-conformities can be far in excess of any individual occurrence if the result is deterioration of the integrity and reliability of the records or records system.

As stated in the Introduction, the consequences of risk events are identified as the loss of, or damage to, records which are therefore no longer useable, reliable, authentic, complete, or unaltered, and therefore can fail to support the organization's purposes.

An event can have a range of impacts of different magnitudes, and affect a range of different objectives and different stakeholders. The types of consequence to be analysed and the stakeholders affected are identified when the organization's criteria for the risk assessment project is established. When assessing the impact of change, uncertainty, and adverse events in relation to records, the priority accorded to the records is taken into account. The priority of the records affects the assessment of consequences in that an adverse event which is assessed as minor quantitatively can in fact be major if the records damaged or lost are critical to disaster responses or are identified as core business records.

7.2 Evaluating impact of adverse events

Factors to take into account include the following:

a) numbers of users and other stakeholders affected;

b) effect of damage or loss of records on current operations of the organization;

c) measures already in place to respond to interruption to access to the records;

d) time and effort to recover or replace the records affected;

e) impact of the loss of or damage to records on the rights or property of the organization;

f) impact of the loss of or damage to records on the organization's ability to discharge its obligations to all stakeholders;

g) legal and regulatory requirements to disclose information about damage, loss, or unauthorised access to records;

h) impact on the public standing of the organization.

This list is not exhaustive. The selection of factors to consider will be determined by the size and nature of the organization.

The potential impact of adverse events can be classified following the example in Table 2 using the factors identified as most relevant to the organization's size and nature of its activities.

Table 2 — Example of classification of impact assessment of adverse events

Minor	Moderate	Major	Severe
Anomalous breach of access restriction	Unauthorised access to records	Unauthorised access to records — shall be reported	Widespread loss, unauthorised access and damage
Damage to small quantity of records in one area of operations	Damage to significant quantity of records in one area of operations	Damage to core records of operations spreading to several areas	Damage to core records in a majority of areas of operations
Limited loss of data	Loss of data/damage to reliability	Loss of data/damage to reliability; damage to reputation	Loss of data/loss of reliability/loss of public trust
Recoverable loss	Operations not disrupted; records recoverable with effort	Loss admitted; disruption to more than one area of operations; recovery effort costly	Operations shut down; recovery effort costly and time-consuming; records not recoverable

7.3 Evaluating the risk

The scale of impact of adverse events can be put together with a probability table to help identify the adverse events which should be the focus of risk management measures, such as monitoring procedures up to disaster preparedness planning.

An example of how scaling the impact of adverse events can be plotted against probability estimates and presented in a tabular format is provided in Table 3.

The risk evaluation should then be applied to the organization's records processes and systems in order of priority.

Table 3 — Examples of risk evaluation

EVENT			Probability	IMPACT			
Context	**System**	**Process**	**Frequency**	**Minor**	**Moderate**	**Major**	**Severe**
		Records misclassified, wrong access status	High *Monthly or more*	Recoverable under existing procedures			
Changes to privacy protection law			Medium *Once a year*		Affects access restrictions to personnel system; flow on to other operations		
	Indexing function of records system fails		Medium *Once a year*	Recoverable under existing procedures			
		Records wrongly identified for destruction	Medium *Once a year*	Recoverable under existing procedures			
		Unauthorised access to employee records	Low *Once every 3 years*		Not recoverable; apology made to staff		
	Interruption to power supplies for 8 h		Low *Once every 3 years*			Affects all records systems; one day's transactions lost	
Fire destroys building holding records systems			Rare *Once every 10 years*				Loss of significant records; disruption to operations; loss of public trust

To use Table 3 for this purpose, the identified risk events in their appropriate category (on the left side) are inserted in a row at the appropriate frequency level and evaluation made of their impact on the right side. Organizations can score the impact and probability to arrive at a figure which indicates the priority assigned to responding to the risk event.

