The Risk Management Standards and Guidance Collection

BS ISO 31000:2009

BS 31100:2011

BS EN 31010:2010

PD ISO Guide 73:2009

Managing Risk the ISO 31000 Way

bsi.

Using your enhanced PDF collection

These instructions relate to Adobe Reader 9.3.2 and it should be noted that other versions of Adobe Reader, or other PDF viewing applications, might be configured differently. However, the functions described below should still be available. Please consult the documentation provided by your specific application for further guidance.

Hyperlinks

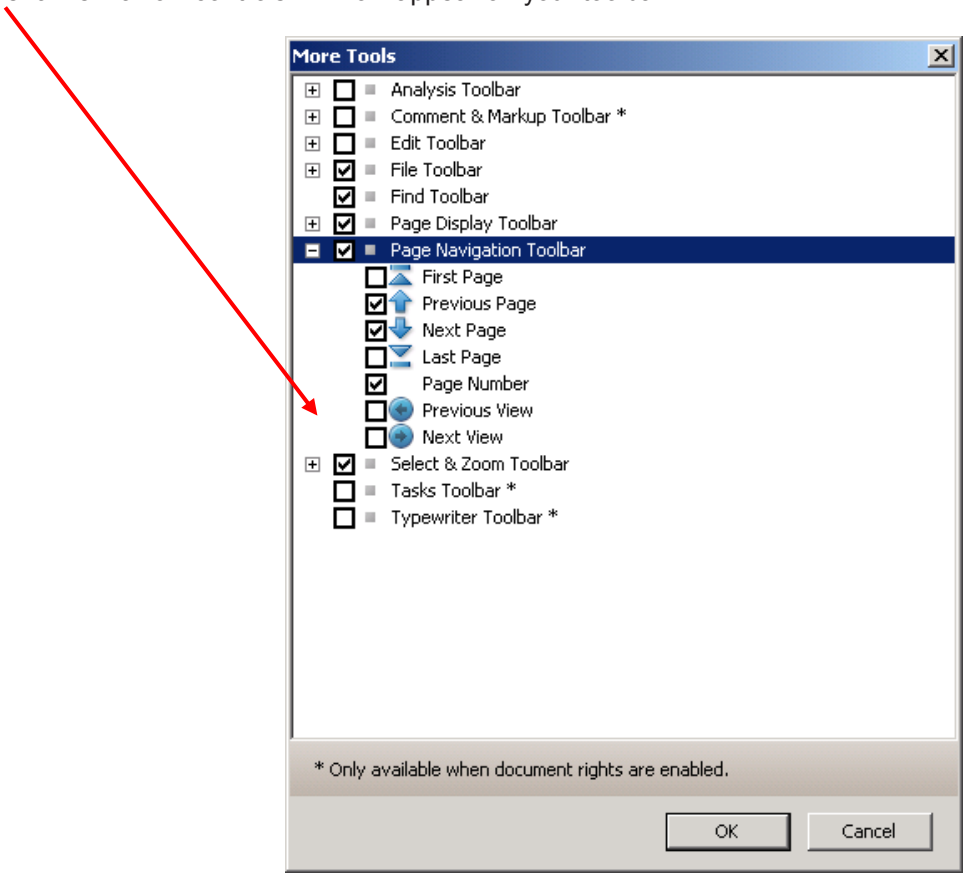
Links between relevant clauses, references, terms and definitions within the collection are signified by blue underlines. Click on a hyperlinked word to be taken instantly to the relevant location. Links to other documents available in the BSI online shop are signified by blue rectangles. Click on a hyperlinked word to be taken to the relevant page in the shop.

Navigation

Having clicked on a hyperlink and been taken to the relevant destination, you might want to return to your previous location. Browser-style navigation controls (i.e. forward and back) are not displayed by default in some versions of Adobe Reader. To enable these controls:

1. From the menu bar, select **View** > **Toolbars** > **More Tools**
2. Check the **Previous View** and **Next View** boxes, indicated in the screenshot below
3. Select **OK**

The **Previous/Next View** arrow controls will now appear on your toolbar.



Bookmarks

Bookmarks provide a full list of sections and subsections for the entire file, enabling you to quickly and easily navigate the document(s) and go directly to specific clauses. If you don't see bookmarks on the left of your screen, select **View > Navigation panels > Bookmarks** from the menu bar. This will bring up a nested structure that allows you to drill down to the lowest level headings in the documents in the collection.

Find

Select **Edit** > **Find** from the menu bar to use the **Find** function. Type in the text you want to find and click through occurrences in the document in sequence.

Search

For a more advanced search function select **Edit** > **Search** from the menu bar. This enables you to specify additional criteria for your search and presents the results in a list, allowing you to click through to any occurrence.

Risk Management Standards

There has never been a more important time for organizations to pay attention to managing their risks. Fortunately, there have recently been substantial developments in the theory and application of risk management techniques, as well as substantially increased corporate governance expectations. Several specialist areas of risk management have also developed, including financial, clinical and project risk management.

However, it was the Global Financial Crisis (GFC) in 2008 that demonstrated the true importance and value of effective risk management. In order to avoid a repeat of the GFC, appropriate attention must be paid to risk management across all the activities and processes of an organization. For financial institutions, credit and market risk management have been identified as priorities, as well as the more commonplace operational risks faced by all organizations.

Not only have organizations been paying increased attention to risk management in recent times, but standards bodies around the world have been developing standards for the management of risk. In fact, the development of risk management standards was taking place before the GFC materialised. If financial institutions had paid more attention to these developing risk management standards, there would have been greater awareness of risk and preparedness for the consequences - and the crisis may not have been as serious.

The most widely accepted of these standards is the international standard BS ISO 31000:2009, *Risk management - Principles and guidelines*. This standard sets out the high-level principles that should apply to any application of the risk management process. It sets out what risk management activities should be undertaken and provides a brief description of how they should be implemented and maintained. The main objective of this standard is to provide an outline of what should be done.

BS 31100:2011, *Risk management - Code of practice and guidance for the implementation of BS ISO 31000* provides guidance on how to undertake the actions described in BS ISO 31000. For example, BS ISO 31000 states that a risk management policy should be prepared, whilst BS 31100 outlines what should be included in such a policy, including what actions

should be taken to integrate risk management with the other activities within the organization and how to improve risk management processes.

One of the most important steps in undertaking successful risk management is the risk assessment process. BS EN 31010:2010, ***Risk management - Risk assessment techniques*** provides information on a wide range of risk assessment techniques. There is reference to qualitative assessment techniques, such as brainstorming workshops and the use of checklists, as well as details of more quantitative approaches, such as hazard and operability studies and failure modes and effects analysis.

Underpinning risk management activities is the need for standardised vocabulary. Risk vocabulary not only needs to be consistent throughout all standards directly concerned with risk, it also needs to be available for the wide range of other standards that make reference to risk and risk management. The standardized vocabulary for use throughout all standards is set out in PD ISO Guide 73:2009, ***Risk management - Vocabulary.***

BRITISH STANDARD

BS ISO
31000:2009

Risk management — Principles and guidelines

ICS 03.100.01

BSI
British Standards

National foreword

This British Standard is the UK implementation of ISO 31000:2009.

The UK participation in its preparation was entrusted to Technical Committee RM/1, Risk management.

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

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

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

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 March 2010

ISBN 978 0 580 67571 3

Amendments/corrigenda issued since publication

Date	Comments

BS ISO 31000:2009

INTERNATIONAL STANDARD

ISO 31000

First edition
2009-11-15

Risk management — Principles and guidelines

Management du risque — Principes et lignes directrices

Reference number
ISO 31000:2009(E)

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

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.

ISO 31000 was prepared by the ISO Technical Management Board Working Group on risk management.

Introduction

Organizations of all types and sizes face internal and external factors and influences that make it uncertain whether and when they will achieve their objectives. The effect this uncertainty has on an organization's objectives is “risk”.

All activities of an organization involve risk. Organizations manage risk by identifying it, analysing it and then evaluating whether the risk should be modified by risk treatment in order to satisfy their risk criteria. Throughout this process, they communicate and consult with stakeholders and monitor and review the risk and the controls that are modifying the risk in order to ensure that no further risk treatment is required. This International Standard describes this systematic and logical process in detail.

While all organizations manage risk to some degree, this International Standard establishes a number of principles that need to be satisfied to make risk management effective. This International Standard recommends that organizations develop, implement and continuously improve a framework whose purpose is to integrate the process for managing risk into the organization's overall governance, strategy and planning, management, reporting processes, policies, values and culture.

Risk management can be applied to an entire organization, at its many areas and levels, at any time, as well as to specific functions, projects and activities.

Although the practice of risk management has been developed over time and within many sectors in order to meet diverse needs, the adoption of consistent processes within a comprehensive framework can help to ensure that risk is managed effectively, efficiently and coherently across an organization. The generic approach described in this International Standard provides the principles and guidelines for managing any form of risk in a systematic, transparent and credible manner and within any scope and context.

Each specific sector or application of risk management brings with it individual needs, audiences, perceptions and criteria. Therefore, a key feature of this International Standard is the inclusion of “establishing the context” as an activity at the start of this generic risk management process. Establishing the context will capture the objectives of the organization, the environment in which it pursues those objectives, its stakeholders and the diversity of risk criteria – all of which will help reveal and assess the nature and complexity of its risks.

The relationship between the principles for managing risk, the framework in which it occurs and the risk management process described in this International Standard are shown in Figure 1.

When implemented and maintained in accordance with this International Standard, the management of risk enables an organization to, for example:

— increase the likelihood of achieving objectives;

— encourage proactive management;

— be aware of the need to identify and treat risk throughout the organization;

— improve the identification of opportunities and threats;

— comply with relevant legal and regulatory requirements and international norms;

— improve mandatory and voluntary reporting;

— improve governance;

— improve stakeholder confidence and trust;

— establish a reliable basis for decision making and planning;

— improve controls;

— effectively allocate and use resources for risk treatment;

— improve operational effectiveness and efficiency;

— enhance health and safety performance, as well as environmental protection;

— improve loss prevention and incident management;

— minimize losses;

— improve organizational learning; and

— improve organizational resilience.

This International Standard is intended to meet the needs of a wide range of stakeholders, including:

a) those responsible for developing risk management policy within their organization;

b) those accountable for ensuring that risk is effectively managed within the organization as a whole or within a specific area, project or activity;

c) those who need to evaluate an organization's effectiveness in managing risk; and

d) developers of standards, guides, procedures and codes of practice that, in whole or in part, set out how risk is to be managed within the specific context of these documents.

The current management practices and processes of many organizations include components of risk management, and many organizations have already adopted a formal risk management process for particular types of risk or circumstances. In such cases, an organization can decide to carry out a critical review of its existing practices and processes in the light of this International Standard.

In this International Standard, the expressions “risk management” and “managing risk” are both used. In general terms, “risk management” refers to the architecture (principles, framework and process) for managing risks effectively, while “managing risk” refers to applying that architecture to particular risks.

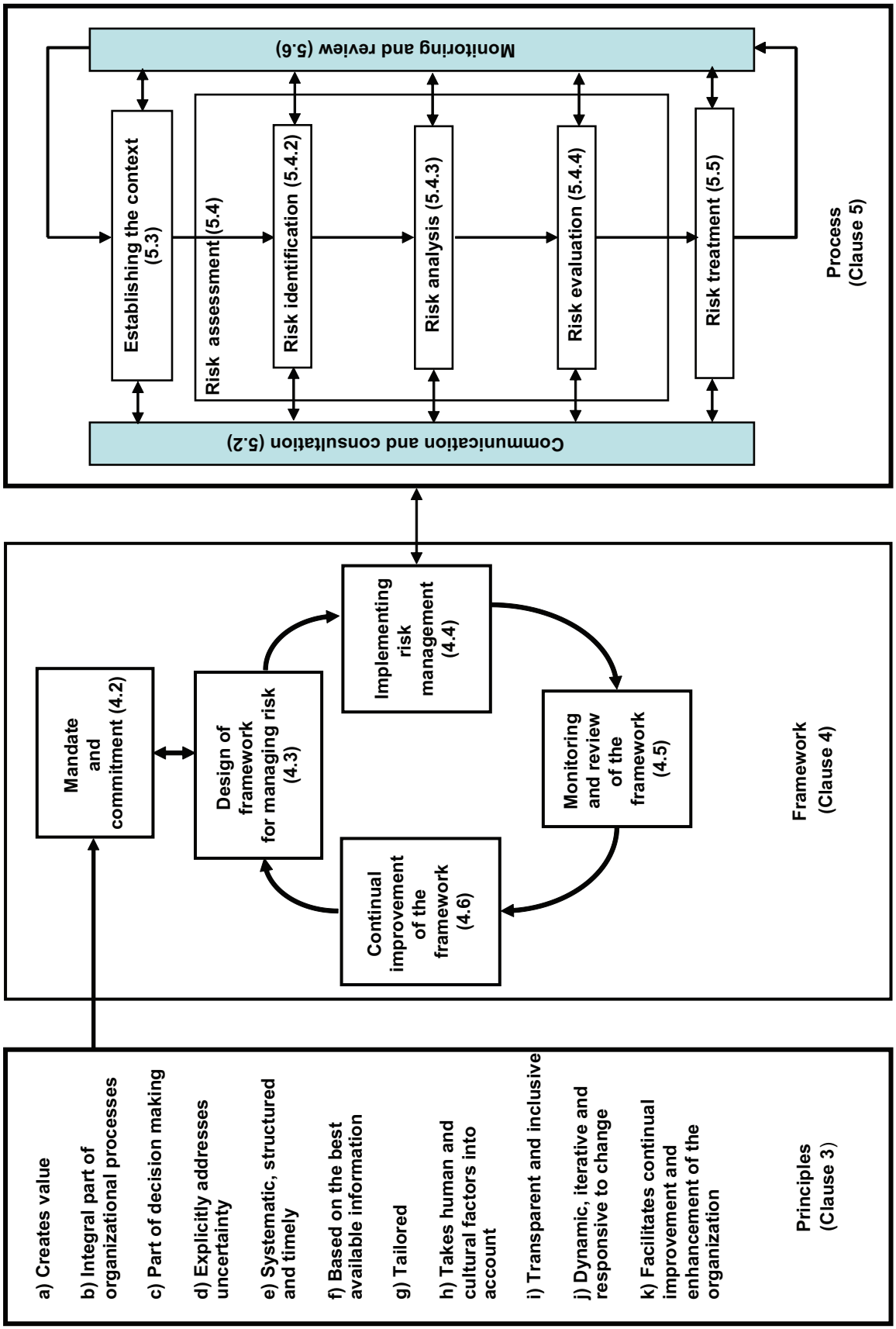


Figure 1 — Relationships between the risk management principles, framework and process

INTERNATIONAL STANDARD **ISO 31000:2009(E)**

Risk management — Principles and guidelines

1 Scope

This International Standard provides principles and generic guidelines on risk management.

This International Standard can be used by any public, private or community enterprise, association, group or individual. Therefore, this International Standard is not specific to any industry or sector.

NOTE For convenience, all the different users of this International Standard are referred to by the general term "organization".

This International Standard can be applied throughout the life of an organization, and to a wide range of activities, including strategies and decisions, operations, processes, functions, projects, products, services and assets.

This International Standard can be applied to any type of risk, whatever its nature, whether having positive or negative consequences.

Although this International Standard provides generic guidelines, it is not intended to promote uniformity of risk management across organizations. The design and implementation of risk management plans and frameworks will need to take into account the varying needs of a specific organization, its particular objectives, context, structure, operations, processes, functions, projects, products, services, or assets and specific practices employed.

It is intended that this International Standard be utilized to harmonize risk management processes in existing and future standards. It provides a common approach in support of standards dealing with specific risks and/or sectors, and does not replace those standards.

This International Standard is not intended for the purpose of certification.

2 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

2.1
risk
effect of uncertainty on objectives

NOTE 1 An effect is a deviation from the expected — positive and/or negative.

NOTE 2 Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process).

NOTE 3 Risk is often characterized by reference to potential **events** (2.17) and **consequences** (2.18), or a combination of these.

NOTE 4 Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated **likelihood** (2.19) of occurrence.

NOTE 5 Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of an event, its consequence, or likelihood.

[ISO Guide 73:2009, definition 1.1]

2.2
risk management
coordinated activities to direct and control an organization with regard to **risk** (2.1)

[ISO Guide 73:2009, definition 2.1]

2.3
risk management framework
set of components that provide the foundations and organizational arrangements for designing, implementing, **monitoring** (2.28), reviewing and continually improving **risk management** (2.2) throughout the organization

NOTE 1 The foundations include the policy, objectives, mandate and commitment to manage **risk** (2.1).

NOTE 2 The organizational arrangements include plans, relationships, accountabilities, resources, processes and activities.

NOTE 3 The risk management framework is embedded within the organization's overall strategic and operational policies and practices.

[ISO Guide 73:2009, definition 2.1.1]

2.4
risk management policy
statement of the overall intentions and direction of an organization related to **risk management** (2.2)

[ISO Guide 73:2009, definition 2.1.2]

2.5
risk attitude
organization's approach to assess and eventually pursue, retain, take or turn away from **risk** (2.1)

[ISO Guide 73:2009, definition 3.7.1.1]

2.6
risk management plan
scheme within the **risk management framework** (2.3) specifying the approach, the management components and resources to be applied to the management of **risk** (2.1)

NOTE 1 Management components typically include procedures, practices, assignment of responsibilities, sequence and timing of activities.

NOTE 2 The risk management plan can be applied to a particular product, process and project, and part or whole of the organization.

[ISO Guide 73:2009, definition 2.1.3]

2.7
risk owner
person or entity with the accountability and authority to manage a **risk** (2.1)

[ISO Guide 73:2009, definition 3.5.1.5]

2.8
risk management process
systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, **monitoring** (2.28) and reviewing **risk** (2.1)

[ISO Guide 73:2009, definition 3.1]

2.9
establishing the context
defining the external and internal parameters to be taken into account when managing risk, and setting the scope and **risk criteria** (2.22) for the **risk management policy** (2.4)

[ISO Guide 73:2009, definition 3.3.1]

2.10
external context
external environment in which the organization seeks to achieve its objectives

NOTE External context can include:

— the cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;

— key drivers and trends having impact on the objectives of the organization; and

— relationships with, and perceptions and values of external **stakeholders** (2.13).

[ISO Guide 73:2009, definition 3.3.1.1]

2.11
internal context
internal environment in which the organization seeks to achieve its objectives

NOTE Internal context can include:

— governance, organizational structure, roles and accountabilities;

— policies, objectives, and the strategies that are in place to achieve them;

— the capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);

— information systems, information flows and decision-making processes (both formal and informal);

— relationships with, and perceptions and values of, internal stakeholders;

— the organization's culture;

— standards, guidelines and models adopted by the organization; and

— form and extent of contractual relationships.

[ISO Guide 73:2009, definition 3.3.1.2]

2.12
communication and consultation
continual and iterative processes that an organization conducts to provide, share or obtain information and to engage in dialogue with **stakeholders** (2.13) regarding the management of **risk** (2.1)

NOTE 1 The information can relate to the existence, nature, form, **likelihood** (2.19), significance, evaluation, acceptability and treatment of the management of risk.

NOTE 2 Consultation is a two-way process of informed communication between an organization and its stakeholders on an issue prior to making a decision or determining a direction on that issue. Consultation is:

— a process which impacts on a decision through influence rather than power; and

— an input to decision making, not joint decision making.

[ISO Guide 73:2009, definition 3.2.1]

2.13
stakeholder
person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity

NOTE A decision maker can be a stakeholder.

[ISO Guide 73:2009, definition 3.2.1.1]

2.14
risk assessment
overall process of **risk identification** (2.15), **risk analysis** (2.21) and **risk evaluation** (2.24)

[ISO Guide 73:2009, definition 3.4.1]

2.15
risk identification
process of finding, recognizing and describing **risks** (2.1)

NOTE 1 Risk identification involves the identification of **risk sources** (2.16), **events** (2.17), their causes and their potential **consequences** (2.18).

NOTE 2 Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and **stakeholder**'s (2.13) needs.

[ISO Guide 73:2009, definition 3.5.1]

2.16
risk source
element which alone or in combination has the intrinsic potential to give rise to **risk** (2.1)

NOTE A risk source can be tangible or intangible.

[ISO Guide 73:2009, definition 3.5.1.2]

2.17
event
occurrence or change of a particular set of circumstances

NOTE 1 An event can be one or more occurrences, and can have several causes.

NOTE 2 An event can consist of something not happening.

NOTE 3 An event can sometimes be referred to as an “incident” or “accident”.

NOTE 4 An event without **consequences** (2.18) can also be referred to as a “near miss”, “incident”, “near hit” or “close call”.

[ISO Guide 73:2009, definition 3.5.1.3]

2.18
consequence
outcome of an **event** (2.17) affecting objectives

NOTE 1 An event can lead to a range of consequences.

NOTE 2 A consequence can be certain or uncertain and can have positive or negative effects on objectives.

NOTE 3 Consequences can be expressed qualitatively or quantitatively.

NOTE 4 Initial consequences can escalate through knock-on effects.

[ISO Guide 73:2009, definition 3.6.1.3]

2.19
likelihood
chance of something happening

NOTE 1 In risk management terminology, the word "likelihood" is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period).

NOTE 2 The English term "likelihood" does not have a direct equivalent in some languages; instead, the equivalent of the term "probability" is often used. However, in English, "probability" is often narrowly interpreted as a mathematical term. Therefore, in risk management terminology, "likelihood" is used with the intent that it should have the same broad interpretation as the term "probability" has in many languages other than English.

[ISO Guide 73:2009, definition 3.6.1.1]

2.20
risk profile
description of any set of **risks** (2.1)

NOTE The set of risks can contain those that relate to the whole organization, part of the organization, or as otherwise defined.

[ISO Guide 73:2009, definition 3.8.2.5]

2.21
risk analysis
process to comprehend the nature of **risk** (2.1) and to determine the **level of risk** (2.23)

NOTE 1 Risk analysis provides the basis for **risk evaluation** (2.24) and decisions about **risk treatment** (2.25).

NOTE 2 Risk analysis includes risk estimation.

[ISO Guide 73:2009, definition 3.6.1]

2.22
risk criteria
terms of reference against which the significance of a **risk** (2.1) is evaluated

NOTE 1 Risk criteria are based on organizational objectives, and **external** (2.10) and **internal context** (2.11).

NOTE 2 Risk criteria can be derived from standards, laws, policies and other requirements.

[ISO Guide 73:2009, definition 3.3.1.3]

2.23
level of risk
magnitude of a **risk** (2.1) or combination of risks, expressed in terms of the combination of **consequences** (2.18) and their **likelihood** (2.19)

[ISO Guide 73:2009, definition 3.6.1.8]

2.24
risk evaluation
process of comparing the results of **risk analysis** (2.21) with **risk criteria** (2.22) to determine whether the **risk** (2.1) and/or its magnitude is acceptable or tolerable

NOTE Risk evaluation assists in the decision about **risk treatment** (2.25).

[ISO Guide 73:2009, definition 3.7.1]

2.25
risk treatment
process to modify **risk** (2.1)

NOTE 1 Risk treatment can involve:

— avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;

— taking or increasing risk in order to pursue an opportunity;

— removing the **risk source** (2.16);

— changing the **likelihood** (2.19);

— changing the **consequences** (2.18);

— sharing the risk with another party or parties (including contracts and risk financing); and

— retaining the risk by informed decision.

NOTE 2 Risk treatments that deal with negative consequences are sometimes referred to as “risk mitigation”, “risk elimination”, “risk prevention” and “risk reduction”.

NOTE 3 Risk treatment can create new risks or modify existing risks.

[ISO Guide 73:2009, definition 3.8.1]

2.26
control
measure that is modifying **risk** (2.1)

NOTE 1 Controls include any process, policy, device, practice, or other actions which modify risk.

NOTE 2 Controls may not always exert the intended or assumed modifying effect.

[ISO Guide 73:2009, definition 3.8.1.1]

2.27
residual risk
risk (2.1) remaining after **risk treatment** (2.25)

NOTE 1 Residual risk can contain unidentified risk.

NOTE 2 Residual risk can also be known as “retained risk”.

[ISO Guide 73:2009, definition 3.8.1.6]

2.28
monitoring
continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected

NOTE Monitoring can be applied to a **risk management framework** (2.3), **risk management process** (2.8), **risk** (2.1) or **control** (2.26).

[ISO Guide 73:2009, definition 3.8.2.1]

2.29
review
activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives

NOTE Review can be applied to a **risk management framework** (2.3), **risk management process** (2.8), **risk** (2.1) or **control** (2.26).

[ISO Guide 73:2009, definition 3.8.2.2]

3 Principles

For risk management to be effective, an organization should at all levels comply with the principles below.

a) **Risk management creates and protects value**.

Risk management contributes to the demonstrable achievement of objectives and improvement of performance in, for example, human health and safety, security, legal and regulatory compliance, public acceptance, environmental protection, product quality, project management, efficiency in operations, governance and reputation.

b) **Risk management is an integral part of all organizational processes**.

Risk management is not a stand-alone activity that is separate from the main activities and processes of the organization. Risk management is part of the responsibilities of management and an integral part of all organizational processes, including strategic planning and all project and change management processes.

c) **Risk management is part of decision making**.

Risk management helps decision makers make informed choices, prioritize actions and distinguish among alternative courses of action.

d) **Risk management explicitly addresses uncertainty**.

Risk management explicitly takes account of uncertainty, the nature of that uncertainty, and how it can be addressed.

e) **Risk management is systematic, structured and timely**.

A systematic, timely and structured approach to risk management contributes to efficiency and to consistent, comparable and reliable results.

f) **Risk management is based on the best available information**.

The inputs to the process of managing risk are based on information sources such as historical data, experience, stakeholder feedback, observation, forecasts and expert judgement. However, decision makers should inform themselves of, and should take into account, any limitations of the data or modelling used or the possibility of divergence among experts.

g) **Risk management is tailored**.

Risk management is aligned with the organization's external and internal context and risk profile.

h) **Risk management takes human and cultural factors into account**.

Risk management recognizes the capabilities, perceptions and intentions of external and internal people that can facilitate or hinder achievement of the organization's objectives.

i) **Risk management is transparent and inclusive**.

Appropriate and timely involvement of stakeholders and, in particular, decision makers at all levels of the organization, ensures that risk management remains relevant and up-to-date. Involvement also allows stakeholders to be properly represented and to have their views taken into account in determining risk criteria.

j) **Risk management is dynamic, iterative and responsive to change**.

Risk management continually senses and responds to change. As external and internal events occur, context and knowledge change, monitoring and review of risks take place, new risks emerge, some change, and others disappear.

k) **Risk management facilitates continual improvement of the organization**.

Organizations should develop and implement strategies to improve their risk management maturity alongside all other aspects of their organization.

Annex A provides further advice for organizations wishing to manage risk more effectively.

4 Framework

4.1 General

The success of risk management will depend on the effectiveness of the management framework providing the foundations and arrangements that will embed it throughout the organization at all levels. The framework assists in managing risks effectively through the application of the risk management process (see Clause 5) at varying levels and within specific contexts of the organization. The framework ensures that information about risk derived from the risk management process is adequately reported and used as a basis for decision making and accountability at all relevant organizational levels.

This clause describes the necessary components of the framework for managing risk and the way in which they interrelate in an iterative manner, as shown in Figure 2.

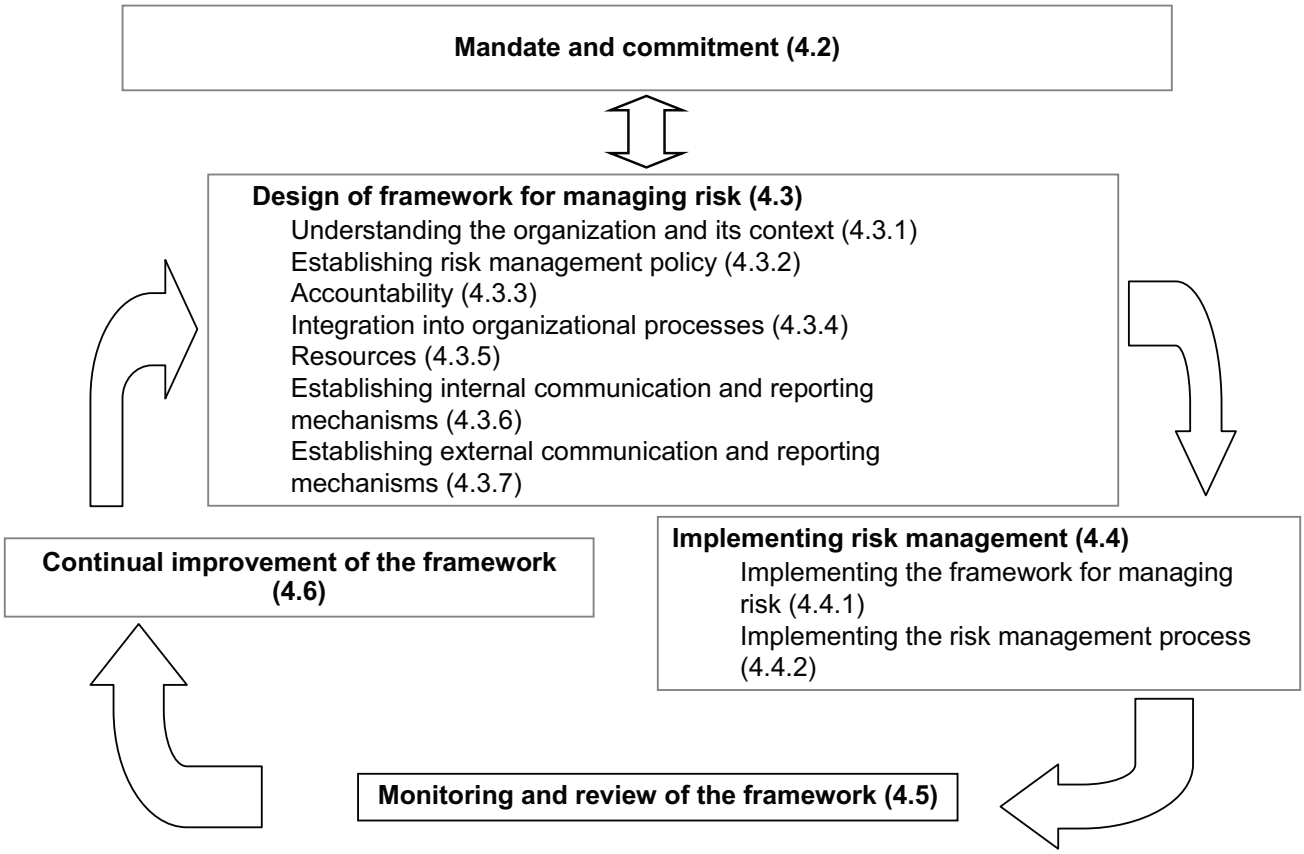


Figure 2 — Relationship between the components of the framework for managing risk

This framework is not intended to prescribe a management system, but rather to assist the organization to integrate risk management into its overall management system. Therefore, organizations should adapt the components of the framework to their specific needs.

If an organization's existing management practices and processes include components of risk management or if the organization has already adopted a formal risk management process for particular types of risk or situations, then these should be critically reviewed and assessed against this International Standard, including the attributes contained in Annex A, in order to determine their adequacy and effectiveness.

4.2 Mandate and commitment

The introduction of risk management and ensuring its ongoing effectiveness require strong and sustained commitment by management of the organization, as well as strategic and rigorous planning to achieve commitment at all levels. Management should:

— define and endorse the risk management policy;

— ensure that the organization's culture and risk management policy are aligned;

— determine risk management performance indicators that align with performance indicators of the organization;

— align risk management objectives with the objectives and strategies of the organization;

— ensure legal and regulatory compliance;

— assign accountabilities and responsibilities at appropriate levels within the organization;

— ensure that the necessary resources are allocated to risk management;

— communicate the benefits of risk management to all stakeholders; and

— ensure that the framework for managing risk continues to remain appropriate.

4.3 Design of framework for managing risk

4.3.1 Understanding of the organization and its context

Before starting the design and implementation of the framework for managing risk, it is important to evaluate and understand both the external and internal context of the organization, since these can significantly influence the design of the framework.

Evaluating the organization's external context may include, but is not limited to:

a) the social and cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;

b) key drivers and trends having impact on the objectives of the organization; and

c) relationships with, and perceptions and values of, external stakeholders.

Evaluating the organization's internal context may include, but is not limited to:

— governance, organizational structure, roles and accountabilities;

— policies, objectives, and the strategies that are in place to achieve them;

— capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);

— information systems, information flows and decision making processes (both formal and informal);

— relationships with, and perceptions and values of, internal stakeholders;

— the organization's culture;

— standards, guidelines and models adopted by the organization; and

— the form and extent of contractual relationships.

4.3.2 Establishing risk management policy

The risk management policy should clearly state the organization's objectives for, and commitment to, risk management and typically addresses the following:

— the organization's rationale for managing risk;

— links between the organization's objectives and policies and the risk management policy;

— accountabilities and responsibilities for managing risk;

— the way in which conflicting interests are dealt with;

— commitment to make the necessary resources available to assist those accountable and responsible for managing risk;

— the way in which risk management performance will be measured and reported; and

— commitment to review and improve the risk management policy and framework periodically and in response to an event or change in circumstances.

The risk management policy should be communicated appropriately.

4.3.3 Accountability

The organization should ensure that there is accountability, authority and appropriate competence for managing risk, including implementing and maintaining the risk management process and ensuring the adequacy, effectiveness and efficiency of any controls. This can be facilitated by:

— identifying risk owners that have the accountability and authority to manage risks;

— identifying who is accountable for the development, implementation and maintenance of the framework for managing risk;

— identifying other responsibilities of people at all levels in the organization for the risk management process;

— establishing performance measurement and external and/or internal reporting and escalation processes; and

— ensuring appropriate levels of recognition.

4.3.4 Integration into organizational processes

Risk management should be embedded in all the organization's practices and processes in a way that it is relevant, effective and efficient. The risk management process should become part of, and not separate from, those organizational processes. In particular, risk management should be embedded into the policy development, business and strategic planning and review, and change management processes.

There should be an organization-wide risk management plan to ensure that the risk management policy is implemented and that risk management is embedded in all of the organization's practices and processes. The risk management plan can be integrated into other organizational plans, such as a strategic plan.

4.3.5 Resources

The organization should allocate appropriate resources for risk management.

Consideration should be given to the following:

— people, skills, experience and competence;

— resources needed for each step of the risk management process;

— the organization's processes, methods and tools to be used for managing risk;

— documented processes and procedures;

— information and knowledge management systems; and

— training programmes.

4.3.6 Establishing internal communication and reporting mechanisms

The organization should establish internal communication and reporting mechanisms in order to support and encourage accountability and ownership of risk. These mechanisms should ensure that:

— key components of the risk management framework, and any subsequent modifications, are communicated appropriately;

— there is adequate internal reporting on the framework, its effectiveness and the outcomes;

— relevant information derived from the application of risk management is available at appropriate levels and times; and

— there are processes for consultation with internal stakeholders.

These mechanisms should, where appropriate, include processes to consolidate risk information from a variety of sources, and may need to consider the sensitivity of the information.

4.3.7 Establishing external communication and reporting mechanisms

The organization should develop and implement a plan as to how it will communicate with external stakeholders. This should involve:

— engaging appropriate external stakeholders and ensuring an effective exchange of information;

— external reporting to comply with legal, regulatory, and governance requirements;

— providing feedback and reporting on communication and consultation;

— using communication to build confidence in the organization; and

— communicating with stakeholders in the event of a crisis or contingency.

These mechanisms should, where appropriate, include processes to consolidate risk information from a variety of sources, and may need to consider the sensitivity of the information.

4.4 Implementing risk management

4.4.1 Implementing the framework for managing risk

In implementing the organization's framework for managing risk, the organization should:

— define the appropriate timing and strategy for implementing the framework;

— apply the risk management policy and process to the organizational processes;

— comply with legal and regulatory requirements;

— ensure that decision making, including the development and setting of objectives, is aligned with the outcomes of risk management processes;

— hold information and training sessions; and

— communicate and consult with stakeholders to ensure that its risk management framework remains appropriate.

4.4.2 Implementing the risk management process

Risk management should be implemented by ensuring that the risk management process outlined in Clause 5 is applied through a risk management plan at all relevant levels and functions of the organization as part of its practices and processes.

4.5 Monitoring and review of the framework

In order to ensure that risk management is effective and continues to support organizational performance, the organization should:

— measure risk management performance against indicators, which are periodically reviewed for appropriateness;

— periodically measure progress against, and deviation from, the risk management plan;

— periodically review whether the risk management framework, policy and plan are still appropriate, given the organizations' external and internal context;

— report on risk, progress with the risk management plan and how well the risk management policy is being followed; and

— review the effectiveness of the risk management framework.

4.6 Continual improvement of the framework

Based on results of monitoring and reviews, decisions should be made on how the risk management framework, policy and plan can be improved. These decisions should lead to improvements in the organization's management of risk and its risk management culture.

5 Process

5.1 General

The risk management process should be

— an integral part of management,

— embedded in the culture and practices, and

— tailored to the business processes of the organization.

It comprises the activities described in 5.2 to 5.6. The risk management process is shown in Figure 3.

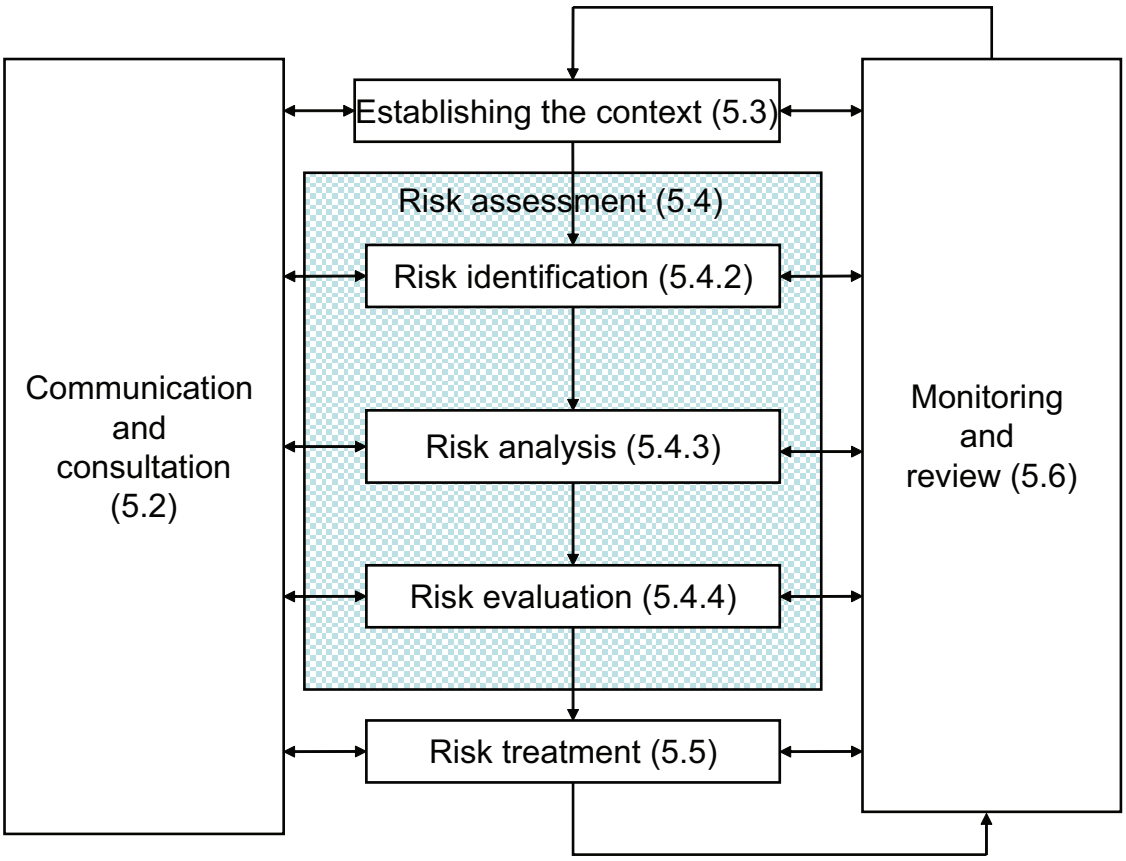


Figure 3 — Risk management process

5.2 Communication and consultation

Communication and consultation with external and internal stakeholders should take place during all stages of the risk management process.

Therefore, plans for communication and consultation should be developed at an early stage. These should address issues relating to the risk itself, its causes, its consequences (if known), and the measures being taken to treat it. Effective external and internal communication and consultation should take place to ensure that those accountable for implementing the risk management process and stakeholders understand the basis on which decisions are made, and the reasons why particular actions are required.

A consultative team approach may:

— help establish the context appropriately;

— ensure that the interests of stakeholders are understood and considered;

— help ensure that risks are adequately identified;

— bring different areas of expertise together for analyzing risks;

— ensure that different views are appropriately considered when defining risk criteria and in evaluating risks;

— secure endorsement and support for a treatment plan;

— enhance appropriate change management during the risk management process; and

— develop an appropriate external and internal communication and consultation plan.

Communication and consultation with stakeholders is important as they make judgements about risk based on their perceptions of risk. These perceptions can vary due to differences in values, needs, assumptions, concepts and concerns of stakeholders. As their views can have a significant impact on the decisions made, the stakeholders' perceptions should be identified, recorded, and taken into account in the decision making process.

Communication and consultation should facilitate truthful, relevant, accurate and understandable exchanges of information, taking into account confidential and personal integrity aspects.

5.3 Establishing the context

5.3.1 General

By establishing the context, the organization articulates its objectives, defines the external and internal parameters to be taken into account when managing risk, and sets the scope and risk criteria for the remaining process. While many of these parameters are similar to those considered in the design of the risk management framework (see 4.3.1), when establishing the context for the risk management process, they need to be considered in greater detail and particularly how they relate to the scope of the particular risk management process.

5.3.2 Establishing the external context

The external context is the external environment in which the organization seeks to achieve its objectives.

Understanding the external context is important in order to ensure that the objectives and concerns of external stakeholders are considered when developing risk criteria. It is based on the organization-wide context, but with specific details of legal and regulatory requirements, stakeholder perceptions and other aspects of risks specific to the scope of the risk management process.

The external context can include, but is not limited to:

— the social and cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;

— key drivers and trends having impact on the objectives of the organization; and

— relationships with, perceptions and values of external stakeholders.

5.3.3 Establishing the internal context

The internal context is the internal environment in which the organization seeks to achieve its objectives.

The risk management process should be aligned with the organization's culture, processes, structure and strategy. Internal context is anything within the organization that can influence the way in which an organization will manage risk. It should be established because:

a) risk management takes place in the context of the objectives of the organization;

b) objectives and criteria of a particular project, process or activity should be considered in the light of objectives of the organization as a whole; and

c) some organizations fail to recognize opportunities to achieve their strategic, project or business objectives, and this affects ongoing organizational commitment, credibility, trust and value.

It is necessary to understand the internal context. This can include, but is not limited to:

— governance, organizational structure, roles and accountabilities;

— policies, objectives, and the strategies that are in place to achieve them;

— capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);

— the relationships with and perceptions and values of internal stakeholders;

— the organization's culture;

— information systems, information flows and decision making processes (both formal and informal);

— standards, guidelines and models adopted by the organization; and

— form and extent of contractual relationships.

5.3.4 Establishing the context of the risk management process

The objectives, strategies, scope and parameters of the activities of the organization, or those parts of the organization where the risk management process is being applied, should be established. The management of risk should be undertaken with full consideration of the need to justify the resources used in carrying out risk management. The resources required, responsibilities and authorities, and the records to be kept should also be specified.

The context of the risk management process will vary according to the needs of an organization. It can involve, but is not limited to:

— defining the goals and objectives of the risk management activities;

— defining responsibilities for and within the risk management process;

— defining the scope, as well as the depth and breadth of the risk management activities to be carried out, including specific inclusions and exclusions;

— defining the activity, process, function, project, product, service or asset in terms of time and location;

— defining the relationships between a particular project, process or activity and other projects, processes or activities of the organization;

— defining the risk assessment methodologies;

— defining the way performance and effectiveness is evaluated in the management of risk;

— identifying and specifying the decisions that have to be made; and

— identifying, scoping or framing studies needed, their extent and objectives, and the resources required for such studies.

Attention to these and other relevant factors should help ensure that the risk management approach adopted is appropriate to the circumstances, to the organization and to the risks affecting the achievement of its objectives.

5.3.5 Defining risk criteria

The organization should define criteria to be used to evaluate the significance of risk. The criteria should reflect the organization's values, objectives and resources. Some criteria can be imposed by, or derived from, legal and regulatory requirements and other requirements to which the organization subscribes. Risk criteria should be consistent with the organization's risk management policy (see 4.3.2), be defined at the beginning of any risk management process and be continually reviewed.

When defining risk criteria, factors to be considered should include the following:

— the nature and types of causes and consequences that can occur and how they will be measured;

— how likelihood will be defined;

— the timeframe(s) of the likelihood and/or consequence(s);

— how the level of risk is to be determined;

— the views of stakeholders;

— the level at which risk becomes acceptable or tolerable; and

— whether combinations of multiple risks should be taken into account and, if so, how and which combinations should be considered.

5.4 Risk assessment

5.4.1 General

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation.

NOTE ISO/IEC 31010 provides guidance on risk assessment techniques.

5.4.2 Risk identification

The organization should identify sources of risk, areas of impacts, events (including changes in circumstances) and their causes and their potential consequences. The aim of this step is to generate a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives. It is important to identify the risks associated with not pursuing an opportunity. Comprehensive identification is critical, because a risk that is not identified at this stage will not be included in further analysis.

Identification should include risks whether or not their source is under the control of the organization, even though the risk source or cause may not be evident. Risk identification should include examination of the knock-on effects of particular consequences, including cascade and cumulative effects. It should also consider a wide range of consequences even if the risk source or cause may not be evident. As well as identifying what might happen, it is necessary to consider possible causes and scenarios that show what consequences can occur. All significant causes and consequences should be considered.

The organization should apply risk identification tools and techniques that are suited to its objectives and capabilities, and to the risks faced. Relevant and up-to-date information is important in identifying risks. This should include appropriate background information where possible. People with appropriate knowledge should be involved in identifying risks.

5.4.3 Risk analysis

Risk analysis involves developing an understanding of the risk. Risk analysis provides an input to risk evaluation and to decisions on whether risks need to be treated, and on the most appropriate risk treatment strategies and methods. Risk analysis can also provide an input into making decisions where choices must be made and the options involve different types and levels of risk.

Risk analysis involves consideration of the causes and sources of risk, their positive and negative consequences, and the likelihood that those consequences can occur. Factors that affect consequences and likelihood should be identified. Risk is analyzed by determining consequences and their likelihood, and other attributes of the risk. An event can have multiple consequences and can affect multiple objectives. Existing controls and their effectiveness and efficiency should also be taken into account.

The way in which consequences and likelihood are expressed and the way in which they are combined to determine a level of risk should reflect the type of risk, the information available and the purpose for which the risk assessment output is to be used. These should all be consistent with the risk criteria. It is also important to consider the interdependence of different risks and their sources.

The confidence in determination of the level of risk and its sensitivity to preconditions and assumptions should be considered in the analysis, and communicated effectively to decision makers and, as appropriate, other stakeholders. Factors such as divergence of opinion among experts, uncertainty, availability, quality, quantity and ongoing relevance of information, or limitations on modelling should be stated and can be highlighted.

Risk analysis can be undertaken with varying degrees of detail, depending on the risk, the purpose of the analysis, and the information, data and resources available. Analysis can be qualitative, semi-quantitative or quantitative, or a combination of these, depending on the circumstances.

Consequences and their likelihood can be determined by modelling the outcomes of an event or set of events, or by extrapolation from experimental studies or from available data. Consequences can be expressed in terms of tangible and intangible impacts. In some cases, more than one numerical value or descriptor is required to specify consequences and their likelihood for different times, places, groups or situations.

5.4.4 Risk evaluation

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.

Decisions should take account of the wider context of the risk and include consideration of the tolerance of the risks borne by parties other than the organization that benefits from the risk. Decisions should be made in accordance with legal, regulatory and other requirements.

In some circumstances, the risk evaluation can lead to a decision to undertake further analysis. The risk evaluation can also lead to a decision not to treat the risk in any way other than maintaining existing controls. This decision will be influenced by the organization's risk attitude and the risk criteria that have been established.

5.5 Risk treatment

5.5.1 General

Risk treatment involves selecting one or more options for modifying risks, and implementing those options. Once implemented, treatments provide or modify the controls.

Risk treatment involves a cyclical process of:

— assessing a risk treatment;

— deciding whether residual risk levels are tolerable;

— if not tolerable, generating a new risk treatment; and

— assessing the effectiveness of that treatment.

Risk treatment options are not necessarily mutually exclusive or appropriate in all circumstances. The options can include the following:

a) avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;

b) taking or increasing the risk in order to pursue an opportunity;

c) removing the risk source;

d) changing the likelihood;

e) changing the consequences;

f) sharing the risk with another party or parties (including contracts and risk financing); and

g) retaining the risk by informed decision.

5.5.2 Selection of risk treatment options

Selecting the most appropriate risk treatment option involves balancing the costs and efforts of implementation against the benefits derived, with regard to legal, regulatory, and other requirements such as social responsibility and the protection of the natural environment. Decisions should also take into account risks which can warrant risk treatment that is not justifiable on economic grounds, e.g. severe (high negative consequence) but rare (low likelihood) risks.

A number of treatment options can be considered and applied either individually or in combination. The organization can normally benefit from the adoption of a combination of treatment options.

When selecting risk treatment options, the organization should consider the values and perceptions of stakeholders and the most appropriate ways to communicate with them. Where risk treatment options can impact on risk elsewhere in the organization or with stakeholders, these should be involved in the decision. Though equally effective, some risk treatments can be more acceptable to some stakeholders than to others.

The treatment plan should clearly identify the priority order in which individual risk treatments should be implemented.

Risk treatment itself can introduce risks. A significant risk can be the failure or ineffectiveness of the risk treatment measures. Monitoring needs to be an integral part of the risk treatment plan to give assurance that the measures remain effective.

Risk treatment can also introduce secondary risks that need to be assessed, treated, monitored and reviewed. These secondary risks should be incorporated into the same treatment plan as the original risk and not treated as a new risk. The link between the two risks should be identified and maintained.

5.5.3 Preparing and implementing risk treatment plans

The purpose of risk treatment plans is to document how the chosen treatment options will be implemented. The information provided in treatment plans should include:

— the reasons for selection of treatment options, including expected benefits to be gained;

— those who are accountable for approving the plan and those responsible for implementing the plan;

— proposed actions;

— resource requirements including contingencies;

— performance measures and constraints;

— reporting and monitoring requirements; and

— timing and schedule.

Treatment plans should be integrated with the management processes of the organization and discussed with appropriate stakeholders.

Decision makers and other stakeholders should be aware of the nature and extent of the residual risk after risk treatment. The residual risk should be documented and subjected to monitoring, review and, where appropriate, further treatment.

5.6 Monitoring and review

Both monitoring and review should be a planned part of the risk management process and involve regular checking or surveillance. It can be periodic or *ad hoc*.

Responsibilities for monitoring and review should be clearly defined.

The organization's monitoring and review processes should encompass all aspects of the risk management process for the purposes of:

— ensuring that controls are effective and efficient in both design and operation;

— obtaining further information to improve risk assessment;

— analyzing and learning lessons from events (including near-misses), changes, trends, successes and failures;

— detecting changes in the external and internal context, including changes to risk criteria and the risk itself which can require revision of risk treatments and priorities; and

— identifying emerging risks.

Progress in implementing risk treatment plans provides a performance measure. The results can be incorporated into the organization's overall performance management, measurement and external and internal reporting activities.

The results of monitoring and review should be recorded and externally and internally reported as appropriate, and should also be used as an input to the review of the risk management framework (see 4.5).

5.7 Recording the risk management process

Risk management activities should be traceable. In the risk management process, records provide the foundation for improvement in methods and tools, as well as in the overall process.

Decisions concerning the creation of records should take into account:

— the organization's needs for continuous learning;

— benefits of re-using information for management purposes;

— costs and efforts involved in creating and maintaining records;

— legal, regulatory and operational needs for records;

— method of access, ease of retrievability and storage media;

— retention period; and

— sensitivity of information.

Annex A
(informative)

Attributes of enhanced risk management

A.1 General

All organizations should aim at the appropriate level of performance of their risk management framework in line with the criticality of the decisions that are to be made. The list of attributes below represents a high level of performance in managing risk. To assist organizations in measuring their own performance against these criteria, some tangible indicators are given for each attribute.

A.2 Key outcomes

A.2.1 The organization has a current, correct and comprehensive understanding of its risks.

A.2.2 The organization's risks are within its risk criteria.

A.3 Attributes

A.3.1 Continual improvement

An emphasis is placed on continual improvement in risk management through the setting of organizational performance goals, measurement, review and the subsequent modification of processes, systems, resources, capability and skills.

This can be indicated by the existence of explicit performance goals against which the organization's and individual manager's performance is measured. The organization's performance can be published and communicated. Normally, there will be at least an annual review of performance and then a revision of processes, and the setting of revised performance objectives for the following period.

This risk management performance assessment is an integral part of the overall organization's performance assessment and measurement system for departments and individuals.

A.3.2 Full accountability for risks

Enhanced risk management includes comprehensive, fully defined and fully accepted accountability for risks, controls and risk treatment tasks. Designated individuals fully accept accountability, are appropriately skilled and have adequate resources to check controls, monitor risks, improve controls and communicate effectively about risks and their management to external and internal stakeholders.

This can be indicated by all members of an organization being fully aware of the risks, controls and tasks for which they are accountable. Normally, this will be recorded in job/position descriptions, databases or information systems. The definition of risk management roles, accountabilities and responsibilities should be part of all the organization's induction programmes.

The organization ensures that those who are accountable are equipped to fulfil that role by providing them with the authority, time, training, resources and skills sufficient to assume their accountabilities.

A.3.3 Application of risk management in all decision making

All decision making within the organization, whatever the level of importance and significance, involves the explicit consideration of risks and the application of risk management to some appropriate degree.

This can be indicated by records of meetings and decisions to show that explicit discussions on risks took place. In addition, it should be possible to see that all components of risk management are represented within key processes for decision making in the organization, e.g. for decisions on the allocation of capital, on major projects and on re-structuring and organizational changes. For these reasons, soundly based risk management is seen within the organization as providing the basis for effective governance.

A.3.4 Continual communications

Enhanced risk management includes continual communications with external and internal stakeholders, including comprehensive and frequent reporting of risk management performance, as part of good governance.

This can be indicated by communication with stakeholders as an integral and essential component of risk management. Communication is rightly seen as a two-way process, such that properly informed decisions can be made about the level of risks and the need for risk treatment against properly established and comprehensive risk criteria.

Comprehensive and frequent external and internal reporting on both significant risks and on risk management performance contributes substantially to effective governance within an organization.

A.3.5 Full integration in the organization's governance structure

Risk management is viewed as central to the organization's management processes, such that risks are considered in terms of effect of uncertainty on objectives. The governance structure and process are based on the management of risk. Effective risk management is regarded by managers as essential for the achievement of the organization's objectives.

This is indicated by managers' language and important written materials in the organization using the term “uncertainty” in connection with risks. This attribute is also normally reflected in the organization's statements of policy, particularly those relating to risk management. Normally, this attribute would be verified through interviews with managers and through the evidence of their actions and statements.

Bibliography

[1] ISO Guide 73:2009, *Risk management — Vocabulary*

[2] ISO/IEC 31010, *Risk management — Risk assessment techniques*

ICS 03.100.01

Price based on 24 pages

This page has been intentionally left blank

BSI - British Standards Institution

BSI is the independent national body responsible for preparing British Standards. It presents the UK view on standards in Europe and at the international level. It is incorporated by Royal Charter.