8 Communicating the identified risks

Assessed risks should be recorded in a risk register (see Annex A for an example). A risk register is the vehicle for communicating risks to the management of the organization. The registered risks and the measures proposed to respond to them should be notified to the area of the organization responsible for the organization's risk management program

The main aim in analysing and communicating risk is to identify and impose priorities and take appropriate actions. Risk communication is part of effective risk management to ensure organization-wide recognition of the risks. In order to ensure that the controls chosen for treating the risks remain effective, the risk assessment should be monitored and reviewed at regular intervals.

Annex A
(informative)

Example of a documented risk entry in a risk register

Risk Description	
Register fields	*Item entries*
Risk ID	4
Risk Name	Inability to determine creator of a document.
Risk Type and/or Grouping	Document
Risk Owner	EDRMS system administrator
Date identified	12/10/2103
Date last updated	15/10/2013
Description	Unable to find out who the creator of a registered record is
Risk manifestation (circumstances within which risk can execute)	Uncertainty about the originating business unit of records
Cost if it materialises (monetary or otherwise)	Low
Probability	Medium
Impact	High
Avoidance strategy	Review and fix document templates within EDRMS
Treatment strategy	Review and fix document templates within EDRMS
Target date	31/12/2013
Action owner/custodian	EDRMS system administrator
Review date	31/01/2014
Cross references related risks	3; 12
Risk status and Risk Action Status	Risk mitigation action started
Date of the last assessment	15/10/2013

Annex B
(informative)

Example: checklists for identifying areas of uncertainty

NOTE This is an example of a checklist which could be used regularly in an organization for identifying changes or areas of uncertainty over a nominated period of time, such as annually.

B.1 External factors

B.1.1 Political-societal context

Does the organization have a process in place to monitor changes in the external environment?

Has monitoring by the organization recorded changes in:

a) legislation and regulation affecting records requirements?

b) government policies which affect records requirements, processes, and systems?

c) new codes of practice or changes in standards relating to records processes and systems?

d) demand for records services?

e) expectations of stakeholders regarding records?

Have there been any events or changes in external circumstances which have affected the organization's reputation or public standing over the past year?

B.1.2 Macro-economic and technological environment

Have there been changes in ownership, structures, or functions of the organization in the past year?

Have there been changes in revenues, the client base or other changes to the business environment which affect records requirements?

Have there been changes in regulatory or litigation activity?

Have there been technological developments in society, which have potential impact on the organization?

B.1.3 Physical environment and infrastructure

Are regional or local, extreme weather events or other natural disasters included in disaster-preparedness planning?

Are catastrophic, man-made events (acts of war or terrorism, major accidents) included in disaster-preparedness planning?

Has the organization prepared for loss of services which will impact records systems and storage?

B.1.4 External security threats

Are the information security measures in place to protect records systems from unauthorised access and/or malicious damage adequate?

Is the physical security of the organization's records storage (paper- and electronic-format storage) adequate and checked regularly?

Is the security of the organization's IT systems adequately monitored and tested regularly?

Has the organization planned for the possible disruption to third-party services needed by the records systems?

B.2 Internal factors

B.2.1 Organizational change

Is the ownership of records in all parts of the organization established and documented?

Are procedures in place for managing transfer or migration of records or amalgamation of systems following organizational change?

Following transfer or change in ownership, have rights of access by relevant parties been agreed and documented?

Can the records systems be readily amalgamated with other systems following major organisational change?

Are records systems, including legacy systems, adequately documented and is the documentation accessible?

Are appropriate contractual conditions in place for ownership, retention, and control of records in outsourcing, off-shoring, or cloud arrangements?

Can the organization cope with change of terms in third-party service contracts for supporting/managing the records systems?

Is there a process in place to review and update policies and procedures relating to records systems at regular intervals?

Has planning included contingencies for dealing with loss of key personnel responsible for records systems or processes?

Are procedures in place for the records systems to respond to changes in personnel (i.e. training, budget, and cuts in numbers)?

Is there a procedure for reviewing and updating disaster-preparedness plans following organizational change?

B.2.2 Technological change

Will change in technologies affect interoperability between records systems and other systems?

Are changing technologies compatible with the current records systems' platforms and operating systems?

Is the procedure for undertaking migration of records/systems current, documented, and adequate?

Are processes in place to ensure that records metadata are fully migrated when new technologies are introduced and are there checks for information loss or corruption?

Are processes in place to prevent unauthorised disposition or retention of records no longer needed when systems are migrated or upgraded?

Is there a procedure in place to manage re-configuration of records systems and processes?

Are responsibilities for re-configuration of records systems, processes, and controls documented and up-to-date?

Is the project of implementing change in technology affecting records systems adequately managed?

Do current policies adequately cover new technologies as the organization adopts them?

Are the IT professionals and management aware of the implications for records systems and system documentation when introducing new technology?

Can the organization's current technological infrastructure support technological change in the records systems?

B.2.3 Resources: People and competencies

Are current numbers of personnel sufficient to undertake the records processes and manage the records systems?

Are the organization's personnel adequately informed of the policies and processes relating to records?

Is records management supported by top management?

Are risks to records processes and systems understood by top management as risks to the organization which should be mitigated?

Are records responsibilities included in job descriptions where relevant?

Are the capacities present or attainable to respond to changes in the external, regulatory environment affecting the organization's records policies and procedures?

Are responsibilities of the records systems' administrators understood and documented in relation to the users of the systems?

Are processes in place to ensure transfer of vital skills and operational know-how among personnel responsible for records?

Is a continuous training program available for personnel responsible for records?

Is there a monitoring process to assess skills and competencies of personnel responsible for records?

B.2.4 Resources: Finances and materials

Is records management adequately funded to achieve the records policy objectives and undertake the records procedures of the organization?

Are the records systems adequately funded and supported, including system upgrades and maintenance?

B.3 Records Systems

B.3.1 System design

Does the system documentation include defining what all the records elements are?

Is there adequate documentation of the system's metadata and processes?

Are retention requirements adequately managed by the system and documented?

Are all records processes managed by the system identified and documented?

Is the technology selected an appropriate fit for the size, complexity, and activities of the organization?

Does the technology adequately support the functionality of the records systems?

Does the system depend on vendor support and is the service contract current and services sufficiently defined?

Is the vendor documentation adequate including all necessary elements and the encoding schemes?

B.3.2 Maintenance

Are there frequent changes to the design or other aspects such as security of systems?

Does the organization have adequate change management procedures to ensure systems changes are authorized, planned, and controlled?

Are the skill levels of system administrators and their understanding of records requirements in systems appropriate and up to date?

Are systems suppliers reviewed regularly for their ability to keep the systems up to date?

Is the documentation of maintenance procedures of the records systems accessible, reviewed regularly, and updated?

Are failures or dysfunctions of technology which affect the operations of the records systems monitored and documented?

Is the technical systems documentation accessible and up to date?

Are back-up and restore processes for the records systems regularly tested, documented, and reviewed?

B.3.3 Sustainability and continuity

Are the records systems regularly monitored and reviewed, in line with changes in the external and internal context which affect the organization's records requirements?

Is the quality assurance monitoring of the records systems reviewed to identify updating or other changes in requirements?

Has an assessment been done of what financial resources are required to implement and maintain the records systems adequately and for appropriately competent personnel to be responsible for those systems?

Has the organization identified all systems that create, hold, or manage records?

Are the records systems' specifications adequately documented and accessible?

Are procedures for operational maintenance established and documented?

Are the decisions taken in the implementation of records systems documented, maintained, and available to all users who need them?

Is the records system's capability to maintain the usability of records regularly tested?

Is there regular monitoring and reporting on performance of records systems against their objectives?

Is there an established procedure for managing migration of records to a new records system?

Is there tested capacity in the records systems to import records from legacy, or other business, systems?

Are changes to other systems on which the records systems are dependent, or otherwise linked, monitored and managed?

Where external service providers, such as cloud-based storage, are used, has the export of records and re-integration with the organization's records systems been tested?

Are the record systems' event histories reviewed at regular intervals and are their dependencies on other systems adequately managed?