Revisions

British Standards are updated by amendment or revision. Users of British Standards should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using this British Standard would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover. Tel: +44 (0)20 8996 9000. Fax: +44 (0)20 8996 7400.

BSI offers members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of standards.

Buying standards

Orders for all BSI, international and foreign standards publications should be addressed to Customer Services. Tel: +44 (0)20 8996 9001. Fax: +44 (0)20 8996 7001 Email: orders@bsigroup.com You may also buy directly using a debit/credit card from the BSI Shop on the Website http://www.bsigroup.com/shop

In response to orders for international standards, it is BSI policy to supply the BSI implementation of those that have been published as British Standards, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Library and its Technical Help to Exporters Service. Various BSI electronic information services are also available which give details on all its products and services. Contact Information Centre. Tel: +44 (0)20 8996 7111 Fax: +44 (0)20 8996 7048 Email: info@bsigroup.com

Subscribing members of BSI are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration. Tel: +44 (0)20 8996 7002 Fax: +44 (0)20 8996 7001 Email: membership@bsigroup.com

Information regarding online access to British Standards via British Standards Online can be found at http://www.bsigroup.com/BSOL

Further information about BSI is available on the BSI website at http://www.bsigroup.com

Copyright

BSI Group
Headquarters 389
Chiswick High Road,
London, W4 4AL, UK
Tel +44 (0)20 8996 9001
Fax +44 (0)20 8996 7001
www.bsigroup.com/
standards

BS 31100:2011

Risk management – Code of practice and guidance for the implementation of BS ISO 31000

BS 31100:2011

Risk management – Code of practice and guidance for the implementation of BS ISO 31000

Publishing and copyright information

ISBN 978 0 580 71607 2

ICS 03.100.01

The following BSI references relate to the work on this standard:
Committee reference RM/1
Draft for comment 11/30228063 DC

Publication history

First published October 2008
Second (present) edition, June 2011

Amendments issued since publication

Date	Text affected

Contents

Summary of pages

This document comprises a front cover, an inside front cover, pages i to iv, pages 1 to 46, an inside back cover and a back cover.

Foreword

Publishing information

This British Standard was published by BSI and came into effect on 30 June 2011. It was prepared by technical Committee RM/1, *Risk management*. A list of organizations represented on this committee can be obtained on request to its secretary.

This British Standard has been developed by practitioners throughout the risk management community, drawing upon their considerable academic, technical and practical experiences of risk management.

Supersession

BS 31100:2011 supersedes BS 31100:2008, which is withdrawn.

Relationship with other documents

BS ISO 31000, *Risk management – Principles and guidelines on implementation*, and ISO/IEC Guide 73, *Risk management – Vocabulary*, were published after the first edition of BS 31100, so that there were some minor structural differences between the documents. This edition was drafted to be consistent with the principles and guidelines on risk management in BS ISO 31000:2009 (see Introduction), and to acknowledge HM Treasury's Orange Book [1], the Office of Government Commerce publication, "Management of risk: Guidance for practitioners" [2], "Enterprise Risk Management – Integrated Framework" and application techniques published by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) [3], and the risk management standard developed by the Institute of Risk Management (IRM), the Association of Insurance and Risk Managers (Airmic) and Alarm [4].

Use of this document

As a code of practice, this British Standard takes the form of guidance and recommendations. It should not be quoted as if it were a specification and particular care should be taken to ensure that claims of compliance are not misleading.

The provisions in this standard are presented in roman (i.e. upright) type. Its recommendations are expressed in sentences in which the principal auxiliary verb is "should".

The word "may" is used in the text to express permissibility, e.g. as an alternative to the primary recommendation of the clause. The word "can" is used to express possibility, e.g. a consequence of an action or an event.

Commentary, explanation and general informative material is presented in smaller italic type, and does not constitute a normative element.

Any user claiming compliance with this British Standard is expected to be able to justify any course of action that deviates from its recommendations.

Presentational conventions

The word "should" is used to express the recommendations of this standard, with which the user has to comply in order to comply with the standard. The word "may" is used in the text to express permissibility, e.g. as an alternative to the primary recommendation of the clause. The word "can" is used to express possibility, e.g. a consequence of an action or an event.

Contractual and legal considerations

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

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

This page deliberately left blank

Introduction

This code of practice gives recommendations for implementing the principles and guidelines on risk management in BS ISO 31000:2009.

This edition of BS 31100 closely matches the structure, terminology and diagrams of BS ISO 31000:2009 and ISO Guide 73:2009 to make it easier to use the three documents side by side. This edition also expands on the recommendations of BS 31100:2008.

The principles in BS ISO 31000:2009 are as follows.

a) Risk management creates and protects value.

b) Risk management is an integral part of all organizational processes.

c) Risk management is part of decision-making.

d) Risk management explicitly addresses uncertainty.

e) Risk management is systematic, structured and timely.

f) Risk management is based on the best available information.

g) Risk management is tailored.

h) Risk management takes human and cultural factors into account.

i) Risk management is transparent and inclusive.

j) Risk management is dynamic, iterative and responsive to change.

k) Risk management facilitates continual improvement of the organization.

The recommendations in this code of practice will help organizations implement these principles in a way that is right for each organization. The recommendations are more practical and specific than the principles and guidelines, but they focus on the key aspects of management and allow for variations in the detail of techniques.

Risks are best managed by people following a defined risk management process. In large organizations there could be many groups and many processes, each with its own scope, meetings, documents and methods. This could be because they are working at different management levels in the organization and have different perspectives (see Figure 1), are working in different organizational sub-units, or are focusing on different types of risks.

The approach recommended here is to provide an outline risk management process that can be followed and interpreted so that each group works in a way that is appropriate for them, and there is consistency and communication across the organization.

Each example of a risk management process within an organization is called an instance of the risk management process.

The outline risk management process is just one component of a broader risk management framework that also contains activities to govern one or more instances of the risk management process and to drive improvements over time.

The recommendations cover the whole organization and all risks. This includes outcomes that are better than expected, as well as those that are worse than expected. In keeping with the definition of risk as "the effect of uncertainty on objectives" the approach encourages people to think widely about what might happen, not just to look for potential dangers. It also encourages greater awareness of uncertainty.

This is achieved using a process and language that apply equally to all risks. For example, risks are "modified" by controls rather than "mitigated" because a risk whose consequences are mostly desirable is one to promote or exploit rather than reduce.

EXAMPLE

A major construction project on a city site had very little land for storing materials and so needed many costly lorry deliveries. There was space on an adjacent site where another developer was working. If a deal could be made it would be possible to use that space to store materials. This possibility was recorded as a risk with predominantly positive consequences, and evaluated. Although there would be an up-front commitment to the other developer, there were possible beneficial consequences from lower transport costs and reduced likelihood of interruptions to work due to late deliveries. Actions were identified to increase the likelihood of the risk being realized, such as working out delivery times and access routes that would avoid interference between the projects. Subsequently, the risk was realized: a deal was made benefiting both developers.

Risk management needs to be integrated into all management activities. This code of practice gives recommendations on how to achieve this integration.

The recommendations in this British Standard have been written for organizations of all types and sizes, and include guidance on how to choose an approach that is appropriate. Table 1 gives examples of how large and small organizations might tailor their risk management.

Figure 1 **Risk management perspectives**

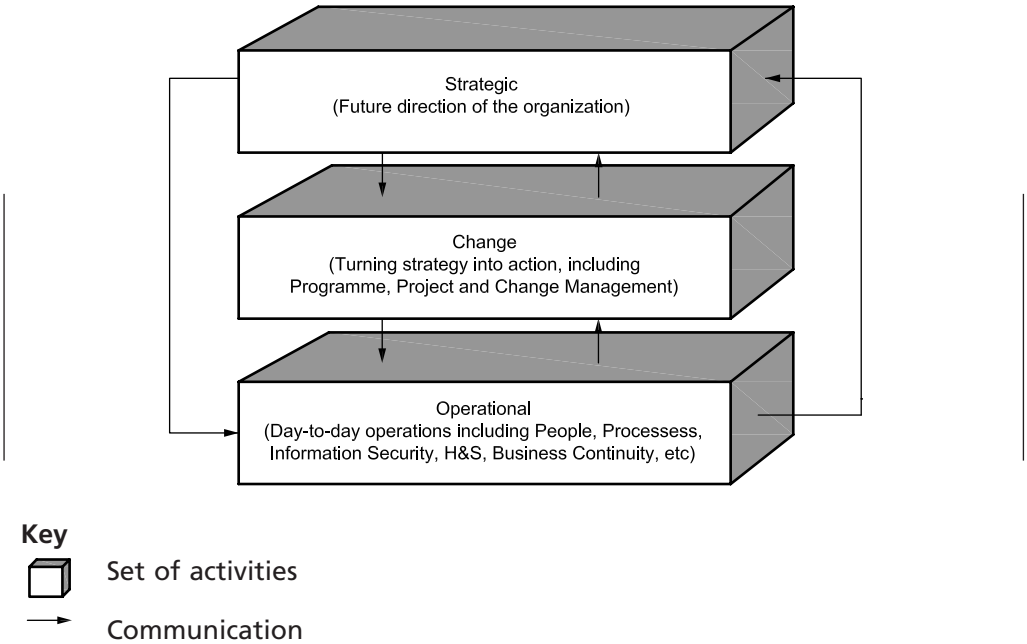


Table 1 **Examples of tailoring**

Point of difference	Small organization	Large organization
Business	Law partnership	Food manufacturer
Employees	10	15,000
Business units and locations	One business unit in one office	36 business units in 27 countries
Ongoing projects	None (presently)	Hundreds
Risk management framework description	A 12-page document	A database with several documents and tools, including risk analysis software
Delegation of risk management activities by the board (or equivalent)	Very little – the partners do almost everything	The main board delegates risk management activities extensively to sub-committees, a risk management support team, and business unit management. Extra assurance is provided by internal auditors.
Instances of the risk management process	One	Hundreds due to the many business units and projects
Detail in procedures for initiating and terminating instances of the risk management process	Described in one paragraph just in case a project is started that justifies it	Described in detail and this activity is tracked using a database
Range of risk analysis techniques	Almost entirely by judgement and conversations among the partners	Varies from conversations and judgement to mathematical modelling (particularly for food safety risks and commodity price hedging) and reliability analyses based on models of manufacturing systems
Quantity and usefulness of risk data generated by the business	Low volume and of limited use	Huge volume, providing a strong basis for quantitative analyses
Detail in procedures for internal reporting about risk management	Described in one paragraph as a topic in the regular partner meetings	Described in detail, with committees involved, help from the risk management support team, and a computer system
Required external reporting about risk management	Limited – for certain activities	Extensive, mainly because of stock market listings and health and safety laws

1 Scope

This British Standard gives recommendations for implementing the principles and guidelines in BS ISO 31000:2009, including the risk management framework and process. It provides a basis for understanding, developing, implementing and maintaining proportionate and effective risk management throughout an organization, in order to enhance the organization's likelihood of achieving its objectives.

This British Standard is intended for use by anyone with responsibility for, or involved in, any of the following:

a) ensuring an organization achieves its objectives;

b) ensuring risks are proactively managed in specific areas or activities;

c) overseeing risk management in an organization;

d) providing assurance about the effectiveness of an organization's risk management; and/or

e) reporting to stakeholders, e.g. through disclosures in annual financial statements, corporate governance reports and corporate social responsibility reports.

2 Terms and definitions

For the purposes of this British Standard the following terms and definitions apply.

2.1 board (or equivalent)
organization's governing body

NOTE This includes a board of directors, head of a legislative body or agency, supervisory board, or the board of trustees or governors of a not-for-profit organization.

2.2 business continuity management
holistic management process that identifies potential threats to an organization and the impacts to business operations that those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities

[BS 25999, modified]

2.3 communication and consultation
continual and iterative processes that an organization conducts to provide, share or obtain information, and to engage in dialogue with stakeholders regarding the management of risk

NOTE 1 The information can relate to the existence, nature, form, likelihood, significance, evaluation, acceptability and treatment of the management of risk.

NOTE 2 Consultation is a two-way process of informed communication between an organization and its stakeholders on an issue prior to making a decision or determining a direction on that issue. Consultation is:

- *a process which impacts on a decision through influence rather than power; and*
- *an input to decision-making, not joint decision-making.*

[ISO Guide 73]

2.4 consequence
outcome of an event (**2.6**) affecting objectives

NOTE 1 An event can lead to a range of consequences.

NOTE 2 A consequence can be certain or uncertain and can have positive or negative effects on objectives.

NOTE 3 Consequences can be expressed qualitatively or quantitatively.

NOTE 4 Initial consequences can escalate through knock-on effects.

[ISO Guide 73]

2.5 control
measure that is modifying risk

NOTE 1 Controls include any process, policy, device, practice, or other actions designed to modify risk.

NOTE 2 Controls may not always exert the intended or assumed modifying effect.

[ISO Guide 73]

2.6 event
occurrence or change of a particular set of circumstances

NOTE 1 An event can be one or more occurrences, and can have several causes.

NOTE 2 An event can consist of something not happening.

NOTE 3 An event can sometimes be referred to as an "incident" or "accident".

NOTE 4 An event without consequences can also be referred to as a "near miss", "incident", "near hit" or "close call".

[ISO Guide 73]

2.7 exposure
extent to which an organization and/or stakeholder is subject to an event

[ISO Guide 73]

2.8 external context
external environment in which the organization seeks to achieve its objectives

NOTE External context can include:

- *the cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;*
- *key drivers and trends having impact on the objectives of the organization; and*
- *relationships with, and perceptions and values of external stakeholders.*

[ISO Guide 73]

2.9 governance
system, structures, tone and behaviours by which the organization is directed and controlled, and accountabilities clearly assigned

NOTE Governance permits decisions to be effectively made, objectives set and performance monitored to ensure the efficient and effective use of resources and safeguard assets.

2.10 inherent risk
exposure arising from a specific risk before any action has been taken to manage it

2.11 instance of the risk management process
specific application of the risk management process described in the risk management framework to a specific, logical set of risks related to a particular area or activity of the organization

2.12 internal context
internal environment in which the organization seeks to achieve its objectives

NOTE Internal context can include:

- *governance, organizational structure, roles and accountabilities;*
- *policies, objectives, and the strategies that are in place to achieve them;*
- *the capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);*
- *information systems, information flows and decision-making processes (both formal and informal);*
- *relationships with, and perceptions and values of internal stakeholders;*
- *the organization's culture;*

- *standards, guidelines and models adopted by the organization; and*
- *form and extent of contractual relationships.*

[ISO Guide 73]

2.13 level of risk
magnitude of a risk or combination of risks, expressed in terms of the combination of consequences and their likelihood

[ISO Guide 73]

2.14 likelihood
chance of something happening

NOTE 1 In risk management terminology, the word "likelihood" is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically [such as a probability or a frequency over a given time period].

NOTE 2 The English term "likelihood" does not have a direct equivalent in some languages; instead, the equivalent of the term "probability" is often used. However, in English, "probability" is often narrowly interpreted as a mathematical term. Therefore, in risk management terminology, "likelihood" is used with the intent that it should have the same broad interpretation as the term "probability" has in many languages other than English.

[ISO Guide 73]

2.15 near miss
operational failure that did not result in a loss or give rise to an inadvertent gain

2.16 operational risk
risk of loss or gain, resulting from inadequate or failed internal processes, people and systems or from external events

2.17 programme risk
risk associated with transforming strategy into solutions via a collection of projects

2.18 project risk
risk relating to delivery of a product, service or change, usually within the constraints of time, cost and quality

2.19 residual risk
risk remaining after risk treatment

NOTE 1 Residual risk can contain unidentified risk.

NOTE 2 Residual risk can also be known as "retained risk".

[ISO Guide 73]

2.20 risk
effect of uncertainty on objectives

NOTE 1 An effect is a deviation from the expected – positive and/or negative.

NOTE 2 Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process).

[ISO Guide 73]

2.21 risk aggregation
combination of a number of risks into one risk to develop a more complete understanding of the overall risk

[ISO Guide 73]

2.22 risk analysis
process to comprehend the nature of risk and to determine the level of risk

NOTE 1 Risk analysis provides the basis for risk evaluation and decisions about risk treatment.

NOTE 2 Risk analysis includes risk estimation.

[ISO Guide 73]

2.23 risk appetite
amount and type of risk that an organization is willing to pursue or retain

[ISO Guide 73]

2.24 risk assessment
overall process of risk identification, risk analysis and risk evaluation

[ISO Guide 73]

2.25 risk avoidance
informed decision not to be involved in, or to withdraw from, an activity in order not to be exposed to a particular risk

NOTE Risk avoidance can be based on the result of risk evaluation and/or legal and regulatory obligations.

[ISO Guide 73]

2.26 risk criteria
terms of reference against which the significance of a risk is evaluated

NOTE 1 Risk criteria are based on organizational objectives, and external and internal context.

NOTE 2 Risk criteria can be derived from standards, laws, policies and other requirements.

[ISO Guide 73]

2.27 risk evaluation
process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable

NOTE Risk evaluation assists in the decision about risk treatment.

[ISO Guide 73]

2.28 risk financing
form of risk treatment involving contingent arrangements for the provision of funds to meet or modify the financial consequences should they occur

[ISO Guide 73]

2.29 risk identification
process of finding, recognizing and describing risks

NOTE 1 Risk identification involves the identification of risk sources, events, their causes and their potential consequences.

NOTE 2 Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and the stakeholders' needs.

[ISO Guide 73]

2.30 risk management
coordinated activities to direct and control an organization with regard to risk

[ISO Guide 73]

2.31 risk management framework
set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization

NOTE 1 The foundations include the policy, objectives, mandate and commitment to manage risk.

NOTE 2 The organizational arrangements include plans, relationships, accountabilities, resources, processes and activities.

NOTE 3 The risk management framework is embedded within the organization's overall strategic and operational policies and practices.

[ISO Guide 73]

2.32 risk management policy
statement of the overall intentions and direction of an organization related to risk management

[ISO Guide 73]

2.33 risk management process
systematic application of management policies, procedures and practices to the tasks of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk

[ISO Guide 73]

2.34 risk modification
measures taken to change the characteristics of risks in desired ways

2.35 risk owner
person or entity with the accountability and authority to manage a risk

[ISO Guide 73]

2.36 risk profile
description of any set of risks

NOTE The set of risks can contain those that relate to the whole organization, part of the organization, or as otherwise defined.

[ISO Guide 73]

2.37 risk register
record of information about identified risks

NOTE The term "risk log" is sometimes used instead of "risk register".

[ISO Guide 73]

2.38 risk reporting
form of communication intended to inform particular internal or external stakeholders by providing information regarding the current state of risk and its management

[ISO Guide 73]

2.39 risk response
acceptance of a risk or action taken to address it

2.40 risk retention
acceptance of the potential benefit of gain, or burden of loss, from a particular risk

NOTE 1 Risk retention includes the acceptance of residual risks.

NOTE 2 The level of risk retained can depend on risk criteria.

[ISO Guide 73]

2.41 risk sharing
form of risk treatment involving the agreed distribution of risk with other parties

NOTE 1 Legal or regulatory requirements can limit, prohibit or mandate risk sharing.

NOTE 2 Risk sharing can be carried out through insurance or other forms of contract.

NOTE 3 The extent to which risk is distributed can depend on the reliability and clarity of the sharing arrangements.

NOTE 4 Risk transfer is a form of risk sharing.

[ISO Guide 73]

2.42 risk source
element which alone or in combination has the intrinsic potential to give rise to risk

NOTE A risk source can be tangible or intangible.

[ISO Guide 73]

2.43 risk tolerance
organization's or stakeholder's readiness to bear the risk after risk treatment in order to achieve its objectives

NOTE Risk tolerance can be limited by legal or regulatory requirements.

[ISO Guide 73]

2.44 risk transfer
sharing with another party the burden of loss or benefit of gain for a risk

NOTE This might be achieved through legislation, contract, insurance or other means.

2.45 risk treatment
process to modify risk

NOTE 1 Risk treatment can involve:

- *avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;*
- *taking or increasing risk in order to pursue an opportunity;*

- *removing the risk source;*
- *changing the likelihood;*
- *changing the consequences;*
- *sharing the risk with another party or parties [including contracts and risk financing]; and*
- *retaining the risk by informed decision.*

NOTE 2 Risk treatments that deal with negative consequences are sometimes referred to as "risk mitigation", "risk elimination", "risk prevention" and "risk reduction".

NOTE 3 Risk treatment can create new risks or modify existing risks.

[ISO Guide 73]

2.46 stakeholder
person or organization that can affect, be affected by, or perceive themselves to be affected by decision or activity

NOTE A decision maker can be a stakeholder.

[ISO Guide 73]

2.47 strategic risk
risk concerned with where the organization wants to go, how it plans to get there, and how it can ensure survival

3 Framework

3.1 General

The organization should put in place a risk management framework. The components of its framework should support:

a) implementation and longer term development of risk management throughout the organization; and

b) ongoing management of one or more instances of its risk management process.

The extent to which the organization's risk management framework supports ongoing management of one or more instances of its risk management process should be tailored to its internal and external context (see Figure 2). In particular, a large organization, perhaps also with many projects, may find that multiple instances of its process are more appropriate than one large process (see Figure 3). Its framework should, therefore, include elements to maintain appropriate consistency between instances, initiate and terminate them when required (e.g. at the start of a new project or when a new business unit is created or acquired), and promote communication. These are not necessary for a small organization that expects to operate just one instance of its process.

EXAMPLE

Multiple instances of the risk management process might be needed because of outsourcing. A UK-based funds management organization executes thousands of funds transfers a day, having to ensure their timeliness, accuracy, probity and traceability. The processing work has been outsourced to India for some years and more recently the supervision of this has been outsourced to another company in the organization's home country. Consequently, risk management of this work is covered by four instances: 1) the enterprise-wide level, 2) in-house monitoring of funds transfers, 3) outsourced monitoring of funds transfers, and 4) the company in India that processes the transfers. Information flows up and down between these and the entire risk management effort is justified by the strategic importance of the identified risks.

Figure 2 **Relationships between the context, principles, framework and process**

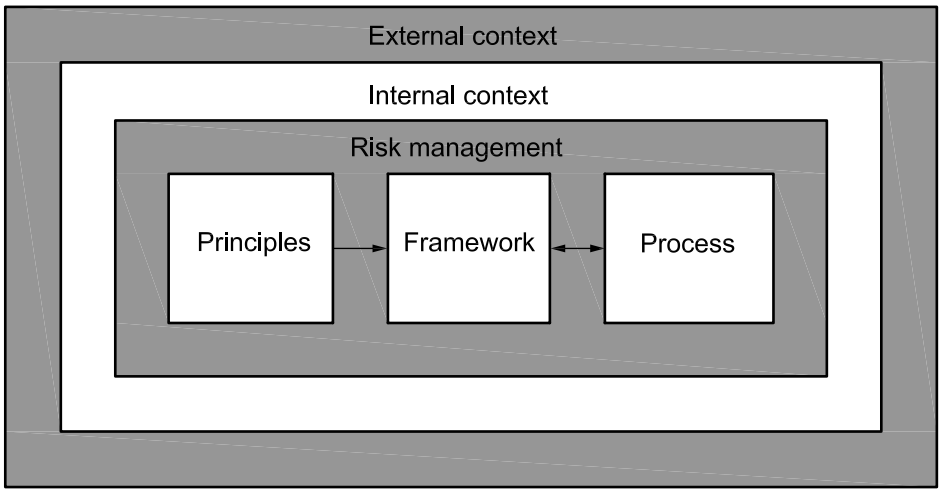
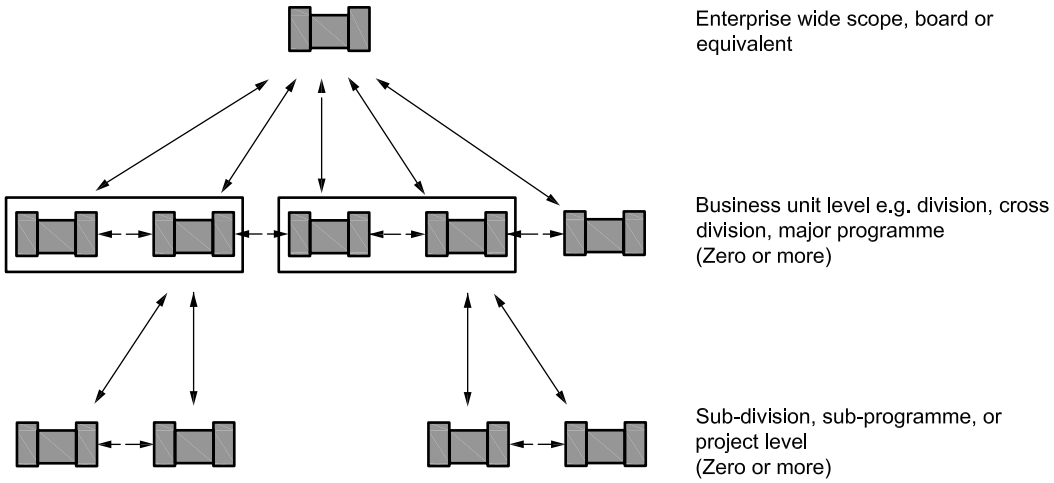


Figure 3 **Illustrative set of instances of the risk management process in a larger organization**



Key

Instance of the risk management process

In the same business unit

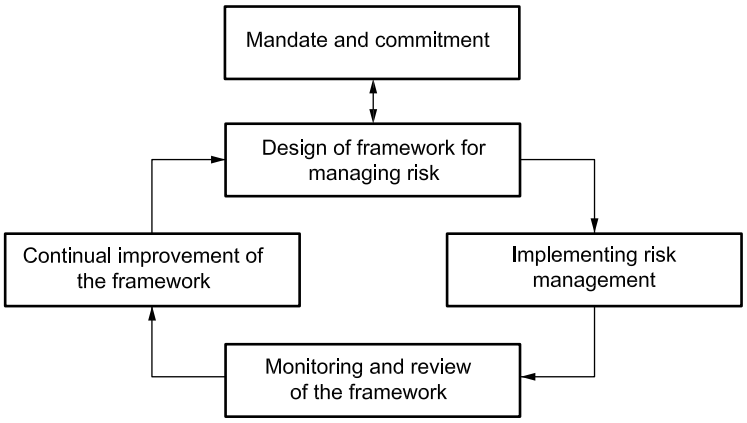
Sharing information, e.g. about risks and controls

Sharing information and command and control

When activities to develop risk management throughout the organization are first performed, the sequence of activities (see Figure 4) should be:

1) obtain mandate and commitment (see **3.2**);
2) design the risk management framework (see **3.3**);
3) implement risk management (see **3.4**); and
4) monitor and review (see **3.5**).

Figure 4 **Development of components of the risk management framework**



Key

Activity

Initial/main sequence of activities

Subsequently, these activities should be maintained, leading to continual improvement and adaptation, either through frequent small changes or less frequent larger changes, or a combination of both. Commitment and monitoring should be maintained over time, but refreshing the formal mandate for risk management and major reviews of progress may be periodic events.

Initial implementation of risk management can take some time to achieve. Subsequent small improvements may be implemented as they arise or redesign and reimplementation may be performed only periodically.

3.2 Mandate and commitment

The board (or equivalent) should require the development of a risk management policy and, as the framework is designed and implemented, the board (or equivalent) should approve the risk management policy and support its implementation.

The organization's mandate for, and commitment to, risk management should acknowledge that:

a) risk management is important to creating and protecting value;

b) risk management is part of the organization's governance and operational management;

c) the board is accountable for risk management;

d) the ultimate goal is to integrate risk management with all processes and activities.

3.3 Design of framework for managing risk

*NOTE This subclause covers activities to design the framework for managing risk (subclauses **3.3.1** to **3.3.3**) and gives recommendations for features of the framework design (subclauses **3.3.4** to **3.3.13**).*

3.3.1 Understanding the organization and its context

The organization should gain an understanding of the external and internal context of its risk management and aim to design a risk management framework that is appropriate.

Before designing the risk management framework, the organization should therefore:

a) consult with its stakeholders to understand their capabilities and expectations;

b) recognize constraints on the organization's capacity to deliver;

c) identify legal and regulatory obligations;

d) review its existing processes and understanding of risk management; and

e) consider ways to use existing experience and resources, such as by extending the use of tools and documentation already in use.

Before designing the way that risk management will be developed over time throughout the organization, the organization should also:

1) examine the other parts of the risk management framework to identify key competence requirements;

2) identify weaknesses in its existing risk management framework, including weaknesses in elements that might hinder development of other elements, such as:

   i) limited commitment and resources from the board (or equivalent);

ii) lack of clear roles and ownerships;

iii) failure to integrate risk management into other management activities; and

iv) those charged with implementing risk management having insufficient skills or an inadequate mandate; and

3) aim to meet a chosen level of capability in a way that is efficient for the organization.

3.3.2 Establishing risk management policy

The organization should develop:

a) objectives for risk management;

b) plans for embedding and maintaining risk management throughout the organization; and

c) plans for all other elements of the risk management framework.

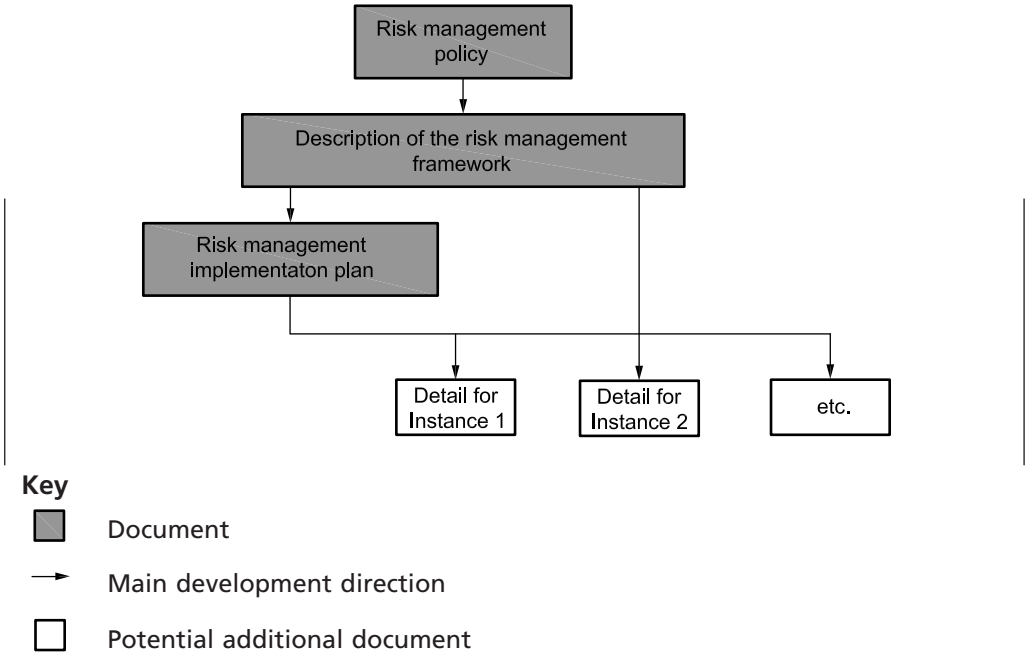
This should include documenting (see Figure 5):

1) the risk management policy, which is for approval by senior management and the board (or equivalent); and

2) the risk management framework, including plans for risk management processes, which is for guidance to everyone involved in risk management in the organization.

Small organizations should have the same elements in their documentation set as large organizations, but may create much shorter documents that reflect their size, simplicity and the lower number of instances of their risk management process.

Figure 5 **Typical documentation for risk management**



The risk management policy should be developed, documented, approved by senior management and the board (or equivalent), and communicated effectively.

The risk management policy may be brief, with the detail appearing in the framework design. It should set the direction, scope and objectives for risk management, and take into consideration the context, key stakeholders and the organization's existing risk management capability and maturity.

Depending on the organization's size and management style, the risk management policy may also include:

i) the risk management activities to be undertaken to meet the objectives, and the timeframes for these;

ii) the resources required, including people, knowledge and budget;

iii) risk criteria and other policies to control risk-taking and exposure;

iv) the chosen level of risk management capability;

v) specific activities to be taken to develop and embed risk management in the organization, and the timeframes for these; and

vi) how progress against the risk management policy will be monitored, reviewed, reported and communicated.

Approval for the risk criteria (see **3.3.12**) and any other risk policies to control risk-taking and exposure (see **3.3.13**) may be obtained either as part of approval of the risk management policy or as part of the approval of the strategy and implementation plans.

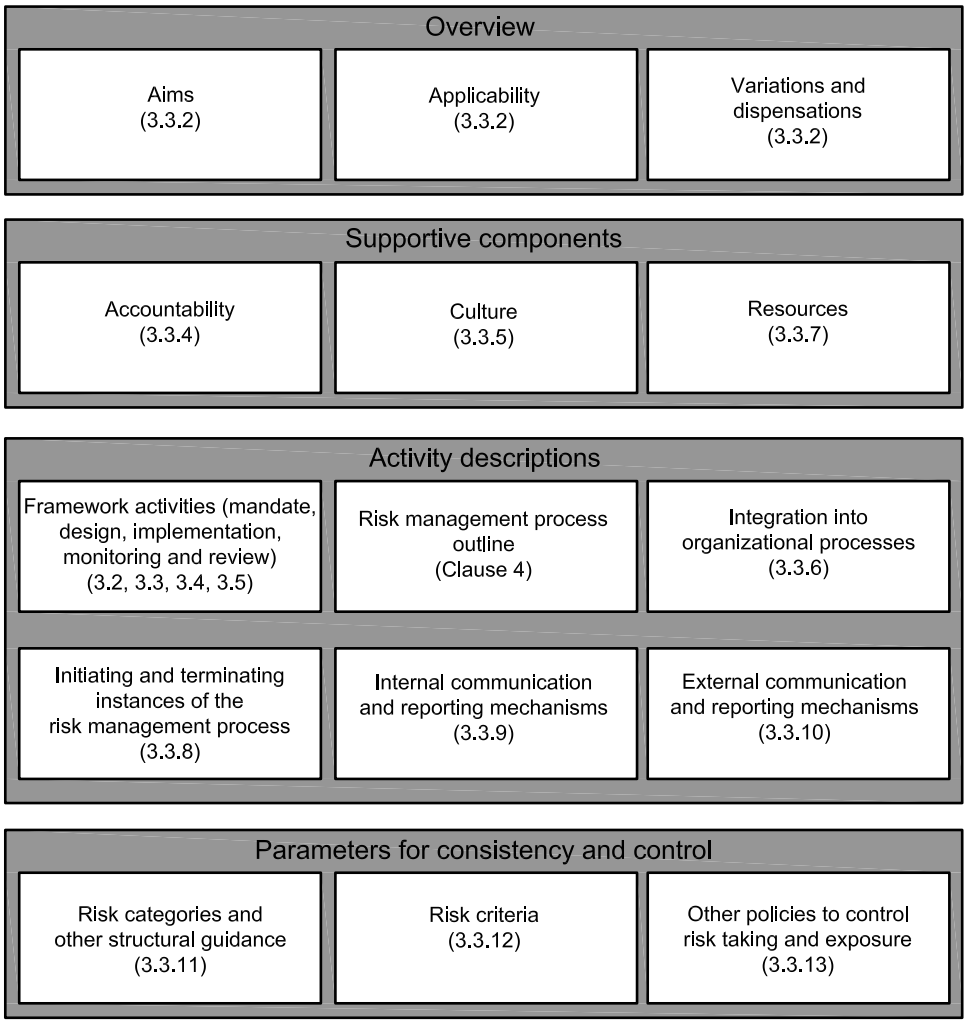
3.3.3 Documenting and communicating the framework

The design of the organization's risk management framework should be documented, agreed by appropriately senior management, and communicated effectively.

The documentation of the risk management framework should provide a clear and concise statement and explanation of the organization's requirements for risk management. The design of the risk management framework should make risk management an integral part of the organization's overall approach to governance.

The description of the risk management framework should be based on the topics shown in Figure 6.

Figure 6 **Items to include in the description of the framework**



The outline of the organization's risk management process should provide guidance that allows people to create an instance of the risk management process.

The description of the risk management process given in Clause **4** may be adopted for this purpose, but additional or alternative guidance consistent with Clause **4** may be used to, for example:

a) achieve greater consistency within the organization;

b) make use of particular tools; or

c) use language and concepts more familiar to people in the organization and suited to the interpretation of the process the organization wishes to encourage.

The design of the risk management framework should be:

1) owned by a manager, preferably at board (or equivalent) level;

2) developed in consultation with key stakeholders;

3) developed with consideration of how the organization will monitor adherence to the risk management policy and reference any relevant standards, regulations and policies that have to be included or taken into account; and

4) subject to quality assurance practices, e.g. document, change and version control.

3.3.4 Accountability

3.3.4.1 Identification

The organization's risk management framework should define and document roles in terms of responsibilities, authorities and accountabilities for risk management, and should allocate the roles to people and to groups (e.g. existing teams, committees).

This allocation should align with existing roles and responsibilities, and be documented in the description of the risk management framework and communicated through existing means of communicating roles (e.g. written job descriptions).

NOTE These roles do not have to be full-time appointments or assigned to different people, so this approach can be applied even to very small organizations.

All the work implied by the organization's framework and process should be included. The breakdown of roles shown in Table 2 may be used.

Table 2 **One possible breakdown of roles**

Role	Illustrative allocation in a large organization
Framework	
longer term development of risk management in the organization, including development and implementation of the risk management framework	a committee of the board (or equivalent) supported by a risk manager
overall coordination of instances of the risk management process	a committee of the board (or equivalent) supported by a risk manager with a team
providing independent assurance	internal audit and some external reviews
Process	
operating an instance of the risk management process	a committee of the board (or equivalent) operates at least one instance while other instances are operated by groups such as business unit management teams, project management teams and risk specialists
monitoring a particular risk and relevant controls (i.e. being a risk owner)	managers at a variety of levels (often people included in the group operating the relevant instance of the risk management process)
monitoring a particular control (i.e. being a control owner) • implementing a control • operating a control	people at a variety of levels, often people included in the group operating the relevant instance of the risk management process everyone is responsible for managing risk as it affects their jobs
providing information on the internal and external context, and on controls	everyone
providing independent assurance	internal audit and some external reviews

The allocation of roles should reflect the size and structure of the organization. Ultimate responsibility for risk management lies with the board (or equivalent), but this should be delegated appropriately. Table 2 illustrates possible allocations of roles in a large organization. In a smaller organization the extent of delegation will be correspondingly less. The roles that may be delegated most extensively are those for:

a) operating instances of the risk management process (except for those covering all risks across the whole organization);

b) implementing and operating controls; and

c) providing information.

The responsibilities in Table 3 should be retained by the board (or equivalent) or a committee of its members (perhaps acting as a risk oversight committee), and not delegated.

Table 3 **Leadership responsibilities**

1) Approve the risk management policy and take the lead on setting the tone and culture for managing risk and embedding risk management, not least by their own example.
2) Ensure there is an appropriate risk management framework and process in place and that risk management is adequately resourced.
3) Provide strategic direction on the appropriate consideration of risk in decisions and setting risk criteria and other policies to control risk-taking and exposure.
4) Operate an instance of the risk management process covering the whole organization and all types of risk.
5) Provide direction and receive assurance on the effectiveness of risk management and compliance with the risk management framework.
6) Report on risk management to stakeholders and sign off public disclosures related to risk and risk management.

Responsibility for risk management should be delegated so that everyone in the organization has some role in risk management, including at least those responsibilities shown in Table 4.

Table 4 **Minimum responsibilities for everyone in the organization**

1) Be aware of the risks that relate to their roles and their activities.
2) Continuously improve their management of risk.
3) Provide information to help operate the risk management framework and process, such as information that helps to identify risks and assess controls.
4) Implement controls, or support the implementation of controls, as part of their day-to-day duties.
5) Report ineffective and/or inefficient controls.

3.3.4.2 Risk and control owners

All risks and controls should be allocated owners as part of the risk management process.

The owner of a risk should own the organization's assessment of the risk, monitor it, and report its status. The owner of a control should respond to the risk, contribute to the development and maintenance of the control, and report its status. Risks and their related controls may be owned by the same person.

3.3.4.3 Risk management manager or team

The organization may, depending on its size and complexity, have a dedicated manager or risk management department to support its risk management. The role of the risk manager and/or risk management function may include the items shown in Table 5.

Table 5 **Role of a risk management function**

1) Develop, implement and review the risk management framework and process.
2) Promote effective risk management at all levels of the organization.
3) Encourage an appropriate risk culture and develop resources for risk management within the organization, for example, by providing education and training.
4) Coordinate other functions that advise on specific aspects of risk management.
5) Coordinate responses where risks impact more than one area, e.g. security, business continuity, communications, health and safety and supply chain security.
6) Report, escalate and communicate risk management issues to key stakeholders.
7) Provide assurance regarding risk management within the organization.

3.3.4.4 Internal audit

If the organization has an internal audit function, this may provide independent assurance on:

a) the design, operation and effectiveness of the risk management framework and instances of the process;

b) management of key risks, including the effectiveness of the controls;

c) reporting of risk and control status; and

d) the reliability of assurances provided by management relating to risk management.

The organization's risk and internal audit functions may operate independently. They should share information and coordinate their activities. The information shared may include:

1) each function's annual activity plans;

2) key risks;

3) methods of managing risks effectively;

4) key control issues;

5) output from risk management process activity and audits; and

6) reporting and management information.

3.3.5 Risk management culture

The risk management framework should incorporate the means to shape an effective risk management culture that encourages and motivates people to:

a) give appropriate attention and resources to achieve risk management objectives;

b) comply with the intent and details of risk management policies and procedures;

c) solve practical difficulties in implementing risk management policies and procedures, and do so in a way that is consistent with good risk management principles;

d) manage risk in ways that go beyond compliance with formal policies and procedures; and

e) communicate about risk openly and appropriately.

EXAMPLE

A medium sized investment bank managed risk very effectively with just a few full-time risk management staff. This was possible because employees felt rather like members of a family, were proud of their company and each other, and normal human mistakes were tolerated. This made it easier for people to admit to mistakes, weaknesses and risks. This openness was seen as everyday good practice within the company, part of improving service to clients and increasing revenue.

Features of culture that may be considered include the following helpful features.

1) Focus on thinking widely about the future and what is uncertain, rather than focusing only on what could go wrong or what is already understood.

2) Emphasis on using risk management to help the organization do difficult things rather than create obstacles.

3) Low power distance (i.e. differences in organizational status should not imply important differences in social status).

4) Low collectivism (i.e. the desire for consensus should not lead to lack of clear responsibility for action).

5) Long-term thinking and the avoidance of short-termism.

6) Limited emphasis on targets and also avoidance of thresholds linked to powerful incentives, such as large financial rewards or job loss.

7) Avoidance of blaming.

8) Pursuit of objectivity and lack of bias, avoiding baseless optimism and positive thinking.

9) Attention to evidence.

10) Participation and sharing of information generally.

11) Acceptance of formality.

The arrangements in the framework should allow the organization to monitor and develop its risk management culture through, for example:

i) monitoring attitudes to risk management;

ii) demonstrating effective risk management leadership at senior levels as an example to others (which can often be the main method in smaller organizations);

iii) monitoring and communicating the value added by risk management, either proven by measurement over time, or anticipated when an acknowledged improvement to a plan or process is made as a result of risk management;

iv) providing education and training in risk management, including practical examples;

v) including risk management within individual objectives and performance appraisals;

vi) integrating risk management into organizational processes (see **3.3.6**); and

vii) continually maintaining and improving risk management.

3.3.6 Integration into organizational processes

The risk management framework should be designed to integrate risk management with other activities in the organization through:

a) controls that are well integrated into the organization's processes, systems, tools, skills, etc.; and

b) integration of other activities that are part of the risk management framework and process with other management activities, including those for managing performance by:

1) establishing objectives and strategies;

2) forecasting;

3) planning, including annual planning and planning of investment; and

4) appraising individual and team performance and deciding rewards.

Features of risk management that contribute to integration include:

i) teams for risk management being the same as, or similar to, those for other management activities;

ii) risk management being covered in meetings at the same time as other management matters;

iii) management information reports including risk-related information, rather than all risk reporting being separate from other reporting;

iv) risk analysis and reporting providing analyses of risks that are the risks involved in decision-making, including strategic decisions;

v) risk analysis supporting the development of objectives and strategies as well as helping to achieve objectives and strengthen strategies;

vi) risk information being used in general management meetings; and

vii) where any risk management activities are separate from other management activities, the schedules are coordinated so that outputs from risk management are available at the right time.

EXAMPLE

In a large company that delivers hundreds of capital projects, project risk management has been integrated with project management and with the process by which funding for projects is approved. Guidance on risk management is woven in with other requirements in the project management framework guidance, instead of being in a separate section or document. At funding gateway meetings, where decisions to fund projects are made, risk information has to be included along with other information. The risk information is provided in a standard format from a database of risks and has to be aligned with risk funds shown in the accounting system.

3.3.7 Resources

3.3.7.1 General

The risk management framework should identify the resources of all kinds to be applied to:

a) develop risk management over time; and

b) manage instances of the risk management process.

The risk management framework may identify the resources to be applied to operate instances of the risk management process already in place or planned.

The framework may also provide estimated resource requirements for:

1) operating additional instances of the risk management process (e.g. for projects not yet planned); and/or

2) implementing and operating risk responses.

3.3.7.2 Tools

The framework should provide tools (e.g. techniques, templates, software, documents) that help people manage risk. These tools should fit the organization's framework and process, and its maturity.

The organization should communicate information about the tools to those who ought to use them, with guidance on where to get the tools and who to contact for further assistance.

NOTE Annex A provides examples of risk management tools, linked to the part(s) of the risk management process to which they relate, and gives guidance on the selection of tools.

3.3.7.3 Competence

The framework should include arrangements to ensure that any person performing risk management tasks is competent to do so, on the basis of appropriate education, training or experience.

To build the capability needed to embed risk management throughout the organization and develop risk management maturity, the framework should provide relevant people with appropriate experience, skills and knowledge covering the items listed in Table 6.

Table 6 **Items to cover related to risk management competence**

1) Current corporate governance requirements and their source.
2) The legislative and compliance context of the organization's risk management.
3) The organization's risk management framework and process, including:
   a) roles, accountabilities and responsibilities (see **3.3.4**);
   b) how to identify, assess and manage risks;
   c) the organization's risk criteria and other policies to control risk-taking and exposure;
   d) risk tools and how and where they are applied;
   e) risk reporting requirements.
4) Statements on controls.
5) Where the organization's risk management capability stands (its risk management maturity).
6) An assessment of performance as part of the organization's overall appraisal system.

3.3.8 Initiating and terminating instances of the risk management process

3.3.8.1 General

Risks should be managed through one or more instances of the risk management process outlined in the framework, each tailored to fit its context but consistent with the others. The framework should include rules that govern what instances will be operated.

The design of the risk management framework should also include appropriate arrangements for:

a) initiating new instances of the risk management process;

b) revising the terms of reference of existing instances of the risk management process; and

c) terminating instances of the risk management process.

In a small organization expecting to operate only one instance of its risk management process, these arrangements may be very simple, providing enough guidance to start and modify that instance. In a large organization with many projects the arrangements should be more fully developed.

These arrangements should be designed to ensure that:

1) responsibility for initiating, revising or terminating each instance is clearly allocated;

2) there is always at least one instance whose scope covers all risks across the whole organization, and that those responsible for operating that instance are appropriately senior;

3) the number and scope of instances remains appropriate to the context of the organization, including its governance, structure, size and complexity; and

4) instances operate effectively together.

EXAMPLE

A multinational conglomerate with an effective, but aggressive, acquisition, restructuring and disposals strategy puts its success in this area down to a strong focus on the initiation, evolution and termination of instances of its "risks and opportunities" regime. This starts with an instance of its risk management process being a workstream within its acquisition and due diligence projects. Once a company is acquired this instance of the risk management is turned into one that addresses the risks in the various stages of transforming the business, to bring forward the time at which most benefit from the acquisition is gained.

Once the transformation is complete the project is terminated along with its instance of the risk management process, and information from it is fed into operational and strategic direction activities. On disposal, an instance of the risk management process is initiated to maximize value from the disposal. Their process for initiating new instances clearly communicates the scope, objectives and considerations for each instance.

3.3.8.2 Initiating instances of the risk management process

The approach to initiating new instances of the risk management process should be designed to ensure that:

a) new instances are created promptly when trigger events happen (i.e. events mentioned in the rules [see **3.3.8.1**] for what instances will be operated, such as the creation of a new organizational unit, the start of a project, or a regulatory change);

b) those operating new instances are given clear terms of reference covering the scope of risks they should consider, the nature of the team and any special resources allocated;

c) those operating new instances have the ability to carry out the instance, including the required resources and knowledge of the risk management process; and

d) new instances are included in internal and external reporting to the appropriate extent.

Instances of the risk management process may differ as to the types of risk within their scope, the parts of the organization whose risks are included, and the people operating them.

To help integrate risk management into other management activities, those operating instances of the risk management process may be existing line management or project management teams. Alternatively, committees may be formed specifically to gain a perspective that is not provided by existing management teams.

3.3.8.3 Terminating instances of the risk management process

The approach to terminating instances of the risk management process should be designed to ensure that:

a) instances are terminated promptly when trigger events happen [see **3.3.8.2**a)];

b) termination of an instance does not lead to an unintended gap in risk management and specific risks identified by the instance are covered by another instance or do not need to be; and

c) any tools of instances terminated are reviewed to see if they should be reused elsewhere.

3.3.9 Establishing internal communication and reporting mechanisms

The risk management framework should include arrangements for communication (including formal reporting) about risk management. These should support:

a) operation of each instance of the risk management process;

b) ongoing management of one or more instances of the risk management process (including, where appropriate: initiating, revising and terminating instances of the process; monitoring; and communication between instances of the process); and

c) development of risk management capability, including implementation of the risk management framework itself.

Communication, whether or not as formal reporting, should encompass all roles involved in risk management (see **3.3.4**) and all relevant information.

The organization's internal reporting should be aligned with its governance structure and allow the flow of risk information through the organization. Reporting about risk should be integrated with other internal reporting for efficiency and integration with other management activities.

The organization should identify the specific risk information, and its level of detail and frequency, that allows those involved to fulfil their roles. The structure and process for internal reporting should be documented, and a timetable developed detailing responsibilities and timescales.

3.3.10 Establishing external communication and reporting mechanisms

The organization's framework should include arrangements for external communication and reporting mechanisms that support:

a) consultation with appropriate external stakeholders; and

b) reporting on the current risk profile, ongoing risk management performance, and development of risk management over time.

The organization's external risk reporting should be:

1) based upon an understanding of the stakeholders' needs, priorities and time scales, and aligned to their responsibilities;

2) timely, concise, specific and reliable;

3) sufficiently detailed that the stakeholders can gain an appropriate understanding of the key issues;

4) integrated with other reporting processes where practical and appropriate;

5) delivered in time to let recipients adequately review the content; and

6) independently reviewed periodically to validate its quality and ensure it is aligned to its stakeholders.

3.3.11 Risk categories and other structural guidance

The organization's framework should include a system of risk categories and/or other structural guidance for risk analysis that suits its context, aligns with its risk management process and tools, and is appropriate for the maturity of its risk management.

NOTE 1 Grouping similar risks in risk categories and/or applying guidelines for structuring models helps to:

a) organize risk identification and promote comprehensive coverage; and

b) identify similar risks appearing in risk analyses by different organizational units.

NOTE 2 Risk categories and other structural guidance can be seen as parameters of the risk management process that can be varied while its procedures stay the same.

Where there are multiple instances of the risk management process, risk categories and/or other structural guidance should be designed to promote consistency between risk analyses in different instances.

Risk categories and other structural guidance may also be used to improve alignment with other management activities by ensuring that risk analyses provide assessments for the risks that are considered in decision-making, such as in annual business planning, mergers and acquisitions, or software development projects.

NOTE 3 While risk categories differ between organizations, risk categories in common use include:

a) strategic risk;

b) programme risk;

c) project risk;

d) financial risk;

e) safety risk;

f) compliance risk; and

g) operational risk.

The choice of risk categories can be influenced by legal and regulatory requirements or sector practice.

Other structural guidance can, for example, guide model structures and the structure of individual risk definitions.

3.3.12 Risk criteria

3.3.12.1 General

To enable risks to be assessed consistently the framework should include appropriate risk criteria that guide people in deciding the significance of each risk based on its possible effects and their likelihoods.

NOTE These criteria are another important parameter of the risk management process and allow overall direction as to the extent to which controls are evaluated as necessary or worthwhile.

3.3.12.2 Characteristics of effective risk criteria

Risk criteria should be designed to help people choose the control changes to implement by considering:

a) the possible net benefits from changing risks compared with the cost of implementing and operating the controls;

b) the relative cost-benefit of different control changes considered; and

c) any legal or regulatory requirements or social responsibility factors that might override a cost-benefit analysis and necessitate a specific control change.

NOTE 1 Analysis of costs and benefits need not be purely in financial terms or be fully quantified.

Risk criteria should state the following.

1) The consequences to be considered in judging the importance of risks (such as lives lost, financial gain or loss, legal penalties or awards, reputation effects and environmental impact). This should include guidelines for deciding the time periods over which consequences are to be considered.

2) Measures of the level of risk, taking into account the likelihoods of different levels of the consequences. These should combine the different consequences and simplify distributions of effects into a level of risk. They should include guidelines for deciding which expectations to use in assessing the effects of risks.

3) The importance of different levels of risk, for use in decision-making. This may be demonstrated using thresholds that determine when action has to be taken to manage risk, and/or by defining scales of importance linked to level of risk.

Once instances of the risk management process have begun to operate and risks have been identified and considered, additional risk criteria may be developed that apply to particular risks or sets of risks considered together. These criteria should identify the risks involved and the instances of the risk management process where those risks have been identified.

The organization's risk criteria should allow for all risks to be measured, including those that do not naturally lend themselves to numerical analysis.

Measures of risk should adequately reflect the realistic possibility of unusual levels of consequences, not just typical or average levels.

Where thresholds are applied to risks they should be appropriate to each risk so that, if a risk is split into components or some risks are pooled into one, the decisions resulting from applying the risk criteria are not unduly changed.

Risk criteria should take into account combinations of multiple risks if decisions involving multiple risks are to be taken (e.g. where multiple risks affect a strategic decision or are addressed by the same control, and where the combined effect of multiple risks is to be compared with some risk limit).

*NOTE 2 Risk criteria that take into account combinations of multiple risks (as mentioned in BS ISO 31000:2009, **5.3.5**) are usually required.*

Where risk criteria take into account combinations of multiple risks they should:

i) identify in principle, or enumerate, the sets of risks the criteria are applicable to; and

ii) take into account the effect of dependencies between risks in a combination.

NOTE 3 Dependencies usually mean that the level of risk for a set of risks is not equal to the sum of the level of risk for each risk individually.

EXAMPLE 1

In financial services companies, risk-adjusted performance measures have become increasingly common risk criteria. These express results such as profit in a way that is adjusted to reflect the risks run by engaging in different business activities. The most common technique is risk-adjusted return on capital (RAROC). The risk adjustments mean that risk is considered in decisions such as how to judge the performance of different business units and products, and how to allocate capital between them.

EXAMPLE 2

One approach to choosing healthcare interventions and allocating resources is to express consequences in terms of quality-adjusted life years (QALY). These represent the number of extra years of life provided by a treatment, adjusted if that life is lived in less than perfect health (e.g. because of pain or loss of mobility). The QALY impact of alternative treatments can be estimated over possible outcomes, taking into account their likelihood, and may be expressed in terms of cost per QALY.

3.3.12.3 Approach to developing risk criteria

The approach taken to developing risk criteria should ensure that the interests of legitimate stakeholders are fairly reflected in accordance with the organization's governance arrangements.