Does the business continuity planning specifically include the records systems?

Do the records systems support business continuity by providing access to records in the event of a disaster?

Are contingency plans in place for managing disruption of service to the record systems?

B.3.4 Interoperability

Has the organization identified and specified what interoperability is required between business systems and the systems that keep records?

Are the dependencies of the records systems on external data sources or other systems, including external services such as cloud-based storage, identified, documented, and appropriately managed?

For the interoperability identified, does the organization use compatible standards or specifications to ensure exchange of records between those systems is sustainable?

Are changes (such as software upgrades) to systems on which the records systems are dependent, or need to maintain interoperability with, monitored and appropriately managed?

Is the exchange of records between systems recorded adequately in the metadata of both systems and appropriately managed?

B.3.5 Security

See also Annex C which maps controls for information security from ISO/IEC 27001 against provisions in this text.

NOTE ISO/IEC 27005, Annexes B to D, also include examples of areas of uncertainty that apply to any information system.

Does the organization's (information) security policy deal adequately with security for the records, records processes, and systems?

Are restrictions on users' permissions to access, create, and change records enforceable, enforced in practice and documented?

Are security procedures in place for changing user access rights to systems when personnel change roles or terminate employment?

Are there policy and procedures for control of third parties working on behalf of the organization that specifically deal with managing the secure storage, access, and processing of records and records systems?

Is the effectiveness of the information security policy and controls regularly assessed, and corrective action taken?

B.4 Records Processes

B.4.1 Records design

Was/is the analysis of records requirements of the organization's business activities

a) based on adequate knowledge of the business of the organization,

b) comprehensive,

c) inclusive of all relevant legislation and regulation, and

d) inclusive of all interested parties?

Does the design cover all documented uses of the existing records of the activities?

Does the design of the records for each specified system meet the requirements in metadata for identity, description, use, event history, and event planning?

Where used, do the naming conventions and classification schemes fit the terminology of the organization?

B.4.2 Records creation and records system implementation

Is the record-creating or capturing process appropriate to the business process and system, that is, is it based on an appropriate technology, reliable, systematic, and timely?

Are the records adequately identified and controlled from the point of capture or creation?

As far as possible, is the records creation or capture process integrated with the business process or closely associated with the completion of the transaction?

Are records creators adequately trained in the processes?

Are the records creation or capture responsibilities adequately documented, and where appropriate, distinguished from the responsibilities of the users of the business system?

Are the responsibilities and processes for capturing records from external environments defined, allocated, and documented?

Is access to the records consistent with legal/mandatory requirements and appropriately recorded and monitored?

B.4.3 Metadata

Are the metadata specifications (including the technical specifications) documented and accessible for updating?

B.4.4 Use of records and records systems

Are users able to access records consistently when they need them?

Are user permissions – to create or capture, to access or modify records – managed appropriately in the system?

Are permissions role-based, not person-based?

Are records of access to, and modification of, the records maintained in the system over time?

Can restrictions on access be over-ridden in the system, are they recorded, and are there appropriate mechanisms in place to resolve such conflicts?

Are users of the records adequately trained in the systems' processes?

Are processes in place to prevent misuse or unauthorised disclosure of records?

B.4.5 Maintaining usability

Is the context of the records' creation and use adequately documented and accessible over time?

Are mechanisms in place to manage the records' dependencies on external systems (data or other links) to maintain the comprehensibility of the records?

Are the processes to sustain the records' reliability and authenticity over time (for example, security from unauthorised access or modification) robust, documented, and monitored?

Where encryption is used when storing/transmitting records, can it be decrypted?

Can revisions, comments, and notes on, and the version history of, a record be accessed for as long as needed?

Are the event histories of the records adequately maintained to ensure they remain comprehensible over time?

Is there a procedure in place to check on the usability of older records, for example, software and hardware dependencies, adequacy of physical storage for records in various formats?

B.4.6 Disposition of records

Are there disposition authorities in place which are current and relevant?

Is there a process for reviewing existing disposition authorities?

Are there procedures in place for the disposition of records?

Are roles and responsibilities for disposition defined and documented?

Is disposition undertaken on a regular and routine basis?

a) Is there a process for handling exceptions?

b) Is disposition including authorization documented as appropriate?

c) Is there appropriate training for implementing disposition in place for employees responsible for records?

d) Are disposition methods appropriate to the level of security required?

Are there processes in place to ensure destruction of records is complete — noting the need to prevent restoration of records from electronic devices and storage media?

Annex C
(informative)

Guide to using controls from ISO/IEC 27001, Annex A

When identifying risks relating to systems in organizations which have implemented ISO/IEC 27001 controls, records professionals should take into account how some of these controls act on the mitigation of risks from some areas of uncertainty. In organizations where ISO/IEC 27001 controls are implemented, the task of risk assessment for records processes and systems undertaken by the records professional will benefit from in-depth knowledge and alignment with ISO/IEC 27001. In organizations where ISO/IEC 27001 is not implemented, its controls can be used as a source for mitigation actions. Further reading of ISO/IEC 27001 standards is highly recommended.

The following table maps areas of uncertainty identified in 5.4 to controls in ISO/IEC 27001.

In the right column, "Observations", where appropriate, some tips are provided to help understand the ISO/IEC 27001 information security controls from a records systems point of view.

	ISO/TR 18128:2014, 5.4 **Record Systems Areas of uncertainty**	ISO/IEC 27001:2013, Annex A **Controls**	**Observations**
Areas of uncertainty: Systems design			
1	Definition of records so system creates and manages records adequate to the system's purposes.	**Without related** ISO/IEC 27001 **control**	
2	Sufficient identification of retention requirements.	**Without related** ISO/IEC 27001 **control**	Disposition is not a focus of information security, but from a records system point of view is an important area of uncertainty, especially when systems which create and control records fail to implement disposal decisions.
3	Identification and documentation of all necessary records processes to be managed by the system.	**Without related** ISO/IEC 27001 **control**	
4	Effectiveness of design of the records system appropriate to organization's personnel and technology.	**A.10.3.1 System planning and acceptance.** The use of resources shall be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.	Capacity requirements and use of resources are only two aspects of assessing the effectiveness of records systems, which should be principally tested against operational requirements.

	ISO/TR 18128:2014, 5.4 **Record Systems Areas of uncertainty**	ISO/IEC 27001:2013, Annex A **Controls**	**Observations**
5	Management of dependence on vendor support.	**A.12.5.5 Outsourced software development.** Outsourced software development shall be supervised and monitored by the organization.	If the records systems are based on commercial software provided by external supplier, the reliability of the external supplier needs to be taken into account when identifying risks. ISO/IEC 27001 control can be too general from the records systems point of view.
6	Access to vendor documentation.	**A.10.1.1 Documented operating procedures.** Operating procedures shall be documented, maintained, and made available to all users who need them.	ISO/IEC 27001 should be applied for records systems to any software documentation which includes internal procedures to maintain them.
Areas of uncertainty: Maintenance			
1	Changes in business and operating systems affecting records systems.	**A.10.1.2 Change management.** Changes to information processing facilities and systems shall be controlled. **A.10.10.4 Administrator and operator logs.** System administrator and system operator activities shall be logged. **A.10.10.5 Fault logging.** Faults shall be logged, analysed, and appropriate action taken.	ISO/IEC 27001 controls should be supplemented by communication requirements to ensure records professionals are made aware of such changes.
2	Skill level of system administrators and their understanding of requirements for managing records in systems.	**A.10.3.1 Capacity management.** The use of resources shall be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance. **A.10.3.2 System acceptance.** Acceptance criteria for new information systems, upgrades, and new versions shall be established and suitable tests of the system(s) carried out during development and prior to acceptance.	ISO/IEC 27001 controls cannot be sufficient to mitigate uncertainties about the skill level of system administrators regarding records requirements. Special attention should be paid in this area.