Factors that may be taken into consideration when determining the importance of different levels of risk include:

a) the potential for particular levels of consequences to cause or contribute to a serious outcome, such as commercial ruin or loss of life, or to lead to dramatic benefits, such as winning an important competition;

b) the organization's resources and reserves, now and in future, and the variability of those resources;

c) the organization's financial flexibility;

d) the organization's ability to withstand or exploit risk occurrences efficiently, which is influenced by its commitments, management style and other factors;

e) the greater opportunity to prepare for outcomes anticipated with certainty, and reduced cost arising from not preparing for outcomes that do not occur; and

f) the interests of stakeholders, including external stakeholders where relevant.

Where criteria are applied to particular risks or sets of risks, the likely cost and effectiveness of potential controls should also be considered.

To integrate risk management with other management activities, and to link risk-taking with rewards, decisions on risk criteria may be made in conjunction with other planning decisions, such as those on revenue and growth targets, and budgets.

The risk criteria may be interpreted and developed in detail when the risk management process is applied.

3.3.13 Other policies to control risk-taking and exposure

In addition to providing guidance on risk criteria, the risk management framework may provide further rules that constrain decision-making on risk-taking and exposure, and that are applicable to the whole organization.

These may be set and stated separately from risk criteria, or with them.

NOTE 1 Statements of rules on risk-taking and exposure are sometimes called "risk appetite statements" and often include risk criteria in addition to rules that go beyond risk criteria by using measures that are not risk measures (e.g. level of investment), requiring a wider range of actions (e.g. escalation of decisions) and applying to decisions outside instances of the risk management process,

NOTE 2 Such statements, and their implementation, may also be regarded as controls.

Similar to risk criteria, these further policies may include rules that:

a) prescribe approaches to taking particular decisions and to taking risk into consideration; and

b) provide values for decision-making parameters such as limits, weights or thresholds for escalation of decisions, defined using:

   1) levels of particular risks or sets of risks; and/or

   2) levels of other measures related to risk, such as indicators of inherent risk, indicators of the operation or performance of controls and actual results achieved by the organization.

These rules should clearly specify when they are to be applied (the circumstances or times) and what they require, such as escalation of decisions, consideration of factors, weighting of risks, or adaptation of controls. Where a statement concerns a quantity then that quantity should be clearly defined and helpfully named.

Where rules apply to particular risks or sets of risks, the rules should identify both the risks and the instance(s) of the risk management process whose risk analysis contains them.

The rules should recognize that higher-than-expected risk in some areas can be compensated for by lower than expected risk in others.

The organization may monitor a wide range of indicators related to risk for which there are no such rules.

Application of these rules should be integrated into management activities, including the risk management process and risk management framework.

3.4 Implementing risk management

3.4.1 Implementing the framework for managing risk

A risk management implementation plan should be prepared and carried out, and progress in implementing changes should be monitored.

The risk management implementation plan should allocate owners to the actions planned to embed and maintain risk management throughout the organization and provide a schedule for their implementation. The schedule, including frequency of reviews, should be appropriate for the context of the organization, including its size and level of risk management maturity. The plan should include communication to each person in the organization, covering the content of the risk management framework that is relevant to them.

The risk management framework and risk management implementation plan should be revised appropriately in light of what is learned during implementation. Methods and tools may be trialled to accelerate improvement.

Depending on the context, the information in the risk management implementation plan may also include:

a) objectives and strategy;

b) budget for risk management activities;

c) risk management performance indicators;

d) background of individuals, particularly for a new team; and

e) references to supporting information such as templates and techniques.

A large or medium sized organization may have one or more sub-plans for different levels, such as organizational unit, programme, project and different risk functions such as financial and operational risk.

The risk management implementation plan may be integrated into other organizational plans.

3.4.2 Implementing the risk management process

The risk management implementation plan should also cover implementation of the risk management process.

The risk management process (or any revision to it) should be implemented mainly using the processes in the risk management framework for initiating, revising and terminating instances of the risk management process (see **3.3.8**). However, where this implies a lot of change, as when introducing formal risk management for the first time, additional activities may be planned to ensure success.

3.5 Monitoring and review of the framework

3.5.1 General

The organization should ensure that changes to the context or other factors affecting the suitability or cost of risk management, are identified and addressed.

Monitoring should identify where the set of instances of the risk management process currently operating is inconsistent with the risk management framework. In particular, it should identify missing instances and instances with the wrong scope and ensure that problems are promptly resolved.

A review process should be undertaken, as a minimum annually, to determine whether:

a) the framework and processes are fit-for-purpose and aligned to the objectives and priorities of the organization;

b) the framework and processes adopted are operating as planned;

c) risks are being managed in accordance with the risk criteria and other policies to control risk-taking and exposure;

d) relevant stakeholders are receiving sufficient reporting to enable them to discharge their roles and responsibilities in the governance structure;

e) people across the organization have sufficient risk management skills, knowledge and competence to carry out any risk role, or risk element of a role, they are required to perform on a daily basis;

f) the risk management resources are adequate;

g) lessons have been learned from actual outcomes, including losses, near misses and opportunities that were identified in advance, occurred and yet were not acted on; and

h) overall current risk management maturity and capability achieve the objectives set out in its risk management policy.

More frequent reviews may be performed during periods of rapid change to the risk management framework, the organization or its environment, and where the risks being managed are themselves volatile and/or severe.

NOTE The review may take a variety of forms, and range from self-assessment and internal audit to detailed reviews by independent external experts.

3.5.2 Learning from outcomes

The organization should learn from actual outcomes, including those captured within risk analyses and those that perhaps ought to have been. These should include losses, near misses, and opportunities that were identified in advance, occurred, and yet were not acted on.

Individually significant outcomes should be reviewed promptly to identify relevant mechanisms. Points that may be considered in such a review include:

a) what happened;

b) how and why the risk occurrence came about;

c) what action has been taken (if any) in response;

d) the likelihood of the risk occurrence happening again;

e) any additional responses or steps to be taken; and

f) key learning points and who they need to be communicated to.

Outcomes that were significant collectively, where consequences were insignificant but might not be in future, or that could point to important trends, should also be reviewed. This may be carried out in a statistical way.

This may involve implementing suitable reporting and recording procedures, and a database.

In addition, the organization should consider readily available information about relevant outcomes of other organizations (e.g. industry peers) and the controls they have used.

3.5.3 Risk management development reporting

The organization might be required, or may decide, to report to applicable stakeholders, setting out its risk management policy and framework, and their effectiveness.

The organization should understand specific external risk reporting obligations, time scales and requirements, which can cover:

a) the organization's risk management framework, including management responsibilities for risk management;

b) the key risks and the primary control systems in place to manage these;

c) the monitoring and review of control systems in place; and

d) any major deficiencies uncovered and the steps taken to deal with them.

3.6 Continual improvement of the framework

The organization should continue to improve the effectiveness of its risk management framework through, for example:

a) a review process (see **3.5**).

b) learning from risk outcomes and the application of controls; and

c) internal audit (if an internal audit function is present).

Lessons learned should be applied to adapt and improve components of the risk management framework through continuing with the activities described in **3.2** to **3.5**.

4 Process

4.1 General

Each instance of the risk management process should provide a systematic, effective and efficient way by which risks can be managed. It should be consistent with the risk management process (see Figure 7) outlined in the risk management framework, but should be tailored to the context in which it is to operate. Each instance should be:

a) an ongoing undertaking by a group of people within the organization as an integral part of their decision-making; and

b) operated using the parameters set out by the risk management framework (e.g. risk criteria, risk categories).

The organization's risk management process should, as a minimum, comprise the following activities:

1) communication and consultation (see **4.2**);

2) establishing the context (see **4.3**);

3) risk assessment (see **4.4**);

4) risk treatment (see **4.5**); and

5) monitoring and review (see **4.6**).

When the activities of the risk management process are carried out for the first time the sequence of activities should be: 1) establish the context, 2) assess risks and 3) treat risks. Communication, consultation, monitoring and review should occur throughout.

Subsequently, the activities should continue so that risks are reassessed and risk treatment is revised at appropriate times. This may be in response to new information or new insights about risk, or new ideas for risk responses, and may also be carried out regularly to draw in new information and generate insights and new ideas. The context may also be re-established in response to events, and regularly, but need not be on the same schedule as risk assessment and treatment.

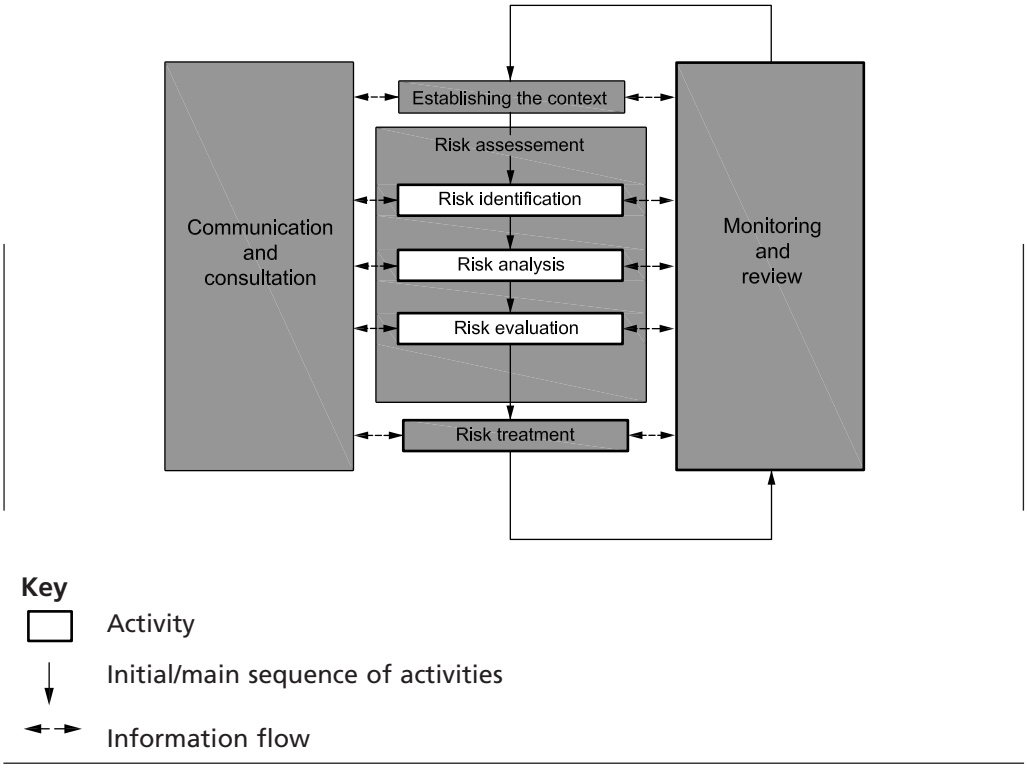
The main direction of inferences should be from risk assessment to risk treatment, but ideas on risk treatment should also influence risk assessment because they are one of the reasons for grouping or aggregating risks (see **4.4.2**).

NOTE 1 As skill in applying the risk management process increases it can become easier to apply it responsively and to cope with inter-related risks and decisions.

NOTE 2 There are many tools for presenting and communicating the results of risk management; examples can be found in Annex A.

The scheduling of these activities should be designed to help integrate them with other management activities.

Figure 7 **The risk management process**



4.2 Communication and consultation

Communication and consultation should take place when an instance of the risk management process is being designed and when particular risks are being managed.

The extent of consultation, particularly with external stakeholders, should be proportionate. Consultation should focus on those stakeholders and matters that are important, within the constraints of any requirements for confidentiality.

Plans for communication and consultation may cover individual risks, groups of risks, or all risks covered by the instance of the risk management process. More detail may be added for particular risks once they have been identified and evaluated as important, or once their proposed treatment has emerged as costly or requiring more discussion.

4.3 Establishing the context

Those involved in an instance should gain an understanding of the internal and external context and create an interpretation of the risk management process that fits them.

Each instance of the risk management process should be aligned with other management activities through its schedule, team composition, risk analysis, reporting channels, and other details.

Those involved in an instance should:

a) consider the terms of reference provided for their instance of the risk management process, including its team composition, organizational scope and types of risk to be covered;

b) confirm the scope and ground rules for the risk management process;

c) review the relevant elements of the risk management framework, including the description of the risk management process, risk communication mechanisms, risk categories and other structural guidance, and risk criteria;

d) consider the external context and other aspects of the internal context, including relevant objectives and strategies;

e) select appropriate procedures, tools and techniques, and a schedule for the instance of the risk management process;

f) define the risk criteria, either accepting or interpreting those defined by the risk management framework;

g) involve appropriate people at each stage; and

h) establish relevant documentation.

These decisions should be reviewed over time as the context changes and more is learned about the nature of the risks to be managed.

4.4 Risk assessment

4.4.1 General

Risks should be assessed to determine the level of risk and provide input to decisions on where responses to reduce or exploit risk are necessary or likely to be worthwhile.

The scope of risk assessment should include revising views of risks previously identified and identifying new (perhaps emerging) risks. This may involve replacing some risks with new ones that better describe the total risk faced.

The risk assessment activity should involve:

a) risk identification;

b) risk analysis; and

c) risk evaluation.

4.4.2 Risk identification

Risk identification should be carried out to develop a set of well-defined risks.

Risk identification should aim to include all risk, but not necessarily enumerate individually every possible outcome or every stage of every possible sequence of cause and effect.

Risk identification should be approached methodically and iteratively so that it is thorough, efficient and, wherever possible, has the features listed in Table 7.

Table 7 **Features of risk identification**

1) The full scope of the instance of the risk management process is explored.
2) All significant risk sources potentially affecting the achievement of objectives are identified and considered, including conflicts between stakeholders or objectives, which can be a significant source of risk, and dependencies on other business areas.
3) The results of early iterations of risk assessment guide later iterations, so that the analysis continues to identify important risks.
4) Risks are clearly defined and there are no unintended gaps or overlaps.
5) Good and bad consequences are addressed as appropriate (see Annex B).
6) Each risk's causes and effects are examined.
7) Assumptions are challenged.
8) The risks are given owners.
9) Existing risk responses perceived to be addressing the risks, and the owners of these responses, are identified.

The process of identifying risks should be iterative and one of refining the output until it is appropriate and at least adequately reflects the risks without being excessively detailed.

The initial set of risks should be reviewed and revised to take account of situations where links between risks or common risk responses suggest that risks could be split or aggregated, or considered in groups. Risks that are interlinked may be aggregated or considered together, while risks that contain independent elements may be split up. Also, risks that are addressed by a common response may be aggregated or grouped, while risks that have elements addressed by separate responses may be split.

Rapid checks should be made as the identification process progresses to ensure that it remains relevant and that risks are adequately recorded.

Models of various kinds, ranging from conceptual diagrams to computer simulations, may be used to help structure risk identification, examine chains of cause and effect including inter-relationships between risks, and understand cumulative effects.

Risks should be recorded consistently and explicitly to allow review and development of effective responses.

4.4.3 Risk analysis

Risk analysis should be carried out to develop an understanding of the risks and assign a risk level to each one. Confidence in the assessment of the level of risk should be considered and communicated.

NOTE 1 A risk can have a number of consequences, some positive and some negative, some uncertain, and some positive or negative depending on what actions are taken to manage the risk.

Risk analysis should be performed in accordance with the risk criteria. Analysis may be qualitative or quantitative, or a combination of these provided it is consistent with the risk criteria.

Risk analysis may be undertaken to varying degrees of detail depending upon the risk, the purpose of the analysis, and the information and resources available. Each risk should be analysed to an appropriate extent, considering its consequences, and summarized in terms of the consequences arising and their likelihood.

Risk analysis should be iterative, being repeated as more information becomes available. It should take account of the controls in place. Inherent risk may also be considered.

NOTE 2 An understanding of inherent risk can help ensure that responses are proportionate to the overall exposures. It can also help the organization understand what its full exposure could be if controls fail, and thereby recognize the contribution of certain controls to overall risk modification.

Residual risk reflects inherent risk and the effect of all relevant controls, but residual risk levels may be estimated directly from evidence of past risk occurrence. If residual risk is estimated by considering inherent risk and the effect of controls, then controls should be ascertained, documented, and mapped to risks to clarify the residual risk currently being retained, and documentation that supports this many-to-many mapping should be used.

To allow appropriate methods of analysis to be applied to each risk, the documentation should support the methods used.

Confidence in the level of risk may be communicated in a variety of ways, depending on circumstances. They may range from explicit statements of statistical confidence to statements about the type of evidence used or the source of the information. Understanding the information used to determine the level of risk can lead to decisions to get more information.

4.4.4 Risk evaluation

Those managing risk should apply the risk criteria to establish the importance of acting on the risks, taking into account their level of risk, proximity (how soon the risks might materialize) and manageability.

This should take account of the context of the risks and the views of stakeholders.

The risk evaluation process should compile/calculate risk profiles by appropriately combining/aggregating analysed risks and applying the risk criteria.

4.5 Risk treatment

4.5.1 General

Risk treatment options (i.e. ideas for actions to change controls) should be developed, selected and implemented to adapt and/or improve the existing set of controls (if any).

This may be achieved by designing a revised set of controls to have in place and then working out the risk treatments that will change the existing set of controls to this revised set.

4.5.2 Selection of risk treatment options

4.5.2.1 Developing ideas for changes to risk responses

At each iteration of the risk management process, ideas for changes to controls (adaptations or improvements) relevant to the risks being considered should be developed in enough detail to inform decision-making about what changes to implement.

These changes may include implementing additional controls, removing controls and using different controls, or a decision may be taken to continue with no controls at all. Controls may be actions that are repeated, either regularly or in response to events, or they may be one-off actions or decisions. Controls may be changes to existing plans or procedures, which may be more efficient and integrated than adding additional activities such as checks.

A control may be implemented to:

a) avoid risk;

b) seek risk (take opportunity);

c) modify risk;

d) share risk; and/or

e) retain risk.

NOTE 1 It is often worth gathering more information about risks.

NOTE 2 Further information on possible controls is given in Annex C.

Controls may include policies, expressed in words or numbers, that aim to constrain risk-taking and risk exposure, and go beyond risk criteria by applying to risk-related indicators (e.g. level of investment, duration of a project) as well as to risk measures. These policies reinforce the risk criteria and may use targets, single limits, bands, multiple thresholds, or other techniques to provide planning guidance, determine limits on authority, trigger alternative control procedures or escalation, and influence decision-making in other ways.

Such policies, if used, should be set and revised as part of existing processes for strategy making and planning, possibly at the same time as risk criteria. The policies may be part of the risk management framework (see **3.3.13**).

Consideration should be given to the work needed to develop and implement the possible control changes, as well as to operate the controls.

Controls may be considered individually, but controls considered as an integrated system are likely to be more effective and efficient.

4.5.2.2 Deciding which control changes to make

When deciding which control changes to implement, those managing risk should assess, in accordance with the risk criteria:

a) the possible net benefits compared with the cost of implementing and operating the controls, taking into account the effects on all risks affected by each control;

b) the relative cost-benefit of different control changes considered;

c) any legal or regulatory requirements, social responsibility factors or limits within the risk criteria or other policies on risk-taking and exposure that might override a cost-benefit analysis and necessitate or prevent a specific control change; and

d) any additional risks that might be introduced by a particular control change.

Control change decisions should take into account the perceptions and concerns of stakeholders.

All changes to controls and the resulting retained residual risk should be appropriately documented and authorized by the organization in accordance with risk management roles and any applicable policies to control risk-taking and exposure.

4.5.3 Preparing and implementing risk treatment plans

Risk treatment plans should be prepared and implemented, and progress towards implementation should be monitored.

In preparing risk treatment plans, those managing risk should:

a) prioritize changes to controls, taking into account the impact on other activities and the availability of resources;

b) allocate risks response owners to the control changes selected; and

c) prepare a schedule for their implementation.

The number of separate plans and the detail they contain should be appropriate, taking into consideration the size and complexity of the organization and the changes to be made. Integrated documentation can reduce repetition.

The controls implemented should be documented.

4.6 Monitoring and review

4.6.1 General

Monitoring and review by those operating an instance of the risk management process should cover:

a) the risks and controls that are within the scope of the instance of the risk management process; and

b) the performance of the instance, with a view to how it might be adapted and improved.

Information should be provided to others, as required by the risk management framework, to allow them to monitor and review.

4.6.2 Monitoring operation and performance of controls

The organization should monitor and test its controls to ensure:

a) they have named owners;

b) they are specified, communicated and understood;

c) they are operating as designed;

d) that where deficiencies in the implementation or operation of controls are identified:

1) the implications of control deficiencies not being remedied are understood and options for resolution are identified;

2) they are reported so that the consequence for the risk profile can be assessed; and

3) the resolution of control deficiencies is planned and carried out;

e) that if their implementation introduced any additional risks, then these have been considered; and

f) they are operating effectively and efficiently, each is worthwhile, and collectively they managed the risk to a level agreed to be acceptable.

NOTE Assurance as to the effectiveness of controls may take a variety of forms and range from self-assessment, through to internal audit and/or to detailed reviews by independent external experts. Relevant evidence of controls' effectiveness is usually available from routine monitoring of activities.

After control changes have been implemented, data should be gathered to support a revised estimate of the residual risk and used in future iterations of risk assessment and risk treatment.

4.7 Monitoring performance of the instance of the risk management process

Those carrying out the instance of the risk management process should regularly review their experiences, outputs, and results to identify opportunities to improve the instance, including any where they need assistance.

NOTE Matters requiring attention can include:

a) poor compliance with the process;

b) insufficient resources, lack of competence, or unsuitable tools or document formats;

c) inadequate information to support risk assessments;

d) risk analyses that are disorderly or do not support other management decision-making;

e) poorly defined risks, inadequate cross-referencing, anomalous risk levels, unsuitable risk summaries, or lack of ideas for effective risk responses;

f) difficulties integrating risk management with other management activities;

g) inadequate information to support assessments of the effectiveness of controls; and

h) slow or otherwise ineffective implementation of risk treatments.

This information should be used within continuing work to establish the context of the instance of the risk management process as recommended in **4.3** and assistance should be obtained where necessary.

4.8 Providing information to others

The key outputs from the instance of the risk management process and lessons learned about the framework and process should be communicated to the relevant stakeholders as part of ongoing communication and consultation, as described in the risk management framework.

This reporting should provide an appropriate level of detail, and be specific, relevant, timely and reliable.

If circumstances indicate that the instance of the risk management process ought to be terminated or its scope revised then this information should be communicated and appropriate action taken.

4.9 Recording the risk management process

Risk management should be recorded.

Records of the instance of the risk management process should include documentation of:

a) the design of the instance of the risk management process and key decisions taken in arriving at that design;

b) the thinking involved in risk assessment and risk treatment decisions, including risks, risk evaluations, risk responses, risk treatments and risk treatment plans;

c) mappings between risks and responses, between controls and risk treatments, and between risk treatments and risk treatment plans;

d) owners for risks and risk responses; and

e) dates for versions of the documentation.

Further, records should include:

1) the status of key risks identified by the process, highlighting:

   i) any material changes that alter their likelihoods and/or consequences, particularly if these are likely to affect what responses are worthwhile; and

   ii) any risk(s) for which completion of an important risk treatment is outstanding;

2) the status of risk responses for key risks, for example where progress is behind agreed target or is significantly threatened;

3) any significant emerging risks that need to be assessed and monitored;

4) a description of the uncertainty related to a particular activity, process or event; and

5) the possible consequence(s) of risks, described in terms of the effect on a business, activity or project, rather than just the specific consequence, e.g. financial loss/gain;

Records may also include:

i) the underlying causes/sources of risk(s), e.g. a particular activity or process;

ii) information about the timing of risks;

iii) the dates risks were raised, in order to monitor ageing of risks with respect to the progress of modification;

iv) the link between an identified source(s) of risk and the relevant performance objectives;

v) the links between risks; and

vi) separate analysis between risk responses in operation, agreed risk responses not yet in operation, and newly proposed risk responses.

The documentation should be able to capture links between items and provide appropriate summaries.

NOTE Documentation that records the thinking involved in risk management may use paper or electronic storage.

The documentation used to record risk management may also be used for reporting, where its design is suitable.

Annex A (informative)

Risk management tools

Tools can be powerful aids to effective risk management. They can enable those managing risk to capture information in a consistent way, engage with stakeholders, provide more thorough and reliable analyses, make explicit the risks associated with different options, prioritize actions, improve communication, and produce a reliable audit trail.

There are many tools and each is suitable for particular tasks in particular situations (see Table A.1). Some choices of tool are easy while others are harder. Tool selection should be based on:

a) characteristics of the user
   1) competence and experience with the tool
   2) ability to understand the benefits of using the tool
   3) willingness to use the tool

b) characteristics of the task
   1) purpose of the risk management activity
   2) desired output
   3) uses to which risk management outputs will be put
   4) stage of the activity being undertaken
   5) time available for the risk study
   6) the importance of the risks involved
   7) required level of detail

c) characteristics of the tool
   1) availability of information on the productive use of the tool
   2) availability of information on the tools' functionality
   3) ease of use
   4) cost

d) characteristics of risk management within the organization
   1) degree to which risk management is embedded in the organization
   2) complexity of its framework and the number of instances of its process
   3) complexity of instances.

Table A.1 **Examples of risk management tools (including techniques)**

Tool	Risk identification	Risk analysis and evaluation	Risk treatment and decisions
Types of meeting/collaboration: Interviews, focus groups, scenario analysis and planning, horizon scanning, brainstorming, Delphi technique, nominal group technique, SWOT (strengths, weaknesses, opportunities and threats) analysis, risk questionnaires	✓	✓	✓
For exploring and visualizing the context: stakeholder engagement matrices, PESTLE (political, economic, sociological, technological, legislation and environment) analysis, Boston grid, gap analysis, Pareto analysis	✓		
Structural guidance for risk analysis: risk checklists/prompt lists, project profile model (PPM), risk breakdown structure, risk taxonomy	✓		
Modelling styles: process mapping, flow charts, cause-and-effect diagrams, hazard and operability study (HAZOPs), failure mode effects analysis (FMEA), fault and event tree modelling, probability trees, critical path analysis (CPA), cash flow analysis, portfolio analysis	✓	✓	✓
Data analysis: descriptive statistics, model fitting		✓	✓
Model analysis methods and tools: risk simulation (Monte Carlo/Latin Hypercube), sensitivity analysis, stress testing		✓	✓
Risk recording and visualization techniques and tools: heat maps, RAG status reports, graphs of distributions, bar chart/radar chart, risk mapping, risk profiling, probability and consequence grid, risk Indicators, risk register/database	✓	✓	✓
Decision bases: expected value, utility theory, cost-benefit analysis			✓

Annex B (normative) Incorporating potentially positive consequences of risk

B.1 Potentially positive consequences

The definition of "risk" used by this Code of Practice and ISO Guide 73 reflects the modern approach to risk management that includes good consequences, as well as bad.

Incorporating potentially desirable consequences requires the approach to risk management to have appropriate features.

B.2 Language

Where an organization chooses to include potentially positive consequences in its risk management process it should ensure that the words it uses do not introduce bias. In particular, since most people identify the word "risk" with undesirable potential events only, the technical view of risk should be explained effectively or alternative language used, e.g. referring to risks as "potential problems and potential opportunities", "upside and downside risks", or as "uncertainties". When identifying risks, circumstances that drive risk can be described as "threats and opportunities".

B.3 Characterizing risks

When risks are characterized in terms of consequences and likelihoods the methods used should be appropriate for the intended types of risk. It should be possible to characterize and communicate those risks whose consequences are predominantly desirable, as well as those whose consequences are predominantly undesirable.

Where a consequence of a risk could be anywhere within a range it might be that this range includes desirable and undesirable consequence levels. Summarizing this range of consequences using its average is likely to be misleading because desirable and undesirable possibilities could balance, indicating zero risk level even though important uncertainty exists. Alternatives include presenting the range in some way and using a measure of spread. In quantitative risk assessments the standard deviation is often used as a measure of spread.

B.4 Incorporating risks in decisions

The organization should have clearly defined approaches to incorporating risk in decisions. These should ensure that decision-making involves consideration of all potential consequences, including those better and those worse than expected or planned. If a course of action carries a risk whose potential consequence is positive then this will make the course of action more attractive. Further, if that potential consequence is increased and still positive then this will make the course of action even more attractive. This is why consideration of costs and net benefits of risk treatments is necessary in addition to any comparison with a risk limit.

Annex C (informative) Effects of controls

C.1 Avoid risk

Where risks cannot be influenced by the organization and/or cannot be managed to an acceptable level, the only option might be to not proceed with an activity or to withdraw from it. Risk avoidance may also be justified as a cost-effective way to manage a risk.

The scope for avoiding an activity can be severely limited in the public sector, compared to the private sector, due to legal and regulatory obligations to provide certain services.

Withdrawing from an activity can be an important option in project management if it becomes clear that the costs of achieving the project objectives are too high, or that the objectives might not be realized irrespective of cost. In such a case, the correct response may be to terminate the project.

Avoiding risk can occur inappropriately if an organization or individual is unnecessarily risk averse or has incorrectly assessed the risks or rewards involved. In these circumstances avoiding a risk might increase the importance of other risks or result in failure to make the most of opportunities.

C.2 Seek risk

Risks with desirable potential consequences can make an activity more attractive and lead an organization to pursue that activity, just as risks with undesirable potential consequences can motivate avoidance.

There are more potential opportunities than is sometimes appreciated but appropriate focus, procedures and language can allow them to be identified and included in decision-making.

C.3 Modify risk

The majority of risks are managed in this way. Using risk modification involves changing causes and/or effects to increase the likelihoods of desired consequences and/or decrease the likelihoods of undesired consequences. This may involve preventative measures, contingency plans, or additional funding.

A number of measures to modify a risk may be considered and implemented, either individually or in combination.

C.4 Transfer risk

For some risks the most appropriate response may be to transfer them (often referred to as "risk sharing"). This might be achieved by conventional insurance, by contractual arrangements, or through arrangements such as partnerships and joint ventures where exposures and liabilities are shared, as well as the potential for gain.

It is important to recognize the limitations of risk transfer. Where risks are transferred, in whole or in part, the organization transferring the risk acquires a new risk that the organization to which the risk is transferred might not manage the risk effectively. Many risks can never be transferred completely, for example:

a) insurance might provide the funds to rebuild a production plant which has been destroyed by fire, but it does not solve the problem of how to maintain the business in the interim;

b) outsourcing the operation of IT systems to a specialist service provider does not eliminate the risk of IT systems failure or remove the need to have contingency plans if the systems fail; and

c) contracting other organizations to manufacture products or supply services on the organization's behalf does not remove the risk to the organization's reputation; in many cases, it is of no concern to a customer that the failure was with a contractor.

In practice, risk transfer is typically used in combination with one or more of the other risk response options.

C.5 Retain risk

Retaining a residual risk means planning no further action to respond to it, for the time being. A risk might be retained because no further worthwhile actions can be devised, or because the only remaining responses are unacceptable for some reason or cannot yet be implemented. Risk retention has to be a conscious decision based on the results of the risk analysis and evaluation process, but might need to be reviewed in future if circumstances change. Self-insurance and similar internal risk financing arrangements are forms of risk retention. Retention of risks by default because of a failure to identify or appropriately manage them ought not to be tolerated.

Bibliography

For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

Standards publications

BS 25999, *Business continuity management*

BS ISO 31000, *Risk management – Principles and guidelines on implementation*

ISO/IEC Guide 73, *Risk management – Vocabulary*

Other publications

[1] HM Treasury: *Management of Risk – Principles and Concepts* (the Orange Book), London: 2004

[2] Office of Government Commerce: *Management of Risk: Guidance for Practitioners* (Third Edition), London: 2010

[3] COSO: *Enterprise Risk Management – Integrated Framework*, 2004 (for application of the Framework, see: http://www.coso.org/Publications/ErM/COSO_ErM. ppt#258,1,applying COSO's Enterprise risk Management – integrated Framework)

[4] AIRMIC, Alarm, IRM: *A Standard for Risk Management*, London: 2002.

British Standards Institution (BSI)

BSI is the independent national body responsible for preparing British Standards and other standards-related publications, information and services.
It presents the UK view on standards in Europe and at the international level.

It is incorporated by Royal Charter.

Revisions

British Standards are updated by amendment or revision. Users of British Standards should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using this British Standard would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover.

Tel: +44 (0)20 8996 9001 Fax: +44 (0)20 8996 7001

BSI offers Members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of standards.

Tel: +44 (0)20 8996 7669 Fax: +44 (0)20 8996 7001
Email: plus@bsigroup.com

Buying standards

You may buy PDF and hard copy versions of standards directly using a credit card from the BSI Shop on the website **www.bsigroup.com/shop.** In addition all orders for BSI, international and foreign standards publications can be addressed to BSI Customer Services.

Tel: +44 (0)20 8996 9001 Fax: +44 (0)20 8996 7001
Email: orders@bsigroup.com

In response to orders for international standards, it is BSI policy to supply the BSI implementation of those that have been published as British Standards, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Knowledge Centre.

Tel: +44 (0)20 8996 7004 Fax: +44 (0)20 8996 7005
Email: knowledgecentre@bsigroup.com

Various BSI electronic information services are also available which give details on all its products and services.

Tel: +44 (0)20 8996 7111 Fax: +44 (0)20 8996 7048
Email: info@bsigroup.com

BSI Subscribing Members are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration.

Tel: +44 (0)20 8996 7002 Fax: +44 (0)20 8996 7001
Email: membership@bsigroup.com

Information regarding online access to British Standards via British Standards Online can be found at **www.bsigroup.com/BSOL**

Further information about BSI is available on the BSI website at **www.bsigroup.com/standards**

Copyright

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Tel +44 (0)20 8996 9001
Fax +44 (0)20 8996 7001
www.bsigroup.com/standards

raising standards worldwide™

This British Standard gives recommendations for implementing the principles and guidelines in BS ISO 31000:2009, including the risk management framework and process. It provides a basis for understanding, developing, implementing and maintaining proportionate and effective risk management throughout an organization, in order to enhance the organization's likelihood of achieving its objectives.

This British Standard is intended for use by anyone with responsibility for, or involved in, any of the following:

a) ensuring an organization achieves its objectives;
b) ensuring risks are proactively managed in specific areas or activities;
c) overseeing risk management in an organization;
d) providing assurance about the effectiveness of an organization's risk management; and/or
e) reporting to stakeholders, e.g. through disclosures in annual financial statements, corporate governance reports and corporate social responsibility reports.

BSI
389 Chiswick High Road
London W4 4AL
United Kingdom

Tel: +44 (0)20 8996 9001
Fax: +44 (0)20 8996 7001
Website: www.bsigroup.com
Email: info@bsigroup.com

ISBN 978-0-580-71607-2
9 780580 716072

BS EN 31010:2010

BSI Standards Publication

Risk management

Risk assessment techniques

raising standards worldwide™

National foreword

This British Standard is the UK implementation of EN 31010:2010. It is identical to IEC/ISO 31010:2009.

The UK participation in its preparation was entrusted to Technical Committee DS/1, Dependability and terotechnology.

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

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

ISBN 978 0 580 63461 1

ICS 03.100.01

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

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 June 2010.

Amendments issued since publication

Amd. No.	Date	Text affected

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 31010

May 2010

ICS 03.100.01

English version

Risk management - Risk assessment techniques
(IEC/ISO 31010:2009)

Gestion des risques - Techniques d'évaluation des risques (CEI/ISO 31010:2009)

Risikomanagement - Verfahren zur Risikobeurteilung (IEC/ISO 31010:2009)

This European Standard was approved by CENELEC on 2010-05-01. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the Central Secretariat or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the Central Secretariat has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

CENELEC

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

Management Centre: Avenue Marnix 17, B - 1000 Brussels

Ref. No. EN 31010:2010 E

Foreword

The text of document 56/1329/FDIS, future edition 1 of IEC/ISO 31010, prepared by IEC TC 56, Dependability, together with the ISO TMB “Risk management” working group, was submitted to the IEC-CENELEC parallel vote and was approved by CENELEC as EN 31010 on 2010-05-01.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN and CENELEC shall not be held responsible for identifying any or all such patent rights.

The following dates were fixed:

– latest date by which the EN has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	2011-02-01
– latest date by which the national standards conflicting with the EN have to be withdrawn	(dow)	2013-05-01

Annex ZA has been added by CENELEC.

Endorsement notice

The text of the International Standard IEC/ISO 31010:2009 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

IEC 60300-3-11	NOTE	Harmonized as EN 60300-3-11.
IEC 61078	NOTE	Harmonized as EN 61078.
IEC 61165	NOTE	Harmonized as EN 61165.
IEC 61508 series	NOTE	Harmonized in EN 61508 series (not modified)
IEC 61511 series	NOTE	Harmonized in EN 61511 series (not modified)
IEC 61649	NOTE	Harmonized as EN 61649.
ISO 22000	NOTE	Harmonized as EN ISO 22000.

Annex ZA
(normative)

Normative references to international publications with their corresponding European publications

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

NOTE When an international publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

Publication	Year	Title	EN/HD	Year
ISO/IEC Guide 73	-	Risk management - Vocabulary - Guidelines for use in standards	-	-
ISO 31000	-	Risk management - Principles and guidelines	-	-

CONTENTS

INTRODUCTION

Organizations of all types and sizes face a range of risks that may affect the achievement of their objectives.

These objectives may relate to a range of the organization's activities, from strategic initiatives to its operations, processes and projects, and be reflected in terms of societal, environmental, technological, safety and security outcomes, commercial, financial and economic measures, as well as social, cultural, political and reputation impacts.

All activities of an organization involve risks that should be managed. The risk management process aids decision making by taking account of uncertainty and the possibility of future events or circumstances (intended or unintended) and their effects on agreed objectives.

Risk management includes the application of logical and systematic methods for

- communicating and consulting throughout this process;
- establishing the context for identifying, analysing, evaluating, treating risk associated with any activity, process, function or product;
- monitoring and reviewing risks;
- reporting and recording the results appropriately.

Risk assessment is that part of risk management which provides a structured process that identifies how objectives may be affected, and analyses the risk in term of consequences and their probabilities before deciding on whether further treatment is required.

Risk assessment attempts to answer the following fundamental questions:

- what can happen and why (by risk identification)?
- what are the consequences?
- what is the probability of their future occurrence?
- are there any factors that mitigate the consequence of the risk or that reduce the probability of the risk?

Is the level of risk tolerable or acceptable and does it require further treatment? This standard is intended to reflect current good practices in selection and utilization of risk assessment techniques, and does not refer to new or evolving concepts which have not reached a satisfactory level of professional consensus.

This standard is general in nature, so that it may give guidance across many industries and types of system. There may be more specific standards in existence within these industries that establish preferred methodologies and levels of assessment for particular applications. If these standards are in harmony with this standard, the specific standards will generally be sufficient.

RISK MANAGEMENT – RISK ASSESSMENT TECHNIQUES

1 Scope

This International Standard is a supporting standard for ISO 31000 and provides guidance on selection and application of systematic techniques for risk assessment.

Risk assessment carried out in accordance with this standard contributes to other risk management activities.

The application of a range of techniques is introduced, with specific references to other international standards where the concept and application of techniques are described in greater detail.

This standard is not intended for certification, regulatory or contractual use.

This standard does not provide specific criteria for identifying the need for risk analysis, nor does it specify the type of risk analysis method that is required for a particular application.

This standard does not refer to all techniques, and omission of a technique from this standard does not mean it is not valid. The fact that a method is applicable to a particular circumstance does not mean that the method should necessarily be applied.

NOTE This standard does not deal specifically with safety. It is a generic risk management standard and any references to safety are purely of an informative nature. Guidance on the introduction of safety aspects into IEC standards is laid down in ISO/IEC Guide 51.

2 Normative references

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

ISO/IEC Guide 73, *Risk management – Vocabulary – Guidelines for use in standards*

ISO 31000, *Risk management – Principles and guidelines*

3 Terms and definitions

For the purposes of this document, the terms and definitions of ISO/IEC Guide 73 apply.

4 Risk assessment concepts

4.1 Purpose and benefits

The purpose of risk assessment is to provide evidence-based information and analysis to make informed decisions on how to treat particular risks and how to select between options.

Some of the principal benefits of performing risk assessment include:

- understanding the risk and its potential impact upon objectives;

- providing information for decision makers;
- contributing to the understanding of risks, in order to assist in selection of treatment options;
- identifying the important contributors to risks and weak links in systems and organizations;
- comparing of risks in alternative systems, technologies or approaches;
- communicating risks and uncertainties;
- assisting with establishing priorities;
- contributing towards incident prevention based upon post-incident investigation;
- selecting different forms of risk treatment;
- meeting regulatory requirements;
- providing information that will help evaluate whether the risk should be accepted when compared with pre-defined criteria;
- assessing risks for end-of-life disposal.

4.2 Risk assessment and the risk management framework

This standard assumes that the risk assessment is performed within the framework and process of risk management described in ISO 31000.

A risk management framework provides the policies, procedures and organizational arrangements that will embed risk management throughout the organization at all levels.

As part of this framework, the organization should have a policy or strategy for deciding when and how risks should be assessed.

In particular, those carrying out risk assessments should be clear about

- the context and objectives of the organization,
- the extent and type of risks that are tolerable, and how unacceptable risks are to be treated,
- how risk assessment integrates into organizational processes,
- methods and techniques to be used for risk assessment, and their contribution to the risk management process,
- accountability, responsibility and authority for performing risk assessment,
- resources available to carry out risk assessment,
- how the risk assessment will be reported and reviewed.

4.3 Risk assessment and the risk management process

4.3.1 General

Risk assessment comprises the core elements of the risk management process which are defined in ISO 31000 and contain the following elements:

- communication and consultation;
- establishing the context;
- risk assessment (comprising risk identification, risk analysis and risk evaluation);
- risk treatment;
- monitoring and review.

Risk assessment is not a stand-alone activity and should be fully integrated into the other components in the risk management process.

4.3.2 Communication and consultation

Successful risk assessment is dependent on effective communication and consultation with stakeholders.

Involving stakeholders in the risk management process will assist in

- developing a communication plan,
- defining the context appropriately,
- ensuring that the interests of stakeholders are understood and considered,
- bringing together different areas of expertise for identifying and analysing risk,
- ensuring that different views are appropriately considered in evaluating risks,
- ensuring that risks are adequately identified,
- securing endorsement and support for a treatment plan.

Stakeholders should contribute to the interfacing of the risk assessment process with other management disciplines, including change management, project and programme management, and also financial management.

4.3.3 Establishing the context

Establishing the context defines the basic parameters for managing risk and sets the scope and criteria for the rest of the process. Establishing the context includes considering internal and external parameters relevant to the organization as a whole, as well as the background to the particular risks being assessed.

In establishing the context, the risk assessment objectives, risk criteria, and risk assessment programme are determined and agreed.

For a specific risk assessment, establishing the context should include the definition of the external, internal and risk management context and classification of risk criteria:

a) Establishing the external context involves familiarization with the environment in which the organization and the system operates including :
   - cultural, political, legal, regulatory, financial, economic and competitive environment factors, whether international, national, regional or local;
   - key drivers and trends having impact on the objectives of the organization; and
   - perceptions and values of external stakeholders.

b) Establishing the internal context involves understanding
   - capabilities of the organization in terms of resources and knowledge,
   - information flows and decision-making processes,
   - internal stakeholders,
   - objectives and the strategies that are in place to achieve them,
   - perceptions, values and culture,
   - policies and processes,
   - standards and reference models adopted by the organization, and
   - structures (e.g. governance, roles and accountabilities).

c) Establishing the context of the risk management process includes
   - defining accountabilities and responsibilities,
   - defining the extent of the risk management activities to be carried out, including specific inclusions and exclusions,

- defining the extent of the project, process, function or activity in terms of time and location,
- defining the relationships between a particular project or activity and other projects or activities of the organization,
- defining the risk assessment methodologies,
- defining the risk criteria,
- defining how risk management performance is evaluated,
- identifying and specifying the decisions and actions that have to be made, and
- identifying scoping or framing studies needed, their extent, objectives and the resources required for such studies.

d) Defining risk criteria involves deciding

- the nature and types of consequences to be included and how they will be measured,
- the way in which probabilities are to be expressed,
- how a level of risk will be determined,
- the criteria by which it will be decided when a risk needs treatment,
- the criteria for deciding when a risk is acceptable and/or tolerable,
- whether and how combinations of risks will be taken into account.

Criteria can be based on sources such as

- agreed process objectives,
- criteria identified in specifications,
- general data sources,
- generally accepted industry criteria such as safety integrity levels,
- organizational risk appetite,
- legal and other requirements for specific equipment or applications.

4.3.4 Risk assessment

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation.

Risks can be assessed at an organizational level, at a departmental level, for projects, individual activities or specific risks. Different tools and techniques may be appropriate in different contexts.

Risk assessment provides an understanding of risks, their causes, consequences and their probabilities. This provides input to decisions about:

- whether an activity should be undertaken;
- how to maximize opportunities;
- whether risks need to be treated;
- choosing between options with different risks;
- prioritizing risk treatment options;
- the most appropriate selection of risk treatment strategies that will bring adverse risks to a tolerable level.

4.3.5 Risk treatment

Having completed a risk assessment, risk treatment involves selecting and agreeing to one or more relevant options for changing the probability of occurrence, the effect of risks, or both, and implementing these options.

This is followed by a cyclical process of reassessing the new level of risk, with a view to determining its tolerability against the criteria previously set, in order to decide whether further treatment is required.

4.3.6 Monitoring and review

As part of the risk management process, risks and controls should be monitored and reviewed on a regular basis to verify that

- assumptions about risks remain valid;
- assumptions on which the risk assessment is based, including the external and internal context, remain valid;
- expected results are being achieved;
- results of risk assessment are in line with actual experience;
- risk assessment techniques are being properly applied;
- risk treatments are effective.

Accountability for monitoring and performing reviews should be established.

5 Risk assessment process

5.1 Overview

Risk assessment provides decision-makers and responsible parties with an improved understanding of risks that could affect achievement of objectives, and the adequacy and effectiveness of controls already in place. This provides a basis for decisions about the most appropriate approach to be used to treat the risks. The output of risk assessment is an input to the decision-making processes of the organization.

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation (see Figure 1). The manner in which this process is applied is dependent not only on the context of the risk management process but also on the methods and techniques used to carry out the risk assessment.

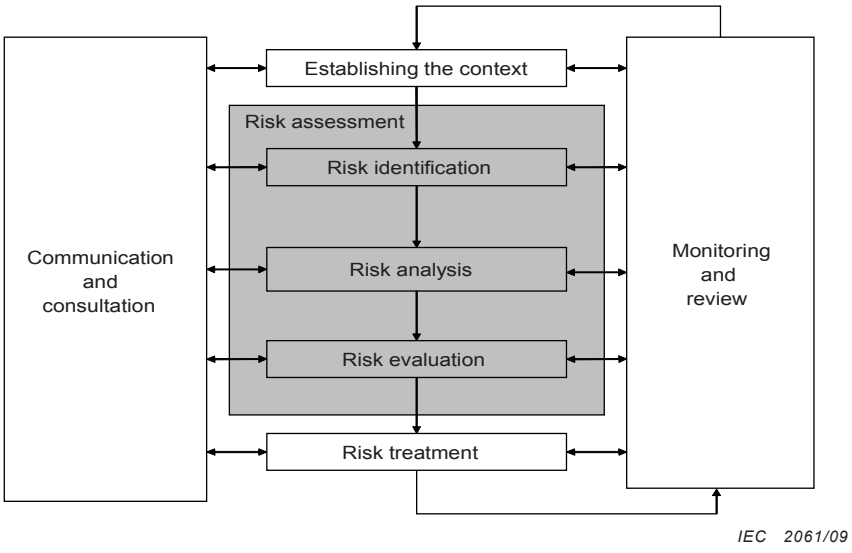


Figure 1 – Contribution of risk assessment to the risk management process

Risk assessment may require a multidisciplinary approach since risks may cover a wide range of causes and consequences.

5.2 Risk identification

Risk identification is the process of finding, recognizing and recording risks.

The purpose of risk identification is to identify what might happen or what situations might exist that might affect the achievement of the objectives of the system or organization. Once a risk is identified, the organization should identify any existing controls such as design features, people, processes and systems.

The risk identification process includes identifying the causes and source of the risk (hazard in the context of physical harm), events, situations or circumstances which could have a material impact upon objectives and the nature of that impact

Risk identification methods can include:

- evidence based methods, examples of which are check-lists and reviews of historical data;
- systematic team approaches where a team of experts follow a systematic process to identify risks by means of a structured set of prompts or questions;
- inductive reasoning techniques such as HAZOP.

Various supporting techniques can be used to improve accuracy and completeness in risk identification, including brainstorming, and Delphi methodology.

Irrespective of the actual techniques employed, it is important that due recognition is given to human and organizational factors when identifying risk. Hence, deviations of human and organizational factors from the expected should be included in the risk identification process as well as "hardware" or "software" events.

5.3 Risk analysis

5.3.1 General

Risk analysis is about developing an understanding of the risk. It provides an input to risk assessment and to decisions about whether risks need to be treated and about the most appropriate treatment strategies and methods.

Risk analysis consists of determining the consequences and their probabilities for identified risk events, taking into account the presence (or not) and the effectiveness of any existing controls. The consequences and their probabilities are then combined to determine a level of risk.

Risk analysis involves consideration of the causes and sources of risk, their consequences and the probability that those consequences can occur. Factors that affect consequences and probability should be identified. An event can have multiple consequences and can affect multiple objectives. Existing risk controls and their effectiveness should be taken into account. Various methods for these analyses are described in Annex B. More than one technique may be required for complex applications.

Risk analysis normally includes an estimation of the range of potential consequences that might arise from an event, situation or circumstance, and their associated probabilities, in order to measure the level of risk. However in some instances, such as where the consequences are likely to be insignificant, or the probability is expected to be extremely low, a single parameter estimate may be sufficient for a decision to be made

In some circumstances, a consequence can occur as a result of a range of different events or conditions, or where the specific event is not identified. In this case, the focus of risk assessment is on analysing the importance and vulnerability of components of the system with a view to defining treatments which relate to levels of protection or recovery strategies.

Methods used in analysing risks can be qualitative, semi-quantitative or quantitative. The degree of detail required will depend upon the particular application, the availability of reliable data and the decision-making needs of the organization. Some methods and the degree of detail of the analysis may be prescribed by legislation.

Qualitative assessment defines consequence, probability and level of risk by significance levels such as “high”, “medium” and “low”, may combine consequence and probability, and evaluates the resultant level of risk against qualitative criteria.

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

Quantitative analysis estimates practical values for consequences and their probabilities, and produces values of the level of risk in specific units defined when developing the context. Full quantitative analysis may not always be possible or desirable due to insufficient information about the system or activity being analysed, lack of data, influence of human factors, etc. or because the effort of quantitative analysis is not warranted or required. In such circumstances, a comparative semi-quantitative or qualitative ranking of risks by specialists, knowledgeable in their respective field, may still be effective.

In cases where the analysis is qualitative, there should be a clear explanation of all the terms employed and the basis for all criteria should be recorded.

Even where full quantification has been carried out, it needs to be recognized that the levels of risk calculated are estimates. Care should be taken to ensure that they are not attributed a level of accuracy and precision inconsistent with the accuracy of the data and methods employed.

Levels of risk should be expressed in the most suitable terms for that type of risk and in a form that aids risk evaluation. In some instances, the magnitude of a risk can be expressed as a probability distribution over a range of consequences.

5.3.2 Controls assessment

The level of risk will depend on the adequacy and effectiveness of existing controls. Questions to be addressed include:

- what are the existing controls for a particular risk?
- are those controls capable of adequately treating the risk so that it is controlled to a level that is tolerable?
- in practice, are the controls operating in the manner intended and can they be demonstrated to be effective when required?

These questions can only be answered with confidence if there are proper documentation and assurance processes in place.

The level of effectiveness for a particular control, or suite of related controls, may be expressed qualitatively, semi-quantitatively or quantitatively. In most cases, a high level of accuracy is not warranted. However, it may be valuable to express and record a measure of risk control effectiveness so that judgments can be made on whether effort is best expended in improving a control or providing a different risk treatment.

5.3.3 Consequence analysis

Consequence analysis determines the nature and type of impact which could occur assuming that a particular event situation or circumstance has occurred. An event may 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 will have been decided when the context was established.

Consequence analysis can vary from a simple description of outcomes to detailed quantitative modelling or vulnerability analysis.

Impacts may have a low consequence but high probability, or a high consequence and low probability, or some intermediate outcome. In some cases, it is appropriate to focus on risks with potentially very large outcomes, as these are often of greatest concern to managers. In other cases, it may be important to analyse both high and low consequence risks separately. For example, a frequent but low-impact (or chronic) problem may have large cumulative or long-term effects. In addition, the treatment actions for dealing with these two distinct kinds of risks are often quite different, so it is useful to analyse them separately.

Consequence analysis can involve:

- taking into consideration existing controls to treat the consequences, together with all relevant contributory factors that have an effect on the consequences;
- relating the consequences of the risk to the original objectives;
- considering both immediate consequences and those that may arise after a certain time has elapsed, if this is consistent with the scope of the assessment;
- considering secondary consequences, such as those impacting upon associated systems, activities, equipment or organizations.

5.3.4 Likelihood analysis and probability estimation

Three general approaches are commonly employed to estimate probability; they may be used individually or jointly:

a) The use of relevant historical data to identify events or situations which have occurred in the past and hence be able to extrapolate the probability of their occurrence in the future. The data used should be relevant to the type of system, facility, organization or activity being considered and also to the operational standards of the organization involved. If historically there is a very low frequency of occurrence, then any estimate of probability will be very uncertain. This applies especially for zero occurrences, when one cannot assume the event, situation or circumstance will not occur in the future.

b) Probability forecasts using predictive techniques such as fault tree analysis and event tree analysis (see Annex B). When historical data are unavailable or inadequate, it is necessary to derive probability by analysis of the system, activity, equipment or organization and its associated failure or success states. Numerical data for equipment, humans, organizations and systems from operational experience, or published data sources are then combined to produce an estimate of the probability of the top event. When using predictive techniques, it is important to ensure that due allowance has been made in the analysis for the possibility of common mode failures involving the co-incidental failure of a number of different parts or components within the system arising from the same cause. Simulation techniques may be required to generate probability of equipment and structural failures due to ageing and other degradation processes, by calculating the effects of uncertainties.

c) Expert opinion can be used in a systematic and structured process to estimate probability. Expert judgements should draw upon all relevant available information including historical, system-specific, organizational-specific, experimental, design, etc. There are a number of formal methods for eliciting expert judgement which provide an aid to the formulation of appropriate questions. The methods available include the Delphi approach, paired comparisons, category rating and absolute probability judgements.

5.3.5 Preliminary analysis

Risks may be screened in order to identify the most significant risks, or to exclude less significant or minor risks from further analysis. The purpose is to ensure that resources will be focussed on the most important risks. Care should be taken not to screen out low risks which occur frequently and have a significant cumulative effect

Screening should be based on criteria defined in the context. The preliminary analysis determines one or more of the following courses of action:

- decide to treat risks without further assessment;
- set aside insignificant risks which would not justify treatment;
- proceed with more detailed risk assessment.

The initial assumptions and results should be documented.

5.3.6 Uncertainties and sensitivities

There are often considerable uncertainties associated with the analysis of risk. An understanding of uncertainties is necessary to interpret and communicate risk analysis results effectively. The analysis of uncertainties associated with data, methods and models used to identify and analyse risk plays an important part in their application. Uncertainty analysis involves the determination of the variation or imprecision in the results, resulting from the collective variation in the parameters and assumptions used to define the results. An area closely related to uncertainty analysis is sensitivity analysis.

Sensitivity analysis involves the determination of the size and significance of the magnitude of risk to changes in individual input parameters. It is used to identify those data which need to be accurate, and those which are less sensitive and hence have less effect upon overall accuracy.

The completeness and accuracy of the risk analysis should be stated as fully as possible. Sources of uncertainty should be identified where possible and should address both data and model/method uncertainties. Parameters to which the analysis is sensitive and the degree of sensitivity should be stated.