	ISO/TR 18128:2014, 5.4 **Record Systems Areas of uncertainty**	ISO/IEC 27001:2013, Annex A **Controls**	**Observations**
3	Reliability of systems suppliers and their ability to maintain and keep the systems technologically up to date.	**A.12.5.5 Outsourced software development.** Outsourced software development shall be supervised and monitored by the organization.	If the records systems are based on commercial software provided by external suppliers, the reliability of the external supplier needs to be taken into account when identifying risks. ISO/IEC 27001 control can be too general from the records systems point of view.
4	Adequacy of documentation of procedures for operational maintenance.	**A.10.1.1 Documented operating procedures.** Operating procedures shall be documented, maintained, and made available to all users who need them.	Systems documentation (technical and procedures) should be treated as records and maintained accordingly.
5	Adequacy of technical documentation of the systems.	**A.10.1.1 Documented operating procedures.** Operating procedures shall be documented, maintained, and made available to all users who need them.	Systems documentation (technical and procedures) should be treated as records and maintained accordingly.
6	Adequacy of documented back-up procedures for the records systems.	**A.10.5.1 Information back-up.** Back-up copies of information and software shall be taken and tested regularly in accordance with the agreed backup policy.	ISO/IEC 27001 control on back-up does not cover all uncertainties related to maintenance of usability or disposition of records.
7	Adequacy of restoration from back-ups.	**A.10.5.1 Information back-up.** Backup copies of information and software shall be taken and tested regularly in accordance with the agreed backup policy.	ISO/IEC 27001 control on back-up does not cover all uncertainties related to maintenance of usability or disposition of records.
Area of uncertainty: Sustainability and Continuity			
1	Change in external and internal context affecting the organization's records requirements.	**Without related** ISO/IEC 27001 **control**	

	ISO/TR 18128:2014, 5.4 **Record Systems Areas of uncertainty**	ISO/IEC 27001:2013, Annex A **Controls**	**Observations**
2	Adequacy of quality assurance monitoring to identify changes in records requirements.	**A.10.10.1 Audit logging.** Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring. **A.10.10.2 Monitoring System.** Use Procedures for monitoring use of information processing facilities shall be established and the results of the monitoring activities reviewed regularly.	ISO/IEC 27001 control identifies one aspect of system monitoring, but records systems require more extensive quality assurance monitoring.
3	Adequacy of assessment of actual costs of implementation and maintenance of the records systems including human resources.	**A.6.1.3 Allocation of information security responsibilities.** All information security responsibilities shall be clearly defined. **A.10.3.1 System planning and acceptance.** The use of resources shall be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.	ISO/IEC 27001 controls do not cover economic aspects of systems, except for the control which includes the responsibilities for information security in internal organization. The economy aspects of records systems could be an important area of uncertainty in an organization implementing cost reducing policies.
4	Adequacy of identification and documentation of records systems.	**A.7.1.2 Ownership of assets.** All information and assets associated with information processing facilities shall be owned by a designated part of the organization.	ISO/IEC 27001 control identifies need to document ownership of systems but adequate identification and documentation of the records systems are also required.

	ISO/TR 18128:2014, 5.4 **Record Systems Areas of uncertainty**	ISO/IEC 27001:2013, Annex A **Controls**	**Observations**
5	Maintenance and accessibility of system specifications and documentation.	**A.10.7.4 Security of system documentation.** System documentation shall be protected against unauthorized access.	ISO/IEC 27001 control is focused on the protection of documentation to avoid risks on information security. From the records systems point of view, uncertainties arise also from whether it is accessible when needed. Protection and accessibility need to be balanced as both of them are sources of potential risks.
6	Adequate documentation of decisions taken in the implementation of records systems available to all users who need them.	**A.10.7.4 Security of system documentation.** System documentation shall be protected against unauthorized access.	See above.
7	Ability of the records system to maintain the usability of records.	**Without related** ISO/IEC 27001 **control**	Usability is not a focus of information security, but from records point of view could be a significant area of uncertainty.
8	Capacity to import records from legacy or other business systems.	**Without related** ISO/IEC 27001 **control**	
9	Migration of records to new records system due to either change in records requirements or in technology.	**A.12.5.2 Technical review of applications after operating system changes.** When operating systems are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.	Apart from changes in the operating systems, migration from one system to another should be identified as an area of uncertainty regarding maintenance of the characteristics of records over time.
10	Changes to other systems upon which the records system is dependent.	**Without related** ISO/IEC 27001 **control**	
11	Ability of cloud-based systems to export records when required and to re-integrate them into the organization's systems.	**Without related** ISO/IEC 27001 **control**	
12	Adequacy of the records systems' event history, including its retention for the life of the system and management of dependence on other systems to ensure it remains meaningful over time.	**A.10.10.1 Audit logging.** Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring.	ISO/IEC 27001 audit log of users' activities is limited from the records point of view; audit log should be supplemented with other actions performed on the records to constitute the event history.

	ISO/TR 18128:2014, 5.4 **Record Systems Areas of uncertainty**	ISO/IEC 27001:2013, Annex A **Controls**	**Observations**
13	Ability of records systems to support business continuity by providing access to records in a disaster event.	**A.14.1.3 Developing and implementing continuity plans including information security.** Plans shall be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes. **A.14.1.4 Business continuity planning framework.** A single framework of business continuity plans shall be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance. **A.14.1.5 Testing, maintaining, and reassessing business continuity plans.** Business continuity plans shall be tested and updated regularly to ensure that they are up to date and effective. **A.15.1.3 Protection of organizational records.** Important records shall be protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements.	ISO/IEC 27001 controls on business continuity management are focused in information security requirements. From the records points of view, these controls can be complemented with records requirements primarily focused on core operational records.
14	Contingency planning for disruptions of service.	**A.14.1.3 Developing and implementing continuity plans including information security**. Plans shall be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to or failure of critical business processes.	ISO/IEC 27001 controls on business continuity management are focused in information security requirements. From the records points of view, these controls can be complemented with records requirements primarily focused on business continuity concerns.
Areas of uncertainty: Interoperability			

	ISO/TR 18128:2014, 5.4 **Record Systems Areas of uncertainty**	ISO/IEC 27001:2013, Annex A **Controls**	**Observations**
1	Adequacy of identification and specification of interoperability required between records systems and other business systems.	**A.10.8.1 Information Exchange policies and procedures.** Formal exchange policies, procedures, and controls shall be in place to protect the exchange of information through the use of all types of communication facilities. **A.10.8.2 Exchange agreements.** Agreements shall be established for the exchange of information and software between the organization and external parties. **A.10.8.5 Business information systems.** Policies and procedures shall be developed and implemented to protect information associated with the interconnection of business information systems.	ISO/IEC 27001 controls focus on information security formal documentation for exchange of information between systems. From the records point of view, interoperability between records systems and other systems can be a routine, operational matter and, therefore, a broader area of uncertainty. Failure in systems interoperability can affect access to and usability of records.
2	Dependency of records systems on data sources external to the records system and capacity to exchange data with these systems (e.g. cloud, other external storage services).	**A.6.2.1 Identification of risks related to external parties:** The risks to the organization's information and information processing facilities from business processes involving external parties shall be identified and appropriate controls implemented before granting access. **A.6.2.3 Addressing security in third party agreements**: Agreements with third parties involving accessing, processing, communicating, or managing the organization's information or information processing facilities or adding products or services to information processing facilities shall cover all relevant security requirements.	Security of data in third-party service providers are not the only consideration from a records system point of view, but controls are appropriate.
3	Compatibility of standards or specifications for the exchange of records or interoperability between systems.	**A.15.2.2 Technical compliance checking Information.** Systems shall be regularly checked for compliance with security implementation standards.	ISO/IEC 27001 controls focus on security implementation standards. From the records point of view, as the use of this International Standard in the records systems could be an area of uncertainty, this control could be broadened to records exchange and interoperability standards.