5.4 Risk evaluation

Risk evaluation involves comparing estimated levels of risk with risk criteria defined when the context was established, in order to determine the significance of the level and type of risk.

Risk evaluation uses the understanding of risk obtained during risk analysis to make decisions about future actions. Ethical, legal, financial and other considerations, including perceptions of risk, are also inputs to the decision.

Decisions may include:

- whether a risk needs treatment;
- priorities for treatment;
- whether an activity should be undertaken;
- which of a number of paths should be followed.

The nature of the decisions that need to be made and the criteria which will be used to make those decisions were decided when establishing the context but they need to be revisited in more detail at this stage now that more is known about the particular risks identified.

The simplest framework for defining risk criteria is a single level which divides risks that need treatment from those which do not. This gives attractively simple results but does not reflect

the uncertainties involved both in estimating risks and in defining the boundary between those that need treatment and those that do not.

The decision about whether and how to treat the risk may depend on the costs and benefits of taking the risk and the costs and benefits of implementing improved controls.

A common approach is to divide risks into three bands:

a) an upper band where the level of risk is regarded as intolerable whatever benefits the activity may bring, and risk treatment is essential whatever its cost;

b) a middle band (or 'grey' area) where costs and benefits, are taken into account and opportunities balanced against potential consequences;

c) a lower band where the level of risk is regarded as negligible, or so small that no risk treatment measures are needed.

The 'as low as reasonably practicable' or ALARP criteria system used in safety applications follows this approach, where, in the middle band, there is a sliding scale for low risks where costs and benefits can be directly compared, whereas for high risks the potential for harm must be reduced, until the cost of further reduction is entirely disproportionate to the safety benefit gained.

5.5 Documentation

The risk assessment process should be documented together with the results of the assessment. Risks should be expressed in understandable terms, and the units in which the level of risk is expressed should be clear.

The extent of the report will depend on the objectives and scope of the assessment. Except for very simple assessments, the documentation can include:

- objectives and scope;
- description of relevant parts of the system and their functions;
- a summary of the external and internal context of the organization and how it relates to the situation, system or circumstances being assessed;
- risk criteria applied and their justification;
- limitations, assumptions and justification of hypotheses;
- assessment methodology;
- risk identification results;
- data, assumptions and their sources and validation;
- risk analysis results and their evaluation;
- sensitivity and uncertainty analysis;
- critical assumptions and other factors which need to be monitored;
- discussion of results;
- conclusions and recommendations;
- references.

If the risk assessment supports a continuing risk management process, it should be performed and documented in such a way that it can be maintained throughout the life cycle of the system, organization, equipment or activity. The assessment should be updated as significant new information becomes available and the context changes, in accordance with the needs of the management process.

5.6 Monitoring and reviewing risk assessment

The risk assessment process will highlight context and other factors that might be expected to vary over time and which could change or invalidate the risk assessment. These factors should be specifically identified for on-going monitoring and review, so that the risk assessment can be updated when necessary.

Data to be monitored in order to refine the risk assessment should also be identified and collected.

The effectiveness of controls should also be monitored and documented in order to provide data for use in risk analysis. Accountabilities for creation and reviewing the evidence and documentation should be defined.

5.7 Application of risk assessment during life cycle phases

Many activities, projects and products can be considered to have a life cycle starting from initial concept and definition through realization to a final completion which might include decommissioning and disposal of hardware.

Risk assessment can be applied at all stages of the life cycle and is usually applied many times with different levels of detail to assist in the decisions that need to be made at each phase.

Life cycles phases have different requirements and need different techniques For example, during the concept and definition phase, when an opportunity is identified, risk assessment may be used to decide whether to proceed or not.

Where several options are available risk assessment can be used to evaluate alternative concepts to help decide which provides the best balance of positive and negative risks.

During the design and development phase, risk assessment contributes to

- ensuring that system risks are tolerable,
- the design refinement process,
- cost effectiveness studies,
- identifying risks impacting upon subsequent life-cycle phases.

As the activity proceeds, risk assessment can be used to provide information to assist in developing procedures for normal and emergency conditions.

6 Selection of risk assessment techniques

6.1 General

This clause describes how techniques for risk assessment may be selected. The annexes list and further explain a range of tools and techniques that can be used to perform a risk assessment or to assist with the risk assessment process. It may sometimes be necessary to employ more than one method of assessment.

6.2 Selection of techniques

Risk assessment may be undertaken in varying degrees of depth and detail and using one or many methods ranging from simple to complex. The form of assessment and its output should be consistent with the risk criteria developed as part of establishing the context. Annex A illustrates the conceptual relationship between the broad categories of risk assessment techniques and the factors present in a given risk situation, and provides illustrative examples

of how organizations can select the appropriate risk assessment techniques for a particular situation.

In general terms, suitable techniques should exhibit the following characteristics:

- it should be justifiable and appropriate to the situation or organization under consideration;
- it should provide results in a form which enhances understanding of the nature of the risk and how it can be treated;
- it should be capable of use in a manner that is traceable, repeatable and verifiable.

The reasons for the choice of techniques should be given, with regard to relevance and suitability. When integrating the results from different studies, the techniques used and outputs should be comparable.

Once the decision has been made to perform a risk assessment and the objectives and scope have been defined, the techniques should be selected, based on applicable factors such as:

- the objectives of the study. The objectives of the risk assessment will have a direct bearing on the techniques used. For example, if a comparative study between different options is being undertaken, it may be acceptable to use less detailed consequence models for parts of the system not affected by the difference;
- the needs of decision-makers. In some cases a high level of detail is needed to make a good decision, in others a more general understanding is sufficient;
- the type and range of risks being analysed;
- the potential magnitude of the consequences. The decision on the depth to which risk assessment is carried out should reflect the initial perception of consequences (although this may have to be modified once a preliminary evaluation has been completed);
- the degree of expertise, human and other resources needed. A simple method, well done, may provide better results than a more sophisticated procedure poorly done, so long as it meets the objectives and scope of the assessment. Ordinarily, the effort put into the assessment should be consistent with the potential level of risk being analysed;
- the availability of information and data. Some techniques require more information and data than others;
- the need for modification/updating of the risk assessment. The assessment may need to be modified/updated in future and some techniques are more amendable than others in this regard;
- any regulatory and contractual requirements.

Various factors influence the selection of an approach to risk assessment such as the availability of resources, the nature and degree of uncertainty in the data and information available, and the complexity of the application (see Table A.2).

6.3 Availability of resources

Resources and capabilities which may affect the choice of risk assessment techniques include:

- the skills experience capacity and capability of the risk assessment team;
- constraints on time and other resources within the organization;
- the budget available if external resources are required.

6.4 The nature and degree of uncertainty

The nature and degree of uncertainty requires an understanding of the quality, quantity and integrity of information available concerning the risk under consideration. This includes the extent to which sufficient information about the risk, its sources and causes, and its

consequences to the achievement of objectives is available. Uncertainty can stem from poor data quality or the lack of essential and reliable data. To illustrate, data collection methods may change, the way organizations use such methods may change or the organization may not have an effective collection method in place at all, for collecting data about the identified risk.

Uncertainty can also be inherent in the external and internal context of the organization. Available data do not always provide a reliable basis for the prediction of the future. For unique types of risks, historical data may not be available or there may be different interpretations of available data by different stakeholders. Those undertaking risk assessment need to understand the type and nature of the uncertainty and appreciate the implications for the reliability of the risk assessment results. These should always be communicated to decision-makers.

6.5 Complexity

Risks can be complex in themselves, as, for example, in complex systems which need to have their risks assessed across the system rather than treating each component separately and ignoring interactions. In other cases, treating a single risk can have implications elsewhere and can impact on other activities. Consequential impacts and risk dependencies need to be understood to ensure that in managing one risk, an intolerable situation is not created elsewhere. Understanding the complexity of a single risk or of a portfolio of risks of an organization is crucial for the selection of the appropriate method or techniques for risk assessment.

6.6 Application of risk assessment during life cycle phases

Many activities, projects and products can be considered to have a life cycle starting from initial concept and definition through realization to a final completion which might include decommissioning and disposal of hardware.

Risk assessment can be applied at all stages of the life cycle and is usually applied many times with different levels of detail to assist in the decisions that need to be made at each phase.

Life cycle phases have different needs and require different techniques For example during the concept and definition phase, when an opportunity is identified, risk assessment may be used to decide whether to proceed or not.

Where several options are available, risk assessment can be used to evaluate alternative concepts to help decide which provides the best balance of risks.

During the design and development phase, risk assessment contributes to

- ensuring that system risks are tolerable,
- the design refinement process,
- cost effectiveness studies,
- identifying risks impacting upon subsequent life-cycle phases.

As the activity proceeds, risk assessment can be used to provide information to assist in developing procedures for normal and emergency conditions.

6.7 Types of risk assessment techniques

Risk assessment techniques can be classified in various ways to assist with understanding their relative strengths and weaknesses. The tables in Annex A correlate some potential techniques and their categories for illustrative purposes.

Each of the techniques is further elaborated upon in Annex B as to the nature of the assessment they provide and guidance to their applicability for certain situations.

Annex A
(informative)

Comparison of risk assessment techniques

A.1 Types of technique

The first classification shows how the techniques apply to each step of the risk assessment process as follows:

- risk identification;
- risk analysis – consequence analysis;
- risk analysis – qualitative, semi-quantitative or quantitative probability estimation;
- risk analysis – assessing the effectiveness of any existing controls;
- risk analysis – estimation the level of risk;
- risk evaluation.

For each step in the risk assessment process, the application of the method is described as being either strongly applicable, applicable or not applicable (see Table A.1).

A.2 Factors influencing selection of risk assessment techniques

Next the attributes of the methods are described in terms of

- complexity of the problem and the methods needed to analyse it,
- the nature and degree of uncertainty of the risk assessment based on the amount of information available and what is required to satisfy objectives,
- the extent of resources required in terms of time and level of expertise, data needs or cost,
- whether the method can provide a quantitative output.

Examples of types of risk assessment methods available are listed in Table A.2 where each method is rated as high medium or low in terms of these attributes.

Table A.1 – Applicability of tools used for risk assessment

Tools and techniques	Risk assessment process					See Annex
	Risk Identification	Risk analysis			Risk evaluation	
		Consequence	Probability	Level of risk		
Brainstorming	SA[1)]	NA[2)]	NA	NA	NA	B 01
Structured or semi-structured interviews	SA	NA	NA	NA	NA	B 02
Delphi	SA	NA	NA	NA	NA	B 03
Check-lists	SA	NA	NA	NA	NA	B 04
Primary hazard analysis	SA	NA	NA	NA	NA	B 05
Hazard and operability studies (HAZOP)	SA	SA	A[3)]	A	A	B 06
Hazard Analysis and Critical Control Points (HACCP)	SA	SA	NA	NA	SA	B 07
Environmental risk assessment	SA	SA	SA	SA	SA	B 08
Structure « What if? » (SWIFT)	SA	SA	SA	SA	SA	B 09
Scenario analysis	SA	SA	A	A	A	B 10
Business impact analysis	A	SA	A	A	A	B 11
Root cause analysis	NA	SA	SA	SA	SA	B 12
Failure mode effect analysis	SA	SA	SA	SA	SA	B 13
Fault tree analysis	A	NA	SA	A	A	B 14
Event tree analysis	A	SA	A	A	NA	B 15
Cause and consequence analysis	A	SA	SA	A	A	B 16
Cause-and-effect analysis	SA	SA	NA	NA	NA	B 17
Layer protection analysis (LOPA)	A	SA	A	A	NA	B 18
Decision tree	NA	SA	SA	A	A	B 19
Human reliability analysis	SA	SA	SA	SA	A	B 20
Bow tie analysis	NA	A	SA	SA	A	B 21
Reliability centred maintenance	SA	SA	SA	SA	SA	B 22
Sneak circuit analysis	A	NA	NA	NA	NA	B 23
Markov analysis	A	SA	NA	NA	NA	B 24
Monte Carlo simulation	NA	NA	NA	NA	SA	B 25
Bayesian statistics and Bayes Nets	NA	SA	NA	NA	SA	B 26
FN curves	A	SA	SA	A	SA	B 27
Risk indices	A	SA	SA	A	SA	B 28
Consequence/probability matrix	SA	SA	SA	SA	A	B 29
Cost/benefit analysis	A	SA	A	A	A	B 30
Multi-criteria decision analysis (MCDA)	A	SA	A	SA	A	B 31

[1)] Strongly applicable.

[2)] Not applicable.

[3)] Applicable.

Table A.2 – Attributes of a selection of risk assessment tools

Type of risk assessment technique	Description	Relevance of influencing factors			Can provide Quantitative output
		Resources and capability	Nature and degree of uncertainty	Complexity	
LOOK-UP METHODS					
Check-lists	A simple form of risk identification. A technique which provides a listing of typical uncertainties which need to be considered. Users refer to a previously developed list, codes or standards	Low	Low	Low	No
Preliminary hazard analysis	A simple inductive method of analysis whose objective is to identify the hazards and hazardous situations and events that can cause harm for a given activity, facility or system	Low	High	Medium	No
SUPPORTING METHODS					
Structured Interview and brainstorming	A means of collecting a broad set of ideas and evaluation, ranking them by a team. Brainstorming may be stimulated by prompts or by one-on-one and one-on-many interview techniques	Low	Low	Low	No
Delphi technique	A means of combining expert opinions that may support the source and influence identification, probability and consequence estimation and risk evaluation. It is a collaborative technique for building consensus among experts. Involving independent analysis and voting by experts	Medium	Medium	Medium	No
SWIFT Structured "what-if")	A system for prompting a team to identify risks. Normally used within a facilitated workshop. Normally linked to a risk analysis and evaluation technique	Medium	Medium	Any	No
Human reliability analysis (HRA)	Human reliability assessment (HRA) deals with the impact of humans on system performance and can be used to evaluate human error influences on the system	Medium	Medium	Medium	Yes
SCENARIO ANALYSIS					
Root cause analysis (single loss analysis)	A single loss that has occurred is analysed in order to understand contributory causes and how the system or process can be improved to avoid such future losses. The analysis shall consider what controls were in place at the time the loss occurred and how controls might be improved	Medium	Low	Medium	No

Type of risk assessment technique	Description	Relevance of influencing factors			Can provide Quantitative output
		Resources and capability	Nature and degree of uncertainty	Complexity	
Scenario analysis	Possible future scenarios are identified through imagination or extrapolation from the present and different risks considered assuming each of these scenarios might occur. This can be done formally or informally qualitatively or quantitatively	Medium	High	Medium	No
Toxicological risk assessment	Hazards are identified and analysed and possible pathways by which a specified target might be exposed to the hazard are identified. Information on the level of exposure and the nature of harm caused by a given level of exposure are combined to give a measure of the probability that the specified harm will occur	High	High	Medium	Yes
Business impact analysis	Provides an analysis of how key disruption risks could affect an organization's operations and identifies and quantifies the capabilities that would be required to manage it	Medium	Medium	Medium	No
Fault tree analysis	A technique which starts with the undesired event (top event) and determines all the ways in which it could occur. These are displayed graphically in a logical tree diagram. Once the fault tree has been developed, consideration should be given to ways of reducing or eliminating potential causes / sources	High	High	Medium	Yes
Event tree analysis	Using inductive reasoning to translate probabilities of different initiating events into possible outcomes	Medium	Medium	Medium	Yes
Cause/ consequence analysis	A combination of fault and event tree analysis that allows inclusion of time delays. Both causes and consequences of an initiating event are considered	High	Medium	High	Yes
Cause-and-effect analysis	An effect can have a number of contributory factors which may be grouped into different categories. Contributory factors are identified often through brainstorming and displayed in a tree structure or fishbone diagram	Low	Low	Medium	No

Example type of risk assessment method and technique	Description	Relevance of influencing factors			Quantitative output possible?
FUNCTION ANALYSIS					
FMEA and FMECA	FMEA (Failure Mode and Effect Analysis) is a technique which identifies failure modes and mechanisms, and their effects. There are several types of FMEA: Design (or product) FMEA which is used for components and products, System FMEA which is used for systems, Process FMEA which is used for manufacturing and assembly processes, Service FMEA and Software FMEA. FMEA may be followed by a criticality analysis which defines the significance of each failure mode, qualitatively, semi-qualitatively, or quantitatively (FMECA). The criticality analysis may be based on the probability that the failure mode will result in system failure, or the level of risk associated with the failure mode, or a risk priority number	Medium	Medium	Medium	Yes
Reliability-centred maintenance	A method to identify the policies that should be implemented to manage failures so as to efficiently and effectively achieve the required safety, availability and economy of operation for all types of equipment	Medium	Medium	Medium	Yes
Sneak analysis (Sneak circuit analysis)	A methodology for identifying design errors. A sneak condition is a latent hardware, software, or integrated condition that may cause an unwanted event to occur or may inhibit a desired event and is not caused by component failure. These conditions are characterized by their random nature and ability to escape detection during the most rigorous of standardized system tests. Sneak conditions can cause improper operation, loss of system availability, program delays, or even death or injury to personnel	Medium	Medium	Medium	No
HAZOP Hazard and operability studies	A general process of risk identification to define possible deviations from the expected or intended performance. It uses a guideword based system. The criticalities of the deviations are assessed	Medium	High	High	No
HACCP Hazard analysis and critical control points	A systematic, proactive, and preventive system for assuring product quality, reliability and safety of processes by measuring and monitoring specific characteristics which are required to be within defined limits	Medium	Medium	Medium	No

Example type of risk assessment method and technique	Description	Relevance of influencing factors			Quantitative output possible?
CONTROLS ASSESSMENT					
LOPA (Layers of protection analysis	(May also be called barrier analysis). It allows controls and their effectiveness to be evaluated	Medium	Medium	Medium	Yes
Bow tie analysis	A simple diagrammatic way of describing and analysing the pathways of a risk from hazards to outcomes and reviewing controls. It can be considered to be a combination of the logic of a fault tree analysing the cause of an event (represented by the knot of a bow tie) and an event tree analysing the consequences	Medium	High	Medium	Yes
STATISTICAL METHODS					
Markov analysis	Markov analysis, sometimes called *State-space* analysis, is commonly used in the analysis of repairable complex systems that can exist in multiple states, including various degraded states	High	Low	High	Yes
Monte-Carlo analysis	Monte Carlo simulation is used to establish the aggregate variation in a system resulting from variations in the system, for a number of inputs, where each input has a defined distribution and the inputs are related to the output via defined relationships. The analysis can be used for a specific model where the interactions of the various inputs can be mathematically defined. The inputs can be based upon a variety of distribution types according to the nature of the uncertainty they are intended to represent. For risk assessment, triangular distributions or beta distributions are commonly used	High	Low	High	Yes
Bayesian analysis	A statistical procedure which utilizes prior distribution data to assess the probability of the result. Bayesian analysis depends upon the accuracy of the prior distribution to deduce an accurate result. Bayesian belief networks model cause-and-effect in a variety of domains by capturing probabilistic relationships of variable inputs to derive a result	High	Low	High	Yes

Annex B
(informative)

Risk assessment techniques

B.1 Brainstorming

B.1.1 Overview

Brainstorming involves stimulating and encouraging free-flowing conversation amongst a group of knowledgeable people to identify potential failure modes and associated hazards, risks, criteria for decisions and/or options for treatment. The term “brainstorming” is often used very loosely to mean any type of group discussion. However true brainstorming involves particular techniques to try to ensure that people's imagination is triggered by the thoughts and statements of others in the group.

Effective facilitation is very important in this technique and includes stimulation of the discussion at kick-off, periodic prompting of the group into other relevant areas and capture of the issues arising from the discussion (which is usually quite lively).

B.1.2 Use

Brainstorming can be used in conjunction with other risk assessment methods described below or may stand alone as a technique to encourage imaginative thinking at any stage of the risk management process and any stage of the life cycle of a system. It may be used for high-level discussions where issues are identified, for more detailed review or at a detailed level for particular problems.

Brainstorming places a heavy emphasis on imagination. It is therefore particularly useful when identifying risks of new technology, where there is no data or where novel solutions to problems are needed.

B.1.3 Inputs

A team of people with knowledge of the organization, system, process or application being assessed.

B.1.4 Process

Brainstorming may be formal or informal. Formal brainstorming is more structured with participants prepared in advance and the session has a defined purpose and outcome with a means of evaluating ideas put forward. Informal brainstorming is less structured and often more ad-hoc.

In a formal process:

- the facilitator prepares thinking prompts and triggers appropriate to the context prior to the session;
- objectives of the session are defined and rules explained;
- the facilitator starts off a train of thought and everyone explores ideas identifying as many issues as possible There is no discussion at this point about whether things should or should not be in a list or what is meant by particular statements because this tends to inhibit free-flowing thought. All input is accepted and none is criticized and the group moves on quickly to allow ideas to trigger lateral thinking;

- the facilitator may set people off on a new track when one direction of thought is exhausted or discussion deviates too far. The idea however, is to collect as many diverse ideas as possible for later analysis.

B.1.5 Outputs

Outputs depend on the stage of the risk management process at which it is applied, for example at the identification stage, outputs might be a list of risks and current controls.

B.1.6 Strengths and limitations

Strengths of brainstorming include:

- it encourages imagination which helps identify new risks and novel solutions;
- it involves key stakeholders and hence aids communication overall;
- it is relatively quick and easy to set up.

Limitations include:

- participants may lack the skill and knowledge to be effective contributors;
- since it is relatively unstructured, it is difficult to demonstrate that the process has been comprehensive, e.g. that all potential risks have been identified;
- there may be particular group dynamics where some people with valuable ideas stay quiet while others dominate the discussion. This can be overcome by computer brainstorming, using a chat forum or nominal group technique. Computer brainstorming can be set up to be anonymous, thus avoiding personal and political issues which may impede free flow of ideas. In nominal group technique ideas are submitted anonymously to a moderator and are then discussed by the group.

B.2 Structured or semi-structured interviews

B.2.1 Overview

In a structured interview, individual interviewees are asked a set of prepared questions from a prompting sheet which encourages the interviewee to view a situation from a different perspective and thus identify risks from that perspective. A semi-structured interview is similar, but allows more freedom for a conversation to explore issues which arise.

B.2.2 Use

Structured and semi-structured interviews are useful where it is difficult to get people together for a brainstorming session or where free-flowing discussion in a group is not appropriate for the situation or people involved. They are most often used to identify risks or to assess effectiveness of existing controls as part of risk analysis. They may be applied at any stage of a project or process. They are a means of providing stakeholder input to risk assessment.

B.2.3 Inputs

Inputs include:

- a clear definition of the objectives of the interviews;
- a list of interviewees selected from relevant stakeholders;
- a prepared set of questions.

B.2.4 Process

A relevant question set, is created to guide the interviewer. Questions should be open-ended where possible, should be simple, in appropriate language for the interviewee and cover one issue only. Possible follow-up questions to seek clarification are also prepared.

Questions are then posed to the person being interviewed. When seeking elaboration, questions should be open-ended. Care should be taken not to “lead” the interviewee.

Responses should be considered with a degree of flexibility in order to provide the opportunity of exploring areas into which the interviewee may wish to go.

B.2.5 Outputs

The outputs are the stakeholder’s views on the issues which are the subject of the interviews.

B.2.6 Strengths and limitations

The strengths of structured interviews are as follows :

- structured interviews allow people time for considered thought about an issue;
- one-to-one communication may allow more in-depth consideration of issues;
- structured interviews enable involvement of a larger number of stakeholders than brainstorming which uses a relatively small group.

Limitations are as follows:

- it is time-consuming for the facilitator to obtain multiple opinions in this way;
- bias is tolerated and not removed through group discussion;
- the triggering of imagination which is a feature of brainstorming may not be achieved.

B.3 Delphi technique

B.3.1 Overview

The Delphi technique is a procedure to obtain a reliable consensus of opinion from a group of experts. Although the term is often now broadly used to mean any form of brainstorming, an essential feature of the Delphi technique, as originally formulated, was that experts expressed their opinions individually and anonymously while having access to the other expert’s views as the process progresses.

B.3.2 Use

The Delphi technique can be applied at any stage of the risk management process or at any phase of a system life cycle, wherever a consensus of views of experts is needed.

B.3.3 Inputs

A set of options for which consensus is needed.

B.3.4 Process

A group of experts are questioned using a semi-structured questionnaire. The experts do not meet so their opinions are independent.

The procedure is as follows:

- formation of a team to undertake and monitor the Delphi process;

- selection of a group of experts (may be one or more panels of experts);
- development of round 1 questionnaire;
- testing the questionnaire;
- sending the questionnaire to panellists individually;
- information from the first round of responses is analysed and combined and re-circulated to panellists;
- panellists respond and the process is repeated until consensus is reached.

B.3.5 Outputs

Convergence toward consensus on the matter in hand.

B.3.6 Strengths and limitations

Strengths include:

- as views are anonymous, unpopular opinions are more likely to be expressed;
- all views have equal weight, which avoids the problem of dominating personalities;
- achieves ownership of outcomes;
- people do not need to be brought together in one place at one time.

Limitations include:

- it is labour intensive and time consuming;
- participants need to be able to express themselves clearly in writing.

B.4 Check-lists

B.4.1 Overview

Check-lists are lists of hazards, risks or control failures that have been developed usually from experience, either as a result of a previous risk assessment or as a result of past failures.

B.4.2 Use

A check-list can be used to identify hazards and risks or to assess the effectiveness of controls. They can be used at any stage of the life cycle of a product, process or system. They may be used as part of other risk assessment techniques but are most useful when applied to check that everything has been covered after a more imaginative technique that identifies new problems has been applied.

B.4.3 Inputs

Prior information and expertise on the issue, such that a relevant and preferably validated check-list can be selected or developed.

B.4.4 Process

The procedure is as follows:

- the scope of the activity is defined;
- a check-list is selected which adequately covers the scope. Check-lists need to be carefully selected for the purpose. For example a check-list of standard controls cannot be used to identify new hazards or risks;

- the person or team using the check-list steps through each element of the process or system and reviews whether items on the check-list are present.

B.4.5 Outputs

Outputs depend on the stage of the risk management process at which they are applied. For example output may be a list of controls which are inadequate or a list of risks.

B.4.6 Strengths and limitations

Strengths of check-lists include:

- they may be used by non experts;
- when well designed, they combine wide ranging expertise into an easy to use system;
- they can help ensure common problems are not forgotten.

Limitations include:

- they tend to inhibit imagination in the identification of risks;
- they address the ‘known known’s’, not the ‘known unknown’s or the ‘unknown unknowns’.
- they encourage ‘tick the box’ type behaviour;
- they tend to be observation based, so miss problems that are not readily seen.

B.5 Preliminary hazard analysis (PHA)

B.5.1 Overview

PHA is a simple, inductive method of analysis whose objective is to identify the hazards and hazardous situations and events that can cause harm for a given activity, facility or system.

B.5.2 Use

It is most commonly carried out early in the development of a project when there is little information on design details or operating procedures and can often be a precursor to further studies or to provide information for specification of the design of a system. It can also be useful when analysing existing systems for prioritizing hazards and risks for further analysis or where circumstances prevent a more extensive technique from being used.

B.5.3 Inputs

Inputs include:

- information on the system to be assessed;
- such details of the design of the system as are available and relevant.

B.5.4 Process

A list of hazards and generic hazardous situations and risks is formulated by considering characteristics such as:

- materials used or produced and their reactivity;
- equipment employed;
- operating environment;
- layout;
- interfaces among system components, etc.

Qualitative analysis of consequences of an unwanted event and their probabilities may be carried out to identify risks for further assessment.

PHA should be updated during the phases of design, construction and testing in order to detect any new hazards and make corrections, if necessary. The results obtained may be presented in different ways such as tables and trees.

B.5.5 Outputs

Outputs include:

- a list of hazards and risks;
- recommendations in the form of acceptance, recommended controls, design specification or requests for more detailed assessment.

B.5.6 Strengths and limitations

Strengths include:

- that it is able to be used when there is limited information;
- it allows risks to be considered very early in the system lifecycle.

Limitations include:

- a PHA provides only preliminary information; it is not comprehensive, neither does it provide detailed information on risks and how they can best be prevented.

B.6 HAZOP

B.6.1 Overview

HAZOP is the acronym for **HA**Zard and **OP**erability study and, is a structured and systematic examination of a planned or existing product, process, procedure or system. It is a technique to identify risks to people, equipment, environment and/or organizational objectives. The study team is also expected, where possible, to provide a solution for treating the risk.

The HAZOP process is a qualitative technique based on use of guide words which question how the design intention or operating conditions might not be achieved at each step in the design, process, procedure or system. It is generally carried out by a multi-disciplinary team during a set of meetings.

HAZOP is similar to FMEA in that it identifies failure modes of a process, system or procedure their causes and consequences. It differs in that the team considers unwanted outcomes and deviations from intended outcomes and conditions and works back to possible causes and failure modes, whereas FMEA starts by identifying failure modes.

B.6.2 Use

The HAZOP technique was initially developed to analyse chemical process systems, but has been extended to other types of systems and complex operations. These include mechanical and electronic systems, procedures, and software systems, and even to organizational changes and to legal contract design and review.

The HAZOP process can deal with all forms of deviation from design intent due to deficiencies in the design, component(s), planned procedures and human actions.

It is widely used for software design review. When applied to safety critical instrument control and computer systems it may be known as CHAZOP (**C**ontrol **HA**zards and **OP**erability Analysis or computer hazard and operability analysis).

A HAZOP study is usually undertaken at the detail design stage, when a full diagram of the intended process is available, but while design changes are still practicable. It may however, be carried out in a phased approach with different guidewords for each stage as a design develops in detail. A HAZOP study may also be carried out during operation but required changes can be costly at that stage.

B.6.3 Inputs

Essential inputs to a HAZOP study include current information about the system, the process or procedure to be reviewed and the intention and performance specifications of the design. The inputs may include: drawings, specification sheets, flow sheets, process control and logic diagrams, layout drawings, operating and maintenance procedures, and emergency response procedures. For non-hardware related HAZOP the inputs can be any document that describes functions and elements of the system or procedure under study. For example, inputs can be organizational diagrams and role descriptions, a draft contract or even a draft procedure.

B.6.4 Process

HAZOP takes the “design” and specification of the process, procedure or system being studied and reviews each part of it to discover what deviations from the intended performance can occur, what are the potential causes and what are the likely consequences of a deviation. This is achieved by systematically examining how each part of the system, process or procedure will respond to changes in key parameters by using suitable guidewords. Guidewords can be customized to a particular system, process or procedure or generic words can be used that encompass all types of deviation. Table B.1 provides examples of commonly used guidewords for technical systems. Similar guidewords such as ‘too early’, ‘too late’, ‘too much’, ‘too little’, ‘too long’, ‘too short’, ‘wrong direction’, on ‘wrong object’, ‘wrong action’ can be used to identify human error modes.

The normal steps in a HAZOP study include:

- nomination of a person with the necessary responsibility and authority to conduct the HAZOP study and to ensure that any actions arising from the study are completed;
- definition of the objectives and scope of the study;
- establishing a set of key or guidewords for the study;
- defining a HAZOP study team; this team is usually multidisciplinary and should include design and operations personnel with appropriate technical expertise to evaluate the effects of deviations from intended or current design. It is recommended that the team include persons not directly involved in the design or the system, process or procedure under review;
- collection of the required documentation.

Within a facilitated workshop with the study team:

- splitting the system, process or procedure into smaller elements or sub-systems or sub-processes or sub-elements to make the review tangible;
- agreeing the design intent for each subsystem, sub-process or sub-element and then for each item in that subsystem or element applying the guidewords one after the other to postulate possible deviations which will have undesirable outcomes;
- where an undesirable outcome is identified, agreeing the cause and consequences in each case and suggesting how they might be treated to prevent them occurring or mitigate the consequences if they do;
- documenting the discussion and agreeing specific actions to treat the risks identified.

Table B.1 – Example of possible HAZOP guidewords

Terms	Definitions
No or not	No part of the intended result is achieved or the intended condition is absent
More (higher)	Quantitative increase in output or in the operating condition
Less (lower)	Quantitative decrease
As well as	Quantitative increase (e.g. additional material)
Part of	Quantitative decrease (e.g. only one or two components in a mixture)
Reverse /opposite	Opposite (e.g. backflow)
Other than	No part of the intention is achieved, something completely different happens (e.g. flow or wrong material)
Compatibility	Material; environment
Guide words are applied to parameters such as	
	Physical properties of a material or process
	Physical conditions such as temperature, speed
	A specified intention of a component of a system or design (e.g. information transfer)
	Operational aspects

B.6.5 Outputs

Minutes of the HAZOP meeting(s) with items for each review point recorded. This should include: the guide word used, the deviation(s), possible causes, actions to address the identified problems and person responsible for the action.

For any deviation that cannot be corrected, then the risk for the deviation should be assessed.

B.6.6 Strengths and limitations

A HAZOP analysis offers the following advantages:

- it provides the means to systematically and thoroughly examine a system, process or procedure;
- it involves a multidisciplinary team including those with real-life operational experience and those who may have to carry out treatment actions;
- it generates solutions and risk treatment actions;
- it is applicable to a wide range of systems, processes and procedures;
- it allows explicit consideration of the causes and consequences of human error;
- it creates a written record of the process which can be used to demonstrate due diligence.

The limitations include:

- a detailed analysis can be very time-consuming and therefore expensive;
- a detailed analysis requires a high level of documentation or system/process and procedure specification;
- it can focus on finding detailed solutions rather than on challenging fundamental assumptions (however, this can be mitigated by a phased approach);
- the discussion can be focused on detail issues of design, and not on wider or external issues;

- it is constrained by the (draft) design and design intent, and the scope and objectives given to the team;
- the process relies heavily on the expertise of the designers who may find it difficult to be sufficiently objective to seek problems in their designs.

B.6.7 Reference document

IEC 61882, *Hazard and operability studies (HAZOP studies) – Application guide*

B.7 Hazard analysis and critical control points (HACCP)

B.7.1 Overview

Hazard analysis and critical control point (HACCP) provides a structure for identifying hazards and putting controls in place at all relevant parts of a process to protect against the hazards and to maintain the quality reliability and safety of a product. HACCP aims to ensure that risks are minimized by controls throughout the process rather than through inspection of the end product.

B.7.2 Use

HACCP was developed to ensure food quality for the NASA space program. It is now used by organizations operating anywhere within the food chain to control risks from physical, chemical or biological contaminants of food. It has also been extended for use in manufacture of pharmaceuticals and to medical devices. The principle of identifying things which can influence product quality, and defining points in a process where critical parameters can be monitored and hazards controlled, can be generalized to other technical systems.

B.7.3 Inputs

HACCP starts from a basic flow diagram or process diagram and information on hazards which might affect the quality, safety or reliability of the product or process output. Information on the hazards and their risks and ways in which they can be controlled is an input to HACCP.

B.7.4 Process

HACCP consists of the following seven principles:

- identifies hazards and preventive measures related to such hazards;
- determines the points in the process where the hazards can be controlled or eliminated (the critical control points or CCPs);
- establishes critical limits needed to control the hazards, i.e. each CCP should operate within specific parameters to ensure the hazard is controlled;
- monitors the critical limits for each CCP at defined intervals;
- establishes corrective actions if the process falls outside established limits;
- establishes verification procedures;
- implements record keeping and documentation procedures for each step.

B.7.5 Outputs

Documented records including a hazard analysis worksheet and a HACCP **plan**.

The hazard analysis worksheet lists for each step of the process:

- hazards which could be introduced, controlled or exacerbated at this step;

- whether the hazards present a significant risk (based on consideration of consequence and probability from a combination of experience, data and technical literature);
- a justification for the significance;
- possible preventative measures for each hazard;
- whether monitoring or control measures can be applied at this step (i.e. is it a CCP?).

The HACCP plan delineates the procedures to be followed to assure the control of a specific design, product, process or procedure. The plan includes a list of all CCPs and for each CCP:

- the critical limits for preventative measures;
- monitoring and continuing control activities (including what, how, and when monitoring will be carried out and by whom);
- corrective actions required if deviations from critical limits are detected;
- verification and record-keeping activities.

B.7.6 Strengths and limitations

Strengths include:

- a structured process that provides documented evidence for quality control as well as identifying and reducing risks;
- a focus on the practicalities of how and where, in a process, hazards can be prevented and risks controlled;
- better risk control throughout the process rather than relying on final product inspection;
- an ability to identify hazards introduced through human actions and how these can be controlled at the point of introduction or subsequently.

Limitations include:

- HACCP requires that hazards are identified, the risks they represent defined, and their significance understood as inputs to the process. Appropriate controls also need to be defined. These are required in order to specify critical control points and control parameters during HACCP and may need to be combined with other tools to achieve this;
- taking action when control parameters exceed defined limits may miss gradual changes in control parameters which are statistically significant and hence should be actioned.

B.7.7 Reference document

ISO 22000, *Food safety management systems – Requirements for any organization in the food chain*

B.8 Toxicity assessment

B.8.1 Overview

Environmental risk assessment is used here to cover the process followed in assessing risks to plants, animals and humans as a result of exposure to a range of environmental hazards. Risk management refers to decision-making steps including risk evaluation and risk treatment.

The method involves analysing the hazard or source of harm and how it affects the target population, and the pathways by which the hazard can reach a susceptible target population. This information is then combined to give an estimate of the likely extent and nature of harm.

B.8.2 Use

The process is used to assess risks to plants, animals and humans as a result of exposure to hazards such as chemicals, micro-organisms or other species.

Aspects of the methodology, such as pathway analysis which explore different routes by which a target might be exposed to a source of risk, can be adapted and used across a very wide range of different risk areas, outside human health and the environment, and is useful in identifying treatments to reduce risk.

B.8.3 Inputs

The method requires good data on the nature and properties of hazards, the susceptibilities of the target population (or populations) and the way in which the two interact. This data is normally based on research which may be laboratory based or epidemiological.

B.8.4 Process

The procedure is as follows:

a) Problem formulation – this includes setting the scope of the assessment by defining the range of target populations and hazard types of interest;

b) Hazard identification – this involves identifying all possible sources of harm to the target population from hazards within the scope of the study. Hazard identification normally relies on expert knowledge and a review of literature;

c) Hazard analysis – this involves understanding the nature of the hazard and how it interacts with the target. For example, in considering human exposure to chemical effects, the hazard might include acute and chronic toxicity, the potential to damage DNA, or the potential to cause cancer or birth defects. For each hazardous effect, the magnitude of the effect (the response) is compared to the amount of hazard to which the target is exposed (the dose) and, wherever possible, the mechanism by which the effect is produced is determined. The levels at which there is No Observable Effect (NOEL) and no Observable Adverse Effect (NOAEL) are noted. These are sometimes used as criteria for acceptability of the risk.

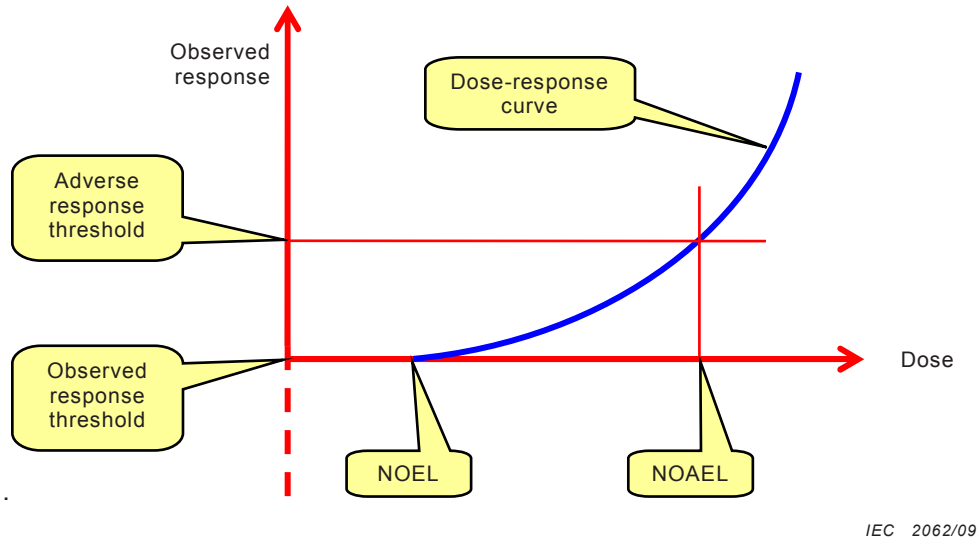


Figure B.1 – Dose-response curve

For chemical exposure, test results are used to derive dose-response curves such as that shown schematically in Figure B.1. These are usually derived from tests on animals or from experimental systems such as cultured tissues or cells.

Effects of other hazards such as micro-organisms or introduced species may be determined from field data and epidemiological studies. The nature of the interaction of diseases or pests with the target is determined and the probability that a particular level of harm from a particular exposure to the hazard is estimated.

d) Exposure analysis – this step examines how a hazardous substance or its residues might reach a susceptible target population and in what amount. It often involves a pathway analysis which considers the different routes the hazard might take, the barriers which might prevent it from reaching the target and the factors that might influence the level of exposure. For example, in considering the risk from chemical spraying the exposure analysis would consider how much chemical was sprayed, in what way and under what conditions, whether there was any direct exposure of humans or animals, how much might be left as residue on plant life, the environmental fate of pesticides reaching the ground, whether it can accumulate in animals or whether it enters groundwater. In bio security, the pathway analysis might consider how any pests entering the country might enter the environment, become established and spread.

e) Risk characterization – in this step, the information from the hazard analysis and the exposure analysis are brought together to estimate the probabilities of particular consequences when effects from all pathways are combined. Where there are large numbers of hazards or pathways, an initial screening may be carried out and the detailed hazard and exposure analysis and risk characterization carried out on the higher risk scenarios.

B.8.5 Outputs

The output is normally an indication of the level of risk from exposure of a particular target to a particular hazard in the context concerned. The risk may be expressed quantitatively semi-quantitatively or qualitatively. For example, the risk of cancer is often expressed quantitatively as the probability, that a person will develop cancer over a specified period given a specified exposure to a contaminant. Semi-quantitative analysis may be used to derive a risk index for a particular contaminant or pest and qualitative output may be a level of risk (e.g. high, medium, low) or a description with practical data of likely effects.

B.8.6 Strengths and limitations

The strength of this analysis is that it provides a very detailed understanding of the nature of the problem and the factors which increase risk.

Pathway analysis is a useful tool, generally, for all areas of risk and permits the identification of how and where it may be possible to improve controls or introduce new ones.

It does, however, need good data which is often not available or has a high level of uncertainty associated with it. For example, dose response curves derived from exposing animals to high levels of a hazard should be extrapolated to estimate the effects of very low levels of the contaminants to humans and there are multiple models by which this is achieved. Where the target is the environment rather than humans and the hazard is not chemical, data which is directly relevant to the particular conditions of the study may be limited.

B.9 Structured “What-if” Technique (SWIFT)

B.9.1 Overview

SWIFT was originally developed as a simpler alternative to HAZOP. It is a systematic, team-based study, utilizing a set of ‘prompt’ words or phrases that is used by the facilitator within a workshop to stimulate participants to identify risks. The facilitator and team use standard ‘what-if’ type phrases in combination with the prompts to investigate how a system, plant item,

organization or procedure will be affected by deviations from normal operations and behaviour. SWIFT is normally applied at more of a systems level with a lower level of detail than HAZOP.

B.9.2 Use

While SWIFT was originally designed for chemical and petrochemical plant hazard study, the technique is now widely applied to systems, plant items, procedures, organizations generally. In particular it is used to examine the consequences of changes and the risks thereby altered or created.

B.9.3 Inputs

The system, procedure, plant item and/or change has to be carefully defined before the study can commence. Both the external and internal contexts are established through interviews and through the study of documents, plans and drawings by the facilitator. Normally, the item, situation or system for study is split into nodes or key elements to facilitate the analysis process but this rarely occurs at the level of definition required for HAZOP.

Another key input is the expertise and experience present in the study team which should be carefully selected. All stakeholders should be represented if possible together with those with experience of similar items, systems, changes or situations.

B.9.4 Process

The general process is as follows:

a) Before the study commences, the facilitator prepares a suitable prompt list of words or phrases that may be based on a standard set or be created to enable a comprehensive review of hazards or risks.

b) At the workshop the external and internal context of the item, system, change or situation and the scope of the study are discussed and agreed.

c) The facilitator asks the participants to raise and discuss:
   - known risks and hazards;
   - previous experience and incidents;
   - known and existing controls and safeguards;
   - regulatory requirements and constraints.

d) Discussion is facilitated by creating a question using a ‘what-if’ phrase and a prompt word or subject. The ‘what-if’ phrases to be used are “what if…”, “what would happen if…”, “could someone or something…”, “has anyone or anything ever….” The intent is to stimulate the study team into exploring potential scenarios, their causes and consequences and impacts.

e) Risks are summarized and the team considers controls in place.

f) The description of the risk, its causes, consequences and expected controls are confirmed with the team and recorded.

g) The team considers whether the controls are adequate and effective and agree a statement of risk control effectiveness. If this is less than satisfactory, the team further considers risk treatment tasks and potential controls are defined.

h) During this discussion further ‘what-if’ questions are posed to identify further risks.

i) The facilitator uses the prompt list to monitor the discussion and to suggest additional issues and scenarios for the team to discuss.

j) It is normal to use a qualitative or semi-quantitative risk assessment method to rank the actions created in terms of priority. This risk assessment is normally conducted by taking into account the existing controls and their effectiveness.

B.9.5 Outputs

Outputs include a risk register with risk-ranked actions or tasks. These tasks can then become the basis for a treatment plan.

B.9.6 Strengths and limitations

Strengths of SWIFT:

- it is widely applicable to all forms of physical plant or system, situation or circumstance, organization or activity;
- it needs minimal preparation by the team;
- it is relatively rapid and the major hazards and risks quickly become apparent within the workshop session;
- the study is 'systems orientated' and allows participants to look at the system response to deviations rather than just examining the consequences of component failure;
- it can be used to identify opportunities for improvement of processes and systems and generally can be used to identify actions that lead to and enhance their probabilities of success;
- involvement in the workshop by those who are accountable for existing controls and for further risk treatment actions, reinforces their responsibility;
- it creates a risk register and risk treatment plan with little more effort;
- while often a qualitative or semi-quantitative form of risk rating is used for risk assessment and to prioritize attention on the resulting actions, SWIFT can be used to identify risks and hazards that can be taken forward into a quantitative study.

Limitations of SWIFT:

- it needs an experienced and capable facilitator to be efficient;
- careful preparation is needed so that the workshop team's time is not wasted;
- if the workshop team does not have a wide enough experience base or if the prompt system is not comprehensive, some risks or hazards may not be identified;
- the high-level application of the technique may not reveal complex, detailed or correlated causes.

B.10 Scenario analysis

B.10.1 Overview

Scenario analysis is a name given to the development of descriptive models of how the future might turn out. It can be used to identify risks by considering possible future developments and exploring their implications. Sets of scenarios reflecting (for example) 'best case', 'worst case' and 'expected case' may be used to analyse potential consequences and their probabilities for each scenario as a form of sensitivity analysis when analysing risk.

The power of scenario analysis is illustrated by considering major shifts over the past 50 years in technology, consumer preferences, social attitudes, etc. Scenario analysis cannot predict the probabilities of such changes but can consider consequences and help organizations develop strengths and the resilience needed to adapt to foreseeable changes.

B.10.2 Use

Scenario analysis can be used to assist in making policy decisions and planning future strategies as well as to consider existing activities. It can play a part in all three components of risk assessment. For identification and analysis, sets of scenarios reflecting (for example) best case, worst case and 'expected' case may be used to identify what might happen under

particular circumstances and analyse potential consequences and their probabilities for each scenario.

Scenario analysis may be used to anticipate how both threats and opportunities might develop and may be used for all types of risk with both short and long term time frames. With short time frames and good data, likely scenarios may be extrapolated from the present. For longer time frames or with weak data, scenario analysis becomes more imaginative and may be referred to as futures analysis.

Scenario analysis may be useful where there are strong distributional differences between positive outcomes and negative outcomes in space, time and groups in the community or an organization.

B.10.3 Inputs

The prerequisite for a scenario analysis is a team of people who between them have an understanding of the nature of relevant changes (for example possible advances in technology) and imagination to think into the future without necessarily extrapolating from the past. Access to literature and data about changes already occurring is also useful.

B.10.4 Process

The structure for scenario analysis may be informal or formal.

Having established a team and relevant communication channels, and defined the context of the problem and issues to be considered, the next step is to identify the nature of changes that might occur. This will need research into the major trends and the probable timing of changes in trends as well as imaginative thinking about the future.

Changes to be considered may include:

- external changes (such as technological changes);
- decisions that need to be made in the near future but which may have a variety of outcomes;
- stakeholder needs and how they might change;
- changes in the macro environment (regulatory, demographics, etc). Some will be inevitable and some will be uncertain.

Sometimes, a change may be due to the consequences of another risk. For example, the risk of climate change is resulting in changes in consumer demand related to food miles. This will influence which foods can be profitably exported as well as which foods can be grown locally.

The local and macro factors or trends can now be listed and ranked for (1) importance (2) uncertainty. Special attention is paid to the factors that are most important and most uncertain. Key factors or trends are mapped against each other to show areas where scenarios can be developed.

A series of scenarios is proposed with each one focussing on a plausible change in parameters.

A “story” is then written for each scenario that tells how you might move from here towards the subject scenario. The stories may include plausible details that add value to the scenarios.

The scenarios can then be used to test or evaluate the original question. The test takes into account any significant but predictable factors (e.g. use patterns), and then explores how ‘successful’ the policy (activity) would be in this new scenario, and ‘pre-tests’ outcomes by using ‘what if’ questions based on model assumptions.

When the question or proposal has been evaluated with respect to each scenario, it may be obvious that it needs to be modified to make it more robust or less risky. It should also be possible to identify some leading indicators that show when change is occurring. Monitoring and responding to leading indicators can provide opportunity for change in planned strategies.

Since scenarios are only defined 'slices' of possible futures, it is important to make sure that account is taken of the probability of a particular outcome (scenario) occurring, i.e. to adopt a risk framework. For example, where best case, worst case and expected case scenarios are used, some attempt should be made to qualify, or express the probability of each scenario occurring.

B.10.5 Outputs

There may be no best-fit scenario but one should end with a clearer perception of the range of options and how to modify the chosen course of action as indicators move.

B.10.6 Strengths and limitations

Scenario analysis takes account of a range of possible futures which may be preferable to the traditional approach of relying on high-medium-low forecasts that assume, through the use of historical data, that future events will probably continue to follow past trends. This is important for situations where there is little current knowledge on which to base predictions or where risks are being considered in the longer term future.

This strength however has an associated weakness which is that where there is high uncertainty some of the scenarios may be unrealistic.

The main difficulties in using scenario analysis are associated with the availability of data, and the ability of the analysts and decision makers to be able to develop realistic scenarios that are amenable to probing of possible outcomes.

The dangers of using scenario analysis as a decision-making tool are that the scenarios used may not have an adequate foundation; that data may be speculative; and that unrealistic results may not be recognized as such.

B.11 Business impact analysis (BIA)

B.11.1 Overview

Business impact analysis, also known as business impact assessment, analyses how key disruption risks could affect an organization's operations and identifies and quantifies the capabilities that would be needed to manage it. Specifically, a BIA provides an agreed understanding of:

- the identification and criticality of key business processes, functions and associated resources and the key interdependencies that exist for an organization;
- how disruptive events will affect the capacity and capability of achieving critical business objectives;
- the capacity and capability needed to manage the impact of a disruption and recover the organization to agreed levels of operation.

B.11.2 Use

BIA is used to determine the criticality and recovery timeframes of processes and associated resources (people, equipment, information technology) to ensure the continued achievement of objectives. Additionally, the BIA assists in determining interdependencies and interrelationships between processes, internal and external parties and any supply chain linkages.

B.11.3 Inputs

Inputs include:

- a team to undertake the analysis and develop a plan;
- information concerning the objectives, environment, operations and interdependencies of the organization;
- details on the activities and operations of the organization, including processes, supporting resources, relationships with other organizations, outsourced arrangements, stakeholders;
- financial and operational consequences of loss of critical processes;
- prepared questionnaire;
- list of interviewees from relevant areas of the organization and/or stakeholders that will be contacted.

B.11.4 Process

A BIA can be undertaken using questionnaires, interviews, structured workshops or combinations of all three, to obtain an understanding of the critical processes, the effects of the loss of those processes and the required recovery timeframes and supporting resources.

The key steps include:

- based on the risk and vulnerability assessment, confirmation of the key processes and outputs of the organization to determine the criticality of the processes;
- determination of the consequences of a disruption on the identified critical processes in financial and/or operational terms, over defined periods;
- identification of the interdependencies with key internal and external stakeholders. This could include mapping the nature of the interdependencies through the supply chain;
- determination of the current available resources and the essential level of resources needed to continue to operate at a minimum acceptable level following a disruption;
- identification of alternate workarounds and processes currently in use or planned to be developed. Alternate workarounds and processes may need to be developed where resources or capability are inaccessible or insufficient during the disruption;
- determination of the maximum acceptable outage time (MAO) for each process based on the identified consequences and the critical success factors for the function. The MAO represents the maximum period of time the organization can tolerate the loss of capability;
- determination of the recovery time objective(s) (RTO) for any specialized equipment or information technology. The RTO represents the time within which the organization aims to recover the specialized equipment or information technology capability;
- confirmation of the current level of preparedness of the critical processes to manage a disruption. This may include evaluating the level of redundancy within the process (e.g. spare equipment) or the existence of alternate suppliers.

B.11.5 Outputs

The outputs are as follows:

- a priority list of critical processes and associated interdependencies;
- documented financial and operational impacts from a loss of the critical processes;
- supporting resources needed for the identified critical processes;
- outage time frames for the critical process and the associated information technology recovery time frames.

B.11.6 Strengths and limitations

Strengths of the BIA include:

- an understanding of the critical processes that provide the organization with the ability to continue to achieve their stated objectives;
- an understanding of the required resources;
- an opportunity to redefine the operational process of an organization to assist in the resilience of the organization.

Limitations include:

- lack of knowledge by the participants involved in completing questionnaires, undertaking interviews or workshops;
- group dynamics may affect the complete analysis of a critical process;
- simplistic or over-optimistic expectations of recovery requirements;
- difficulty in obtaining an adequate level of understanding of the organization's operations and activities.

B.12 Root cause analysis (RCA)

B.12.1 Overview

The analysis of a major loss to prevent its reoccurrence is commonly referred to as Root Cause Analysis (RCA), Root Cause Failure Analysis (RCFA) or loss analysis. RCA is focused on asset losses due to various types of failures while loss analysis is mainly concerned with financial or economic losses due to external factors or catastrophes. It attempts to identify the root or original causes instead of dealing only with the immediately obvious symptoms. It is recognized that corrective action may not always be entirely effective and that continuous improvement may be required. RCA is most often applied to the evaluation of a major loss but may also be used to analyse losses on a more global basis to determine where improvements can be made.

B.12.2 Use

RCA is applied in various contexts with the following broad areas of usage:

- safety-based RCA is used for accident investigations and occupational health and safety;
- failure analysis is used in technological systems related to reliability and maintenance;
- production-based RCA is applied in the field of quality control for industrial manufacturing;
- process-based RCA is focused on business processes;
- system-based RCA has developed as a combination of the previous areas to deal with complex systems with application in change management, risk management and systems analysis.

B.12.3 Inputs

The basic input to an RCA is all of the evidence gathered from the failure or loss. Data from other similar failures may also be considered in the analysis. Other inputs may be results that are carried out to test specific hypotheses.

B.12.4 Process

When the need for an RCA is identified, a group of experts is appointed to carry out the analysis and make recommendations. The type of expert will mostly be dependent on the specific expertise needed to analyse the failure.

Even though different methods can be used to perform the analysis, the basic steps in executing an RCA are similar and include:

- forming the team;
- establishing the scope and objectives of the RCA;
- gathering data and evidence from the failure or loss;
- performing a structured analysis to determine the root cause;
- developing solutions and make recommendations;
- implementing the recommendations;
- verifying the success of the implemented recommendations.

Structured analysis techniques may consist of one of the following:

- "5 whys" technique, i.e. repeatedly asking 'why?' to peel away layers of cause and sub cause);
- failure mode and effects analysis;
- fault tree analysis;
- Fishbone or Ishikawa diagrams;
- Pareto analysis;
- root cause mapping.

The evaluation of causes often progresses from initially evident physical causes to human-related causes and finally to underlying management or fundamental causes. Causal factors have to be able to be controlled or eliminated by involved parties in order for corrective action to be effective and worthwhile.

B.12.5 Outputs

The outputs from an RCA include:

- documentation of data and evidence gathered;
- hypotheses considered;
- conclusion about the most likely root causes for the failure or loss;
- recommendations for corrective action.

B.12.6 Strengths and limitations

Strengths include:

- involvement of applicable experts working in a team environment;
- structured analysis;
- consideration of all likely hypotheses;
- documentation of results;
- need to produce final recommendations.

Limitations of an RCA:

- required experts may not be available;
- critical evidence may be destroyed in the failure or removed during clean-up;
- the team may not be allowed enough time or resources to fully evaluate the situation;
- it may not be possible to adequately implement recommendations.

B.13 Failure modes and effects analysis (FMEA) and failure modes and effects and criticality analysis (FMECA)

B.13.1 Overview

Failure modes and effects analysis (FMEA) is a technique used to identify the ways in which components, systems or processes can fail to fulfil their design intent.

FMEA identifies:

- all potential failure modes of the various parts of a system (a failure mode is what is observed to fail or to perform incorrectly);
- the effects these failures may have on the system;
- the mechanisms of failure;
- how to avoid the failures, and/or mitigate the effects of the failures on the system.

FMECA extends an FMEA so that each fault mode identified is ranked according to its importance or criticality

This criticality analysis is usually qualitative or semi-quantitative but may be quantified using actual failure rates.

B.13.2 Use

There are several applications of FMEA: Design (or product) FMEA which is used for components and products, System FMEA which is used for systems, Process FMEA which is used for manufacturing and assembly processes, Service FMEA and Software FMEA.

FMEA/FMECA may be applied during the design, manufacture or operation of a physical system.

To improve dependability, however, changes are usually more easily implemented at the design stage. FMEA AND FMECA may also be applied to processes and procedures. For example, it is used to identify potential for medical error in healthcare systems and failures in maintenance procedures.

FMEA/FMECA can be used to

- assist in selecting design alternatives with high dependability,
- ensure that all failure modes of systems and processes, and their effects on operational success have been considered,
- identify human error modes and effects,
- provide a basis for planning testing and maintenance of physical systems,
- improve the design of procedures and processes,
- provide qualitative or quantitative information for analysis techniques such as fault tree analysis.

FMEA and FMECA can provide input to other analyses techniques such as fault tree analysis at either a qualitative or quantitative level.

B.13.3 Inputs

FMEA and FMECA need information about the elements of the system in sufficient detail for meaningful analysis of the ways in which each element can fail. For a detailed Design FMEA the element may be at the detailed individual component level, while for higher level Systems FMEA, elements may be defined at a higher level.

Information may include:

- drawings or a flow chart of the system being analysed and its components, or the steps of a process;
- an understanding of the function of each step of a process or component of a system;
- details of environmental and other parameters, which may affect operation;
- an understanding of the results of particular failures;
- historical information on failures including failure rate data where available.

B.13.4 Process

The FMEA process is as follows:

a) define the scope and objectives of the study;
b) assemble the team;
c) understand the system/process to be subjected to the FMECA;
d) breakdown of the system into its components or steps;
e) define the function of each step or component;
f) for every component or step listed identify:
   - how can each part conceivably fail?
   - what mechanisms might produce these modes of failure?
   - what could the effects be if the failures did occur?
   - is the failure harmless or damaging?
   - how is the failure detected?
g) identify inherent provisions in the design to compensate for the failure.

For FMECA, the study team goes on to classify each of the identified failure modes according to its criticality

There are several ways this may be done. Common methods include

- the mode criticality index,
- the level of risk,
- the risk priority number.

The model criticality is a measure of the probability that the mode being considered will result in failure of the system as a whole; it is defined as:

Failure effect probability * Mode failure rate * Operating time of the system

It is most often applied to equipment failures where each of these terms can be defined quantitatively and failure modes all have the same consequence.

The risk level is obtained by combining the consequences of a failure mode occurring with the probability of failure. It is used when consequences of different failure modes differ and can be applied to equipment systems or processes. Risk level can be expressed qualitatively, semi-quantitatively or quantitatively.

The risk priority number (RPN) is a semi-quantitative measure of criticality obtained by multiplying numbers from rating scales (usually between 1 and 10) for consequence of failure, likelihood of failure and ability to detect the problem. (A failure is given a higher priority if it is difficult to detect.) This method is used most often in quality assurance applications

Once failure modes and mechanisms are identified, corrective actions can be defined and implemented for the more significant failure modes.

FMEA is documented in a report that contains:

- details of the system that was analysed;
- the way the exercise was carried out;
- assumptions made in the analysis;
- sources of data;
- the results, including the completed worksheets;
- the criticality (if completed) and the methodology used to define it;
- any recommendations for further analyses, design changes or features to be incorporated in test plans, etc.

The system may be reassessed by another cycle of FMEA after the actions have been completed.

B.13.5 Outputs

The primary output of FMEA is a list of failure modes, the failure mechanisms and effects for each component or step of a system or process (which may include information on the likelihood of failure). Information is also given on the causes of failure and the consequences to the system as a whole. The output from FMECA includes a rating of importance based on the likelihood that the system will fail, the level of risk resulting from the failure mode or a combination of the level of risk and the 'detectability' of the failure mode.

FMECA can give a quantitative output if suitable failure rate data and quantitative consequences are used.

B.13.6 Strengths and limitations

The strengths of FMEA/FMECA are as follows:

- widely applicable to human, equipment and system failure modes and to hardware, software and procedures;
- identify component failure modes, their causes and their effects on the system, and present them in an easily readable format;
- avoid the need for costly equipment modifications in service by identifying problems early in the design process;
- identify single point failure modes and requirements for redundancy or safety systems;
- provide input to the development monitoring programmes by highlighting key features to be monitored.

Limitations include:

- they can only be used to identify single failure modes, not combinations of failure modes;
- unless adequately controlled and focussed, the studies can be time consuming and costly;
- they can be difficult and tedious for complex multi-layered systems.

B.13.7 Reference document

IEC 60812, *Analysis techniques for system reliability – Procedures for failure mode and effect analysis (FMEA)*

B.14 Fault tree analysis (FTA)

B.14.1 Overview

FTA is a technique for identifying and analysing factors that can contribute to a specified undesired event (called the “top event”). Causal factors are deductively identified, organized in a logical manner and represented pictorially in a tree diagram which depicts causal factors and their logical relationship to the top event.

The factors identified in the tree can be events that are associated with component hardware failures, human errors or any other pertinent events which lead to the undesired event.

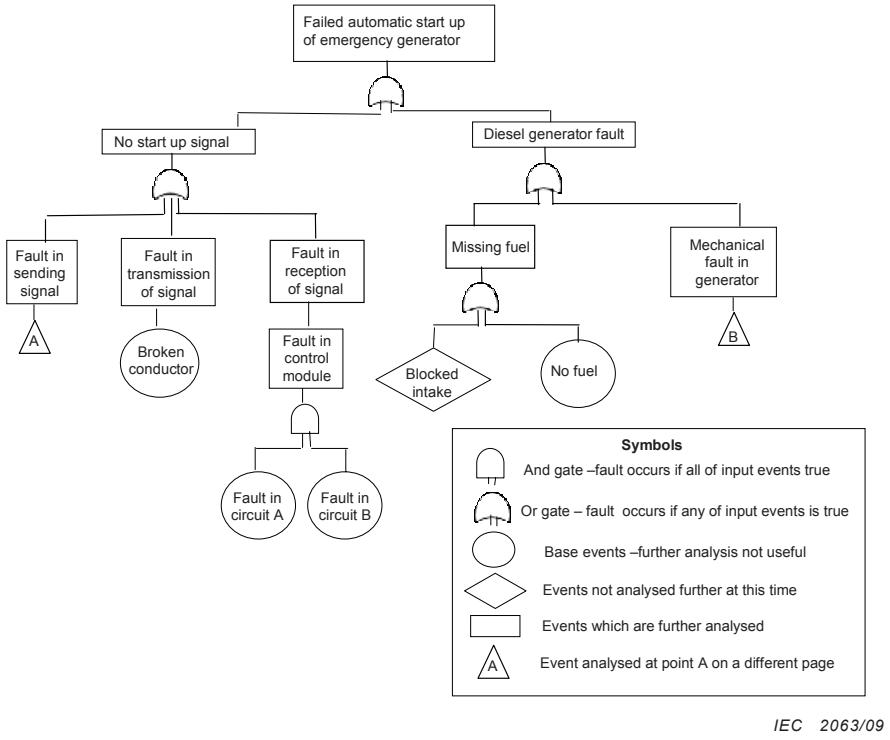


Figure B.2 – Example of an FTA from IEC 60300-3-9

B.14.2 Use

A fault tree may be used qualitatively to identify potential causes and pathways to a failure (the top event) or quantitatively to calculate the probability of the top event, given knowledge of the probabilities of causal events.

It may be used at the design stage of a system to identify potential causes of failure and hence to select between different design options. It may be used at the operating phase to identify how major failures can occur and the relative importance of different pathways to the head event. A fault tree may also be used to analyse a failure which has occurred to display diagrammatically how different events came together to cause the failure.

B.14.3 Inputs

For qualitative analysis, an understanding of the system and the causes of failure is required, as well as a technical understanding of how the system can fail. Detailed diagrams are useful to aid the analysis.

For quantitative analysis, data on failure rates or the probability of being in a failed state for all basic events in the fault tree are required.

B.14.4 Process

The steps for developing a fault tree are as follows:

- The top event to be analysed is defined. This may be a failure or maybe a broader outcome of that failure. Where the outcome is analysed, the tree may contain a section relating to mitigation of the actual failure.
- Starting with the top event, the possible immediate causes or failure modes leading to the top event are identified.
- Each of these causes/fault modes is analysed to identify how their failure could be caused.
- Stepwise identification of undesirable system operation is followed to successively lower system levels until further analysis becomes unproductive. In a hardware system this may be the component failure level. Events and causal factors at the lowest system level analysed are known as base events.
- Where probabilities can be assigned to base events the probability of the top event may be calculated. For quantification to be valid it must be able to be shown that, for each gate, all inputs are both necessary and sufficient to produce the output event. If this is not the case, the fault tree is not valid for probability analysis but may be a useful tool for displaying causal relationships.

As part of quantification the fault tree may need to be simplified using Boolean algebra to account for duplicate failure modes.

As well as providing an estimate of the probability of the head event, minimal cut sets, which form individual separate pathways to the head event, can be identified and their influence on the top event calculated.

Except for simple fault trees, a software package is needed to properly handle the calculations when repeated events are present at several places in the fault tree, and to calculate minimal cut sets. Software tools help ensure consistency, correctness and verifiability.

B.14.5 Outputs

The outputs from fault tree analysis are as follows:

- a pictorial representation of how the top event can occur which shows interacting pathways where two or more simultaneous events must occur;
- a list of minimal cut sets (individual pathways to failure) with (where data is available) the probability that each will occur;
- the probability of the top event.

B.14.6 Strengths and limitations

Strengths of FTA:

- It affords a disciplined approach which is highly systematic, but at the same time sufficiently flexible to allow analysis of a variety of factors, including human interactions and physical phenomena.
- The application of the "top-down" approach, implicit in the technique, focuses attention on those effects of failure which are directly related to the top event.
- FTA is especially useful for analysing systems with many interfaces and interactions.
- The pictorial representation leads to an easy understanding of the system behaviour and the factors included, but as the trees are often large, processing of fault trees may require computer systems. This feature enables more complex logical relationships to be included (e.g. NAND and NOR) but also makes the verification of the fault tree difficult.

- Logic analysis of the fault trees and the identification of cut sets is useful in identifying simple failure pathways in a very complex system where particular combinations of events which lead to the top event could be overlooked.

Limitations include:

- Uncertainties in the probabilities of base events are included in calculations of the probability of the top event. This can result in high levels of uncertainty where base event failure probabilities are not known accurately; however, a high degree of confidence is possible in a well understood system.
- In some situations, causal events are not bound together and it can be difficult to ascertain whether all important pathways to the top event are included. For example, including all ignition sources in an analysis of a fire as a top event. In this situation probability analysis is not possible.
- Fault tree is a static model; time interdependencies are not addressed.
- Fault trees can only deal with binary states (failed/not failed) only.
- While human error modes can be included in a qualitative fault tree, in general failures of degree or quality which often characterize human error cannot easily be included;
- A fault tree does not enable domino effects or conditional failures to be included easily.

B.14.7 Reference document

IEC 61025, *Fault tree analysis (FTA)*

IEC 60300-3-9, *Dependability management — Part 3: Application guide — Section 9: Risk analysis of technological systems*

B.15 Event tree analysis (ETA)

B.15.1 Overview

ETA is a graphical technique for representing the mutually exclusive sequences of events following an initiating event according to the functioning/not functioning of the various systems designed to mitigate its consequences (see Figure B.3). It can be applied both qualitatively and quantitatively.

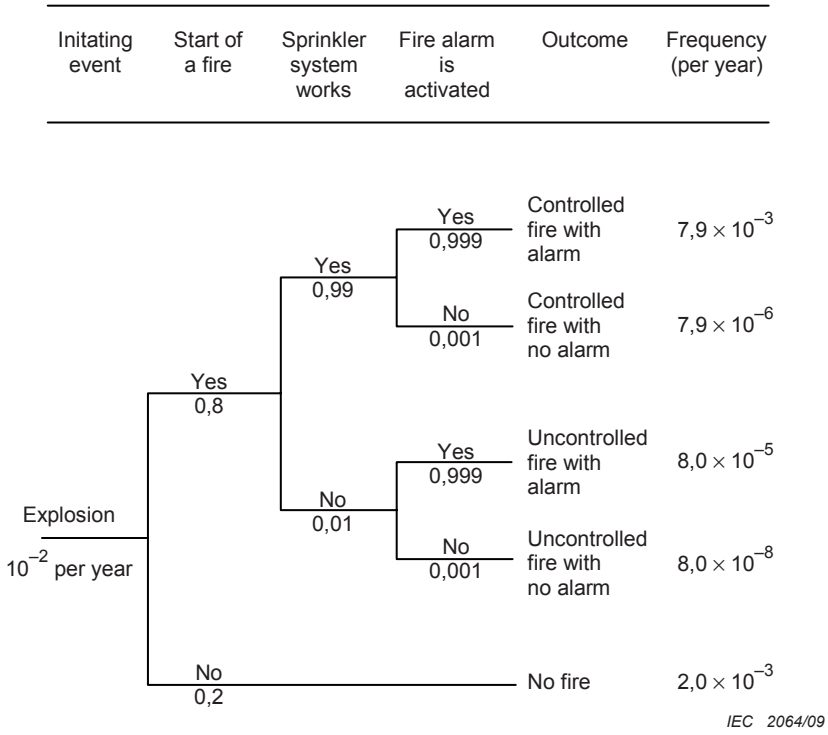


Figure B.3 – Example of an event tree

Figure B.3 shows simple calculations for a sample event tree, when branches are fully independent.

By fanning out like a tree, ETA is able to represent the aggravating or mitigating events in response to the initiating event, taking into account additional systems, functions or barriers.

B.15.2 Use

ETA can be used for modelling, calculating and ranking (from a risk point of view) different accident scenarios following the initiating event

ETA can be used at any stage in the life cycle of a product or process. It may be used qualitatively to help brainstorm potential scenarios and sequences of events following an initiating event and how outcomes are affected by various treatments, barriers or controls intended to mitigate unwanted outcomes.

The quantitative analysis lends itself to consider the acceptability of controls. It is most often used to model failures where there are multiple safeguards.

ETA can be used to model initiating events which might bring loss or gain. However, circumstances where pathways to optimize gain are sought are more often modelled using a decision tree.

B.15.3 Inputs

Inputs include:

- a list of appropriate initiating events;
- information on treatments, barriers and controls, and their failure probabilities (for quantitative analyses);
- understanding of the processes whereby an initial failure escalates.

B.15.4 Process

An event tree starts by selecting an initiating event. This may be an incident such as a dust explosion or a causal event such as a power failure. Functions or systems which are in place to mitigate outcomes are then listed in sequence. For each function or system, a line is drawn to represent their success or failure. A particular probability of failure can be assigned to each line, with this conditional probability estimated e.g. by expert judgement or a fault tree analysis. In this way, different pathways from the initiating event are modelled.

Note that the probabilities on the event tree are conditional probabilities, for example the probability of a sprinkler functioning is not the probability obtained from tests under normal conditions, but the probability of functioning under conditions of fire caused by an explosion.

Each path through the tree represents the probability that all of the events in that path will occur. Therefore, the frequency of the outcome is represented by the product of the individual conditional probabilities and the frequency of the initiation event, given that the various events are independent.

B.15.5 Outputs

Outputs from ETA include the following:

- qualitative descriptions of potential problems as combinations of events producing various types of problems (range of outcomes) from initiating events;
- quantitative estimates of event frequencies or probabilities and relative importance of various failure sequences and contributing events;
- lists of recommendations for reducing risks;
- quantitative evaluations of recommendation effectiveness.

B.15.6 Strengths and limitations

Strengths of ETA include the following:

- ETA displays potential scenarios following an initiating event, are analysed and the influence of the success or failure of mitigating systems or functions in a clear diagrammatic way;
- it accounts for timing, dependence and domino effects that are cumbersome to model in fault trees;
- it graphically represent sequences of events which are not possible to represent when using fault trees.

Limitations include:

- in order to use ETA as part of a comprehensive assessment, all potential initiating events need to be identified. This may be done by using another analysis method (e.g. HAZOP, PHA), however, there is always a potential for missing some important initiating events;
- with event trees, only success and failure states of a system are dealt with, and it is difficult to incorporate delayed success or recovery events;
- any path is conditional on the events that occurred at previous branch points along the path. Many dependencies along the possible paths are therefore addressed. However, some dependencies, such as common components, utility systems and operators, may be overlooked if not handled carefully, may lead to optimistic estimations of risk.

B.16 Cause-consequence analysis

B.16.1 General

Cause-consequence analysis is a combination of fault tree and event tree analysis. It starts from a critical event and analyses consequences by means of a combination of YES/NO logic gates which represent conditions that may occur or failures of systems designed to mitigate the consequences of the initiating event. The causes of the conditions or failures are analysed by means of fault trees (see Clause B.15)

B.16.2 Use

Cause-consequence analysis was originally developed as a reliability tool for safety critical systems to give a more complete understanding of system failures. Like fault tree analysis, it is used to represent the failure logic leading to a critical event but it adds to the functionality of a fault tree by allowing time sequential failures to be analysed. The method also allows time delays to be incorporated into the consequence analysis which is not possible with event trees.

The method is used to analyse the various paths a system could take following a critical event and depending on the behaviour of particular subsystems (such as emergency response systems). If quantified they will give an estimate of the probability of different possible consequences following a critical event.

As each sequence in a cause-consequence diagram is a combination of sub-fault trees, the cause-consequence analysis can be used as a tool to build big fault trees.

Diagrams are complex to produce and use and tend to be used when the magnitude of the potential consequence of failure justifies intensive effort.

B.16.3 Inputs

An understanding of the system and its failure modes and failure scenarios is required.

B.16.4 Process

Figure B.4 shows a conceptual diagram of a typical cause-consequence analysis.

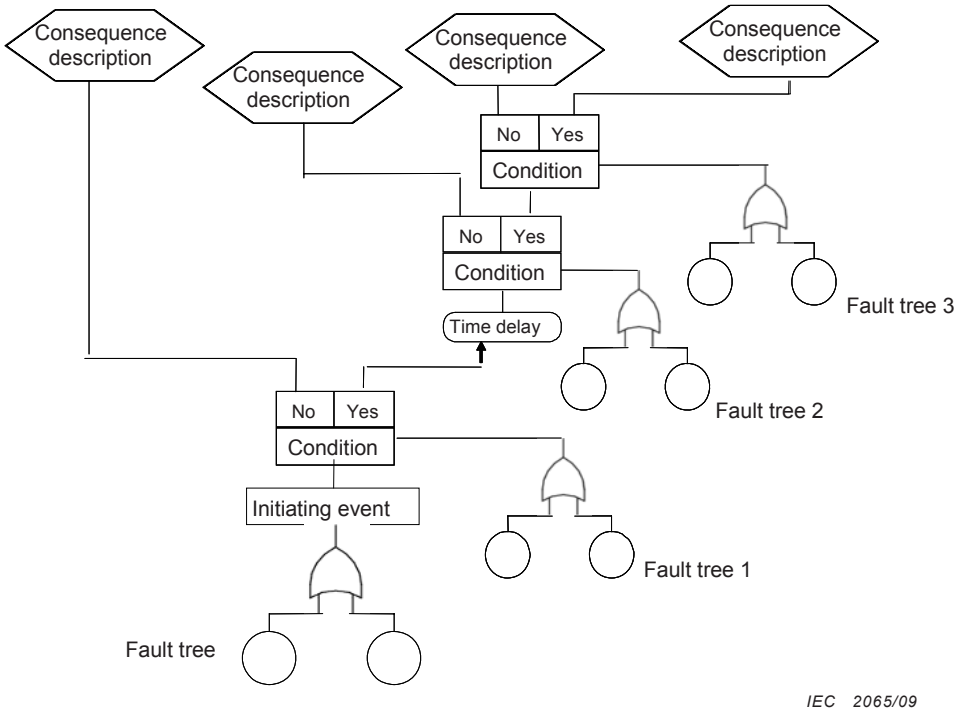


Figure B.4 – Example of cause-consequence analysis

The procedure is as follows:

a) Identify the critical (or initiating) event (equivalent to the top event of a fault tree and the initiating event of an event tree).

b) Develop and validate the fault tree for causes of the initiating event as described in Clause B.14. The same symbols are used as in conventional fault tree analysis.

c) Decide the order in which conditions are to be considered. This should be a logical sequence such as the time sequence in which they occur.

d) Construct the pathways for consequences depending on the different conditions. This is similar to an event tree but the split in pathways of the event tree is shown as a box labelled with the particular condition that applies.

e) Provided the failures for each condition box are independent, the probability of each consequence can be calculated. This is achieved by first assigning probabilities to each output of the condition box (using the relevant fault trees as appropriate) The probability of any one sequence leading to a particular consequence is obtained by multiplying the probabilities of each sequence of conditions which terminates in that particular consequence. If more than one sequence ends up with the same consequence, the probabilities from each sequence are added. If there are dependencies between failures of conditions in a sequence (for example a power failure may cause several conditions to fail) then the dependencies should be dealt with prior to calculation.

B.16.5 Output

The output of cause-consequence analysis is a diagrammatic representation of how a system may fail showing both causes and consequences. An estimation of the probability of occurrence of each potential consequence based on analysis of probabilities of occurrence of particular conditions following the critical event.

B.16.6 Strengths and limitations

The advantages of cause-consequence analysis are the same as those of event trees and fault trees combined. In addition, it overcomes some of the limitations of those techniques by

being able to analyse events that develop over time. Cause-consequence analysis provides a comprehensive view of the system.

Limitations are that it is more complex than fault tree and event tree analysis, both to construct and in the manner in which dependencies are dealt with during quantification.

B.17 Cause-and-effect analysis

B.17.1 Overview

Cause-and-effect analysis is a structured method to identify possible causes of an undesirable event or problem. It organizes the possible contributory factors into broad categories so that all possible hypotheses can be considered. It does not, however, by itself point to the actual causes, since these can only be determined by real evidence and empirical testing of hypotheses. The information is organized in either a Fishbone (also called Ishikawa) or sometimes a tree diagram (see B.17.4).

B.17.2 Use

Cause-and-effect analysis provides a structured pictorial display of a list of causes of a specific effect. The effect may be positive (an objective) or negative (a problem) depending on context.

It is used to enable consideration of all possible scenarios and causes generated by a team of experts and allows consensus to be established as to the most likely causes which can then be tested empirically or by evaluation of available data. It is most valuable at the beginning of an analysis to broaden thinking about possible causes and then to establish potential hypotheses that can be considered more formally.

Constructing a cause-and-effect diagram can be undertaken when there is need to:

- identify the possible root causes, the basic reasons, for a specific effect, problem or condition;
- sort out and relate some of the interactions among the factors affecting a particular process;
- analyse existing problems so that corrective action can be taken.

Benefits from constructing a cause-and-effect diagram include:

- concentrates review members' attention on a specific problem;
- to help determine the root causes of a problem using a structured approach;
- encourages group participation and utilizes group knowledge for the product or process;
- uses an orderly, easy-to-read format to diagram cause-and-effect relationships;
- indicates possible causes of variation in a process;
- identifies areas where data should be collected for further study.

Cause-and-effect analysis can be used as a method in performing root cause analysis (see Clause B.12).

B.17.3 Input

The input to a cause-and-effect analysis may come from expertise and experience from participants or a previously developed model that has been used in the past.

B.17.4 Process

The cause-and-effect analysis should be carried out by a team of experts knowledgeable with the problem requiring resolution.

The basic steps in performing a cause-and-effect analysis are as follows:

- establish the effect to be analysed and place it in a box. The effect may be positive (an objective) or negative (a problem) depending on the circumstances;
- determine the main categories of causes represented by boxes in the Fishbone diagram. Typically, for a system problem, the categories might be people, equipment, environment, processes, etc. However, these are chosen to fit the particular context;
- fill in the possible causes for each major category with branches and sub-branches to describe the relationship between them;
- keep asking “why?” or “what caused that?” to connect the causes;
- review all branches to verify consistency and completeness and ensure that the causes apply to the main effect;
- identify the most likely causes based on the opinion of the team and available evidence.

The results are normally displayed as either a Fishbone or Ishikawa diagram or tree diagram. The Fishbone diagram is structured by separating causes into major categories (represented by the lines off the fish backbone) with branches and sub-branches that describe more specific causes in those categories.

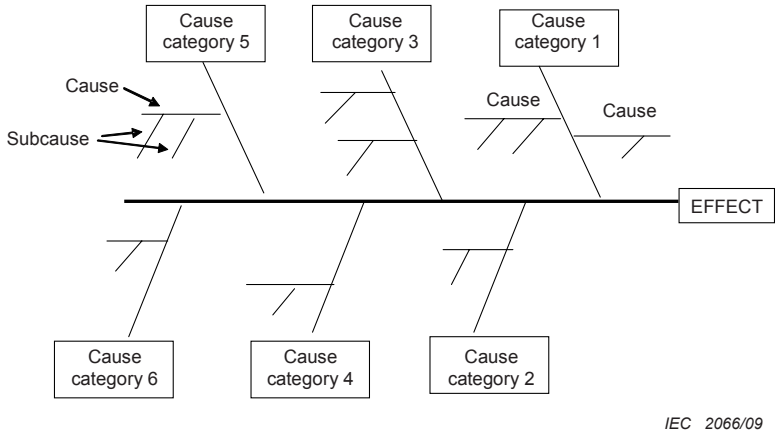


Figure B.5 – Example of Ishikawa or Fishbone diagram

The tree representation is similar to a fault tree in appearance, although it is often displayed with the tree developing from left to right rather than down the page. However, it cannot be quantified to produce a probability of the head event as the causes are possible contributory factors rather than failures with a known probability of occurrence

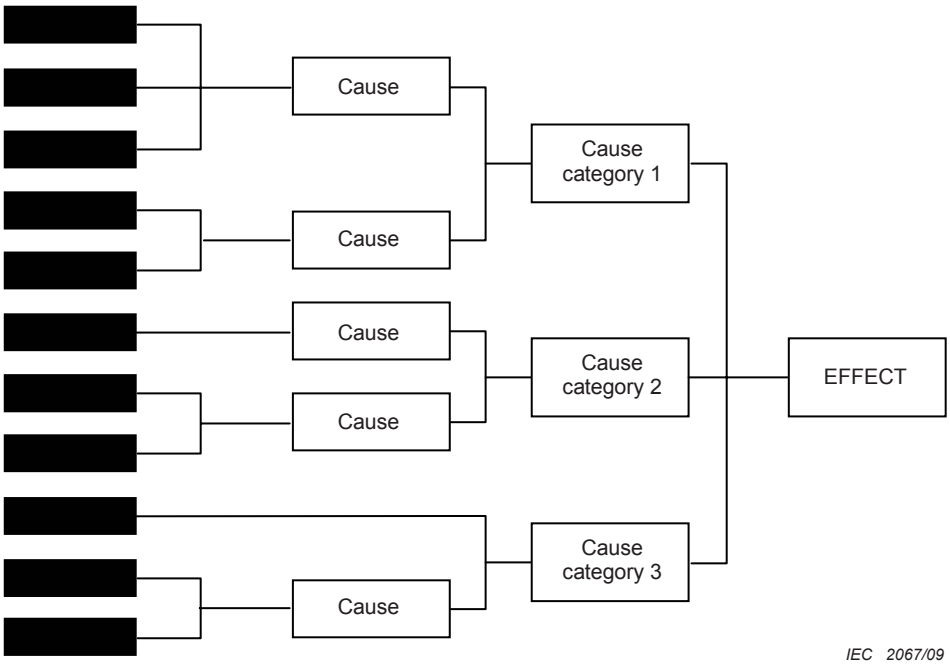


Figure B.6 – Example of tree formulation of cause-and-effect analysis

Cause-and-effect diagrams are generally used qualitatively. It is possible to assume the probability of the problem is 1 and assign probabilities to generic causes, and subsequently to the sub-causes, on the basis of the degree of belief about their relevance. However, contributory factors often interact and contribute to the effect in complex ways which make quantification invalid

B.17.5 Output

The output from a cause-and-effect analysis is a Fishbone or tree diagram that shows the possible and likely causes. This has then to be verified and tested empirically before recommendations can be made.

B.17.6 Strengths and limitations

Strengths include:

- involvement of applicable experts working in a team environment;
- structured analysis;
- consideration of all likely hypotheses;
- graphical easy-to-read illustration of results;
- areas identified where further data is needed;
- can be used to identify contributory factors to wanted as well as unwanted effects. Taking a positive focus on an issue can encourage greater ownership and participation.

Limitations include:

- the team may not have the necessary expertise;
- it is not a complete process in itself and needs to be a part of a root cause analysis to produce recommendations;
- it is a display technique for brainstorming rather than a separate analysis technique;
- the separation of causal factors into major categories at the start of the analysis means that interactions between the categories may not be considered adequately, e.g. where

equipment failure is caused by human error, or human problems are caused by poor design.

B.18 Layers of protection analysis (LOPA)

B.18.1 Overview

LOPA is a semi-quantitative method for estimating the risks associated with an undesired event or scenario. It analyses whether there are sufficient measures to control or mitigate the risk.

A cause-consequence pair is selected and the layers of protection which prevent the cause leading to the undesired consequence are identified. An order of magnitude calculation is carried out to determine whether the protection is adequate to reduce risk to a tolerable level.

B.18.2 Uses

LOPA may be used qualitatively simply to review the layers of protection between a hazard or causal event and an outcome. Normally a semi-quantitative approach would be applied to add more rigour to screening processes for example following HAZOP or PHA.

LOPA provides a basis for the specification of independent protection layers (IPLs) and safety integrity levels (SIL levels) for instrumented systems, as described in the IEC 61508 series and in IEC 61511, in the determination of safety integrity level (SIL) requirements for safety instrumented systems. LOPA can be used to help allocate risk reduction resources effectively by analysing the risk reduction produced by each layer of protection.

B.18.3 Inputs

Inputs to LOPA include

- basic information on risks including hazards, causes and consequences such as provided by a PHA;
- information on controls in place or proposed;
- causal event frequencies, and protection layer failure probabilities, measures of consequence and a definition of tolerable risk;
- initiating cause frequencies, protection layer failure probabilities, measures of consequence and a definition of tolerable risk.

B.18.4 Process

LOPA is carried out using a team of experts who apply the following procedure:

- identify initiating causes for an undesired outcome and seek data on their frequencies and consequences;
- select a single cause-consequence pair;
- layers of protection which prevent the cause proceeding to the undesired consequence are identified and analysed for their effectiveness;
- identify independent protection layers (IPLs) (not all layers of protection are IPLs);
- estimate the probability of failure of each IPL;
- the frequency initiating cause is combined with the probabilities of failure of each IPL and the probabilities of any conditional modifiers (a conditional modifier is for example whether a person will be present to be impacted) to determine the frequency of occurrence of the undesired consequence. Orders of magnitude are used for frequencies and probabilities;

- the calculated level of risk is compared with risk tolerance levels to determine whether further protection is required.

An IPL is a device system or action that is capable of preventing a scenario proceeding to its undesired consequence, independent of the causal event or any other layer of protection associated with the scenario.

IPLs include:

- design features;
- physical protection devices;
- interlocks and shutdown systems;
- critical alarms and manual intervention;
- post event physical protection;
- emergency response systems (procedures and inspections are not IPLs).

B.18.5 Output

Recommendations for any further controls and the effectiveness of these controls in reducing risk shall be given.

LOPA is one of the techniques used for SIL assessment when dealing with safety related/instrumented systems

B.18.6 Strengths and limitations

Strengths include:

- it requires less time and resources than a fault tree analysis or fully quantitative risk assessment but is more rigorous than qualitative subjective judgments;
- it helps identify and focus resources on the most critical layers of protection;
- it identifies operations, systems and processes for which there are insufficient safeguards;
- it focuses on the most serious consequences.

Limitations include:

- LOPA focuses on one cause-consequence pair and one scenario at a time. Complex interactions between risks or between controls are not covered;
- quantified risks may not account for common mode failures;
- LOPA does not apply to very complex scenarios where there are many cause-consequence pairs or where there are a variety of consequences affecting different stakeholders.

B.18.7 Reference documents

IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

IEC 61511, *Functional safety – Safety instrumented systems for the process industry sector*

B.19 Decision tree analysis

B.19.1 Overview

A decision tree represents decision alternatives and outcomes in a sequential manner which takes account of uncertain outcomes. It is similar to an event tree in that it starts from an initiating event or an initial decision and models different pathways and outcomes as a result of events that may occur and different decisions that may be made.

B.19.2 Use

A decision tree is used in managing project risks and in other circumstances to help select the best course of action where there is uncertainty. The graphical display can also help communicate reasons for decisions.

B.19.3 Input

A project plan with decision points. Information on possible outcomes of decisions and on chance events which might affect decisions.

B.19.4 Process

A decision tree starts with an initial decision, for example to proceed with project A rather than project B. As the two hypothetical projects proceed, different events will occur and different predictable decisions will need to be made. These are represented in tree format, similar to an event tree. The probability of the events can be estimated together with the cost or utility of the final outcome of the pathway.

Information concerning the best decision pathway is logically that which produces the highest expected value calculated as the product of all the conditional probabilities along the pathway and the outcome value.

B.19.5 Outputs

Outputs include:

- a logical analysis of the risk displaying different options that may be taken
- a calculation of the expected value for each possible path

B.19.6 Strengths and limitations

Strengths include:

- they provide a clear graphical representation of the details of a decision problem;
- they enable a calculation of the best pathway through a situation.

Limitations include:

- large decisions trees may become too complex for easy communication with others;
- there may be a tendency to oversimplify the situation so as to be able to represent it as a tree diagram.

B.20 Human reliability assessment (HRA)

B.20.1 Overview

Human reliability assessment (HRA) deals with the impact of humans on system performance and can be used to evaluate human error influences on the system.

Many processes contain potential for human error, especially when the time available to the operator to make decisions is short. The probability that problems will develop sufficiently to become serious can be small. Sometimes, however, human action will be the only defence to prevent an initial failure progressing towards an accident.

The importance of HRA has been illustrated by various accidents in which critical human errors contributed to a catastrophic sequence of events. Such accidents are warnings against risk assessments that focus solely on the hardware and software in a system. They illustrate the dangers of ignoring the possibility of human error contribution. Moreover, HRAs are useful in highlighting errors that can impede productivity and in revealing ways in which these errors and other failures (hardware and software) can be "recovered" by the human operators and maintenance personnel.

B.20.2 Use

HRA can be used qualitatively or quantitatively. Qualitatively, it is used to identify the potential for human error and its causes so the probability of error can be reduced. Quantitative HRA is used to provide data on human failures into FTA or other techniques.

B.20.3 Input

Inputs to HRA include:

- information to define tasks that people should perform;
- experience of the types of error that occur in practice and potential for error;
- expertise on human error and its quantification.

B.20.4 Process

The HRA process is as follows:

- **Problem definition**, what types of human involvements are to be investigated/assessed?
- **Task analysis,** how will the task be performed and what type of aids will be needed to support performance?
- **Human error analysis**, how can task performance fail: what errors can occur and how can they be recovered?
- **Representation**, how can these errors or task performance failures be integrated with other hardware, software, and environmental events to enable overall system failure probabilities to be calculated?
- **Screening**, are there any errors or tasks that do not require detailed quantification?
- **Quantification**, how likely are individual errors and failures of tasks?
- **Impact assessment**, which errors or tasks are most important, i.e. which ones have the highest contribution to reliability or risk?
- **Error reduction**, how can higher human reliability be achieved?
- **Documentation**, what details of the HRA need to be documented?

In practice, the HRA process proceeds step-wise although sometimes with parts (e.g. tasks analysis and error identification) proceeding in parallel with one another.

B.20.5 Output

Outputs include:

- a list of errors that may occur and methods by which they can be reduced – preferably through redesign of the system;
- error modes, error types causes and consequences;

- a qualitative or quantitative assessment of the risk posed by the errors.

B.20.6 Strengths and limitations

Strengths of HRA include:

- HRA provides a formal mechanism to include human error in consideration of risks associated with systems where humans often play an important role;
- formal consideration of human error modes and mechanisms can help reduce the probability of failure due to error.

Limitations include:

- the complexity and variability of humans, which make defining simple failure modes and probabilities difficult;
- many activities of humans do not have a simple pass/fail mode. HRA has difficulty dealing with partial failures or failure in quality or poor decision-making.

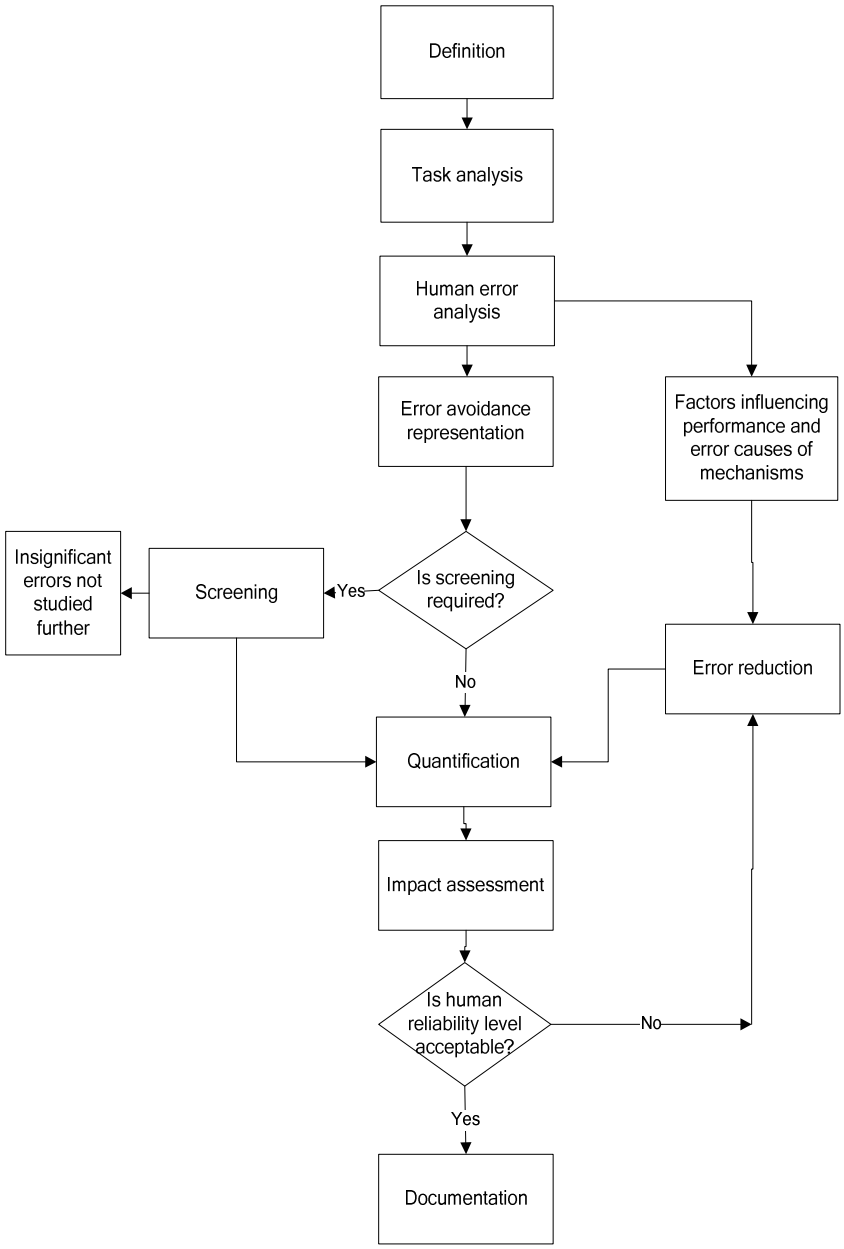


Figure B.7 – Example of human reliability assessment

B.21 Bow tie analysis

B.21.1 Overview

Bow tie analysis is a simple diagrammatic way of describing and analysing the pathways of a risk from causes to consequences. It can be considered to be a combination of the thinking of a fault tree analysing the cause of an event (represented by the knot of a bow tie) and an event tree analysing the consequences. However the focus of the bow tie is on the barriers between the causes and the risk, and the risk and consequences. Bow tie diagrams can be constructed starting from fault and event trees, but are more often drawn directly from a brainstorming session.

B.21.2 Use

Bow tie analysis is used to display a risk showing a range of possible causes and consequences. It is used when the situation does not warrant the complexity of a full fault tree analysis or when the focus is more on ensuring that there is a barrier or control for each failure pathway. It is useful where there are clear independent pathways leading to failure.

Bow tie analysis is often easier to understand than fault and event trees, and hence can be a useful communication tool where analysis is achieved using more complex techniques.

B.21.3 Input

An understanding is required of information on the causes and consequences of a risk and the barriers and controls which may prevent, mitigate or stimulate it.

B.21.4 Process

The bow tie is drawn as follows:

a) A particular risk is identified for analysis and represented as the central knot of a bow tie.

b) Causes of the event are listed considering sources of risk (or hazards in a safety context).

c) The mechanism by which the source of risk leads to the critical event is identified.

d) Lines are drawn between each cause and the event forming the left-hand side of the bow tie. Factors which might lead to escalation can be identified and included in the diagram.

e) Barriers which should prevent each cause leading to the unwanted consequences can be shown as vertical bars across the line. Where there were factors which might cause escalation, barriers to escalation can also be represented. The approach can be used for positive consequences where the bars reflect ‘controls’ that stimulate the generation of the event.

f) On the right-hand side of the bow tie different potential consequences of the risk are identified and lines drawn to radiate out from the risk event to each potential consequence.

g) Barriers to the consequence are depicted as bars across the radial lines. The approach can be used for positive consequences where the bars reflect ‘controls’ that support the generation of consequences.

h) Management functions which support controls (such as training and inspection) can be shown under the bow tie and linked to the respective control.

Some level of quantification of a bow tie diagram may be possible where pathways are independent, the probability of a particular consequence or outcome is known and a figure can be estimated for the effectiveness of a control. However, in many situations, pathways and barriers are not independent and controls may be procedural and hence the effectiveness unclear. Quantification is often more appropriately carried out using FTA and ETA.

B.21.5 Output

The output is a simple diagram showing main risk pathways and the barriers in place to prevent or mitigate the undesired consequences or stimulate and promote desired consequences.

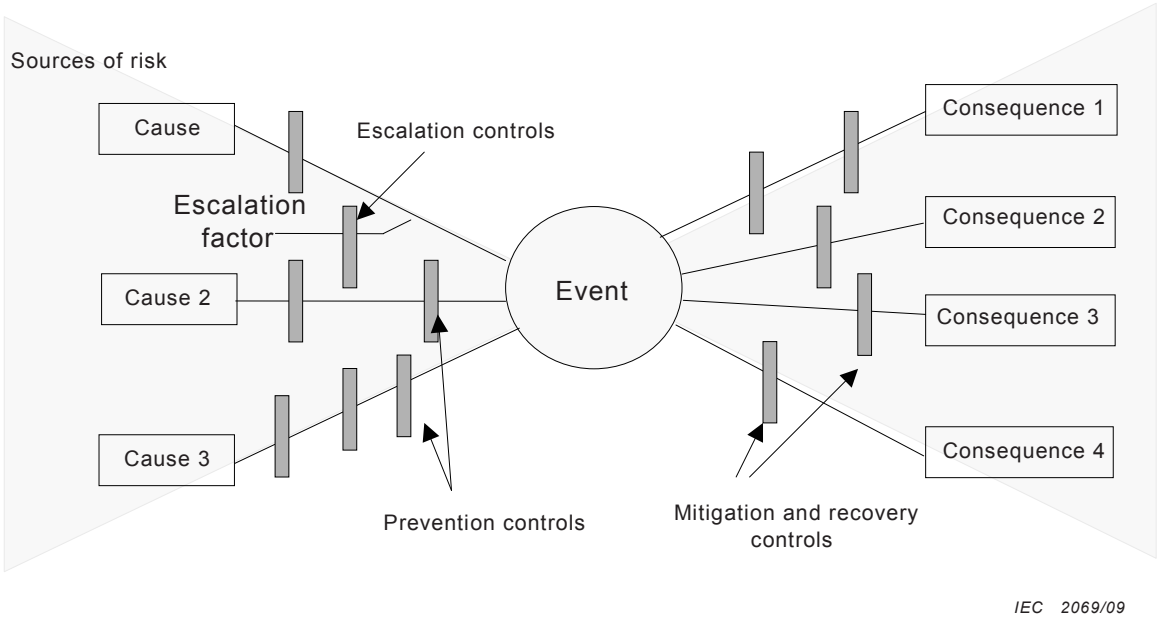


Figure B.8 – Example bow tie diagram for unwanted consequences

B.21.6 Strengths and limitations

Strengths of bow tie analysis:

- it is simple to understand and gives a clear pictorial representation of the problem;
- it focuses attention on controls which are supposed to be in place for both prevention and mitigation and their effectiveness;
- it can be used for desirable consequences;
- it does not need a high level of expertise to use.

Limitations include:

- it cannot depict where multiple causes occur simultaneously to cause the consequences (i.e. where there are AND gates in a fault tree depicting the left-hand side of the bow);
- it may over-simplify complex situations, particularly where quantification is attempted.

B.22 Reliability centred maintenance

B.22.1 Overview

Reliability centred maintenance (RCM) is a method to identify the policies that should be implemented to manage failures so as to efficiently and effectively achieve the required safety, availability and economy of operation for all types of equipment.

RCM is now a proven and accepted methodology used in a wide range of industries.

RCM provides a decision process to identify applicable and effective preventive maintenance requirements for equipment in accordance with the safety, operational and economic consequences of identifiable failures, and the degradation mechanism responsible for those failures. The end result of working through the process is a judgment as to the necessity of performing a maintenance task or other action such as operational changes. Details regarding the use and application of RCM are provided in IEC 60300-3-11.

B.22.2 Use

All tasks are based on safety in respect of personnel and environment, and on operational or economic concerns. However, it should be noted that the criteria considered will depend on the nature of the product and its application. For example, a production process will need to be economically viable, and may be sensitive to strict environmental considerations, whereas an item of defence equipment should be operationally successful, but may have less stringent safety, economic and environmental criteria. Greatest benefit can be achieved through targeting of the analysis to where failures would have serious safety, environmental, economic or operational effects.

RCM is used to ensure that applicable and effective maintenance is performed, and is generally applied during the design and development phase and then implemented during operation and maintenance.

B.22.3 Input

Successful application of RCM needs a good understanding of the equipment and structure, the operational environment and the associated systems, subsystems and items of equipment, together with the possible failures, and the consequences of those failures.

B.22.4 Process

The basic steps of an RCM programme are as follows:

- initiation and planning;
- functional failure analysis;
- task selection;
- implementation;
- continuous improvement.

RCM is risk based since it follows the basic steps in risk assessment. The type of risk assessment is a failure mode, effect and criticality analysis (FMECA) but requires a specific approach to analysis when used in this context.

Risk identification focuses on situations where potential failures may be eliminated or reduced in frequency and/or consequence by carrying out maintenance tasks. It is performed by identifying required functions and performance standards and failures of equipment and components that can interrupt those functions

Risk analysis consists of estimating the frequency of each failure without maintenance being carried out. Consequences are established by defining failure effects. A risk matrix that combines failure frequency and consequences allows categories for levels of risk to be established.

Risk evaluation is then performed by selecting the appropriate failure management policy for each failure mode.

The entire RCM process is extensively documented for future reference and review. Collection of failure and maintenance-related data enables monitoring of results and implementation of improvements.

B.22.5 Output

RCM provides a definition of maintenance tasks such as condition monitoring, scheduled restoration, scheduled replacement, failure-finding or non preventive maintenance. Other possible actions that can result from the analysismay include redesign, changes to operating

or maintenance procedures or additional training. Task intervals and required resources are then identified.

B.22.6 Reference documents

IEC 60300-3-11, *Dependability management – Part 3-11: Application guide – Reliability centred maintenance*

B.23 Sneak analysis (SA)and sneak circuit analysis (SCI)

B.23.1 Overview

Sneak analysis (SA) is a methodology for identifying design errors. A sneak condition is a latent hardware, software or integrated condition that may cause an unwanted event to occur or may inhibit a desired event and is not caused by component failure. These conditions are characterized by their random nature and ability to escape detection during the most rigorous of standardized system tests. Sneak conditions can cause improper operation, loss of system availability, program delays, or even death or injury to personnel.

B.23.2 Use

Sneak circuit analysis (SCA) was developed in the late 1960s for NASA to verify the integrity and functionality of their designs. It served as a useful tool for discovering unintentional electrical circuit paths, and assisted in devising solutions to isolate each function. However, as technology advanced, the tools for sneak circuit analysis also had to advance. Sneak analysis includes and far exceeds the coverage of sneak circuit analysis. It can locate problems in both hardware and software using any technology. The sneak analysis tools can integrate several analyses such as fault trees, failure mode and effects analysis (FMEA), reliability estimates, etc. into a single analysis saving time and project expenses.

B.23.3 Input

Sneak analysis is unique from the design process in that it uses different tools (network trees, forests, and clues or questions to help the analyst identify sneak conditions) to find a specific type of problem. The network trees and forests are topological groupings of the actual system. Each network tree represents a sub-function and shows all inputs that may affect the sub-function output. Forests are constructed by combining the network trees that contribute to a particular system output. A proper forest shows a system output in terms of all of its related inputs. These, along with others, become the input to the analysis.

B.23.4 Process

The basic steps in performing a sneak analysis consist of:

- data preparation;
- construction of the network tree;
- evaluation of network paths;
- final recommendations and report.

B.23.5 Output

A sneak circuit is an unexpected path or logic flow within a system which, under certain conditions, can initiate an undesired function or inhibit a desired function. The path may consist of hardware, software, operator actions, or combinations of these elements. Sneak circuits are not the result of hardware failure but are latent conditions, inadvertently designed into the system, coded into the software program, or triggered by human error. There are four categories of sneak circuits:

a) sneak paths: unexpected paths along which current, energy, or logical sequence flows in an unintended direction;

b) sneak timing: events occurring in an unexpected or conflicting sequence;

c) sneak indications: ambiguous or false displays of system operating conditions that may cause the system or an operator to take an undesired action;

d) sneak labels: incorrect or imprecise labelling of system functions, e.g. system inputs, controls, display buses that may cause an operator to apply an incorrect stimulus to the system.

B.23.6 Strengths and limitations

Strengths include:

- sneak analysis is good for identifying design errors;
- it works best when applied in conjunction with HAZOP;
- it is very good for dealing with systems which have multiple states such as batch and semi-batch plant.

Limitations may include:

- the process is somewhat different depending on whether it is applied to electrical circuits, process plants, mechanical equipment or software;
- the method is dependent on establishing correct network trees.

B.24 Markov analysis

B.24.1 Overview

Markov analysis is used where the future state of a system depends only upon its present state. It is commonly used for the analysis of repairable systems that can exist in multiple states and the use of a reliability block analysis would be unsuitable to adequately analyse the system. The method can be extended to more complex systems by employing higher order Markov processes and is only restricted by the model, mathematical computations and the assumptions.

The Markov analysis process is a quantitative technique and can be discrete (using probabilities of change between the states) or continuous (using rates of change across the states).

While a Markov analysis can be performed by hand, the nature of the techniques lends itself to the use of computer programmes, many of which exist in the market.

B.24.2 Use

The Markov analysis technique can be used on various system structures, with or without repair, including:

- independent components in parallel;
- independent components in series;
- load-sharing system;
- stand-by system, including the case where switching failure can occur;
- degraded systems.

The Markov analysis technique can also be used for calculating availability, including taking into account the spares components for repairs.

B.24.3 Input

The inputs essential to a Markov analysis are as follows:

- list of various states that the system, sub-system or component can be in (e.g. fully operational, partially operation (i.e. a degraded state), failed state, etc);
- a clear understanding of the possible transitions that are necessary to be modelled. For example, failure of a car tyre needs to consider the state of the spare wheel and hence the frequency of inspection;
- rate of change from one state to another, typically represented by either a probability of change between states for discrete events, or failure rate (λ) and/or repair rate (μ) for continuous events.

B.24.4 Process

The Markov analysis technique is centred around the concept of "states", e.g. "available" and "failed", and the transition between these two states over time based on a constant probability of change. A stochastic transitional probability matrix is used to describe the transition between each of the states to allow the calculation of the various outputs.

To illustrate the Markov analysis technique, consider a complex system that can be in only three states; functioning, degraded and failed, defined as states S1, S2, S3 respectively. Each day, the system exists in one of these three states. Table B.3 shows the probability that tomorrow, the system is in state S*i* where *i* can be 1, 2 or 3.

Table B.2 – Markov matrix

		State today		
		S1	S2	S3
State tomorrow	S1	0,95	0,3	0,2
	S2	0,04	0,65	0,6
	S3	0,01	0,05	0,2

This array of probabilities is called a Markov matrix, or transition matrix. Notice that the sum for each of the columns is 1 as they are the sum of all the possible outcomes in each case. The system, can also be represented by a Markov diagram where the circles represent the states, and the arrows represent the transition, together with the accompanying probability.

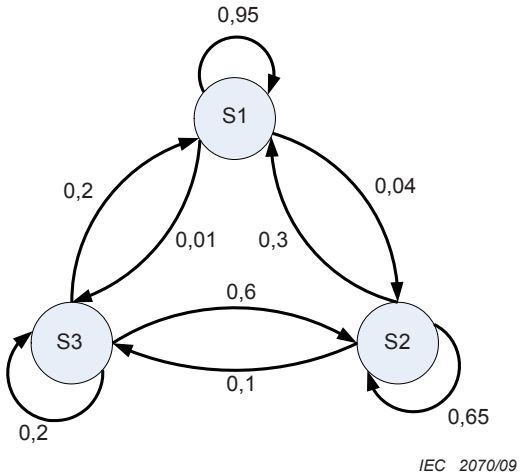


Figure B.9 – Example of system Markov diagram

The arrows from a state to itself are not usually shown, but are shown within these examples for completeness.