	ISO/TR 18128:2014, 5.4 **Record Systems Areas of uncertainty**	ISO/IEC 27001:2013, Annex A **Controls**	**Observations**
4	The effectiveness of system interoperability after changes or technological upgrades to either or both of the integrated systems.	**A.10.3.2 System planning and acceptance.** Acceptance criteria for new information systems, upgrades, and new versions shall be established and suitable tests of the system(s) shall be carried out during development and before acceptance.	
5	Management of metadata relating to record controls between systems to sustain usability and meaning of the records.	**Without related** ISO/IEC 27001 **control**	The ability of records systems to support metadata requirements could be an important area of uncertainty. When records systems cannot manage metadata from records processes, meaning and usability of records are damaged.
Areas of uncertainty: Security (All this area of uncertainty should be covered by ISO/IEC 27001 controls. The following examples are linked to the most important controls.)			
1	Adequacy of the organization's security policy with respect to records, records processes, and records systems.	**A.5.1.1 Information security policy document.** An information security policy document shall be approved by management and published and communicated to all employees and relevant external parties. **A.5.1.2 Review of the information security policy.** The information security policy shall be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.	When identifying risks in this area, records professionals should ensure that the Information security policy of the organization includes the specific needs of records and records systems and also should ensure that records policy and procedures are aligned with the information security policy.

	ISO/TR 18128:2014, 5.4 **Record Systems Areas of uncertainty**	ISO/IEC 27001:2013, Annex A **Controls**	**Observations**
2	Ability to enforce and protect access rules and permissions related to records, records processes, and systems.	**A.11.1.1 Access control policy.** An access control policy shall be established, documented, and reviewed based on business and security requirements for access. **A.11.2.1 User registration.** There shall be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services. **A.11.2.2 Privilege management.** The allocation and use of privileges shall be restricted and controlled. **A.11.2.3 User password management.** The allocation of passwords shall be controlled through a formal management process. **A.11.2.4 Review of user access rights.** Management shall review users' access rights at regular intervals using a formal process. **A.11.6.1 Information Access restriction.** Access to information and application system functions by users and support personnel shall be restricted in accordance with the defined access control policy.	When identifying risks in this area, the records professional should take into account the restrictions on users' permissions to access, create, and change records. Permissions should be aligned with the defined access control policy in the information security policy.

	ISO/TR 18128:2014, 5.4 **Record Systems Areas of uncertainty**	ISO/IEC 27001:2013, Annex A **Controls**	**Observations**
3	Policy and controls for third parties, working on behalf of the organization, that affect the storage, access, and processing of records and records systems.	**A.6.2.3 Addressing security in third-party agreements.** Agreements with third parties involving accessing, processing, communicating, or managing the organization's information or information processing facilities or adding products or services to information processing facilities shall cover all relevant security requirements. **A.10.2.1 Service delivery.** It shall be ensured that the security controls, service definitions and delivery levels included in the third-party service delivery agreement are implemented, operated, and maintained by the third party. **A.10.2.2 Monitoring and review of third party services.** The services, reports, and records provided by the third party shall be regularly monitored and reviewed, and audits shall be carried out regularly. **A.10.2.3 Managing changes to third party services.** Changes to the provision of services, including maintaining and improving existing information security policies, procedures, and controls, shall be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.	

Bibliography

[1] ISO 15489-1:2001, *Information and documentation — Records management — Part 1: General*

[2] ISO/TR 15489-2:2001, *Information and documentation — Records management — Part 2: Guidelines*

[3] ISO 23081-1:2006, *Information and documentation — Records management processes — Metadata for records — Part 1: Principles*

[4] ISO 23081-2:2009, *Information and documentation — Managing metadata for records — Part 2: Conceptual and implementation issues*

[5] ISO/TR 23081-3:2011, *Information and documentation — Managing metadata for records — Part 3: Self-assessment method*

[6] ISO 27001, *Information technology — Security techniques — Information security management systems — Requirements*

[7] ISO/IEC 27005:2011, *Information technology — Security techniques — Information security risk management*

[8] ISO 31000:2009, *Risk management — Principles and guidelines*

[9] IEC 31010:2009, *Risk management — Risk assessment techniques*

ICS 01.140.20

Price based on 37 pages