Let P*i* represent the probability of finding the system in state *i* for *i* = 1, 2, 3, then the simultaneous equations to be solved are:

$$P1 = 0{,}95\ P1 + 0{,}30\ P2 + 0{,}20\ P3 \quad \text{(B.1)}$$

$$P2 = 0{,}04\ P1 + 0{,}65\ P2 + 0{,}60\ P3 \quad \text{(B.2)}$$

$$P3 = 0{,}01\ P1 + 0{,}05\ P2 + 0{,}20\ P3 \quad \text{(B.3)}$$

These three equations are not independent and will not solve the three unknowns. The following equation should be used and one of the above equations discarded.

$$1 = P1 + P2 + P3 \quad \text{(B.4)}$$

The solution is 0,85, 0,13, and 0.02 for the respective states 1, 2, 3. The system is fully functioning for 85 % of the time, in the degraded state for 13 % of the time and failed for 2 % of the time.

Consider two items operating in parallel with either required to be operational for the system to function. The items can either be operational or failed and the availability of the system is dependent upon the status of the items.

The states can be considered as:

State 1 Both items are functioning correctly;

State 2 One item has failed and is undergoing repair, the other is functioning;

State 3 Both items have failed and one is undergoing repair.

If the continuous failure rate for each item is assumed to be λ and the repair rate to be μ, then the state transition diagram is:

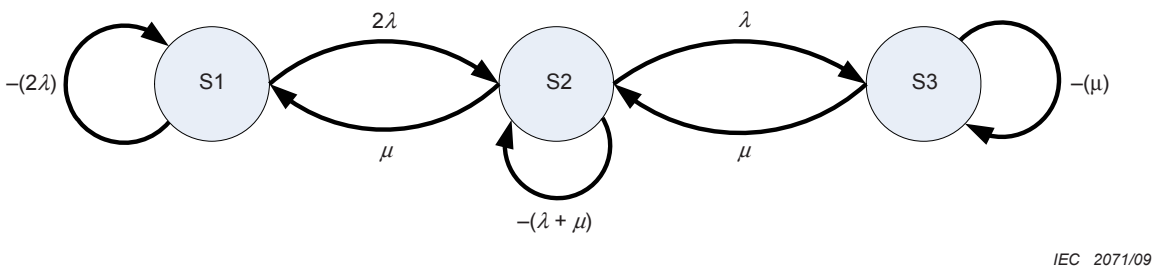


Figure B.10 – Example of state transition diagram

Note that the transition from state 1 to state 2 is 2λ as failure of either of the two items will take the system to state 2.

Let P*i*(*t*) be the probability of being in an initial state *i* at time *t*; and

Let P*i*(*t* + *δt*) be the probability of being in a final state at time *t* + *δt*

The transition probability matrix becomes:

Table B.3 – Final Markov matrix

		Initial state		
		P1(t)	P2(t)	P3(t)
	P1($t + \delta t$)	-2λ	μ	0
Final state	P2($t + \delta t$)	2λ	$-(\lambda + \mu)$	μ
	P3($t + \delta t$)	0	λ	$-\mu$

It is worth noting that the zero values occur as it is not possible to move from state 1 to state 3 or from state 3 to state 1. Also, the columns sum to zero when specifying rates.

The simultaneous equations become:

$$dP1/dt = -2\lambda\, P1(t) + \mu\, P2(t) \quad \text{(B.5)}$$

$$dP2/dt = 2\lambda\, P1(t) + -(\lambda + \mu)\, P2(t) + \mu\, P3(t) \quad \text{(B.6)}$$

$$dP3/dt = \lambda\, P2(t) + -\mu\, P3(t) \quad \text{(B.7)}$$

For simplicity, it will be assumed that the availability required is the steady state availability.

When δt tends to infinity, dPi/dt will tend to zero and the equations become easier to solve. The additional equation as shown in Equation (B.4) above should also be used:

Now the equation $A(t) = P1(t) + P2(t)$ can be expressed as:

$A = P1 + P2$

Hence $A = (\mu^2 + 2\lambda\mu) / (\mu^2 + 2\lambda\mu + \lambda^2)$

B.24.5 Output

The output from a Markov analysis is the various probabilities of being in the various states, and therefore an estimate of the failure probabilities and/or availability, one of the essential components of a system.

B.24.6 Strengths and limitations

Strengths of a Markov analysis include:

- ability to calculate the probabilities for systems with a repair capability and multiple degraded states.

Limitations of a Markov analysis include:

- assumption of constant probabilities of change of state; either failure or repairs;
- all events are statistically independent since future states are independent of all past states, except for the state immediately prior;
- needs knowledge of all probabilities of change of state;
- knowledge of matrix operations;
- results are hard to communicate with non-technical personnel.

B.24.7 Comparisons

Markov analysis is similar to a Petri-Net analysis by being able to monitor and observe system states, although different since Petri-Net can exist in multiple states at the same time.

B.24.8 Reference documents

IEC 61078, *Analysis techniques for dependability – Reliability block diagram and boolean methods*

IEC 61165, *Application of Markov techniques*

ISO/IEC 15909 (all parts), *Software and systems engineering – High-level Petri nets*

B.25 Monte Carlo simulation

B.25.1 Overview

Many systems are too complex for the effects of uncertainty on them to be modelled using analytical techniques, but they can be evaluated by considering the inputs as random variables and running a number N of calculations (so-called simulations) by sampling the input in order to obtain N possible outcomes of the wanted result.

This method can address complex situations that would be very difficult to understand and solve by an analytical method. Systems can be developed using spreadsheets and other conventional tools, but more sophisticated tools are readily available to assist with more complex requirements, many of which are now relatively inexpensive. When the technique was first developed, the number of iterations required for Monte Carlo simulations made the process slow and time consuming, but advances in computers and theoretical developments, such as Latin-hypercube sampling, have made processing time almost insignificant for many applications.

B.25.2 Use

Monte Carlo simulation provides a means of evaluating the effect of uncertainty on systems in a wide range of situations. It is typically used to evaluate the range of possible outcomes and the relative frequency of values in that range for quantitative measures of a system such as cost, duration, throughput, demand and similar measures. Monte Carlo simulation may be used for two different purposes:

- uncertainty propagation on conventional analytical models;
- probabilistic calculations when analytical techniques do not work.

B.25.3 Input

The input to a Monte Carlo simulation is a good model of the system and information on the types of inputs, the sources of uncertainty that are to be represented and the required output. Input data with uncertainty is represented as random variables with distributions which are more or less spread according to the level of uncertainties. Uniform, triangular, normal and log normal distributions are often used for this purpose.

B.25.4 Process

The process is as follows:

a) A model or algorithm is defined which represents as closely as possible the behaviour of the system being studied.

b) The model is run multiple times using random numbers to produce outputs of the model (simulations of the system); Where the application is to model the effects of uncertainty

the model is in the form of an equation providing the relationship between input parameters and an output. The values selected for the inputs are taken from appropriate probability distributions that represent the nature of the uncertainty in these parameters.

c) In either case a computer runs the model multiple times (often up to 10,000 times) with different inputs and produces multiple outputs. These can be processed using conventional statistics to provide information such as average values, standard deviation, confidence intervals.

An example of a simulation is given below.

Consider the case of two items operating in parallel and only one is required for the system to function. The first item has a reliability of 0,9 and the other 0,8.

It is possible to construct a spreadsheet with the following columns.

Table B.4 – Example of Monte Carlo simulation

	Item 1		Item 2		
Simulation number	Random number	Functions?	Random number	Functions?	System
1	0,577 243	YES	0,059 355	YES	1
2	0,746 909	YES	0,311 324	YES	1
3	0,541 728	YES	0,919 765	NO	1
4	0,423 274	YES	0,643 514	YES	1
5	0,917 776	NO	0,539 349	YES	1
6	0,994 043	NO	0,972 506	NO	0
7	0,082 574	YES	0,950 241	NO	1
8	0,661 418	YES	0,919 868	NO	1
9	0,213 376	YES	0,367 555	YES	1
10	0,565 657	YES	0,119 215	YES	1

The random generator creates a number between 0 and 1 which is used to compare with the probability of each item to determine if the system is operational. With just 10 runs, the result of 0,9 should not be expected to be an accurate result. The usual approach is to build in a calculator to compare the total result as the simulation progresses to achieve the level of accuracy required. In this example, a result of 0,979 9 was achieved after 20 000 iterations.

The above model can be extended in a number of ways. For example:

- by extending the model itself (such as considering the second item becoming immediately operational only when the first item fails);
- by changing the fixed probability to a variable (a good example is the triangular distribution) when the probability cannot be accurately defined;
- using failure rates combined with the randomizer to derive a time of failure (exponential, Weibull, or other suitable distribution) and building in repair times.

Applications include, amongst other things, the assessment of uncertainty in financial forecasts, investment performance, project cost and schedule forecasts, business process interruptions and staffing requirements.

Analytical techniques are not able to provide relevant results or when there is uncertainty in the input data and so in the outputs.

B.25.5 Output

The output could be a single value, as determined in the above example, it could be a result expressed as the probability or frequency distribution or it could be the identification of the main functions within the model that has the greatest impact on the output.

In general, a Monte Carlo simulation will be used to assess either the entire distribution of outcomes that could arise or key measures from a distribution such as:

- the probability of a defined outcome arising;
- the value of an outcome in which the problem owners have a certain level of confidence that it will not be exceeded or beaten, a cost that there is less than a 10 % chance of exceeding or a duration that is 80 % certain to be exceeded.

An analysis of the relationships between inputs and outputs can throw light on the relative significance of the factors at work and identify useful targets for efforts to influence the uncertainty in the outcome.

B.25.6 Strengths and limitations

Strengths of the Monte Carlo analysis include the following:

- the method can, in principle, accommodate any distribution in an input variable, including empirical distributions derived from observations of related systems;
- models are relatively simple to develop and can be extended as the need arises;
- any influences or relationships arising in reality can be represented, including subtle effects such as conditional dependencies;
- sensitivity analysis can be applied to identify strong and weak influences;
- models can be easily understood as the relationship between inputs and outputs is transparent;
- efficient behavioural models such as Petri Nets (future IEC 62551) are available which prove to be very efficient for Monte Carlo simulation purposes;
- provides a measure of the accuracy of a result;
- software is readily available and relatively inexpensive.

Limitations are as follows:

- the accuracy of the solutions depends upon the number of simulations which can be performed (this limitation is becoming less important with increased computer speeds);
- it relies on being able to represent uncertainties in parameters by a valid distribution;
- large and complex models may be challenging to the modeller and make it difficult for stakeholders to engage with the process;
- the technique may not adequately weigh high-consequence/low probability events and therefore not allow an organization's risk appetite to be reflected in the analysis.

B.25.7 Reference documents

IEC 61649, *Weibull analysis*

IEC 62551, *Analysis techniques for dependability – Petri net techniques*[1]

ISO/IEC Guide 98-3:2008, *Uncertainty measurement – Part 3: Guide to the of uncertainty in measurement (GUM:1995)*

---

1 Currently under consideration.

B.26 Bayesian statistics and Bayes Nets

B.26.1 Overview

Bayesian statistics are attributed to the Reverend Thomas Bayes. Its premise is that any already known information (the Prior) can be combined with subsequent measurement (the Posterior) to establish an overall probability. The general expression of the Bayes Theorem can be expressed as:

$$P(A \mid B) = \{P(A)P(B \mid A)\} / \sum_i P(B \mid E_i)P(E_i)$$

where

the probability of X is denoted by $P(X)$;

the probability of X on the condition that Y has occurred is denoted by $P(X|Y)$; and

E_i is the ith event.

In its simplest form this reduces to $P(A|B) = \{P(A)P(B|A)\} / P(B)$.

Bayesian statistics differs from classical statistics in that is does not assume that all distribution parameters are fixed, but that parameters are random variables. A Bayesian probability can be more easily understood if it is considered as a person's degree of belief in a certain event as opposed to the classical which is based upon physical evidence. As the Bayesian approach is based upon the subjective interpretation of probability, it provides a ready basis for decision thinking and the development of Bayesian nets (or Belief Nets, belief networks or Bayesian networks).

Bayes nets use a graphical model to represent a set of variables and their probabilistic relationships. The network is comprised of nodes that represent a random variable and arrows which link a parent node to a child node, (where a parent node is a variable that directly influences another (child) variable).

B.26.2 Use

In recent years, the use of Bays' theory and Nets has become widespread partly because of their intuitive appeal and also because of the availability of software computing tools. Bayes nets have been used on a wide range of topics: medical diagnosis, image modelling, genetics, speech recognition, economics, space exploration and in the powerful web search engines used today. They can be valuable in any area where there is the requirement for finding out about unknown variables through the utilization of structural relationships and data. Bayes nets can be used to learn causal relationships to give an understanding about a problem domain and to predict the consequences of intervention.

B.26.3 Input

The inputs are similar to the inputs for a Monte Carlo model. For a Bayes net, examples of the steps to be taken include the following:

- define system variables;
- define causal links between variables;
- specify conditional and prior probabilities;
- add evidence to net;
- perform belief updating;
- extract posterior beliefs.

B.26.4 Process

Bayes theory can be applied in a wide variety of ways. This example will consider the creation of a Bayes table where a medical test is used to determine if the patient has a disease. The belief before taking the test is that 99 % of the population do not have this disease and 1 % have the disease, i.e the Prior information. The accuracy of the test has shown that if the person has the disease, the test result is positive 98 % of the time. There is also a probability that if you do not have the disease, the test result is positive 10 % of the time. The Bayes table provides the following information:

Table B.5 – Bayes' table data

	PRIOR	PROBABILITY	PRODUCT	POSTERIOR
Have disease	0,01	0,98	0,009 8	0,090 1
No disease	0,99	0,10	0,099 0	0,909 9
SUM	1		0,108 8	1

Using Bayes rule, the product is determined by combining the prior and probability. The posterior is found by dividing the product value by the product total. The output shows that a positive test result indicates that the prior has increased from 1 % to 9 % . More importantly, there is a strong chance that even with a positive test, having the disease is unlikely. Examining the equation (0,01×0,98)/((0,01×0,98)+(0,99×0,1)) shows that the 'no disease-positive result' value plays a major role in the posterior values.

Consider the following Bayes net:

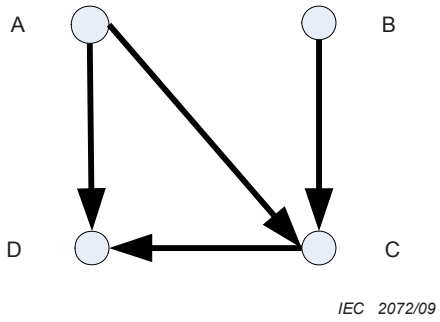


Figure B.11 – Sample Bayes' net

With the conditional prior probabilities defined within the following tables and using the notation that Y indicates positive and N indicates negative, the positive could be "have disease" as above, or could be High and N could be Low.

Table B.6 – Prior probabilities for nodes A and B

P(*A* = *Y*)	P(*A* = *N*)	P(*B* = *Y*)	P(*B* = *N*)
0,9	0,1	0,6	0,4

Table B.7 – Conditional probabilities for node C with node A and node B defined

A	*B*	P(*C* = *Y*)	P(*C* = *N*)
Y	*Y*	0,5	0,5
Y	*N*	0,9	0,1
N	*Y*	0,2	0,8

N	*N*	0,7	0,3

Table B.8 – Conditional probabilities for node D with node A and node C defined

A	*C*	P(*D* = *Y*)	P(*D* = *N*)
Y	*Y*	0,6	0,4
Y	*N*	1,0	0,0
N	*Y*	0,2	0,8
N	*N*	0,6	0,4

To determine the posterior probability of P(*A*|*D*=*N*,*C*=*Y*), it is necessary to first calculate P(*A*,*B*|*D*=*N*,*C*=*Y*).

Using Bayes' rule, the value P(*D*|*A*,*C*)P(*C*|*A*,*B*)P(*A*)P(*B*) is determined as shown below and the last column shows the normalized probabilities which sum to 1 as derived in the previous example (result rounded).

Table B.9 – Posterior probability for nodes A and B with node D and node C defined

A	*B*	P(*D*|*A*,*C*)P(*C*|*A*,*B*)P(*A*)P(*B*)	P(*A*,*B*|*D*=*N*,*C*=*Y*)
Y	*Y*	$0,4 \times 0,5 \times 0,9 \times 0,6 = 0,110$	0,4
Y	*N*	$0,4 \times 0,9 \times 0,9 \times 0,4 = 0,130$	0,48
N	*Y*	$0,8 \times 0,2 \times 0,1 \times 0,6 = 0,010$	0,04
N	*N*	$0,8 \times 0,7 \times 0,1 \times 0,4 = 0,022$	0,08

To derive P(*A*|*D*=*N*,*C*=*Y*), all values of *B* need to be summed:

Table B.10 – Posterior probability for node A with node D and node C defined

P(*A*=*Y*|*D*=*N*,*C*=*Y*)	P(*A*=*N*|*D*=*N*,*C*=*Y*)
0,88	0,12

This shows that the prior for P(*A*=*N*) has increased from 0,1 to a posterior of 0,12 which is only a small change. On the other hand, P(*B*=*N*|*D*=*N*,*C*=*Y*) has changed from 0,4 to 0,56 which is a more significant change.

B.26.5 Outputs

The Bayesian approach can be applied to the same extent as classical statistics with a wide range of outputs, e.g. data analysis to derive point estimators and confidence intervals. Its recent popularity is in relation to Bayes nets to derive posterior distributions. The graphical output provides an easily understood model and the data can be readily modified to consider correlations and sensitivity of parameters.

B.26.6 Strengths and limitations

Strengths:

- all that is needed is knowledge on the priors;
- inferential statements are easy to understand;
- Bayes' rule is all that is required;
- it provides a mechanism for using subjective beliefs in a problem.

Limitations:

- defining all interactions in Bayes nets for complex systems is problematic;
- Bayesian approach needs the knowledge of a multitude of conditional probabilities which are generally provided by expert judgment. Software tools can only provide answers based on these assumptions.

B.27 FN curves

B.27.1 Overview

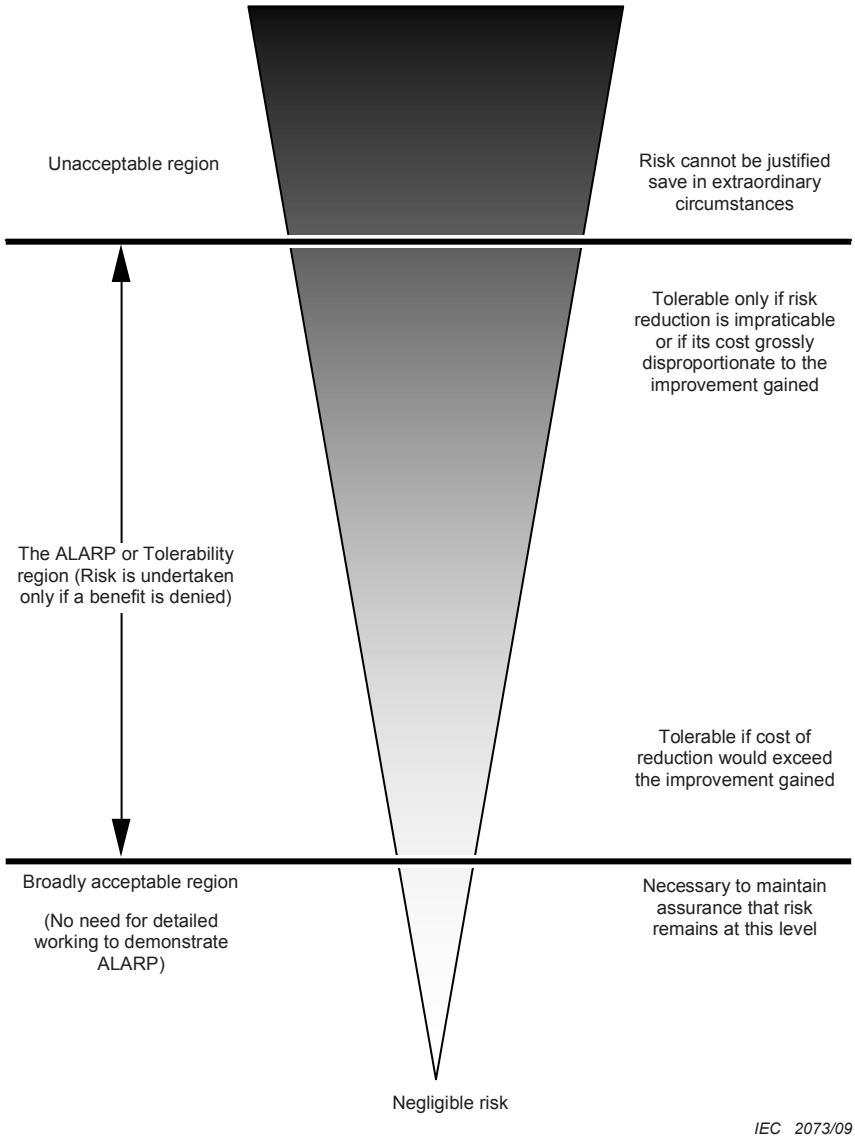


Figure B.12 – The ALARP concept

FN curves are a graphical representation of the probability of events causing a specified level of harm to a specified population. Most often they refer to the frequency of a given number of casualties occurring.

FN curves show the cumulative frequency (*F*) at which *N* or more members of the population that will be affected. High values of *N* that may occur with a high frequency *F* are of significant interest because they may be socially and politically unacceptable.

B.27.2 Use

FN curves are a way of representing the outputs of risk analysis. Many events have a high probability of a low consequence outcome and a low probability of a high consequence outcome. The FN curves provide a representation of the level of risk that is a line describing this range rather than a single point representing one consequence probability pair.

FN curves may be used to compare risks, for example to compare predicted risks against criteria defined as an FN curve, or to compare predicted risks with data from historical incidents, or with decision criteria (also expressed as an F/N curve).

FN curves can be used either for system or process design, or for management of existing systems.

B.27.3 Input

The inputs are either:

- sets of the probability consequence pairs over a given period of time;
- the output of data from a quantitative risk analysis giving estimated probabilities for specified numbers of casualties;
- data from both historical records and a quantitative risk analysis.

B.27.4 Process

The available data is plotted onto a graph with the number of casualties (to a specified level of harm, i.e. death) forming the abscissa with the probability of *N* or more casualties forming the ordinate. Because of the large range of values, both axes are normally on logarithmic scales.

FN curves may be constructed statistically using “real” numbers from past losses or they can be calculated from simulation model estimates. The data used and assumptions made may mean that these two types of FN curve give different information and should be used separately and for different purposes. In general, theoretical FN curves are most useful for system design, and statistical FN curves are most useful for management of a particular existing system.

Both derivation approaches can be very time-consuming so it is not uncommon to use a mixture of both. Empirical data will then form fixed points of precisely known casualties that occurred in known accidents/incident in a specified period of time and the quantitative risk analysis providing other points by extrapolation or interpolation.

The need to consider low-frequency, high-consequence accidents may require consideration of long periods of time to gather enough data for a proper analysis. This in turn may make the available data suspect if the initiating events happen to change over time.

B.27.5 Output

A line representing risk across a range of values of consequence that can be compared with criteria that are appropriate for the population being studied and the specified level of harm.

B.27.6 Strengths and limitations

FN curves are a useful way of presenting risk information that can be used by managers and system designers to help make decisions about risk and safety levels. They are a useful way of presenting both frequency and consequence information in an accessible format.

FN curves are appropriate for comparison of risks from similar situations where sufficient data is available. They should not be used to compare risks of different types with varying characteristics in circumstances where quantity and quality of data varies.

A limitation of FN curves is that they do not say anything about the range of effects or outcomes of incidents other than the number of people impacted, and there is no way of identifying the different ways in which the level of harm may have occurred. They map a particular consequence type, usually harm to people. FN curves are not a risk assessment method, but one way of presenting the results of risk assessment.

They are a well established method for presenting risk assessment results but require preparation by skilled analysts and are often difficult for non specialists to interpret and evaluate

B.28 Risk indices

B.28.1 Overview

A risk index is a semi-quantitative measure of risk which is an estimate derived using a scoring approach using ordinal scales. Risk indices can be used to rate a series of risks using similar criteria so that they can be compared. Scores are applied to each component of risk, for example contaminant characteristics (sources), the range of possible exposure pathways and the impact on the receptors.

Risk indices are essentially a qualitative approach to ranking and comparing risks. While numbers are used, this is simply to allow for manipulation. In many cases where the underlying model or system is not well known or not able to be represented, it is better to use a more overtly qualitative approach.

B.28.2 Use

Indices can be used for classifying different risks associated with an activity if the system is well understood. They permit the integration of a range of factors which have an impact on the level of risk into a single numerical score for level of risk

Indices are used for many different types of risk usually as a scoping device for classifying risk according to level of risk. This may be used to determine which risks need further in-depth and possibly quantitative assessment.

B.28.3 Input

The inputs are derived from analysis of the system, or a broad description of the context. This requires a good understanding of all the sources of risk, the possible pathways and what might be affected. Tools such as fault tree analysis, event tree analysis and general decision analysis can be used to support the development of risk indices.

Since the choice of ordinal scales is, to some extent, arbitrary, sufficient data is needed to validate the index.

B.28.4 Process

The first step is to understand and describe the system. Once the system has been defined, scores are developed for each component in such a way that they can be combined to provide a composite index. For example, in an environmental context, the sources, pathway and receptor(s) will be scored, noting that in some cases there may be multiple pathways and receptors for each source. The individual scores are combined according to a scheme that takes account of the physical realities of the system. It is important that the scores for each part of the system (sources, pathways and receptors) are internally consistent and maintain their correct relationships. Scores may be given for components of risk (e.g. probability, exposure, consequence) or for factors which increase risk.

Scores may be added, subtracted, multiplied and/or divided according to this high level model. Cumulative effects can be taken into account by adding scores (for example, adding scores for different pathways). It is strictly not valid to apply mathematical formulae to ordinal scales. Therefore, once the scoring system has been developed, the model should be validated by applying it to a known system. Developing an index is an iterative approach and several different systems for combining the scores may be tried before the analyst is comfortable with the validation.

Uncertainty can be addressed by sensitivity analysis and varying scores to find out which parameters are the most sensitive.

B.28.5 Output

The output is a series of numbers (composite indices) that relate to a particular source and which can be compared with indices developed for other sources within the same system or which can be modelled in the same way.

B.28.6 Strengths and limitations

Strengths:

- indices can provide a good tool for ranking different risks;
- they allow multiple factors which affect the level of risk to be incorporated into a single numerical score for the level of risk.

Limitations:

- if the process (model) and its output are not well validated, the results may be meaningless. The fact that the output is a numerical value for risk may be misinterpreted and misused, for example in subsequent cost/benefit analysis;
- in many situations where indices are used, there is no fundamental model to define whether the individual scales for risk factors are linear, logarithmic or of some other form, and no model to define how factors should be combined. In these situations, the rating is inherently unreliable and validation against real data is particularly important.

B.29 Consequence/probability matrix

B.29.1 Overview

The consequence/probability matrix is a means of combining qualitative or semi-quantitative ratings of consequence and probability to produce a level of risk or risk rating.

The format of the matrix and the definitions applied to it depend on the context in which it is used and it is important that an appropriate design is used for the circumstances.

B.29.2 Use

A consequence/probability matrix is used to rank risks, sources of risk or risk treatments on the basis of the level of risk. It is commonly used as a screening tool when many risks have been identified, for example to define which risks need further or more detailed analysis, which risks need treatment first, or which need to be referred to a higher level of management. It may also be used to select which risks need not be considered further at this time. This kind of risk matrix is also widely used to determine if a given risk is broadly acceptable, or not acceptable (see 5.4) according to the zone where it is located on the matrix.

The consequence/probability matrix may also be used to help communicate a common understanding for qualitative levels of risks across the organization. The way risk levels are set and decision rules assigned to them should be aligned with the organization's risk appetite.

A form of consequence/probability matrix is used for criticality analysis in FMECA or to set priorities following HAZOP. It may also be used in situations where there is insufficient data for detailed analysis or the situation does not warrant the time and effort for a more quantitative analysis

B.29.3 Input

Inputs to the process are customized scales for consequence and probability and a matrix which combines the two.

The consequence scale (or scales) should cover the range of different types of consequence to be considered (for example: financial loss; safety; environment or other parameters, depending on context) and should extend from the maximum credible consequence to the lowest consequence of concern. A part example is shown in Figure B.6.

The scale may have any number of points. 3, 4 or 5 point scales are most common.

The probability scale may also have any number of points. Definitions for probability need to be selected to be as unambiguous as possible. If numerical guides are used to define different probabilities, then units should be given. The probability scale needs to span the range relevant to the study in hand, remembering that the lowest probability must be acceptable for the highest defined consequence, otherwise all activities with the highest consequence are defined as intolerable. A part example is shown in Figure B.7.

A matrix is drawn with consequence on one axis and probability on the other. Figure B.8 shows part of an example matrix with a 6 point consequence and 5 point probability scales.

The risk levels assigned to the cells will depend on the definitions for the probability/ consequence scales. The matrix may be set up to give extra weight to consequences (as shown) or to probability, or it may be symmetrical, depending on the application. The levels of risk may be linked to decision rules such as the level of management attention or the time scale by which response is needed.

Rating	Financial impact AU$ EBITDA	Investment Return AU$ NPV	Health and Safety	Environment and Community	Reputation	Legal and Compliance
6	$100m+ loss or gain	$300 + loss or gain	• Multiple fatalities, or • Significant irreversible effects to 10's of people	• Irreversible long term environmental harm. • Community outrage- potential large-scale class action.	• International press reporting over several days. • Total loss of shareholder support who act to dis-invest. • CEO departs and board is restructured.	• Major litigation or prosecution with damages of $50m+ plus significant costs. • Custodial sentence for company Executive • Prolonged closure of operations by authorities.
5	$10m - $99m loss or gain	$30m - $299m loss or gain	• Single fatality and/or • Severe irreversible disability to one or more persons	• Prolonged environmental impact. • High-profile community concerns raised – requiring significant remediation measures.	• National press reporting over several days. • Sustained impact on the reputation of shareholders. • Loss of shareholder support for gro • Pressu	• Major litigation costing $10m+ • Investigation by regulato body resulting in lo Interruption to
4	$1m – $9m loss or gain	$3m – $29m loss or gain	• Extensive injuries or Irrevers	• Major spi		
3	$100k – $900 loss or gain					
2	$10 lo					
1						

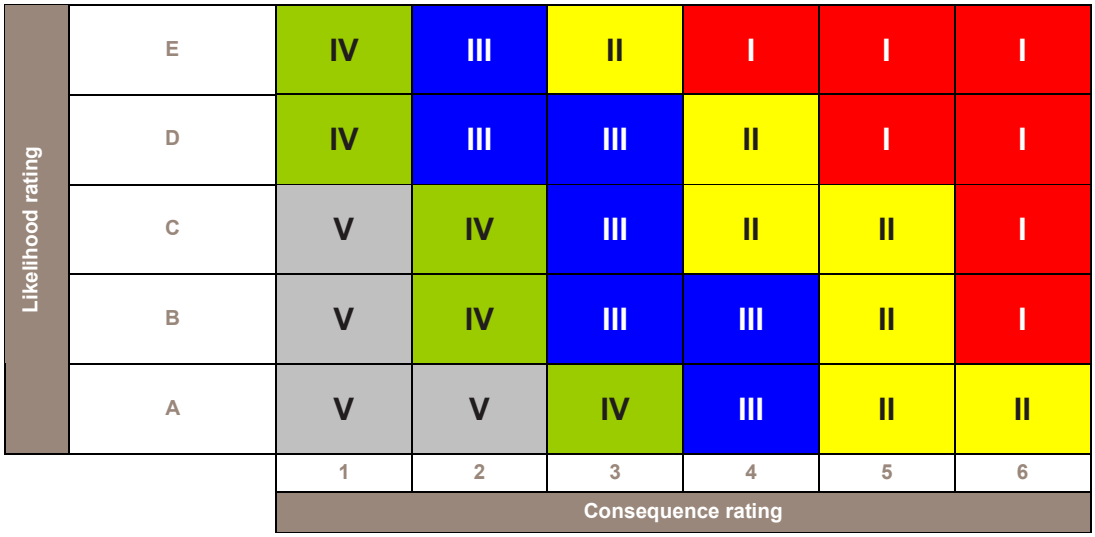
IEC 2074/09

Figure B.13 – Part example of a consequence criteria table

Rating	Criteria
Likely	- balance of probability will occur, or - could occur within "weeks to months"
Possible	- may occur shortly but a distin - could occur within "mo
Unlikely	- may occur but not - could occur in "
Rare	- occurrence re - exceptional' - only occ
Remote	- theor - fr

IEC 2075/09

Figure B.14 – Part example of a risk ranking matrix



IEC 2076/09

Figure B.15 – Part example of a probability criteria matrix

Rating scales and a matrix may be set up with quantitative scales. For example, in a reliability context the probability scale could represent indicative failure rates and the consequence scale the dollar cost of failure.

Use of the tool needs people (ideally a team) with relevant expertise and such data as is available to help in judgements of consequence and probability.

B.29.4 Process

To rank risks, the user first finds the consequence descriptor that best fits the situation then defines the probability with which those consequences will occur. The level of risk is then read off from the matrix.

Many risk events may have a range of outcomes with different associated probability. Usually, minor problems are more common than catastrophes. There is therefore a choice as to whether to rank the most common outcome or the most serious or some other combination. In many cases, it is appropriate to focus on the most serious credible outcomes as these pose the largest threat and are often of most concern. In some cases, it may be appropriate to rank both common problems and unlikely catastrophes as separate risks. It is important that the probability relevant to the selected consequence is used and not the probability of the event as a whole.

The level of risk defined by the matrix may be associated with a decision rule such as to treat or not to treat the risk.

B.29.5 Output

The output is a rating for each risk or a ranked list of risk with significance levels defined.

B.29.6 Strengths and limitations

Strengths:

- relatively easy to use;
- provides a rapid ranking of risks into different significance levels.

Limitations:

- a matrix should be designed to be appropriate for the circumstances so it may be difficult to have a common system applying across a range of circumstances relevant to an organization;
- it is difficult to define the scales unambiguously;
- use is very subjective and there tends to be significant variation between raters;
- risks cannot be aggregated (i.e. one cannot define that a particular number of low risks or a low risk identified a particular number of times is equivalent to a medium risk);
- it is difficult to combine or compare the level of risk for different categories of consequences.

Results will depend of the level of detail of the analysis, i.e. the more detailed the analysis, the higher the number of scenarios, each with a lower probability. This will underestimate the actual level of risk. The way in which scenarios are grouped together in describing risk should be consistent and defined at the start of the study.

B.30 Cost/benefit analysis (CBA)

B.30.1 Overview

Cost/benefit analysis can be used for risk evaluation where total expected costs are weighed against the total expected benefits in order to choose the best or most profitable option. It is an implicit part of many risk evaluation systems. It can be qualitative or quantitative or involve a combination of quantitative and qualitative elements. Quantitative CBA aggregates the monetary value of all costs and all benefits to all stakeholders that are included in the scope and adjusts for different time periods in which costs and benefits accrue. The net present value (NPV) which is produced becomes an input into to decisions about risk. A positive NPV associated with an action would normally mean the action should occur. However, for some negative risks, particularly those involving risks to human life or damage to the environment the ALARP principle may be applied. This divides risks into three regions: a level above which negative risks are intolerable and should not be taken except in extraordinary circumstances; a level below which risks are negligible and need only to be monitored to ensure they remain low; and a central band where risks are made as low as reasonably practicable (ALARP). Towards the lower risk end of this region, a strict cost benefit analysis may apply but where risks are close to intolerable, the expectation of the ALARP principle is that treatment will occur unless the costs of treatment are grossly disproportionate to the benefit gained.

B.30.2 Uses

Cost/benefit analysis can be used to decide between options which involve risk.

For example

- as input into a decision about whether a risk should be treated,
- to differentiate between and decide on the best form of risk treatment,
- to decide between different courses of action.

B.30.3 Inputs

Inputs include information on costs and benefits to relevant stakeholders and on uncertainties in those costs and benefits. Tangible and intangible costs and benefits should be considered. Costs include resources expended and negative outcomes, benefits include positive outcomes, negative outcomes avoided and resources saved.

B.30.4 Process

The stakeholders who may experience costs or receive benefits are identified. In a full cost benefit analysis all stakeholders are included.

The direct and indirect benefits and costs to all relevant stakeholders of the options being considered are identified. Direct benefits are those which flow directly from the action taken, while indirect or ancillary benefits are those which are coincidental but might still contribute significantly to the decision. Examples of indirect benefits include reputation improvement, staff satisfaction and “peace of mind”. (These are often weighted heavily in decision-making).

Direct costs are those that are directly associated with the action. Indirect costs are those additional, ancillary and sunk costs, such as loss of utility, distraction of management time or the diversion of capital away from other potential investments. When applying a cost benefit analysis to a decision on whether to treat a risk, costs and benefits associated with treating the risk, and with taking the risk, should be included

In quantitative cost/benefit analysis, when all tangible and intangible costs and benefits have been identified, a monetary value is assigned to all costs and benefits (including intangible costs and benefits). There are a number of standard ways of doing this including the ‘willingness to pay’ approach and using surrogates. If, as often happens, the cost is incurred over a short period of time (e.g. a year) and the benefits flow for a long period thereafter, it is normally necessary to discount the benefits to bring them into “today’s money” so that a valid comparison can be obtained. All costs and benefits are expressed as a present value. The present value of all costs and all benefits to all stakeholders can be combined to produce a net present value (NPV). A positive NPV implies that the action is beneficial. Benefit cost ratios are also used see B30.5

If there is uncertainty about the level of costs or benefits, either or both terms can be weighted according to their probabilities.

In qualitative cost benefit analysis no attempt is made to find a monetary value for intangible costs and benefits and, rather than providing a single figure summarizing the costs and benefits, relationships and trade-offs between different costs and benefits are considered qualitatively.

A related technique is a cost-effectiveness analysis. This assumes that a certain benefit or outcome is desired, and that there are several alternative ways to achieve it. The analysis looks only at costs and which is the cheapest way to achieve the benefit.

B.30.5 Output

The output of a cost/benefit analysis is information on relative costs and benefits of different options or actions. This may be expressed quantitatively as a net present value (NPV) an internal rate of return (IRR) or as the ratio of the present value of benefits to the present value of costs. Qualitatively the output is usually a table comparing costs and benefits of different types of cost and benefit, drawing attention to trade offs.

B.30.6 Strengths and limitations

Strengths of cost benefit analysis:

- it allows costs and benefits to be compared using a single metric (money);
- it provides transparency of decision making;
- it requires detailed information to be collected on all possible aspects of the decision. This can be valuable in revealing ignorance as well as communicating knowledge.

Limitations:

- quantitative CBA can yield dramatically different numbers, depending on the methods used to assign economic values to non-economic benefits;
- in some applications it is difficult to define a valid discounting rate for future costs and benefits;

- benefits which accrue to a large population are difficult to estimate, particularly those relating to public good which is not exchanged in markets;
- the practice of discounting means that benefits gained in the long term future have negligible influence on the decision depending on the discounting rate chosen. The method becomes unsuitable for consideration of risks affecting future generations unless very low or zero discount rates are set.

B.31 Multi-criteria decision analysis (MCDA)

B.31.1 Overview

The objective is to use a range of criteria to objectively and transparently assess the overall worthiness of a set of options. In general, the overall goal is to produce a preference of order between the available options. The analysis involves the development of a matrix of options and criteria which are ranked and aggregated to provide an overall score for each option.

B.31.2 Use

MCDA can be used for

- comparing multiple options for a first pass analysis to determine preferred and potential options and inappropriate option,
- comparing options where there are multiple and sometimes conflicting criteria,
- reaching a consensus on a decision where different stakeholders have conflicting objectives or values.

B.31.3 Inputs

A set of options for analysis. Criteria, based on objectives that can be used equally across all options to differentiate between them.

B.31.4 Process

In general a group of knowledgeable stakeholders undertakes the following process:

a) define the objective(s);
b) determine the attributes (criteria or performance measures) that relate to each objective;
c) structure the attributes into a hierarchy;
d) develop options to be evaluated against the criteria;
e) determine the importance of the criteria and assign corresponding weights to them;
f) evaluate the alternatives with respect to the criteria. This may be represented as a matrix of scores.
g) combine multiple single-attribute scores into a single aggregate multi attribute score;
h) evaluate the results.

There are different methods by which the weighting for each criteria can be elicited and different ways of aggregating the criteria scores for each option into a single multi-attribute score. For example, scores may be aggregated as a weighted sum or a weighted product or using the analytic hierarchy process, an elicitation technique for the weights and scores based on pairwise comparisons. All these methods assume that the preference for any one criterion does not depend on the values of the other criteria. Where this assumption is not valid, different models are used.

Since scores are subjective, sensitivity analysis is useful to examine the extent to which the weights and scores influence overall preferences between options.

B.31.5 Outputs

Rank order presentation of the options goes from best to least preferred. If the process produces a matrix where the axes of the matrix are criteria weighted and the criteria score for each option, then options that fail highly weighted criteria can also be eliminated.

B.31.6 Strengths and limitations

Strengths:

- provides a simple structure for efficient decision-making and presentation of assumptions and conclusions;
- can make complex decision problems, which are not amenable to cost/benefit analysis, more manageable;
- can help rationally consider problems where tradeoffs need to be made;
- can help achieve agreement when stakeholders have different objectives and hence criteria.

Limitations:

- can be affected by bias and poor selection of the decision criteria;
- most MCDA problems do not have a conclusive or unique solution;
- aggregation algorithms which calculate criteria weights from stated preferences or aggregate differing views can obscure the true basis of the decision.

Bibliography

IEC 61511, *Functional safety – Safety instrumented systems for the process industry sector*

IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

IEC 61882, *Hazard and operability studies (HAZOP studies) – Application guide*

ISO 22000, *Food safety management systems – Requirements for any organization in the food chain*

ISO/IEC Guide 51, *Safety aspects – Guidelines for their inclusion in standards*

IEC 60300-3-11, *Dependability management – Part 3-11: Application guide – Reliability centred maintenance*

IEC 61649, *Weibull analysis*

IEC 61078, *Analysis techniques for dependability – Reliability block diagram and boolean methods*

IEC 61165, *Application of Markov techniques*

ISO/IEC 15909 (all parts), *Software and systems engineering – High-level Petri nets*

IEC 62551, *Analysis techniques for dependability – Petri net techniques*[2]

IEC 61882, *Hazard and operability studies (HAZOP studies) – Application guide*

_____

2 Currently under consideration.

This page deliberately left blank

British Standards Institution (BSI)

BSI is the independent national body responsible for preparing British Standards and other standards-related publications, information and services.
It presents the UK view on standards in Europe and at the international level.

It is incorporated by Royal Charter.

Revisions

British Standards are updated by amendment or revision. Users of British Standards should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using this British Standard would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover.

Tel: +44 (0)20 8996 9001 Fax: +44 (0)20 8996 7001

BSI offers Members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of standards.

Tel: +44 (0)20 8996 7669 Fax: +44 (0)20 8996 7001
Email: plus@bsigroup.com

Buying standards

You may buy PDF and hard copy versions of standards directly using a credit card from the BSI Shop on the website **www.bsigroup.com/shop.** In addition all orders for BSI, international and foreign standards publications can be addressed to BSI Customer Services.

Tel: +44 (0)20 8996 9001 Fax: +44 (0)20 8996 7001
Email: orders@bsigroup.com

In response to orders for international standards, it is BSI policy to supply the BSI implementation of those that have been published as British Standards, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Knowledge Centre.

Tel: +44 (0)20 8996 7004 Fax: +44 (0)20 8996 7005
Email: knowledgecentre@bsigroup.com

Various BSI electronic information services are also available which give details on all its products and services.

Tel: +44 (0)20 8996 7111 Fax: +44 (0)20 8996 7048
Email: info@bsigroup.com

BSI Subscribing Members are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration.

Tel: +44 (0)20 8996 7002 Fax: +44 (0)20 8996 7001
Email: membership@bsigroup.com

Information regarding online access to British Standards via British Standards Online can be found at **www.bsigroup.com/BSOL**

Further information about BSI is available on the BSI website at **www.bsigroup.com/standards**

Copyright

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Tel +44 (0)20 8996 9001
Fax +44 (0)20 8996 7001
www.bsigroup.com/standards

raising standards worldwide™

PD ISO Guide 73:2009

BSI Standards Publication

Risk management — Vocabulary

bsi.

...making excellence a habit.™

National foreword

This Published Document is the UK implementation of ISO Guide 73:2009. It supersedes PD ISO/IEC Guide 73:2002 which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee RM/1, Risk management.

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

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

ISBN 978 0 580 67573 7

ICS 01.040.03; 01.120; 03.100.01

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 30 September 2013.

Amendments issued since publication

Date	Text affected

GUIDE 73

Risk management — Vocabulary

Management du risque — Vocabulaire

First edition 2009
Première édition 2009

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/Publié en Suisse

Contents

Page

Sommaire

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

Draft Guides adopted by the responsible Committee or Group are circulated to the member bodies for voting. Publication as a Guide requires approval by at least 75 % of the member bodies casting a vote.

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.

ISO Guide 73 was prepared by the ISO Technical Management Board Working Group on risk management.

This first edition of ISO Guide 73 cancels and replaces ISO/IEC Guide 73:2002, which has been technically revised.

Avant-propos

L'ISO (Organisation internationale de normalisation) est une fédération mondiale d'organismes nationaux de normalisation (comités membres de l'ISO). L'élaboration des Normes internationales est en général confiée aux comités techniques de l'ISO. Chaque comité membre intéressé par une étude a le droit de faire partie du comité technique créé à cet effet. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO participent également aux travaux. L'ISO collabore étroitement avec la Commission électrotechnique internationale (CEI) en ce qui concerne la normalisation électrotechnique.

Les Normes internationales sont rédigées conformément aux règles données dans les Directives ISO/CEI, Partie 2.

Les projets de Guides adoptés par le comité ou le groupe responsable sont soumis aux comités membres pour vote. Leur publication comme Guides requiert l'approbation de 75 % au moins des comités membres votants.

L'attention est appelée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. L'ISO ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et averti de leur existence.

L'ISO Guide 73 a été élaboré par le groupe de travail du Bureau de gestion technique ISO sur le Management du risque.

Cette première édition de l'ISO Guide 73 annule et remplace l'ISO/CEI Guide 73:2002, qui a fait l'objet d'une révision technique.

Introduction

This Guide provides basic vocabulary to develop common understanding on risk management concepts and terms among organizations and functions, and across different applications and types.

In the context of risk management terminology, it is intended that preference be given to the definitions provided in this Guide.

Risk management is application specific. In some circumstances, it can therefore be necessary to supplement the vocabulary in this Guide. Where terms related to the management of risk are used in a standard, it is imperative that their intended meanings within the context of the standard are not misinterpreted, misrepresented or misused.

In addition to managing threats to the achievement of their objectives, organizations are increasingly applying risk management processes and developing an integrated approach to risk management in order to improve the management of potential opportunities. The terms and definitions in this Guide are, therefore, broader in concept and application than those contained in ISO/IEC Guide 51, which is confined to safety aspects of risk, i.e. with undesirable or negative consequences. Since organizations increasingly adopt a broader approach to the management of risk, this Guide addresses all applications and sectors.

This Guide is generic and is compiled to encompass the general field of risk management. The terms are arranged in the following order:

— terms relating to risk;

— terms relating to risk management;

— terms relating to the risk management process;

— terms relating to communication and consultation;

— terms relating to the context;

— term relating to risk assessment;

— terms relating to risk identification;

— terms relating to risk analysis;

— terms relating to risk evaluation;

— terms relating to risk treatment;

— terms relating to monitoring and measurement.

Introduction

Le présent Guide fournit le vocabulaire de base ayant pour but le développement d'une compréhension des concepts et termes du management du risque qui soit commune aux différents organismes et fonctions, et cela quels que soient leurs types et applications.

Dans le contexte de la terminologie du management du risque, la préférence est à donner aux définitions figurant dans le présent Guide.

Le management du risque est spécifique des applications. Dans certaines circonstances, il peut par conséquent être nécessaire de compléter le vocabulaire contenu dans ce Guide. Lorsque des termes relatifs au management du risque sont utilisés dans une norme, il est impératif que leur sens dans le contexte de la norme ne soit pas sujet à des erreurs d'interprétation, de représentation ou d'utilisation.

Outre la gestion des menaces pouvant peser sur la réalisation de leurs objectifs, les organismes font de plus en plus appel aux processus de management du risque et développent une approche intégrée de management du risque dans le but d'améliorer la gestion des opportunités potentielles. Les termes et définitions du présent Guide ont donc une acception plus large, du point de vue tant conceptuel que pratique, que ceux qui sont recensés dans l'ISO/CEI Guide 51, ce dernier se limitant aux aspects du risque relatifs à la sécurité, c'est-à-dire ceux qui ont des conséquences indésirables ou négatives. Les organismes adoptant de plus en plus fréquemment une approche plus large du management du risque, ce Guide concerne toutes les applications et tous les secteurs.

Le présent Guide est générique et de ce fait concerne le domaine général du management du risque. Les termes y figurent dans l'ordre suivant:

— termes relatifs au risque;

— termes relatifs au management du risque;

— termes relatifs au processus de management du risque;

— termes relatifs à la communication et à la concertation;

— termes relatifs au contexte;

— termes relatifs à l'appréciation du risque;

— termes relatifs à l'identification des risques;

— termes relatifs à l'analyse du risque;

— termes relatifs à l'évaluation du risque;

— termes relatifs au traitement du risque;

— termes relatifs à la surveillance et à la mesure.

Risk management — Vocabulary

Management du risque — Vocabulaire

Scope

This Guide provides the definitions of generic terms related to risk management. It aims to encourage a mutual and consistent understanding of, and a coherent approach to, the description of activities relating to the management of risk, and the use of uniform risk management terminology in processes and frameworks dealing with the management of risk.

This Guide is intended to be used by:

— those engaged in managing risks,

— those who are involved in activities of ISO and IEC, and

— developers of national or sector-specific standards, guides, procedures and codes of practice relating to the management of risk.

For principles and guidelines on risk management, reference is made to ISO 31000:2009.

Domaine d'application

Le présent Guide fournit les définitions de termes génériques relatifs au management du risque. Son but est d'encourager une compréhension commune homogène et une approche cohérente de la description des activités relatives au management du risque, ainsi qu'une utilisation uniforme de la terminologie du management du risque dans les processus et cadres organisationnels en rapport avec ce domaine.

Le présent Guide est à l'usage

— des personnes chargées du management des risques,

— des personnes impliquées dans les activités de l'ISO et de la CEI, et

— des personnes chargées de rédiger des normes, guides, procédures et codes de bonne pratique relatifs au management du risque, soit spécifiques d'un secteur, soit à l'échelle nationale.

Concernant les principes et lignes directrices du management du risque, il est fait référence à l'ISO 31000:2009.

1 Terms relating to risk

1.1
risk
effect of uncertainty on objectives

NOTE 1 An effect is a deviation from the expected — positive and/or negative.

NOTE 2 Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process).

1 Termes relatifs au risque

1.1
risque
effet de l'incertitude sur l'atteinte des objectifs

NOTE 1 Un effet est un écart, positif et/ou négatif, par rapport à une attente.

NOTE 2 Les objectifs peuvent avoir différents aspects (par exemple buts financiers, de santé et de sécurité, ou environnementaux) et peuvent concerner différents niveaux (niveau stratégique, niveau d'un projet, d'un produit, d'un processus ou d'un organisme tout entier).

NOTE 3 Risk is often characterized by reference to potential **events** (3.5.1.3) and **consequences** (3.6.1.3), or a combination of these.

NOTE 4 Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated **likelihood** (3.6.1.1) of occurrence.

NOTE 5 Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

2 Terms relating to risk management

2.1
risk management
coordinated activities to direct and control an organization with regard to **risk** (1.1)

2.1.1
risk management framework
set of components that provide the foundations and organizational arrangements for designing, implementing, **monitoring** (3.8.2.1), reviewing and continually improving **risk management** (2.1) throughout the organization

NOTE 1 The foundations include the policy, objectives, mandate and commitment to manage **risk** (1.1).

NOTE 2 The organizational arrangements include plans, relationships, accountabilities, resources, processes and activities.

NOTE 3 The risk management framework is embedded within the organization's overall strategic and operational policies and practices.

2.1.2
risk management policy
statement of the overall intentions and direction of an organization related to **risk management** (2.1)

2.1.3
risk management plan
scheme within the **risk management framework** (2.1.1) specifying the approach, the management components and resources to be applied to the management of **risk** (1.1)

NOTE 3 Un risque est souvent caractérisé en référence à des **événements** (3.5.1.3) et des **conséquences** (3.6.1.3) potentiels ou à une combinaison des deux.

NOTE 4 Un risque est souvent exprimé en termes de combinaison des conséquences d'un événement (incluant des changements de circonstances) et de sa **vraisemblance** (3.6.1.1).

NOTE 5 L'incertitude est l'état, même partiel, de défaut d'information concernant la compréhension ou la connaissance d'un événement, de ses conséquences ou de sa vraisemblance.

2 Termes relatifs au management du risque

2.1
management du risque
activités coordonnées dans le but de diriger et piloter un organisme vis-à-vis du **risque** (1.1)

2.1.1
cadre organisationnel de management du risque
ensemble d'éléments établissant les fondements et dispositions organisationnelles présidant à la conception, la mise en œuvre, la **surveillance** (3.8.2.1), la revue et l'amélioration continue du **management du risque** (2.1) dans tout l'organisme

NOTE 1 Les fondements incluent la politique, les objectifs, le mandat et l'engagement envers le management du **risque** (1.1).

NOTE 2 Les dispositions organisationnelles incluent les plans, les relations, les responsabilités, les ressources, les processus et les activités.

NOTE 3 Le cadre organisationnel du management du risque fait partie intégrante des politiques stratégiques et opérationnelles ainsi que des pratiques de l'ensemble de l'organisme.

2.1.2
politique de management du risque
déclaration des intentions et des orientations générales d'un organisme en relation avec le **management du risque** (2.1)

2.1.3
plan de management du risque
programme inclus dans le **cadre organisationnel de management du risque** (2.1.1), spécifiant l'approche, les composantes du management et les ressources auxquelles doit avoir recours le management du **risque** (1.1)

NOTE 1 Management components typically include procedures, practices, assignment of responsibilities, sequence and timing of activities.

NOTE 2 The risk management plan can be applied to a particular product, process and project, and part or whole of the organization.

3 Terms relating to the risk management process

3.1
risk management process
systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, **monitoring** (3.8.2.1) and reviewing **risk** (1.1)

3.2 Terms relating to communication and consultation

3.2.1
communication and consultation
continual and iterative processes that an organization conducts to provide, share or obtain information, and to engage in dialogue with **stakeholders** (3.2.1.1) regarding the management of **risk** (1.1)

NOTE 1 The information can relate to the existence, nature, form, **likelihood** (3.6.1.1), significance, evaluation, acceptability and treatment of the management of risk.

NOTE 2 Consultation is a two-way process of informed communication between an organization and its stakeholders on an issue prior to making a decision or determining a direction on that issue. Consultation is:

— a process which impacts on a decision through influence rather than power; and

— an input to decision making, not joint decision making.

3.2.1.1
stakeholder
person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity

NOTE A decision maker can be a stakeholder.

NOTE 1 Les composantes du management incluent, par exemple, les procédures, les pratiques, l'attribution des responsabilités, le déroulement chronologique des activités.

NOTE 2 Le plan de management du risque peut être appliqué à un produit, un processus, un projet particulier, à une partie de l'organisme ou à l'organisme tout entier.

3 Termes relatifs au processus de management du risque

3.1
processus de management du risque
application systématique de politiques, procédures et pratiques de management aux activités de communication, de concertation, d'établissement du contexte, ainsi qu'aux activités d'identification, d'analyse, d'évaluation, de traitement, de **surveillance** (3.8.2.1) et de revue des **risques** (1.1)

3.2 Termes relatifs à la communication et à la concertation

3.2.1
communication et concertation
processus itératifs et continus mis en œuvre par un organisme afin de fournir, partager ou obtenir des informations et d'engager un dialogue avec les **parties prenantes** (3.2.1.1) concernant le management du **risque** (1.1)

NOTE 1 Ces informations peuvent concerner l'existence, la nature, la forme, la **vraisemblance** (3.6.1.1), l'importance, l'évaluation, l'acceptabilité et le traitement des aspects du management du risque.

NOTE 2 La concertation est un processus de communication argumentée à double sens entre un organisme et ses parties prenantes sur une question donnée avant de prendre une décision ou de déterminer une orientation concernant ladite question. La concertation est

— un processus dont l'effet sur une décision s'exerce par l'influence plutôt que par le pouvoir, et

— une contribution à une prise de décision, et non une prise de décision conjointe.

3.2.1.1
partie prenante
personne ou organisme susceptible d'affecter, d'être affecté ou de se sentir lui-même affecté par une décision ou une activité

NOTE Un décideur peut être une partie prenante.

3.2.1.2
risk perception
stakeholder's (3.2.1.1) view on a **risk** (1.1)

NOTE Risk perception reflects the stakeholder's needs, issues, knowledge, belief and values.

3.2.1.2
perception du risque
point de vue d'une **partie prenante** (3.2.1.1) concernant un **risque** (1.1)

NOTE La perception du risque reflète les besoins, les questions, les connaissances, les convictions et les valeurs de la partie prenante.

3.3 Terms relating to the context

3.3 Termes relatifs au contexte

3.3.1
establishing the context
defining the external and internal parameters to be taken into account when managing risk, and setting the scope and **risk criteria** (3.3.1.3) for the **risk management policy** (2.1.2)

3.3.1
établissement du contexte
définition des paramètres externes et internes à prendre en compte lors du management du risque et définition du domaine d'application ainsi que des **critères de risque** (3.3.1.3) pour la **politique de management du risque** (2.1.2)

3.3.1.1
external context
external environment in which the organization seeks to achieve its objectives

NOTE External context can include:

— the cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;

— key drivers and trends having impact on the objectives of the organization; and

— relationships with, and perceptions and values of external **stakeholders** (3.2.1.1).

3.3.1.1
contexte externe
environnement externe dans lequel l'organisme cherche à atteindre ses objectifs

NOTE Le contexte externe peut inclure

— l'environnement culturel, social, politique, légal, réglementaire, financier, technologique, économique, naturel et concurrentiel, au niveau international, national, régional ou local,

— les facteurs et tendances ayant un impact déterminant sur les objectifs de l'organisme, et

— les relations avec les **parties prenantes** (3.2.1.1) externes, leurs perceptions et leurs valeurs.

3.3.1.2
internal context
internal environment in which the organization seeks to achieve its objectives

NOTE Internal context can include:

— governance, organizational structure, roles and accountabilities;

— policies, objectives, and the strategies that are in place to achieve them;

— the capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);

— information systems, information flows and decision-making processes (both formal and informal);

— relationships with, and perceptions and values of internal stakeholders;

— the organization's culture;

3.3.1.2
contexte interne
environnement interne dans lequel l'organisme cherche à atteindre ses objectifs

NOTE Le contexte interne peut inclure

— la gouvernance, l'organisation, les rôles et responsabilités,

— les politiques, les objectifs et les stratégies mises en place pour atteindre ces derniers,

— les capacités, en termes de ressources et de connaissances (par exemple capital, temps, personnels, processus, systèmes et technologies),

— les systèmes d'information, les flux d'information et les processus de prise de décision (à la fois formels et informels),

— les relations avec les parties prenantes internes, ainsi que leurs perceptions et leurs valeurs,

— la culture de l'organisme,

— standards, guidelines and models adopted by the organization; and

— form and extent of contractual relationships.

— les normes, lignes directrices et modèles adoptés par l'organisme, et

— la forme et l'étendue des relations contractuelles.

3.3.1.3
risk criteria
terms of reference against which the significance of a **risk** (1.1) is evaluated

NOTE 1 Risk criteria are based on organizational objectives, and **external** (3.3.1.1) and **internal context** (3.3.1.2).

NOTE 2 Risk criteria can be derived from standards, laws, policies and other requirements.

3.3.1.3
critères de risque
termes de référence vis-à-vis desquels l'importance d'un **risque** (1.1) est évaluée

NOTE 1 Les critères de risque sont fondés sur les objectifs de l'organisme ainsi que sur le **contexte externe** (3.3.1.1) et **interne** (3.3.1.2).

NOTE 2 Les critères de risque peuvent être issus de normes, de lois, de politiques et d'autres exigences.

3.4 Term relating to risk assessment

3.4.1
risk assessment
overall process of **risk identification** (3.5.1), **risk analysis** (3.6.1) and **risk evaluation** (3.7.1)

3.4 Termes relatifs à l'appréciation du risque

3.4.1
appréciation du risque
ensemble du processus d'**identification des risques** (3.5.1), d'**analyse du risque** (3.6.1) et d'**évaluation du risque** (3.7.1)

3.5 Terms relating to risk identification

3.5.1
risk identification
process of finding, recognizing and describing **risks** (1.1)

NOTE 1 Risk identification involves the identification of **risk sources** (3.5.1.2), **events** (3.5.1.3), their causes and their potential **consequences** (3.6.1.3).

NOTE 2 Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and **stakeholder**'s (3.2.1.1) needs.

3.5 Termes relatifs à l'identification des risques

3.5.1
identification des risques
processus de recherche, de reconnaissance et de description des **risques** (1.1)

NOTE 1 L'identification des risques comprend l'identification des **sources de risque** (3.5.1.2), des **événements** (3.5.1.3), de leurs causes et de leurs **conséquences** (3.6.1.3) potentielles.

NOTE 2 L'identification des risques peut faire appel à des données historiques, des analyses théoriques, des avis d'experts et autres personnes compétentes et tenir compte des besoins des **parties prenantes** (3.2.1.1).

3.5.1.1
risk description
structured statement of risk usually containing four elements: sources, **events** (3.5.1.3), causes and **consequences** (3.6.1.3)

3.5.1.1
description du risque
représentation structurée du risque contenant généralement quatre éléments: les sources, les **événements** (3.5.1.3), les causes et les **conséquences** (3.6.1.3)

3.5.1.2
risk source
element which alone or in combination has the intrinsic potential to give rise to **risk** (1.1)

NOTE A risk source can be tangible or intangible.

3.5.1.3
event
occurrence or change of a particular set of circumstances

NOTE 1 An event can be one or more occurrences, and can have several causes.

NOTE 2 An event can consist of something not happening.

NOTE 3 An event can sometimes be referred to as an "incident" or "accident".

NOTE 4 An event without **consequences** (3.6.1.3) can also be referred to as a "near miss", "incident", "near hit" or "close call".

3.5.1.4
hazard
source of potential harm

NOTE Hazard can be a **risk source** (3.5.1.2).

3.5.1.5
risk owner
person or entity with the accountability and authority to manage a **risk** (1.1)

3.6 Terms relating to risk analysis

3.6.1
risk analysis
process to comprehend the nature of **risk** (1.1) and to determine the **level of risk** (3.6.1.8)

NOTE 1 Risk analysis provides the basis for **risk evaluation** (3.7.1) and decisions about **risk treatment** (3.8.1).

NOTE 2 Risk analysis includes risk estimation.

3.5.1.2
source de risque
tout élément qui, seul ou combiné à d'autres, présente un potentiel intrinsèque d'engendrer un **risque** (1.1)

NOTE Une source de risque peut être tangible ou intangible.

3.5.1.3
événement
occurrence ou changement d'un ensemble particulier de circonstances

NOTE 1 Un événement peut être unique ou se reproduire et peut avoir plusieurs causes.

NOTE 2 Un événement peut consister en quelque chose qui ne se produit pas.

NOTE 3 Un événement peut parfois être qualifié «d'incident» ou «d'accident».

NOTE 4 Un événement sans **conséquences** (3.6.1.3) peut également être appelé «quasi-accident» ou «incident» ou «presque succès».

3.5.1.4
phénomène dangereux
source de dommage potentiel

NOTE Un phénomène dangereux peut être une **source de risque** (3.5.1.2).

3.5.1.5
propriétaire du risque
personne ou entité ayant la responsabilité du **risque** (1.1) et ayant autorité pour le gérer

3.6 Termes relatifs à l'analyse du risque

3.6.1
analyse du risque
processus mis en œuvre pour comprendre la nature d'un **risque** (1.1) et pour déterminer le **niveau de risque** (3.6.1.8)

NOTE 1 L'analyse du risque fournit la base de l'**évaluation du risque** (3.7.1) et les décisions relatives au **traitement du risque** (3.8.1).

NOTE 2 L'analyse du risque inclut l'estimation du risque.

3.6.1.1
likelihood
chance of something happening

NOTE 1 In risk management terminology, the word "likelihood" is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically [such as a **probability** (3.6.1.4) or a **frequency** (3.6.1.5) over a given time period].

NOTE 2 The English term "likelihood" does not have a direct equivalent in some languages; instead, the equivalent of the term "probability" is often used. However, in English, "probability" is often narrowly interpreted as a mathematical term. Therefore, in risk management terminology, "likelihood" is used with the intent that it should have the same broad interpretation as the term "probability" has in many languages other than English.

3.6.1.1
vraisemblance
possibilité que quelque chose se produise

NOTE 1 Dans la terminologie du management du risque, le mot «vraisemblance» est utilisé pour indiquer la possibilité que quelque chose se produise, que cette possibilité soit définie, mesurée ou déterminée de façon objective ou subjective, qualitative ou quantitative, et qu'elle soit décrite au moyen de termes généraux ou mathématiques [telles une **probabilité** (3.6.1.4) ou une **fréquence** (3.6.1.5) sur une période donnée].

NOTE 2 Le terme anglais «likelihood» (vraisemblance) n'a pas d'équivalent direct dans certaines langues et c'est souvent l'équivalent du terme «probability» (probabilité) qui est utilisé à la place. En anglais, cependant, le terme «probability» (probabilité) est souvent limité à son interprétation mathématique. Par conséquent, dans la terminologie du management du risque, le terme «vraisemblance» est utilisé avec l'intention qu'il fasse l'objet d'une interprétation aussi large que celle dont bénéficie le terme «probability» (probabilité) dans de nombreuses langues autres que l'anglais.

3.6.1.2
exposure
extent to which an organization and/or **stakeholder** (3.2.1.1) is subject to an **event** (3.5.1.3)

3.6.1.2
exposition
degré auquel un organisme et/ou une **partie prenante** (3.2.1.1) sont soumis à un **événement** (3.5.1.3)

3.6.1.3
consequence
outcome of an **event** (3.5.1.3) affecting objectives

NOTE 1 An event can lead to a range of consequences.

NOTE 2 A consequence can be certain or uncertain and can have positive or negative effects on objectives.

NOTE 3 Consequences can be expressed qualitatively or quantitatively.

NOTE 4 Initial consequences can escalate through knock-on effects.

3.6.1.3
conséquence
effet d'un **événement** (3.5.1.3) affectant les objectifs

NOTE 1 Un événement peut engendrer une série de conséquences.

NOTE 2 Une conséquence peut être certaine ou incertaine et peut avoir des effets positifs ou négatifs sur l'atteinte des objectifs.

NOTE 3 Les conséquences peuvent être exprimées de façon qualitative ou quantitative.

NOTE 4 Des conséquences initiales peuvent déclencher des réactions en chaîne.

3.6.1.4
probability
measure of the chance of occurrence expressed as a number between 0 and 1, where 0 is impossibility and 1 is absolute certainty

NOTE See definition 3.6.1.1, Note 2.

3.6.1.4
probabilité
mesure de la possibilité d'occurrence exprimée par un chiffre entre 0 et 1, 0 indiquant une impossibilité et 1 indiquant une certitude absolue

NOTE Voir définition 3.6.1.1, Note 2.

3.6.1.5
frequency
number of **events** (3.5.1.3) or outcomes per defined unit of time

NOTE Frequency can be applied to past **events** (3.5.1.3) or to potential future events, where it can be used as a measure of **likelihood** (3.6.1.1)/**probability** (3.6.1.3).

3.6.1.6
vulnerability
intrinsic properties of something resulting in susceptibility to a **risk source** (3.5.1.2) that can lead to an event with a **consequence** (3.6.1.3)

3.6.1.7
risk matrix
tool for ranking and displaying **risks** (1.1) by defining ranges for **consequence** (3.6.1.3) and **likelihood** (3.6.1.1)

3.6.1.8
level of risk
magnitude of a **risk** (1.1) or combination of risks, expressed in terms of the combination of **consequences** (3.6.1.3) and their **likelihood** (3.6.1.1)

3.7 Terms relating to risk evaluation

3.7.1
risk evaluation
process of comparing the results of **risk analysis** (3.6.1) with **risk criteria** (3.3.1.3) to determine whether the **risk** (1.1) and/or its magnitude is acceptable or tolerable

NOTE Risk evaluation assists in the decision about **risk treatment** (3.8.1).

3.7.1.1
risk attitude
organization's approach to assess and eventually pursue, retain, take or turn away from **risk** (1.1)

3.6.1.5
fréquence
nombre d'**événements** (3.5.1.3) ou d'effets par unité de temps donnée

NOTE La fréquence peut s'appliquer à des **événements** (3.5.1.3) passés ou des potentiels événements futurs, où elle peut être utilisée comme mesure de la **vraisemblance** (3.6.1.1)/**probabilité** (3.6.1.3).

3.6.1.6
vulnérabilité
propriétés intrinsèques de quelque chose entraînant une sensibilité à une **source de risque** (3.5.1.2) pouvant induire un événement avec une **conséquence** (3.6.1.3)

3.6.1.7
matrice de risque
outil permettant de classer et de visualiser des **risques** (1.1) en définissant des catégories de **conséquences** (3.6.1.3) et de leur **vraisemblance** (3.6.1.1)

3.6.1.8
niveau de risque
importance d'un **risque** (1.1) ou combinaison de risques, exprimée en termes de combinaison des **conséquences** (3.6.1.3) et de leur **vraisemblance** (3.6.1.1)

3.7 Termes relatifs à l'évaluation du risque

3.7.1
évaluation du risque
processus de comparaison des résultats de l'**analyse du risque** (3.6.1) avec les **critères de risque** (3.3.1.3) afin de déterminer si le **risque** (1.1) et/ou son importance sont acceptables ou tolérables

NOTE L'évaluation du risque aide à la prise de décision relative au **traitement du risque** (3.8.1).

3.7.1.1
attitude face au risque
approche d'un organisme pour apprécier un **risque** (1.1) avant, éventuellement, de saisir ou préserver une opportunité ou de prendre ou rejeter un risque

3.7.1.2
risk appetite
amount and type of **risk** (1.1) that an organization is willing to pursue or retain

3.7.1.3
risk tolerance
organization's or **stakeholder**'s (3.2.1.1) readiness to bear the **risk** (1.1) after **risk treatment** (3.8.1) in order to achieve its objectives

NOTE Risk tolerance can be influenced by legal or regulatory requirements.

3.7.1.4
risk aversion
attitude to turn away from **risk** (1.1)

3.7.1.5
risk aggregation
combination of a number of risks into one **risk** (1.1) to develop a more complete understanding of the overall risk

3.7.1.6
risk acceptance
informed decision to take a particular **risk** (1.1)

NOTE 1 Risk acceptance can occur without **risk treatment** (3.8.1) or during the process of risk treatment.

NOTE 2 Accepted risks are subject to **monitoring** (3.8.2.1) and **review** (3.8.2.2).

3.8 Terms relating to risk treatment

3.8.1
risk treatment
process to modify **risk** (1.1)

NOTE 1 Risk treatment can involve:

— avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;

— taking or increasing risk in order to pursue an opportunity;

— removing the **risk source** (3.5.1.2);

— changing the **likelihood** (3.6.1.1);

3.7.1.2
goût du risque
importance et type de **risque** (1.1) qu'un organisme est prêt à saisir ou à préserver

3.7.1.3
tolérance au risque
disposition d'un organisme ou d'une **partie prenante** (3.2.1.1) à supporter le **risque** (1.1) après un **traitement du risque** (3.8.1) afin d'atteindre ses objectifs

NOTE La tolérance au risque peut être régie par des obligations légales ou réglementaires.

3.7.1.4
aversion pour le risque
attitude de rejet du **risque** (1.1)

3.7.1.5
agrégation de risques
combinaison d'un nombre de risques en un seul **risque** (1.1) afin de développer une compréhension plus complète du risque en général

3.7.1.6
acceptation du risque
décision argumentée en faveur de la prise d'un **risque** (1.1) particulier

NOTE 1 L'acceptation du risque peut avoir lieu sans **traitement du risque** (3.8.1) ou au cours du processus de traitement du risque.

NOTE 2 Les risques acceptés font l'objet d'une **surveillance** (3.8.2.1) et d'une **revue** (3.8.2.2).

3.8 Termes relatifs au traitement du risque

3.8.1
traitement du risque
processus destiné à modifier un **risque** (1.1)

NOTE 1 Le traitement du risque peut inclure

— un refus du risque en décidant de ne pas démarrer ou poursuivre l'activité porteuse du risque,

— la prise ou l'augmentation d'un risque afin de saisir une opportunité,

— l'élimination de la **source de risque** (3.5.1.2),

— une modification de la **vraisemblance** (3.6.1.1),

— changing the **consequences** (3.6.1.3);

— sharing the risk with another party or parties [including contracts and **risk financing** (3.8.1.4)]; and

— retaining the risk by informed decision.

NOTE 2 Risk treatments that deal with negative consequences are sometimes referred to as “risk mitigation”, “risk elimination”, “risk prevention” and “risk reduction”.

NOTE 3 Risk treatment can create new risks or modify existing risks.

— une modification des **conséquences** (3.6.1.3),

— un partage du risque avec une ou plusieurs autres parties [incluant des contrats et un **financement du risque** (3.8.1.4)], et

— un maintien du risque fondé sur une décision argumentée.

NOTE 2 Les traitements du risque portant sur les conséquences négatives sont parfois appelés «atténuation du risque», «élimination du risque», «prévention du risque» et «réduction du risque».

NOTE 3 Le traitement du risque peut créer de nouveaux risques ou modifier des risques existants.

3.8.1.1
control

measure that is modifying **risk** (1.1)

NOTE 1 Controls include any process, policy, device, practice, or other actions which modify risk.

NOTE 2 Controls may not always exert the intended or assumed modifying effect.

3.8.1.1
moyen de maîtrise

mesure qui modifie un **risque** (1.1)

NOTE 1 Un moyen de maîtrise du risque inclut n'importe quels processus, politique, dispositif, pratique ou autres actions qui modifient un risque.

NOTE 2 Un moyen de maîtrise du risque n'aboutit pas toujours nécessairement à la modification voulue ou supposée.

3.8.1.2
risk avoidance

informed decision not to be involved in, or to withdraw from, an activity in order not to be exposed to a particular **risk** (1.1)

NOTE Risk avoidance can be based on the result of **risk evaluation** (3.7.1) and/or legal and regulatory obligations.

3.8.1.2
refus du risque

décision argumentée de ne pas s'engager dans une activité, ou de s'en retirer, afin de ne pas être exposé à un **risque** (1.1) particulier

NOTE Le refus du risque peut être fondé sur le résultat d'une **évaluation du risque** (3.7.1) et/ou sur des obligations légales et réglementaires.

3.8.1.3
risk sharing

form of **risk treatment** (3.8.1) involving the agreed distribution of **risk** (1.1) with other parties

NOTE 1 Legal or regulatory requirements can limit, prohibit or mandate risk sharing.

NOTE 2 Risk sharing can be carried out through insurance or other forms of contract.

NOTE 3 The extent to which risk is distributed can depend on the reliability and clarity of the sharing arrangements.

NOTE 4 Risk transfer is a form of risk sharing.

3.8.1.3
partage du risque

forme de **traitement du risque** (3.8.1) impliquant la répartition consentie du **risque** (1.1) avec d'autres parties

NOTE 1 Des obligations légales ou réglementaires peuvent limiter, interdire ou imposer le partage du risque.

NOTE 2 Le partage du risque peut intervenir sous forme d'assurances ou autres types de contrats.

NOTE 3 Le degré de répartition du risque peut dépendre de la fiabilité et de la clarté des dispositions prises pour le partage.

NOTE 4 Le transfert du risque est une forme de partage du risque.

3.8.1.4
risk financing
form of **risk treatment** (3.8.1) involving contingent arrangements for the provision of funds to meet or modify the financial **consequences** (3.6.1.3) should they occur

3.8.1.4
financement du risque
forme de **traitement du risque** (3.8.1) mettant en jeu des arrangements contingents pour provisionner des fonds afin de faire face à d'éventuelles **conséquences** (3.6.1.3) financières ou de les modifier

3.8.1.5
risk retention
acceptance of the potential benefit of gain, or burden of loss, from a particular **risk** (1.1)

NOTE 1 Risk retention includes the acceptance of **residual risks** (3.8.1.6).

NOTE 2 The **level of risk** (3.6.1.8) retained can depend on **risk criteria** (3.3.1.3).

3.8.1.5
prise de risque
acceptation de l'avantage potentiel d'un gain ou de la charge potentielle d'une perte découlant d'un **risque** (1.1) particulier

NOTE 1 La prise de risque comprend l'acceptation des **risques résiduels** (3.8.1.6).

NOTE 2 Le **niveau de risque** (3.6.1.8) pris peut dépendre des **critères de risque** (3.3.1.3).

3.8.1.6
residual risk
risk (1.1) remaining after **risk treatment** (3.8.1)

NOTE 1 Residual risk can contain unidentified risk.

NOTE 2 Residual risk can also be known as “retained risk”.

3.8.1.6
risque résiduel
risque (1.1) subsistant après le **traitement du risque** (3.8.1)

NOTE 1 Un risque résiduel peut inclure un risque non identifié.

NOTE 2 Un risque résiduel peut également être appelé «risque pris».

3.8.1.7
resilience
adaptive capacity of an organization in a complex and changing environment

3.8.1.7
résilience
capacité d'adaptation d'un organisme dans un environnement complexe et changeant

3.8.2 Terms relating to monitoring and measurement

3.8.2.1
monitoring
continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected

NOTE Monitoring can be applied to a **risk management framework** (2.1.1), **risk management process** (3.1), **risk** (1.1) or **control** (3.8.1.1).

3.8.2 Termes relatifs à la surveillance et à la mesure

3.8.2.1
surveillance
vérification, supervision, observation critique ou détermination de l'état afin d'identifier continûment des changements par rapport au niveau de performance exigé ou attendu

NOTE La surveillance peut s'appliquer à un **cadre organisationnel de management du risque** (2.1.1), un **processus de management du risque** (3.1), un **risque** (1.1) ou un **moyen de maîtrise** (3.8.1.1) du risque.

3.8.2.2
review
activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives

NOTE Review can be applied to a **risk management framework** (2.1.1), **risk management process** (3.1), **risk** (1.1) or **control** (3.8.1.1).

3.8.2.2
revue
activité entreprise afin de déterminer l'adaptation, l'adéquation et l'efficacité de l'objet étudié pour atteindre les objectifs établis

NOTE La revue peut s'appliquer à un **cadre organisationnel de management du risque** (2.1.1), un **processus de management du risque** (3.1), un **risque** (1.1) ou un **moyen de maîtrise** (3.8.1.1) du risque.

3.8.2.3
risk reporting
form of communication intended to inform particular internal or external **stakeholders** (3.2.1.1) by providing information regarding the current state of **risk** (1.1) and its management

3.8.2.3
rapport sur les risques
forme de communication destinée à informer certaines **parties prenantes** (3.2.1.1) internes ou externes en leur fournissant des informations relatives à l'état du **risque** (1.1) présent et à son management

3.8.2.4
risk register
record of information about identified **risks** (1.1)

NOTE The term “risk log” is sometimes used instead of “risk register”.

3.8.2.4
registre des risques
enregistrement des informations relatives aux **risques** (1.1) identifiés

NOTE Le terme «journal des risques» est parfois utilisé à la place de «registre des risques».

3.8.2.5
risk profile
description of any set of **risks** (1.1)

NOTE The set of risks can contain those that relate to the whole organization, part of the organization, or as otherwise defined.

3.8.2.5
profil de risque
description d'un ensemble quelconque de **risques** (1.1)

NOTE Cet ensemble de risques peut inclure les risques relatifs à l'ensemble de l'organisme, à une partie de celui-ci, ou être défini autrement.

3.8.2.6
risk management audit
systematic, independent and documented process for obtaining evidence and evaluating it objectively in order to determine the extent to which the **risk management framework** (2.1.1), or any selected part of it, is adequate and effective

3.8.2.6
audit de management du risque
processus systématique, indépendant et documenté destiné à obtenir des preuves et à les évaluer de façon objective afin de déterminer le degré d'adéquation et d'efficacité du **cadre organisationnel de management du risque** (2.1.1) ou d'une partie particulière de celui-ci

Bibliography

[1] ISO 704, *Terminology work — Principles and methods*

[2] ISO 860, *Terminology work — Harmonization of concepts and terms*

[3] ISO 3534-1, *Statistics — Vocabulary and symbols — Part 1: General statistical terms and terms used in probability*

[4] ISO 9000, *Quality management systems — Fundamentals and vocabulary*

[5] ISO 10241, *International terminology standards — Preparation and layout*

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

[7] ISO/IEC Guide 2, *Standardization and related activities — General vocabulary*

[8] ISO/IEC Guide 51, *Safety aspects — Guidelines for their inclusion in standards*

Bibliographie

[1] ISO 704, *Travail terminologique — Principes et méthodes*

[2] ISO 860, *Travaux terminologiques — Harmonisation des concepts et des termes*

[3] ISO 3534-1, *Statistique — Vocabulaire et symboles — Partie 1: Termes statistiques généraux et termes utilisés en calcul des probabilités*

[4] ISO 9000, *Systèmes de management de la qualité — Principes essentiels et vocabulaire*

[5] ISO 10241, *Normes terminologiques internationales — Élaboration et présentation*

[6] ISO 31000:2009, *Management du risque — Principes et lignes directrices*

[7] ISO/CEI Guide 2, *Normalisation et activités connexes — Vocabulaire général*

[8] ISO/CEI Guide 51, *Aspects liés à la sécurité — Principes directeurs pour les inclure dans les normes*

Alphabetical index

Index alphabétique

International Organization for Standardization
Case postale 56 • CH-1211 GENEVA 20 • Switzerland

Ref. No.: ISO GUIDE 73:2009(E/F)

ICS 01.040.03; 01.120; 03.100.01

Price based on 15 pages / Prix basé sur 15 pages

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

bsi.

...making excellence a habit.™

Managing Risk the ISO 31000 Way

David Smith and Rob Politowski

bsi.

Managing Risk the ISO 31000 Way

Managing Risk the ISO 31000 Way

By David Smith and Rob Politowski

bsi.

First published in the UK in 2013

By
BSI Standards Limited
389 Chiswick High Road
London W4 4AL

Typeset in Great Britain by Letterpart Limited

Printed in Great Britain by Berforts Group, www.berforts.co.uk

British Library Cataloguing in Publication Data

A catalogue record for this book is available from the British Library

ISBN 978-0-580-67512-6

Contents

Acknowledgements

The authors would like to thank the book reviewers and particularly Michael Faber for his constructive comments. The authors would also like to thank GPIC Bahrain and RTA Dubai for allowing them to see the good practices that they have implemented in line with ISO 31000.

Chapter 1 - Introduction

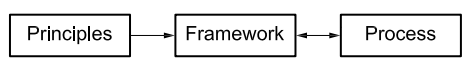
All organizations face many risks, some of which will be well known and managed. Others may pose significant threats to the organization and may well be ignored or poorly managed. It has to be recognized that it is unlikely all risks will be identified, but the aim for all organizations should be to create a framework that:

- manages risks that are identified;
- provides a structure for dealing with risks that emerge which have not been identified; and
- creates a more resilient organization, enabling it to respond to future risks in a time of need.

The whole question of risk has now attracted the attention of the media around the world and examples of poor risk management and governance regularly hit the headlines. The consequences of poor risk management are all too evident in how they can affect us all, as taxpayers, workers and consumers, as well as in the impacts they can have upon the environment and society in general.

Risk and its effective management is the subject of significant numbers of publications and academic work. Whilst these approaches have much merit they are often perceived to be far too complex for the smaller organization and it is the small- to medium-sized businesses at which this book is primarily aimed, i.e. smaller organizations seeking simple guidance on the implementation of an effective risk management system that brings real benefits. This book is intended to help organizations survive and thrive in an ever changing world, a world where those organizations that do not embrace risk management may fail.

The ISO 31000 standard for managing risk has three main components:



The standard identifies 11 core principles of risk management with the intention that these will be addressed by the development of the risk management framework. In turn, the framework assists in managing risk through risk management processes.

In large, complex organizations there may be many hundreds, or even thousands, of risks, many of which will not be significant or will have well-established controls in place, such as emergency evacuation plans. Smaller organizations that are not complex may have fewer significant risks. The framework proposed in ISO 31000 indicates that management of individual processes are typically separate arrangements.

In many organizations there are well-established, formal systems to manage specific risks that are based on international standards such as quality (ISO 9001), environment (ISO 14001), information security (ISO/IEC 27001), food safety (ISO 22000), business continuity (ISO 22301) and occupational health and safety (OHSAS 18001), which have been accommodated within the overall management system of the organization. In some cases, this is a regulatory requirement. The management system in operation, particularly if it is based on an integrated approach such as that prescribed in PAS 99, may well be seen as a foundation for the framework. This book provides guidance in developing a mechanism for managing risk in accordance with ISO 31000, where necessary including the good practices outlined in BS 31100 and PAS 99 for managing processes in an integrated manner.

Whilst the two risk management publications, ISO 31000 and BS 31100, provide an excellent framework, there are a number of areas in both standards where there is no substantive guidance. In these areas, such as policy statements, internal auditing and management reviews, this book provides considerable extra guidance with examples, where appropriate. In those areas where the additional guidance provided by BS 31100 in support of ISO 31000 is good, this information has been used as the basis for the guidance in this book, supplemented with additional material and examples, where appropriate.

The book is based on the international standard ISO 31000 and utilizes support documents such as PAS 99 and IEC/ISO 31010.

In this chapter the following items are covered:

- What is risk management?
- Why should an organization bother with risk management?
- Which organizations should implement risk management systems?
- What are the principles of a risk management system?
- How should this book be used?

What is risk management?

There are many definitions that are used in the area of risk management and, as the reader works through the book and new terms are introduced, the definition and a full explanation is provided where it is felt this is necessary for understanding. Readers may find it useful to consult other specific definitions in ISO 31000, BS 31100 and ISO Guide 73 if they need further clarification.

For those who are starting on the journey, there is a need to put risk and risk management into context. Risk is defined as the:

> effect of uncertainty on objectives
>
> ISO Guide 73, Clause 1.1

This definition may not mean much to those with little experience in the area of risk management. In order to give some more clarity, ISO 31000 provides the following guidance by way of notes to the main definition (see also Figure 1):

> **risk**
> effect of uncertainty on objectives
>
> NOTE 1 An effect is a deviation from the expected — positive and/or negative.
>
> NOTE 2 Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process).
>
> NOTE 3 Risk is often characterized by reference to potential events…and consequences…, or a combination of these.
>
> NOTE 4 Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood…of occurrence.
>
> NOTE 5 Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of an event, its consequence, or likelihood.

Organizations need to plan to achieve their objectives and, in doing so, have to evaluate the benefits of achieving the objectives and determine what might prevent them succeeding. Logistics issues, lack of parts from a supplier, failure of equipment, poor service by the sales department,

etc. can all be issues that may be important in the ability to deliver objectives. Decisions can then be made on whether the risk is worth taking because of the potential benefits and, if so, what treatment or controls should be applied to minimize the risk of not succeeding.

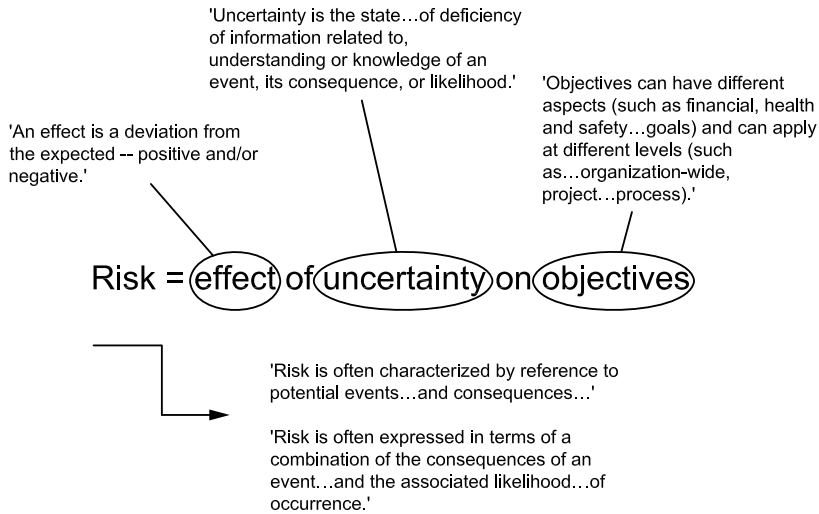


Figure 1 — Definition of risk

ISO 31000 and ISO Guide 73

Risk can be considered as the combination of the likelihood of an event happening and the consequences of that event. At a personal level we all take risks. For example, we may wish to cross a main road to obtain items that can only be conveniently obtained from a shop across the road. The decision to cross a road is an obvious risk. The road is very busy and the risk could be as severe as injury, or even death, if we are involved in an accident.

Various options are available:

- not to bother because the risk is too great (*risk aversion)*;
- ask someone else to undertake the task for us (*risk transfer*);
- cross the road, taking the risk ourselves, having made an assessment (albeit subconsciously) of the situation.

Once the decision has been made to cross the road, accepting the risk, most people would make provision to minimize the risk of harm. The risk could be 'managed' by various means including:

- the use of a pedestrian crossing;
- crossing at a place where traffic is light and there is good visibility.

This simplistic case is given as a case of 'risk management':

> 'co-ordinated activities to direct and control an organization with regard to risk'
>
> ISO Guide 73, Clause 2.1

We identify a risk (the degree of harm in this case and the likelihood) and take steps to manage the risk. We all face a number of differing risks every day and seek to manage these in different ways, e.g. when purchasing a house we take on a financial risk and may decide to insure against loss caused by flooding, a storm, fire, etc.

Why should an organization bother with risk management?

Organizations take risks, whether they are public service bodies, large companies or charities. In taking these risks, they learn more about their activities, enabling them to become more successful in the future. Take, for example, the first heart transplant operation. If the risk had not been incurred and subsequently managed, learning from this process, this procedure would not be the relatively common and comparatively safe operation that is routinely performed today. Businesses have to take a risk when they develop a new product – hoping that their research and development (risk management) was sufficient to generate a return on the investment. Charities can take a risk when they decide to intervene with aid because the aid may not get to the targeted beneficiaries and may be used by exploitive parties for their own benefit.

Examples of the impact of poor risk management upon both organizations and society:

- lending in the subprime mortgage market in the USA;
- rogue traders in the investment banking sector;
- poor management of food hygiene leading to closure of food outlet;
- failure to maintain public service vehicles adequately, leading to withdrawal of operating licence;
- oil leak in Gulf of Mexico in 2010.

Given the myriad of risks that an organization can face, it is clear that there is substantial benefit to be obtained by taking on a more formal risk management approach in order to avoid:

- damage to its reputation;
- loss of its customers through failure to provide a service or product (in the public sector it may mean the loss of patients using a hospital facility);
- damage to financial viability through loss of share value, loss of access to capital, etc.;
- difficulties with interested parties, e.g. neighbours, regulators, customers and workforce.

Whilst the above are some basic reasons why an organization should bother with managing risks, it is not an exhaustive list. Some risks are positive but many see risks as being a negative threat to the organization. In reality, risks need to be managed to positive effect where possible. The approach given in this book should be equally useful to those who deliberately take risks in the hope it will provide positive benefits to the organization.

Risk management is not just something that is important to the financial sector. Poor risk management has led to many catastrophic outcomes and, equally, a positive attitude to risk taking has resulted in many of the great achievements we witness on a daily basis. The primary purpose for organizations to implement and operate effective risk management systems is to survive and thrive.

Effective risk management systems should enable an organization to achieve its objectives by, for example:

- reducing the likelihood of an event that could have an adverse effect on the organization's ability to deliver its product or service, or reducing the consequence should such a situation arise. For example, if a company relies on a particular logistics supplier and there is a risk that it may fail in some way, provision should be made for an alternative arrangement with an in-house backup or an alternative logistics company;
- increasing the likelihood of success by putting effective measures in place, e.g. additional sales support staff when opening a new shop to ensure shoppers get a good experience and feel that there is plenty of help for them when making purchases;
- ensuring that the organization identifies opportunities where taking risks might benefit the organization, e.g. staff suggestion schemes;
- improving accountability, decision making, transparency and visibility in order to ensure that personnel understand their role and the outcome of not managing the risk they impact upon;
- identifying, understanding and managing multiple and cross-organization risks, as it is common to find that each risk cannot necessarily be isolated into one 'box' and may impact on other parties. The introduction of a water-based paint product into a bodywork shop may be advantageous from health and safety and

environmental aspects, but if it slows down production and prevents working on the panels for, say, 24 hours versus 2 hours there could be a number of adverse impacts;
- executing change more effectively and efficiently and improving project management. It is quite common to find that changes can be implemented in the organization, system, etc. without first evaluating the overall impact prior to implementation. The management of change is an essential element to ensure effective and efficient changes;
- providing better understanding of, and compliance with, relevant governance, legal and regulatory requirements, and corporate social responsibility and ethical requirements;
- protecting revenue and enhancing value for money. It is sometimes better to put in place robust measures that protect the revenue, as well as devote resources to marketing and sales. A high turnover in customers is something to avoid, where possible, and it is better to keep existing customers happy as well as seeking new ones. The effort expended in gaining new customers will often greatly exceed what is needed to keep existing customers;
- protecting reputation and stakeholder confidence. Organizations depend on having a good reputation and on their stakeholders, such as customers, insurers, neighbours, workers and suppliers, having confidence in them.
- differentiating you against your competition: demonstrating good risk management can be an enabler to winning business.

Which organizations should implement risk management systems?

Risk management is a universal issue that is common to governments, public bodies, corporations, institutions and charities, regardless of their size or sector.

What are the principles of a risk management system?

One of the first steps when setting up a framework for managing risk is to determine the principles that should be followed. Guidance is provided on this subject in Chapter 3 to support the principles given in ISO 31000, and links are given to show how the implementation of risk management should deliver these principles.

How should this book be used?

This book is primarily written for those organizations that do not necessarily have a formal organization-wide risk management system. It is

recognized that many will have systems for managing occupational health and safety because it is a legal requirement; others will have systems for quality (ISO 9001), environmental management (ISO 14001), information security (ISO/IEC 27001), food safety (ISO 22000), business continuity management (ISO 22301) or social accountability (SA 8000), etc. The frameworks for managing these areas of risk may well be the foundation for the risk management system and it would be both costly and time-consuming to build a totally new system, which could be burdensome and could cause duplication, confusion and unnecessary bureaucracy.

Those organizations that do not have any formal system in place may also find the approach put forward in Chapter 12 helpful, as it will simplify implementation of other management systems at a later stage.

Whilst ISO 31000 provides a foundation, this book offers a full and considered approach that can be applied by those wanting to expand their existing management system to an enterprise-wide risk management system, as well as by those looking at risk management in isolation. To help those readers who are new to this subject a simple case study is used from time to time to give some appreciation of what is involved.

Chapter 2 - Getting started

The following chapters provide a structured approach to implementing a risk management framework and associated processes into an organization. Based upon ISO 31000 and BS 31100, together with supporting guidance, it will help the reader in the implementation and operation of a formalized risk management system. The overlap and repetition found in the standards has been eliminated, where possible, in order to simplify the process whilst retaining important points.

All organizations will have some arrangement in place for managing individual risks, although they may not necessarily realize it, have the formal framework or have any processes in place. The scope of the task for developing and implementing a risk management framework and managing risk is set by the context of the organization. By context we mean the 'world' in which it operates, who it serves, the expectations of its customers and/or shareholders, etc.

The matrix in Table 1 provides the links between the book chapters and the clauses in ISO 31000 and BS 31100, which are aligned in most cases. Subjects such as 'Understanding of the organization and its context' (Clause 4.3.1) and 'Establishing the context' (Clauses 5.3.1, 5.3.2, 5.3.3 and 5.3.4) are covered in Chapter 5, rather than in separate chapters. An additional column is provided for indicating whether the issue has been addressed at your organization.

Table 1 — Initial status review correspondence

Chapter heading	Corresponding clause(s)	Addressed: Yes/No
1 Introduction		
2 Getting started		
3 Principles	3	
4 Leadership, commitment and culture	4.2	
5 Context	4.3.1; 5.3.1; 5.3.2; 5.3.3; 5.3.4	
6 Framework	4	
7 Risk management and implementation	4.4, 5.4	
8 Risk treatment and implementation	5.5	
9 Monitoring and review	4.5; 4.6	
10 Internal auditing	4.5	
11 Recording and reporting	4.3.6; 4.3.7	
12 Integrating your management systems	4.3.4	

Those organizations with established management systems may find a benefit in reading Chapter 5 and Chapter 12 before deciding how to proceed with the development and implementation of a risk management system.

To help smaller organizations, or those new to the subject area, understand how to implement risk management, a hypothetical organization is provided to illustrate some of the key challenges and considerations raised in the following chapters. The journey towards a system for managing risk is picked up at relevant points. The example is not intended to be perfect and the approach taken by the fictitious characters is not necessarily sound all the way through, as this would defeat the objective. The idea is to show what might happen and the thought processes involved along the way.

Case study – Gillie's T 4 2

'Gillie's T 4 2' is a small tea shop and café in a village called Aston-by-Water. It is very successful and is well patronized by the locals, as well as visitors who come to the area for tourism. Gillie is very happy with her success, built up since establishing the business seven years ago. Having said this, she had never thought she would be so successful that she would take the neighbouring shop over and employ 30 employees to cover the various hours the shop and café are open.

One day, a regular customer at her café said: 'May I have a word with you sometime?' She was alarmed in case something was wrong but he quickly reassured her with a charming smile and said: 'I would like to talk to you about us jointly growing your business so you can become a household name.'

As it turned out, Rob, the customer, had been successfully selling second-hand cars and had retired. He now wished to invest. He had built his own business on maintaining high standards and had found that the principles in ISO 9001 had helped him a lot. He had recently read about a new standard for managing risks, which he had found thought-provoking. He said to Gillie: 'Don't worry about how we'll develop your business. I will sort out your "external context" if you can deal with the "internal context" to start with.' Gillie was confused and so Rob went through the ISO 31000 process with her; she needed two pots of coffee to stay awake. Thankfully, Gillie was aware of ISO 9001 for quality management and so was not too fazed by the risk management process that Rob explained so enthusiastically. He had been reading the standard and getting to grips with its implications, and wanted to try it out in practice with a new investment.

Immediately, Gillie wondered how an expansion of her business would affect the relationships with the café's suppliers that were so integral to the success she enjoyed. Her friend, Jane Lovecake, ran the nearby bakery. It was her bread, pastries and cakes that she had used for many years and knew to be as big an attraction for her customers as her tea and service. Gillie grew concerned that if she rapidly expanded her business she would not be able to rely upon the small, local network of businesses to meet the increased demands.

Gillie's journey towards a system for risk management for her business is picked up again in the following chapters.

Chapter 3 - Principles

In this chapter we examine the core principles upon which a system for developing activities to 'direct and control' risk within the organization might be established. These principles are the foundations for risk management, when implementing and operating the risk management arrangements. The core principles for risk management set out in ISO 31000 are listed below.

a) Risk management creates and protects value
b) Risk management is an integral part of all organizational processes
c) Risk management is part of decision making
d) Risk management explicitly addresses uncertainty
e) Risk management is systematic, structured and timely
f) Risk management is based on the best available information
g) Risk management is tailored
h) Risk management takes human and cultural factors into account
i) Risk management is transparent and inclusive
j) Risk management is dynamic, iterative and responsive to change
k) Risk management facilitates continual improvement of the organization

The framework and processes implemented as part of a system for risk management should deliver the principles above. The rest of this chapter deals with each of these principles in turn, including further explanation from ISO 31000 in indented paragraphs, followed by additional, practical commentary.

a) Risk management creates and protects value

> Risk management contributes to the demonstrable achievement of objectives and improvement of performance in, for example, human health and safety, security, legal and regulatory compliance, public acceptance, environmental protection, product quality, project management, efficiency in operations, governance and reputation.
>
> ISO 31000, Clause 3

When making a decision to introduce formal risk management arrangements, an organization should be sure that the development of such a formal structure is of benefit and contributes to the achievement of objectives. To be truly effective, risk management should be an

integral part of the business management system. A stand-alone system is unlikely to work, particularly where risks may need to be managed dynamically in evolving situations. Account should be taken of legislative, regulatory and compliance requirements. Perhaps the most significant aspect to making the arrangements effective is the manner in which those within the organization are engaged with the risk management arrangements. To be truly effective, risk management has to be embedded within the culture of the organization, encompassing the entire workforce, enabling all staff to contribute to its effectiveness, and create and protect value. For additional guidance, see Chapter 4.

b) Risk management is an integral part of all organizational processes

> Risk management is not a stand-alone activity that is separate from the main activities and processes of the organization. Risk management is part of the responsibilities of management and an integral part of all organizational processes, including strategic planning and all project and change management processes.
>
> ISO 31000, Clause 3

Risk management is not something that should exist as a stand-alone activity, divorced from the processes of the organization and taking no account of organizational activities. There are often many management systems' frameworks in use in an organization, some of which are to support regulatory requirements, e.g. occupational health and safety (e.g. Health and Safety at Work, etc. Act 1974). Many of the processes required in systems are very similar or common, and developing an integrated risk management system can enhance value by removing duplication and reducing the possibility of conflict. Introducing formal risk management arrangements is more than simply bringing value to an organization or creating internal efficiency. A structured approach should enable the organization to take new opportunities and reduce the risk of business threats to it in a controlled manner. Making this happen is, in part, the responsibility of the management of an organization, as it is only with its support and action that strategic decisions and investment can be made, and that any new programmes can be seen through to completion.

ISO 31000 makes the point that the framework for managing risk has to be appropriate to the internal and external context of the organization, and 'assist the organization to integrate risk management into its overall management system' (Clause 4.1). If risk management is not fully integrated into the business processes, there is a danger that it is less likely to be conducted and, therefore, some of the benefits could be lost. Organizations that have a number of high risks, or are large, complex

operations, will need to have more robust systems than a small organization with only one or two significant risks to manage.

c) Risk management is part of decision making

> Risk management helps decision makers make informed choices, prioritize actions and distinguish among alternative courses of action.
>
> ISO 31000, Clause 3

Risk management should assist the organization in making decisions about activities that may represent either upside or downside risks. It is quite common to think of risks having a negative impact (downside risk) – a threat to the organization. However, there are also upside risks, e.g. an opportunity to develop or expand that should be taken in the long-term interests of the organization. If upside risks are not taken, the organization may well decline over time. Considering and taking the upside risks, where appropriate, are an important element in the development and continued success of an organization.

> An organization was spending £1 million per year disposing of a waste by-product from its manufacturing processes and the cost was escalating. Investment in research to identify other uses for this material found a new use for the material and the organization was able to exploit the positive consequences of this upside risk.

Decisions will be informed by the organization's 'risk attitude' – defined in ISO 31000, Clause 2.5 as an 'organization's approach to assess and eventually pursue, retain, take or turn away from risk' – and also the organization's 'risk appetite' – the 'amount and type of risk…that an organization is willing to pursue or retain' (ISO Guide 73, Clause 3.7.1.2). In short, organizations have to determine what risks they are prepared to take, e.g. what investment in new plant they can justify and/or what short-term losses they can accept, in order to meet their objectives. All decisions regarding risk management should necessarily be informed by the organization's capabilities and competence to manage these areas.

Effective risk management should help an organization to survive and thrive. It is most effective when it is integrated with management processes and is embedded in the culture of the organization. This is a key output from Turnbull's guidance to listed companies striving to achieve effective governance (Turnbull, et al., 1999).

> 'Successful risk management is crucial to the long term success, and indeed the survival, of all businesses.'
>
> Mazars (2009), 'Review of the effectiveness of the combined code – Summary of the main points raised in responses to the March 2009 call for evidence', Financial Reporting Council, London, July

d) Risk management explicitly addresses uncertainty

> Risk management explicitly takes account of uncertainty, the nature of that uncertainty, and how it can be addressed.
>
> ISO 31000, Clause 3

Activities within the organization should be co-ordinated and controlled in order to clarify the nature of the uncertainty, and how this uncertainty might affect the action the organization should take. There are many options available, e.g. removing the source of the risk, changing the nature of the risk, sharing the risk with another party, seeking an opportunity that may create or enhance the risk, or avoiding the activity (see Chapter 8 for further guidance). These activities are described as 'risk treatment', defined in ISO Guide 73 as the 'process to modify risk'.

Risk management tools can support the organization in determining possible outcomes, and their likelihood, from uncertainties. These are useful for ranking risks and determining priorities, enabling the selection of the most appropriate and cost-effective action. There are many approaches that can be adopted to achieve this objective, including some of those listed in IEC/ISO 31010. An example of some risk management tools and techniques is provided in Appendix A.

e) Risk management is systematic, structured and timely

> A systematic, timely and structured approach to risk management contributes to efficiency and to consistent, comparable and reliable results.
>
> ISO 31000, Clause 3

Risk management can enable an organization to manage its processes more systematically and gives benefits such as:

- a more consistent approach in the way it deals with risk across different disciplines – the management of one risk independently may give rise to a downside risk in another area/discipline/process;
- the efficient use of resources and management tools – it avoids repetitious independent systems and multiple audits;

- the avoidance of duplication – common processes, such as documentation and records, should be combined where they overlap, if it is beneficial;
- enabling better comparison of its performance through reliable results measured in a similar manner.

The methodical application of risk management techniques within the organization should help to ensure that the outputs of the risk management process are reliable, consistent and comparable. This consistency will give decision makers increased confidence that they have the necessary information to inform decisions.

f) Risk management is based on the best available information

> The inputs to the process of managing risk are based on information sources such as historical data, experience, stakeholder feedback, observation, forecasts and expert judgement. However, decision makers should inform themselves of, and should take into account, any limitations of the data or modelling used or the possibility of divergence among experts.
>
> ISO 31000, Clause 3

In common with any process for making decisions, the decisions taken in managing risk should be based upon accurate, timely and verifiable information. The organization should ensure that there are sufficient systems in place to capture appropriate data (preferably, quantitative). Managers should refer to this data when deciding on a particular course of action. These information sources may comprise historical data, experience, expert judgement, subject knowledge and forecasts, etc.

Top management should ensure that information sources are validated for the inputs and the processes used for assessing the risk. It may be that different tools and expert views are considered and risk owners should be aware of the limitations and differing opinions of experts. Over time, risk profiles change; the nature of a risk may become more significant and the way it needs to be managed, reviewed.

What is a 'risk owner'?

A person with the accountability and authority for a risk.

(Based upon ISO Guide 73, Clause 3.5.1.5)

g) Risk management is tailored

> Risk management is aligned with the organization's external and internal context and risk profile.
>
> ISO 31000, Clause 3

The approach to risk management should be proportionate and scaled to the needs of the organization and the business environment in which it operates. All organizations, even those in similar sectors, will operate within a different context. These differences will result from both internal and external aspects of the organization's context. For example, if the organization works on an international scale and provides products and services, then it needs to bear in mind the way in which business is carried out in all of its target markets, any specific regulatory issues and any specific requirements with respect to working conditions.

The size, complexity and nature of work are such that risk management needs to be tailored to the specific organization's needs. For further guidance, see Chapter 5 and principle b), above.

h) Risk management takes human and cultural factors into account

> Risk management recognizes the capabilities, perceptions and intentions of external and internal people that can facilitate or hinder achievement of the organization's objectives.
>
> ISO 31000, Clause 3

For further guidance, see Chapter 5.

i) Risk management is transparent and inclusive

> Appropriate and timely involvement of stakeholders and, in particular, decision makers at all levels of the organization, ensures that risk management remains relevant and up-to-date. Involvement also allows stakeholders to be properly represented and to have their views taken into account in determining risk criteria.
>
> ISO 31000, Clause 3

Top management should ensure that all stakeholders are identified and kept informed, as appropriate. In some cases, they may need to be involved or assist in risk identification and assessment, and the organizational response. An obvious stakeholder that the organization can use to great benefit in the identification of risk is its own workforce. Where the workforce helps in risk identification and understands the

potential impact on the organization of particular risks, it is more likely to help manage the procedures or controls that help manage the risk. For further guidance, see Chapter 4.

j) Risk management is dynamic, iterative and responsive to change

> Risk management continually senses and responds to change. As external and internal events occur, context and knowledge change, monitoring and review of risks take place, new risks emerge, some change, and others disappear.
>
> ISO 31000, Clause 3

Nothing remains constant and organizations need to be able to respond effectively to changes in context, e.g. developments in technology, societal expectations and changes in government. For this reason, the organization should ensure its risk management system continually identifies and responds to changes affecting its operating environment/context. The timing and frequency of this review of risks will depend on the context in which the organization operates. In many organizations, if not all, some risks will need to be reviewed frequently, whereas some will remain constant over long periods of time. For further guidance, see Chapter 9.

k) Risk management facilitates continual improvement of the organization

> Organizations should develop and implement strategies to improve their risk management maturity alongside all other aspects of their organization.
>
> ISO 31000, Clause 3

Risk management standards such ISO 9001, ISO 14001, ISO/IEC 27001 and OHSAS 18001 recognize the need for continual improvement. Over time, the management system for risk will develop and mature to a more stable system. However, there is no room for complacency and there is a constant need to regularly review arrangements. Developments in technology and societal/stakeholder expectations may necessitate improvements and the organization should be looking ahead to ensure it is improving its strategies over time.

There should be regular reviews of the way in which the risk management principles are applied, and these should reflect changes in the organization's nature and context – both internally and externally. For further guidance, see Chapter 9 ('Management review').

The checklist below has been devised to assist in evaluating your organization's adherence to the 11 risk management principles defined above. Score zero if there is *no* implementation, one for *partial* implementation and two if the organization *fully* meets the principle as defined. Clearly, more focus will be required in any areas where the score awarded is not two, and improvements will need to be made to risk management in order to meet the principles set.

Checklist – Evaluating the organization's adherence to the risk management principles

Our organization understands, and is committed to the principle, that risk management creates value.	
Risk management is an integral part of our organizational processes.	
The effect of risk is considered a part of all our decision-making processes.	
We recognize that effective risk management can assist the organization in addressing uncertainty.	
Risk management in our organization is systematic, structured and timely.	
Risk management is based upon the best available information in our organization.	
Risk management is tailored to our organization's internal and external context.	
Risk management takes into account human and cultural factors pertinent to our organization.	
Risk management is transparent and inclusive in our organization and everyone is involved.	
Risk management is dynamic, iterative and responsive to change.	
Risk management facilitates continual improvement of our organization.	

Key learning points

In order to establish an effective risk management system the 11 principles of risk management should be satisfied. A short explanation has been provided on the meaning and expected output.

Chapter 4 - Leadership, commitment and culture

It is widely accepted in all fields, be they commercial, sporting, military or otherwise, that commitment demonstrated by those in control of the organization can make a significant difference in the level of organizational achievement. There has been much written about leadership and culture and it is not intended that this book add to the weight of material already in existence. However, the importance of strong leadership and a positive culture within the organization towards its goals cannot be underestimated and successful risk management is no different.

Leadership and commitment

There is very little guidance in ISO 31000 on the aspects of leadership, commitment and culture, but the standard does state that management should 'ensure that the organization's culture and risk management policy are aligned' (Clause 4.2). Commitment to risk management at the top of the organization is essential if the organization is to be successful in addressing the management of all aspects of risk. It is from the top of the organization that the mandate to implement the risk management system should come.

Top management should demonstrate commitment and leadership and the risk management policy should be a manifestation of these characteristics. For the system to be implemented successfully, it is important that risk management is embedded in the culture of the organization and that all those working on behalf of the organization recognize their role and the responsibility they have in helping the organization to survive and thrive. The guidance given to listed companies in 1999 in the Turnbull Report (Turnbull, et al., 1999) identified the need to embed risk management in the culture of an organization, and the interrelationship can be considered as a three-part structure as shown in Figure 2.

The three inextricably linked components are needed for effective risk management and governance of an organization. However, leadership is essential if this arrangement is to be realized in practice. The most senior management in the organization need to be seen to be fully committed

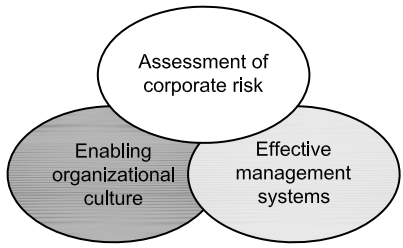


Figure 2 — Three key components for delivering effective corporate governance after the Turnbull Report

to the organization's objectives, and to the effective identification, evaluation and management of risks, if the workforce are to commit themselves to deliver what is expected of them. Senior management, line managers, supervisors and individuals need to understand their role and how important it is in achieving success for the organization. They need to demonstrate their commitment in practice as well as preaching it. This commitment needs to be reinforced so that all those who have responsibilities that can impact on risk treatments undertake their tasks conscientiously. For example, security personnel may be some of the lowest-paid workers within a high-tech company but their vigilance and commitment are an essential component in ensuring the organization's activities are not interrupted, sabotaged or compromised in some manner.

As a clear demonstration of their commitment to risk management the board (or equivalent) should:

- recognize that they are ultimately accountable for risk management;
- define roles, responsibility and accountability for managing and reporting on risk throughout the organization;
- set risk management objectives designed to support and achieve the organization's risk appetite and the approach to recognizing risk in decisions;
- provide achievable goals for risk management;
- ensure that those working within the organization are communicated with, and that all have a clear understanding of the organization's commitment to the management of its risks;
- provide the infrastructure for the implementation of risk management and its continual evaluation of the arrangements that have been established;
- demonstrate that the implications of risk are taken into account when the organization's key business decisions are made;
- demonstrate continued interest in risk management issues;
- ensure that they are made aware of bad news as well as good news;

- demonstrate that risk is managed with the same determination as other key business objectives;
- be prepared to listen to whistle-blowers;
- display an informed interest in risk management issues when meeting workers and visiting different workplaces.

In addition to the above, BS 31100 provides a table outlining specific leadership responsibilities; see Table 2.

Table 2 — Leadership and responsibilities

1) Approve the risk management policy and take the lead on setting the tone and culture for managing risk and embedding risk management, not least by their own example.

2) Ensure there is an appropriate risk management framework and process in place and that risk management is adequately resourced.

3) Provide strategic direction on the appropriate consideration of risk in decisions and setting risk criteria and other policies to control risk-taking and exposure.

4) Operate an instance of the risk management process covering the whole organization and all types of risk.

5) Provide direction and receive assurance on the effectiveness of risk management and compliance with the risk management framework.

6) Report on risk management to stakeholders and sign off public disclosures related to risk and risk management.

BS 31100, Clause 3.3.4, Table 3

The fundamental point is that effective management of risk requires strong and active leadership from the top, worker involvement and a comprehensive assessment and review process.

The responsibilities of all those in the organization are highlighted in Table 3.

Table 3 — Minimum responsibilities for everyone in the organization

1) Be aware of the risks that relate to their roles and their activities.

2) Continuously improve their management of risk.

3) Provide information to help operate the risk management framework and process, such as information that helps to identify risks and assess controls.

4) Implement controls, or support the implementation of controls, as part of their day-to-day duties.

5) Report ineffective and/or inefficient controls.

BS 31100, Clause 3.3.4, Table 4

An area that is often a challenge when expanding a small business is the ability of the owner to control risks that can change quite markedly with the expansion.

Through Gillie's hands-on involvement with all aspects of the business at this stage, her commitment is evident for all the staff to see. It would, of course, become a different matter when the growth of the organization means that she has to manage units from a distance.

Culture

A positive risk management culture is a necessary part of the risk management framework. However, risk culture is not something that can exist in isolation and is usually inseparable from an organization's overall values. Management must be seen to engage with the workforce in the development of an overall approach to successful risk management. The ability of management to engage with the workforce and develop an effective framework for the management of risk is no different from leading its team to achieve any business objective and will focus on one of two primary approaches (or a combination of both):

1. to change attitudes to risk and its control;
2. to change behaviours when dealing with risk issues.

Before it is possible to determine the nature of an organizational culture, it is necessary for everyone to have a clear idea of exactly what is meant by the phrase 'culture'. One suggestion is:

> 'The product of individual and group values, attitudes, competencies and patterns of behaviour that determine the commitment to and the style and proficiency of an organization's approach [to risk]'
>
> BS 18004, Clause 3.32

Establishing a positive culture is something that can take a long time and it is equally possible to destroy many years of good work in a very short time through inappropriate management behaviour that damages trust with employees.

Core elements in the development of an appropriate risk management culture, one that becomes an integral part of the risk management framework, will require the organization to:

a) give appropriate attention and resources to achieve risk management objectives;
b) comply with the intent and details of risk management policies and procedures;
c) solve practical difficulties in implementing risk management policies and procedures, and do so in a way that is consistent with good risk management principles;
d) manage risk in ways that go beyond compliance with formal policies and procedures; and
e) communicate about risk openly and appropriately.

BS 31100, Clause 3.3.5

Having put in a lot of hard work to ensure that the team is fully on board with the management of risk, the organization needs to put in place a mechanism for monitoring and developing its risk management culture.

An effective way of determining the attitude of the workforce and its commitment to the risk measures in place can be the use of surveys. An anonymous survey with suitably worded questions can identify where the organization is strong, where there is good leadership and, importantly, where there are shortfalls that need to be addressed. For an organization to improve, it needs to communicate the findings and address weaknesses in a positive fashion. There is no room for a blame culture but the approach must be one of a learning organization endeavouring to develop its risk maturity.

A question set such as the following example based upon BS 18004, which relates to safety, is equally applicable to other disciplines or to risk management in general. This shows one way of establishing whether the workforce believes top management is committed to the workforce from

a safety aspect. It has been found that an organization which looks after its workers' welfare is more likely to foster a culture where the workers support the organization.

Example of an attitude survey questionnaire

Please tick the appropriate box to show your level of agreement with each of the following statements.

	Strongly dis-agree	Dis-agree	Neither agree nor dis-agree	Agree	Strongly agree
1. Senior management is fully committed to risk management.	1	2	3	4	5
2. Workers are blamed when they make mistakes.	1	2	3	4	5
3. The company is interested in my opinions about risks in the organization.	1	2	3	4	5
4. Management places a high priority on risk training.	1	2	3	4	5
5. Supervisors turn a blind eye to unsafe behaviour.	1	2	3	4	5
6. Health and safety procedures are much too stringent in relation to the risks.	1	2	3	4	5
7. My workmates would criticize me for breaking the health and safety rules.	1	2	3	4	5
8. I am given adequate health and safety training.	1	2	3	4	5
9. Little is done to prevent accidents until someone gets injured.	1	2	3	4	5

	Strongly dis-agree	**Dis-agree**	**Neither agree nor dis-agree**	**Agree**	**Strongly agree**
10. Everyone wears their protective equipment when they are supposed to.	1	2	3	4	5
11. Action is rarely taken when someone breaks the health and safety rules.	1	2	3	4	5
12. I fully understand the health and safety instructions that relate to my job.	1	2	3	4	5
13. Time pressures for completing jobs are reasonable.	1	2	3	4	5
14. I was involved in risk assessments relating to my work.	1	2	3	4	5
15. Workers are praised for working safely.	1	2	3	4	5
16. Action has been taken on the basis of risk assessment findings.	1	2	3	4	5
17. The risk controls do not get in the way of me doing my job.	1	2	3	4	5
18. Knocks and bruises are bound to happen at work no matter how careful you are.	1	2	3	4	5

	Strongly dis-agree	Dis-agree	Neither agree nor dis-agree	Agree	Strongly agree
19. Health and safety briefings are very useful.	1	2	3	4	5
20. My workmates take risks that I would not take myself.	1	2	3	4	5
21. Accidents that happen here are always reported.	1	2	3	4	5
22. Some health and safety rules are only there to protect management's back.	1	2	3	4	5
23. The permit-to-work system leads to unnecessary delays in getting the job done.	1	2	3	4	5
24. I know that if I follow the safety procedures I will not get hurt.	1	2	3	4	5
25. The use of personal protective equipment is strictly enforced.	1	2	3	4	5

Based upon BS 18004, Annex C

Whilst the completion of a workforce survey will provide some indication of attitudes towards risk, the real worth can only be ascertained by repeating the exercise on a regular basis and using the results to improve or maintain performance. There are factors that could impair the development of a culture committed to risk management and organizations where there is a commitment to managing risk effectively will often display similar characteristics.

Consider the checklist below and identify points that you feel may be an issue in your organization, and where steps need to be taken to address the problem.

1. Do top management display risk management leadership at senior levels, setting an example to others?

2. Are workers committed to the aims of the organization and the way in which the organization is managed?
3. Do senior staff and supervisors display commitment to managing risk, and spend time discussing and promoting the identification and management of risk within the organization?
4. Is there monitoring of risk management, and communicating of the value added by risk management, with effective communication of results to all?
5. Is communication within the organization multiway with opportunities for both formal and informal communication?
6. Are formal risk management policies and procedures extended into all organizational processes, including strategic planning, operational processes, and programme, project and change management?
7. Is risk managed throughout the organization with the same determination as other key business objectives?
8. Is there commitment to continually improving and maintaining risk management throughout the organization?
9. Is there appropriate education and training in risk management for all workers, including practical examples?
10. Are workers at all levels seen as a key resource for the organization, a resource through which the organization can achieve its risk management objectives?
11. Is risk management included within individual objectives and performance appraisals?
12. Are attitudes to risk management regularly monitored?

Key learning points

There is an inextricable link between leadership, commitment and culture and this is an important area for the management of any aspect of an organization's operations. The development of good practice in these areas is important for any organization seeking to implement an effective system for the management of risk.

Attitude surveys can help identify weakness in this area.

Links with management systems standards

Those organizations that use ISO 9001 will have addressed the subject areas to some extent by meeting Clause 5.1, and those that use ISO 14001 and OHSAS 18001 will find some links with Clause 4.4.1 in those standards.

Chapter 5 - Context

Any organization has to take both internal and external factors into account when managing its risks. These influences are summed up in the use of the term 'context' in ISO 31000 and can be simply expressed as the:

> '…environment in which the organization seeks to achieve its objectives'
>
> ISO Guide 73

In essence, no organization or single individual can exist in a vacuum and there will be many interactions with other parties during day-to-day operations. The nature of these interactions may vary depending upon whether it is a large organization or a sole trader, but both will undoubtedly be part of a network of suppliers or customers at some stage. ISO 31000 identifies that these interactions can take place with groups that are external to the organization, as well as with groups within the organization, and develops the terms:

> **external context**
> external environment in which the organization seeks to achieve its objectives
>
> ISO 31000, Clause 2.10

> **internal context**
> internal environment in which the organization seeks to achieve its objectives
>
> ISO 31000, Clause 2.11

Guidance on internal and external context is given in two areas of ISO 31000: Clause 4.3.1 covering the framework and Clause 5.3 on processes. In the latter section, the subject matter is confined to the context of the process or processes (i.e. any activity undertaken by the organization that needs to be controlled), whereas the framework (Clause 4.3.1) should be designed to meet the strategic needs of the organization and reflect its capability to manage its risks. At the operational level there may be many processes that deliver the management of a specific risk within the framework.

It is essentially this high-level framework that is impacted upon by society, government, investors, suppliers, customers, regulation, etc. These

factors comprise some elements that are part of the external context. They should be established as they need to be understood and then the framework developed for managing the associated risks. There is also the internal context of the organization to consider, which has an equally important impact on determining what is required for the framework.

At the strategic level, the organization needs to establish what is important in its strategy, policy and objectives. Once established, these areas will inform the design of the framework for managing its risks, and assist in developing a strategy for the implementation of effective risk management. For example, in an organization operating in the mining sector, the detailed arrangements for occupational health and safety and the environment are not something the decision makers need to know. They do, however, need to recognize that environmental issues are a significant risk that will be important to stakeholders in the external context, and occupational health and safety is important with respect to internal and external context.

When identifying the internal and external factors to be considered, it is important to think of opportunities and not just threats. There is often an association of the term 'risk' with negative impacts, e.g. risk is used in this sense when relating to occupational health and safety. This is misguided, even in occupational health and safety, as those organizations that manage occupational health and safety well have demonstrated an ability to win business and retain clients as a result of their good performance in this area, whilst also improving overall business performance through:

- reduction in absenteeism of employees;
- less business interruption;
- decreased insurance premiums.

This is one of the most compelling reasons for considering risk management more holistically, and embedding a risk management programme within an overall management system to maximize benefits, avoid duplication and reduce conflict. An understanding of the positive aspects of risk is central to any organization. This is clearly illustrated in the ISO Guide 73 definition of risk as:

> effect of uncertainty on objectives.

To clarify this definition, ISO Guide 73 expands by way of a note to express that '…a deviation…[can be] positive and/or negative'. Organizations that fail to take risks that are appropriate and proportionate to their activities may find that they stagnate; organizations need to be innovative to survive.

There are many external context factors that can affect an organization and some may be unique. It is difficult to give comprehensive guidance as

to all the factors that should be considered when determining the strategy, policy and framework for managing risks. However, for all organizations an appropriate starting point might be something like the illustration in Figure 3 from the United Kingdom National Risk Register, which succinctly demonstrates many societal aspects of external context and the links with risk. It will be noted that many of these items would appear on a risk management checklist for organizations.

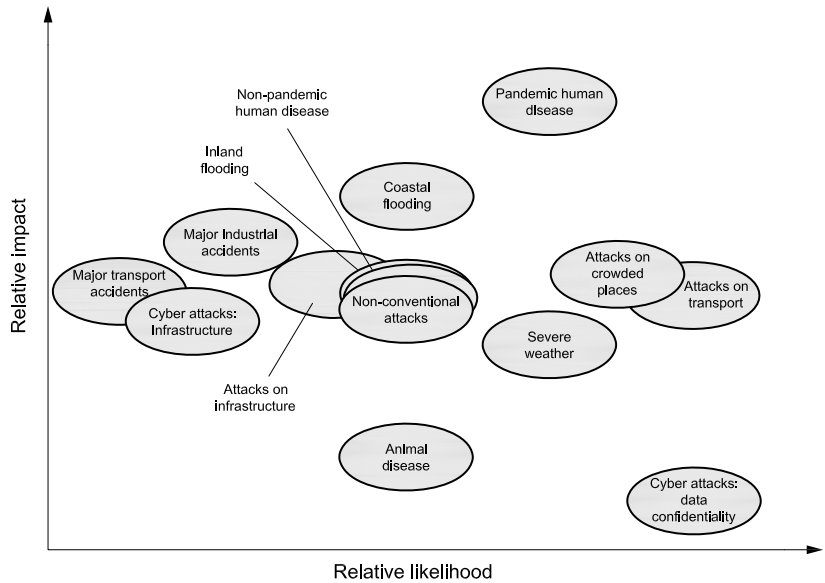


Figure 3 — An illustration of the high consequence risks facing the United Kingdom

National Risk Register of Civil Emergencies, 2010 Edition

Figure 3 indicates the very wide nature of an organization's external context and reinforces the requirement in ISO 31000 that: 'Before starting the design and implementation of the framework for managing risk, it is important to evaluate and understand both the external and internal context of the organization…'.

The internal and external factors/drivers for managing risk may well overlap and, when developing the framework, these interactions need to be considered.

It should be noted that one of the greatest downside risks to an organization is the loss of reputation. A good reputation is an upside opportunity and loss of reputation is a threat. Reputational loss can arise through poor risk management in any discipline, leading to concern and uncertainty amongst the organization's stakeholders.

The aim is to ensure that the organization establishes its context, in order that it establishes an appropriate framework for managing its risks in relation to that context. There needs to be the capability within the organization for managing the risks, and the framework should be developed to meet the specific needs and resources available.

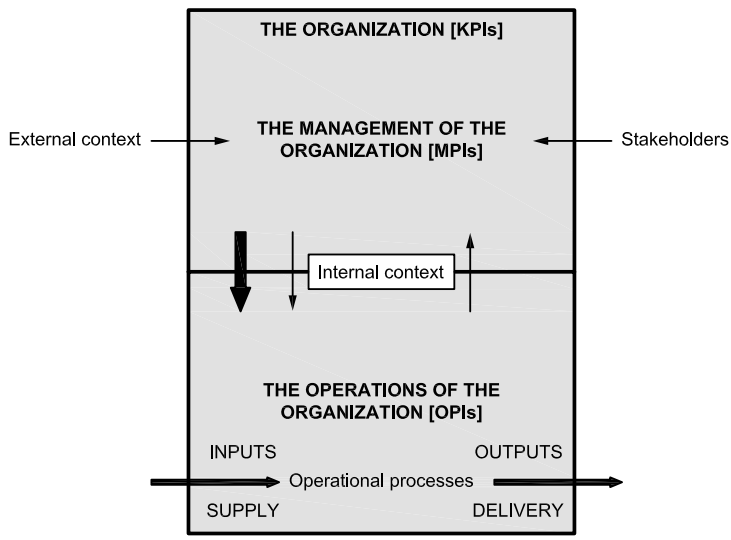
The evaluation of internal and external context and their interrelationship is an essential starting point to enabling the organization to determine a strategy and framework for managing risk. Aspects that should be considered are outlined in ISO 31000, Clause 4.3.1 as below:

> Evaluating the organization's external context may include, but is not limited to:
>
> a) the social and cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;
> b) key drivers and trends having impact on the objectives of the organization; and
> c) relationships with, and perceptions and values of, external stakeholders.
>
> Evaluating the organization's internal context may include, but is not limited to:
>
> - governance, organizational structure, roles and accountabilities;
> - policies, objectives, and the strategies that are in place to achieve them;
> - capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);
> - information systems, information flows and decision making processes (both formal and informal);
> - relationships with, and perceptions and values of, internal stakeholders;
> - the organization's culture;
> - standards, guidelines and models adopted by the organization; and
> - the form and extent of contractual relationships.

There are many ways in which an organization might choose to go about the evaluation required in ISO 31000 and any methods employed will be necessarily as diverse as the organizations and the risks they face. One

approach already employed in environmental management is based upon a simple model outlined in Figure 4. This diagram seeks to describe some of the interrelations between organizational management, operational activities and the influences of external context

The model works in terms of key performance indicators (KPIs), management performance indicators (MPIs) and operational performance indicators (OPIs), and shows the links to the external context. Whilst this may be a simplistic model, it does assist in providing an understanding of the links and controls that are needed when developing the framework for risk management, in the context within which the organization operates.



Key

Information flow

Input and output flows related to the organization

Decision flow

Figure 4 — Relationship between performance indicators

Based upon ISO 14031, Figure 1

In order to develop the theme proposed in ISO 31000, the following checklist is offered as a way of determining the key drivers of an organization, whether they are internal or external.

External context

1. social aspects – including social responsibility;
2. cultural aspects – this includes local culture, customs and expectations;
3. political aspects – the political stability in the country(ies) of operation and the related sourcing of materials and services;
4. legal and regulatory requirements in the country(ies) of operation and the related sourcing of materials/services, and where the product/service is sold;
5. financial aspects – cost of materials currently and the stability and costs of production, etc.;
6. economy in the country(ies) of operation and where the product/service is to be sold;
7. technological aspects – the effect of technological changes that impact on the product/service and the opportunity (or threat);
8. impact on the natural environment;
9. impact from competitors;
10. views of external stakeholders (perceptions and values);
11. trends impacting on organizational objectives;
12. relationships with other bodies;
13. portfolio of assets;
14. neighbours;
15. local community;

Internal context

16. governance;
17. organizational structure;
18. roles and accountabilities;
19. policies and objectives – the strategies that are in place to achieve them;
20. internal capabilities – whether the resources and knowledge are established (e.g. capital, time, people, processes, systems and technologies);
21. information systems – how information flows and decision-making processes (both formal and informal) operate;
22. internal stakeholder relationships – perceptions and values of employees, etc.;
23. organizational culture;
24. standards, guidelines and models adopted by the organization;
25. contractual relationships – the form and extent of them.

Information obtained when identifying both the internal and the external context will inform the organization's ability to determine the nature and significance of the various risks it faces.

The approach identified in Figure 4 can also be used for establishing the internal context for specific risks. However, the internal context may need to be broken down into greater detail in order to consider all the factors present throughout the stages of the process.

Gillie's T 4 2

After some deliberation about how they should proceed and their collective risk appetite, the two partners decided that their immediate goal would be to open just one new operation, mirroring what was on offer in Aston-by-Water, in the next few months. They would evaluate its success and then look at the prospect of opening a number of outlets in rapid succession in subsequent years. They selected a shop that was closing down in the nearby village of Reptune, where there was no immediate competition. It was 10 miles from the current operation and was ideally suited for their expansion evaluation programme.

The external context was mapped out by Rob, who identified the following as key issues for consideration:

- legal and regulatory requirements with respect to planning, parking, licensing, occupational health and safety, fire regulations and trading hours;
- financial issues – cost of:
  - employees;
  - base materials (tea, bread and cakes, being an important component);
  - operation, etc.;
- economy in the community in the areas of operation and proposed operation;
- impact from possible competitors (although there were none to their knowledge);
- views of external stakeholders at the new outlet;
- relationships with other bodies, such as the local authority and regulators;
- neighbours;
- local community.

Internally, Gillie was better able to advise of the main components:

- management;
- organizational structure, roles and responsibilities;

- pay and conditions (and competing employment opportunities for workers);
- internal capabilities of the employees and the operation;
- internal culture/relationships – perceptions and values of employees, etc.;
- standards and guidelines adopted by the organization (processes, food hygiene, fire, occupational health and safety, etc.);
- contractual relationships – the form and extent of them (for bread, cakes, catering equipment, tea blends, etc.).

Key learning points

In order for an organization to manage its risks it needs to understand the environment within which it operates, both the external factors and the internal factors that determine how robust its risk management framework needs to be in order to be effective.

Determining the context also helps with identifying the risks that need treatment.

The key points to consider are:

- Has the organization fully evaluated its external context?
- Has the organization fully evaluated its internal context?
- Has this information been reviewed to establish what the risk management framework needs to deliver?
- Have the resources and competencies been determined that are essential for the framework to operate effectively?

Links with management systems standards

Addressing the requirements of Clause 4.1 in ISO 9001 should help with partially satisfying subject areas of context. Similarly, addressing Clause 4.3.1 of both ISO 14001 and OHSAS 18001 will contribute to establishing the context.

Chapter 6 - Framework

This chapter deals with setting up the framework for risk management, and the key activities that need to take place to ensure it is appropriate and effective for the organization's needs. To help you navigate your way through this important chapter it is broken down as follows:

- design of framework (and the process for managing risk);
- risk management strategy;
- risk management policy;
- building capability and competence;
- accountability, roles, responsibility and authority;
- communication;
- reporting;
- risk appetite and risk profile.

The term 'risk management framework' should be clarified and this is described in ISO 31000 as:

> set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring…, reviewing and continually improving risk management…throughout the organization
>
> ISO 31000, Clause 2.3

Design of framework (and the process for managing risk)

ISO 31000 identifies three clear components of risk management: principles, framework and process. The framework comprises a number of elements, as shown in Figure 5 below.

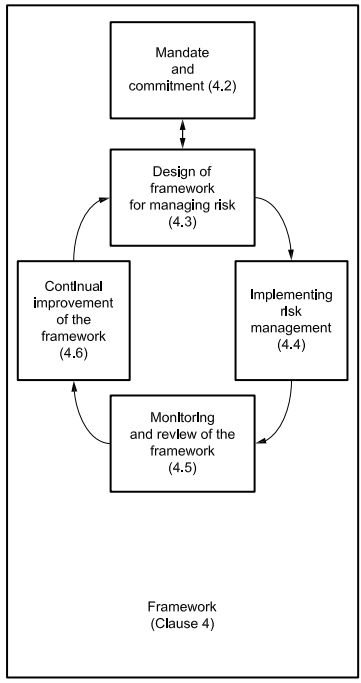


Figure 5 — Design of risk management framework

Adapted from ISO 31000, Figure 1

ISO 31000 emphasizes that 'The success of risk management will depend on the effectiveness of the management framework providing the foundations and arrangements that will embed it throughout the organization at all levels' (Clause 4.1). Additionally, that 'The framework assists in managing risks effectively through the application of the risk management process (see Clause 5) at varying levels and within specific contexts of the organization.'

It is made clear that the framework, as described in ISO 31000, 'is not intended to prescribe a management system, but rather to assist the organization to integrate risk management into its overall management system', the aim being that the organization adapts the components of the framework to suit its specific needs. Where organizations have existing practices and processes, they may be of use in formalizing the risk management framework.

Annex A of ISO 31000 provides a checklist for assessing the adequacy and effectiveness of any current arrangements. Key attributes to be assessed are:

- continual improvement;
- full accountability for risks;
- application of risk management in all decision making;
- continual communications;
- full integration in the organization's governance structure.

In previous chapters we have examined the areas of leadership and commitment (Chapter 4) and context (Chapter 5). Reference has been made to a mandate for a risk management system in Chapter 4. The organization needs to fully understand its context and then mandate (authorize in this context) the necessary actions and resources to ensure the framework is developed to manage its risks arising from its external and internal context.

ISO 31000 does not state what framework and process(es) should be used but states that the standard should '…assist the organization to integrate risk management into its overall management system'. Some organizations may use the integrated enterprise risk management framework proposed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) for financial risk management, and may wish to take on the best elements from both approaches that meet their needs (see Figure 6).

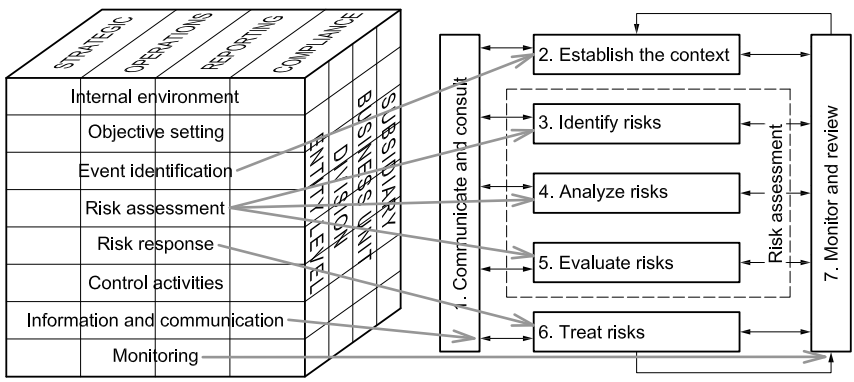


Figure 6 — Correlation between COSO and the ISO 31000 Framework

Provided courtesy of Amair Saleem and Siraj Ismail of Safety, Risk & Regulation Planning Department, Road Transport Authority, Dubai

There should be close interrelationships with the other systems in the organization, for example, those used for business continuity and crisis management.

Highly effective organizations will have the one management system, which is focused on delivering the product(s) and/or service(s), whilst managing the various strategic and operational risks. They need to determine the enterprise-wide risks they face and decide how they will *treat* them. Many risks are unavoidable, even for heavily regulated areas such as occupational health and safety. Establishing a way of managing operational processes within an effective management system should enable the organization to thrive and take on those risks that bring positive benefit, whilst limiting any potential adverse impact.

The risk management framework developed should reflect the external and internal context of the organization, including the size of the organization, its complexity, the nature of its undertakings, the market in which it operates and the risks it faces. So, there is no 'one size fits all' and this needs to be recognized when determining the framework.

It is very likely that most, if not all, the organizations that are implementing risk management will have some formal management systems already in place, and these may be externally certified for business reasons. In such cases, care needs to be exercised when implementing risk management to ensure conflict and confusion do not occur where the systems overlap. If the systems do not overlap, then this would equally be a concern. For instance, if a risk management system does not embrace the business continuity system it is quite likely there will be overlap and some conflict.

To help organizations, three scenarios are covered below and guidance is offered:

1. an organization with a well-developed, effective, overall management system in place;
2. an organization that is starting with very little in place;
3. an organization with formal management systems in place, such as ISO 9001.

1. An organization with a well-developed, effective, overall management system in place

Those organizations with well-developed, effective systems will almost certainly have in place processes for managing some of their risks, e.g. occupational health and safety (which is a legal requirement) and quality. In such cases, the way forward is to carry out a gap analysis of their existing overall management system against the framework and processes in ISO 31000 and identify any shortfalls.

The checklist provided in the 'Risk management policy' section further on in this chapter may help in determining what should be addressed. If the framework and process have evolved and deliver what the organization wants, and the risk management arrangements are 'owned' by the workers, then there would be many advantages in using the existing approach rather than starting afresh. It should be possible to accommodate any additional requirements within the existing overall management system.

2. An organization that is starting with very little in place

If the organization is relatively new, or has few or no formal systems in place, then it may wish to follow what is proposed in ISO 31000. However, those organizations that are relatively small and not complex may find benefit in combining what is outlined in ISO 31000's framework with their core processes and the PAS 99 framework. Where there is the possibility of adopting formal systems at a later date then there is merit in following this approach. Guidance is given in Table 4 below, which should be customized for the individual organization's needs.

Table 4 — Links between the clauses of PAS 99 and clauses in ISO 31000

Clause	PAS 99	ISO 31000	Y/N
4	**Context of the organization**	4.3.1	
4.1	Understanding the organization and its context	4.3.1; 4.3; 5.4; 5.5	
4.2	Understanding the needs and expectations of interested parties	4.3.4	
4.3	Determining the scope of the integrated management system		
4.4	Integrated management system (IMS)		
5	**Leadership**		
5.1	Leadership and commitment	4.2	
5.2	Policy	4.3.2	
5.3	Organizational roles, responsibilities and authorities	4.3.3	

Clause	PAS 99	ISO 31000	Y/N
6	**Planning**		
6.1	Actions to address risks and opportunities	4.4.1; 5.3	
6.2	IMS objectives and planning to achieve them	5.5.3	
7	**Support**		
7.1	Resources	4.3.5	
7.2	Competence	4.3.5	
7.3	Awareness	4.3.5	
7.4	Communication		
7.5	Documented information		
7.5.1	General		
7.5.2	Creating and updating	4.3.6; 4.3.7	
7.5.3	Control of documented information	5.7	
8	**Operation**		
8.1	Operational planning and control	4.4.1; 4.4.2	
9	**Performance evaluation**		
9.1	Monitoring, measurement, analysis and evaluation	4.5; 5.6	
9.2	Internal audit		
9.3	Management review	5.6	
10	**Improvement**		

Clause	PAS 99	ISO 31000	Y/N
10.1	Nonconformity and corrective action		
10.2	Continual improvement	4.6	

3. An organization with formal management systems in place, such as ISO 9001

A suitable starting point for an organization with an ISO 9001 quality management system in place might be a short gap analysis against its present system. The framework in PAS 99, *Specification of common management system requirements as a framework for integration* might be one way of formalizing this gap analysis, given that the PAS was specifically produced to help organizations with multiple systems, and that it provides one set of common requirements for those subject areas that occur in all management system standards.

An effective risk management system should embrace any current stand-alone management system already operating within the organization. A risk requiring treatment can be termed an 'instance of the risk management process' (BS 31100, Introduction) and may use some of the international standards as a model for control, e.g. quality, environment and information security.

Gillie's T 4 2

Deciding what to use as a framework was relatively easy for the newly expanding venture.

Gillie explained to Rob that she was required to apply the hazard analysis and critical control point (HACCP) approach to all the processes for those things she catered for in the shop. This necessitated her identifying all the processes and then determining the risks attached. Those that were classified as critical control points (CCPs) had to have some control in place to ensure that the product was safe for the consumer. For example, in the case of a sandwich, their procedures required that it be kept at a temperature of 6°C or lower.

Rob thought this approach could be extended to the framework for risk management. It also meant that the process itself could follow the same simple approach.

In practice they modified it slightly to accommodate the other technical issues, such as quality and occupational health and safety. It was recognized that they needed to look at everything, from the 'farm to fork', which is what HACCP is really about. In this case, all those things that impacted on T 4 2 needed to be considered in a flow diagram format and evaluated at the various stages.

Risk management strategy

The framework designed for managing the organization's risks should be based upon the factors identified in ISO 31000, Clause 4.3. However, the important step of an implementation strategy hardly features in ISO 31000 or BS 31100. Much depends on the size and complexity of the organization, but those that feel there is a need for a strategy for implementing the framework will need to take into account the organizational context, key stakeholders and the organization's existing capability and maturity. The strategy should set the:

- direction;
- scope;
- priorities of risk management.

An effective strategy will:

- give an indication of how risk management supports the strategy, aims and objectives of the organization;
- be documented and approved by senior management; and
- be communicated effectively.

The strategy may include SMART (specific, measurable, achievable, realistic, time-based) objectives, which define:

- risk management activities to be undertaken;
- the timeframe;
- the resources required, including people, knowledge and budget;
- how progress against the risk management strategy will be monitored, reviewed and reported.

The organization needs to have a clear understanding of its context, and the strategic and operational risks it faces, when determining the framework it is to adopt. Every organization is different and, at first sight, the number of risks it faces may seem daunting (see Figure 7).

Organizations need to have access to information to enable the right decisions to be made to support their risk strategy, in the same way as they would expect to use such information to support any strategic plans. There are many sources of information, including government guidance.

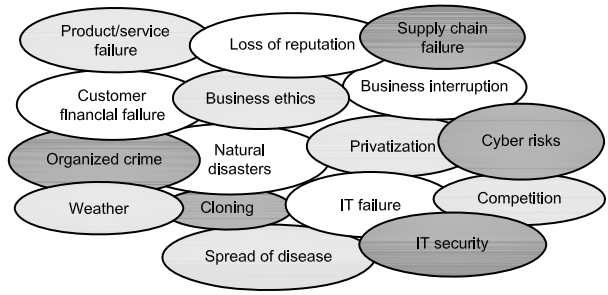


Figure 7 — The number of risks an organization faces may seem daunting

Much of this information relates to acute risks that may have severe impact upon the country as a whole, but it does provide an indication of where organizations might consider making suitable and effective continuity plans in order to mitigate the difficulties that may arise:

- severe weather;
- human disease;
- animal disease;
- major industrial accidents;
- major transport accidents;
- malicious attacks.

Market research carried out by Ipsos found that almost all European financial institutions found the following to be of greatest concern:

- counterparty risk (68 per cent);
- business continuity (58 per cent);
- management liability (52 per cent);
- legal risk (52 per cent);
- fraud (44 per cent);
- mergers and acquisitions (39 per cent);
- outsourcing (37 per cent);
- environmental risk (20 per cent).

Marsh/Ipsos (2009), *New risk management insights for financial institutions*

It is clearly a daunting task for smaller organizations that may not have specialist support to advise them of their best strategy, and the appropriate framework for managing the risks. The organization needs to be able to see the big picture and focus on the priorities that it must manage, be they upside or downside risks. Take, for example, the concept of 'reputation' risk. Many smaller organizations may feel that this is a low priority, but it has been shown that this is a significant area of which all organizations need to be aware. However, it is not really possible to

manage reputation as a single entity. A good reputation is obtained through sustained effort and management of all the risks that significantly impact on the organization. Failure to manage any one particular risk well, for example, product quality, environmental impacts, treatment of workers, investments or finance, can result in bad publicity and damage the credibility of the organization. Strategy should, therefore, focus on those risks that it has to manage well. There may well be many other operational risks that will need to be addressed, but the strategic impact of these may not necessarily be as crucial to the success of the organization.

The development of an overall strategy that determines the organization's direction, the scope and the priorities of risk management that are appropriate to its internal and external context (keeping in mind the risks) are an important foundation of the risk management framework. It is quite likely that the decisions made regarding the framework will not be perfect first time around, and that is why both the framework and the process have iterative steps of continual improvement.

Gillie's T 4 2

The overall strategy for Gillie and Rob's new venture was sustained and sustainable growth in an incremental way. Their plan was to open ventures close to the successful operation and learn what worked best in terms of determining the next location and what the scope and risk priorities were, as they moved forward. The impact of each development was to be logged in order to learn and to use input to manage risks better as the organization expanded. It was felt that this approach was best as it helped to establish which risks were the priorities for treatment/control. More information on risk treatment and how this fits can be found in Chapter 8.

Risk management policy

Having committed to the principles and given a mandate for risk management, the organization should then determine its strategy relevant to its context and develop an appropriate policy for delivering this strategy.

For a policy to be recognized as meaningful its content has to be relevant to the organization and how it operates, and to the community/country/culture within which it applies. The top management should demonstrate that they believe in and own the policy, and should be involved in producing it in consultation with key stakeholders. A

manager at the most senior level in the organization should be appointed to champion the policy and the framework implemented to support it.

An organization may wish to produce a short policy statement or a policy document. If a policy statement is to be produced, it should be relevant and realistic and be authorized by top management, in order to demonstrate the commitment of the organization to managing risks proactively. It should give the direction and commitment for the enterprise to thrive.

For a management system policy in any discipline to be effective it has to commit to deliver its objectives on the discipline covered. A risk management policy is no different in this respect, except it has a much wider scope. The basic content of such a policy should be similar to the theme of many other management system policies and should provide a framework for objective setting and measurement. The guidance given below reflects what is believed to be good practice by the authors, drawing on the guidance found in BS 31100 and various management systems standards.

ISO 31000 gives guidance on what the policy might address. However, the organization should first decide whether it wants a brief policy statement to which people can generally relate, or a detailed policy over a number of pages. In some cases, there will be benefits in both approaches. An example of a short policy statement is provided below, followed by a more detailed example outlining the arrangements more fully, from the British Library.

Folios and Jackets Publications (FJP) Risk Management Policy Statement

FJP is committed to risk management in order to reduce the likelihood of failing to meet our business objectives.

FJP has implemented, and is operating, a risk management framework to ensure that both its strategic and operational risks are evaluated and controlled, in order to support the delivery of objectives and return on investment.

The Governing Board of FJP is responsible for the framework and will act in the interests of its stakeholders.

FJP has formalized a company strategy with due regard to both positive and negative risks in pursuing corporate aims and objectives. KPIs have been assigned to managing risks and these are proactively monitored to ensure all risks are controlled and remain within predefined risk tolerance levels.

The Director of Governance has corporate responsibility for the operation of the framework and for the implementation of risk management strategies. The Head of Risk Management shall also monitor significant risks on behalf of the Board to ensure that the strategies adopted remain effective.

Percy Jackets
Chief Executive Officer
Issue date: 15 March 2012

The British Library Risk Management Policy

Risk Management Policy

A statement defining risk and outlining the Library's policies and limits of responsibility with respect to risk management.

Introduction
The British Library defines risk as the threat that internal or external events will adversely affect its ability to achieve its strategy, policy and operational goals.

It recognises that risk is something that cannot be wholly contained but aims to manage the exposure to those risks to a satisfactory level.

It is the intention that effective, proactive risk management supporting structured well managed risk taking is integrated into the culture of the Library.

Principles
The Library will identify and manage risks that endanger the achievement of the strategic aims defined in its Business Plan or the operational aims defined in Directorate plans.

The approach adopted will meet the requirements of the HM Treasury guidance on Management of Risk – A Strategic Overview ("The Orange Book") and will be enhanced with best practice from other organisations as opportunities arise.

The Library's internal control framework incorporates its risk management approach. Management of risk will be embedded at all levels of the organisation, supported by an active training and education programme.

Risk Assessment
Risks will be assessed against estimation criteria approved by the Board. These criteria cover the potential impact of the risk and the likelihood of its occurrence. The risk will be considered for its effect on strategy, operations, finances or reputation and whether they are external or internal.

Risk Tolerance
The senior manager responsible for the work carrying a risk will, at the start of a year for operational services or at the start of a programme or project, assess the risks that that work may be subject to.

They will use the estimation criteria noted above. They will also be responsible for identifying the acceptable tolerance level for the risks involved and confirming them with the Risk Group.

As risks are managed this tolerance level will be used as the prompt for the escalation of risk reporting to senior management.

Risk Management
Risks will be managed in accordance with an agreed approach ranging from terminating the risk, through possible reduction measures, acceptance and monitoring or passing the risk on. Review of the risks will be carried out by the manager assigned responsibility for it.

Risks will be reviewed:

- Annually by the Board as part of the planning cycle;
- Quarterly by the Exec Team as part of the business plan monitoring process;
- At each of its meetings by the Board Audit Committee;

- Monthly by the Exec Team on an exception basis;
- Monthly by Directorate Management teams for their own subset of risks;
- Local risk registers will be developed as needed based on these policy principles.

Roles and responsibilities
Each level of the Library has a responsibility for risk awareness and management. The main roles and responsibilities are as follows:

Board
The Board is responsible for confirming that the risk management approach will aid the achievement of policy aims.

Board Audit Committee (BAC)
BAC are responsible for annual review of the risk management process and for regular review of progress on risk management actions at thrice yearly meetings.

Accounting Officer
The Accounting Officer is responsible for ensuring that the risk management framework is adequate and that processes are in place to ensure that it is working effectively.

Exec Team
The Exec Team are responsible for risk review in their own areas of responsibility and for championing the required culture change.

Risk Group
This group includes the Compliance Officer, the Head of Estates Risk, the IT Security Officer and the Directorate Finance Managers of each Directorate. It is responsible for the maintenance and management of the risk register ensuring that changes are reflected on a timely basis when necessary. The group is also responsible for providing advice and organising training for managers on risk management issues.

Managers
Managers at all levels are responsible for ensuring that risks to their activities are identified, recorded, assessed and managed on an agreed basis.

Internal Audit
Internal Audit acts as an independent review of the Library's overall internal control framework, including risk management, and reports their findings to the Accounting Officer and BAC.

www.bl.uk/aboutus/foi/pubsch/pubscheme5/riskpolicy.html

The excerpt below from ISO 31000 sets out guidance on what the risk management policy should contain. Whilst in reality it is unlikely that a risk management policy statement that is short and focused on commitments will include detailed information on all of the items listed below, these remain important considerations.

> The risk management policy should clearly state the organization's objectives for, and commitment to, risk management and typically addresses the following:
>
> – the organization's rationale for managing risk;
> – links between the organization's objectives and policies and the risk management policy;
> – accountabilities and responsibilities for managing risk;
> – the way in which conflicting interests are dealt with;
> – commitment to make the necessary resources available to assist those accountable and responsible for managing risk;
> – the way in which risk management performance will be measured and reported;
> – commitment to review and improve the risk management policy and framework periodically and in response to an event or change in circumstances; and
> – the risk management policy should be communicated appropriately.
>
> ISO 31000, Clause 4.3.2

We deal with each of these elements in more detail below.

'the organization's rationale for managing risk'

The policy should be appropriate to the organization's context and strategy, and should explain why the organization is committed to managing its risks effectively. The risks it faces in the business environment in which it operates and the nature of its products and services should be considered when writing the policy. See sample extract below:

> 'The British Library defines risk as the threat that internal or external events will adversely affect its ability to achieve its strategy, policy and operational goals.
>
> It recognises that risk is something that cannot be wholly contained but aims to manage the exposure to those risks to a satisfactory level.' (The British Library)

'links between the organization's objectives and policies and the risk management policy'

The organization may have a number of separate policies devoted to specific risks, such as the environment and occupational health and safety. It will almost certainly have committed to achieving objectives in such areas. The overarching risk management policy should link to these policies and objectives, and provide a framework for setting and reviewing risk management objectives.

> 'The Library will identify and manage risks that endanger the achievement of the strategic aims defined in its Business Plan or the operational aims defined in Directorate plans.' (The British Library)

'accountabilities and responsibilities for managing risk'

Whether the policy is an all-embracing policy, as seen in the British Library example above, or is just a brief statement, as can be seen in the FJP example, will determine how much information can be provided on accountabilities and responsibilities. In a policy statement, commitment to both should be made but the detail would be better included in the general policy arrangements (see example in the full statement from the British Library). It is absolutely imperative that accountabilities, authorities and roles and responsibilities are well defined and everyone knows their role (see 'Accountability, roles, responsibility and authority' section below).

The British Library policy details specific roles for different groups within the organizational structure:

- Board;
- Board Audit Committee (BAC);
- Accounting Officer;
- Exec Team;

- Risk Group;
- Managers;
- Internal Audit.

'the way in which conflicting interests are dealt with'

The organization should commit to prioritize its risk management effort, and this may lead to conflicting interests in some cases. The treatment of one risk may increase the threat of another known risk, or create risks that had not been anticipated or fully evaluated. A general statement to the effect that the organization has a strategy for prioritizing risks and managing areas of conflict could be included in the short policy statement but, again, the detail would be best dealt with outside any short policy statement. The approach will very much depend on the maturity of the organization, its size, culture, stakeholders and context.

'commitment to make the necessary resources available to assist those accountable and responsible for managing risk'

It is indeed important to commit to resources and this means personnel as well as infrastructure, equipment, etc. As has been stated in Chapter 4, risk management requires leadership and commitment and needs to be embedded within the culture of the organization, as exemplified below. This can only be achieved by ensuring that there are sufficient resources for effective risk management. For the avoidance of doubt, the resources will include infrastructure, finance and personnel. Failure to deliver sufficient resources in any particular area or risk discipline is likely to have a negative effect that may well spread throughout the organization. For instance, a commitment to production at 'any cost' may lead employees to see little commitment to their well-being and this could lead to a negative impact on production.

> 'It is the intention that effective, proactive risk management supporting structured well managed risk taking is integrated into the culture of the Library.' (The British Library)

'the way in which risk management performance will be measured and reported'

The detail on how performance will be measured would not normally be included in a policy statement, but commitment to a process of continual evaluation should be included and a commitment to reporting is good practice.

'KPIs have been assigned to managing risks and these are proactively monitored to ensure all risks are controlled and remain within predefined risk tolerance levels.' FJP

'commitment to review and improve the risk management policy and framework periodically and in response to an event or change in circumstances'

It is equally important to commit to review and improve the policy and framework periodically. No policy is likely to be robust enough to not need to be changed over time, particularly if there is new leadership in the organization. It may be that an event or change in circumstances (new product, acquisition, market concerns, etc.) also warrants such a review. If there is a new strategy or objectives, then the policy should reflect such changes.

A review should be conducted at least annually to ensure that the policy has been working as intended and, where this is not the case, that actions are put in place to address any deficiencies or to introduce improvements.

'the risk management policy should be communicated appropriately'

Communication of the policy is important to those within the organization who are expected to deliver it. It may also be necessary to communicate a policy statement to stakeholders, although the organization may not wish to provide all the detailed arrangements to everyone – particularly where there are market sensitivity or security issues.

A checklist is provided below to help you to identify any gaps in your risk management policy.

Checklist – Are there gaps in the organization's risk management policy?

	Yes	No
Does the policy set out how risk is to be governed?		
Does the policy contain a statement of the attitude of the organization to risk?		
Is there a description of the purpose of the policy?		
Does the policy state to whom and to what it applies?		

	Yes	No
Does the policy describe the high-level principles and benefits of implementing risk management?		
Does the policy set out the level and nature of risk that is acceptable?		
Does the policy set out criteria for monitoring and benchmarking risks?		
Does the policy describe the purpose, frequency and scope of reporting?		
Does the policy describe the allocation of management roles, accountabilities and responsibilities for risk management?		
Does the policy set out risk management and internal control objectives?		
Does the policy describe risk management arrangements?		
Does the policy provide details of procedures for risk identification and ranking?		
Does the policy provide an explanation of the relationship between the risk management policy and other policies?		
Does the policy state whether variations are allowed?		
Does the policy describe the process for seeking requests for variations?		
Does the policy commit to the allocation of appropriate resources for risk management?		

Building capability and competence

Embedding risk management throughout the organization, and developing risk management maturity, relies on the organization selecting personnel who have the capability to discharge their duties effectively to work on its behalf. The requirement for competence in managing risk is recognized in ISO 31000, Clause 4.3.3. Embedding risk management and all its facets is fundamental. It relies on leadership and

commitment from the top to provide the basis for a positive culture with respect to the organization and the risks it must manage.

By competence, it is meant that personnel should have the appropriate skills, experience and knowledge. It is insufficient just to send someone on a training course and expect them to be sufficiently skilled. There needs to be some demonstrable measurement that they have understood what is expected of them. Training and communication with personnel should take into account their literacy and knowledge of the indigenous language used.

It will depend on the role an individual has within the organization as to what competence is needed, but throughout the organization there should be the overall capability with respect to:

- corporate governance requirements;
- the organization's risk policy;
- any legislative and regulatory compliance requirements;
- the risk management process;
- the identification, assessment and management of risks;
- risk tools and techniques, and how and where they are applied;
- risk reporting requirements;
- the organization's risk appetite;
- the organization's escalation rules.

The aim should be to enable those persons who can impact on particular risks – those that are under the organization's control – to work and/or act in the organization's best interests, and to do this they should:

- be aware of the risks that they are expected to manage;
- be aware of their roles and responsibilities;
- have the necessary competence to perform tasks that can otherwise impact on managing the risks;
- have the appropriate education or be trained, where necessary, to achieve the required awareness/competence.

If contractors are employed, then the organization should require them to be able to demonstrate that their employees have the competence and/or appropriate training.

The competence requirements for individual tasks should be determined and this should be taken into account when assigning roles and responsibilities. The following factors should be considered when determining the competence needs:

- the identification, assessment and management of risks;
- roles, accountabilities and responsibilities in the organization for the management of risks;
- nature of the tasks to be performed;

- individual capability.

Specific consideration should be given to the competency requirements for those person(s) who will be:

- the top management appointee for risk management;
- directly involved in risk management activities;
- performing audits.

A checklist is provided below for assessing whether the arrangements that are in place meet what is proposed above, for ensuring the organization has the capability to manage its risks.

Checklist — Does the organization have the capability to manage its risks?

	Yes	**No**
Have the competency requirements for the various roles and responsibilities been determined?		
Has specific consideration been given to the competency requirements of top management?		
Have competency requirements been established for those responsible for identifying risks?		
Have the competency requirements been established for risk owners?		
Are personnel trained to manage the risks they have to control?		
Is awareness training given to all personnel on risk management and the organization's risk management policy?		
Are the appropriate people trained in how to use the tools and techniques for risk management?		
Are the appropriate people trained in the requirements of risk reporting?		

Gillie's T 4 2

Gillie looked at the competency skills needed to run the current organization at the management and operational levels. This had not been done in a formal fashion, although she had specified what food hygiene qualifications and basic health and safety training were necessary.

Rob reviewed these with her and one of the supervisors they had identified for running the new venture in Reptune. Their idea was to mirror the operational competency skills used at the Aston-by-Water operation and then extend this where additional skills for the new site were concerned. The new area was subject to some antisocial behaviour. There was also the problem of unruly schoolchildren in the area and their custom might not be welcome.

The new location fell within the control of another local government body (something new in the external context), which was far more rigid over planning and nuisance issues – including tables and chairs affecting pedestrian traffic.

Accountability, roles, responsibility and authority

The arrangements and structure for risk management will depend on the organization: its size, complexity and context, as well as its maturity in managing risk. It is therefore not possible to generalize as to what is needed and the organization will need to tailor the guidance to fit its specific circumstances.

ISO 31000 provides the following guidance:

> The organization should ensure that there is accountability, authority and appropriate competence for managing risk, including implementing and maintaining the risk management process and ensuring the adequacy, effectiveness and efficiency of any controls. This can be facilitated by:
>
> - identifying risk owners that have the accountability and authority to manage risks;
> - identifying who is accountable for the development, implementation and maintenance of the framework for managing risk;
> - identifying other responsibilities of people at all levels in the organization for the risk management process;

- establishing performance measurement and external and/or internal reporting and escalation processes; and
- ensuring appropriate levels of recognition.

ISO 31000, Clause 4.3.3

Larger organizations may well relate to the guidance given in AIRMIC/Alarm/IRM's *A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000* (2010), which identifies risk management responsibilities under the following headings:

- chief executive officer (CEO)/ board;
- business unit manager;
- individual employees;
- risk manager;
- specialist risk management functions;
- internal audit manager.

For smaller organizations with low risks, with, say, 50 people, it is unlikely that such guidance would be appropriate. The principles given above from ISO 31000, Clause 4.3.3 are in themselves sound in terms of what responsibilities should be managed, but how they are assigned is up to the needs of the enterprise.

The term 'risk owner' is commonly used to mean the person or entity with accountability and authority to manage a (specific) risk. They may also be responsible for the identification of those responsible for the development, implementation and maintenance of the framework for managing risk, together with ensuring that all those at the various levels within the organization understand their individual risk management responsibilities where they exist.

A checklist is provided below to enable you to determine how accountability, roles and responsibilities have been determined within your organization. This guidance should be tailored to the organization's needs.

Checklist — How have accountability, roles and responsibilities been determined within the organization?

	Yes	**No**
Has your organization identified, defined and communicated responsibilities for risk management?		
Has senior management created a risk management framework?		
Is the risk management framework up to date?		

	Yes	No
Does senior management ensure that there are sufficient resources for effective risk management?		
Has senior management provided strategic direction on the recognition of risk?		
Has senior management given clear direction on the recognition of risk and the organization's risk appetite?		
Has senior management approved a risk management policy?		
Does senior management recognize the importance of developing a risk management culture?		
Does senior management ensure that the risks faced by the organization are properly assessed and managed?		
Does senior management evaluate the implications of change?		
Does senior management report on risk management to relevant stakeholders?		
Do individuals in the organization understand the risks that relate to their activities?		
Are individuals aware of how effective risk management can contribute to the success of the organization and the achievement of their personal objectives?		
Do individuals recognize the contribution they can make personally to the improvement of risk management in the organization?		
Are individuals aware of the need to report new or emerging risks to senior management?		
Where appropriate to the size and nature of the organization, do you have suitably competent risk owners and risk response owners?		
Where an organization has several departments, do the managers of those departments fully understand		

	Yes	No
their responsibilities for managing risk on an operational basis and promoting risk awareness within their units?		
Have appropriate performance measurements been established?		
Have arrangements been made for reporting risk management performance?		
Are all staff aware of procedures for escalating issues within the risk management system?		

Communication

Both internal and external communications are important functions that should be operating effectively in order to deliver the risk management strategy and policy. It is essential that those working within or on behalf of the organization are aware of their individual responsibilities for risk management. It is equally important to communicate with external stakeholders on those areas they need to be kept informed about regarding the organization's governance, particularly key areas. There should also be a mechanism for dealing with information communicated from external parties.

Internal communication

ISO 31000 identifies the following that should be addressed:

> The organization should establish internal communication and reporting mechanisms in order to support and encourage accountability and ownership of risk. These mechanisms should ensure that:
>
> - key components of the risk management framework, and any subsequent modifications, are communicated appropriately;
> - there is adequate internal reporting on the framework, its effectiveness and the outcomes;
> - relevant information derived from the application of risk management is available at appropriate levels and times; and
> - there are processes for consultation with internal stakeholders.

> These mechanisms should, where appropriate, include processes to consolidate risk information from a variety of sources, and may need to consider the sensitivity of the information.
>
> ISO 31000, Clause 4.3.6

Arrangements should be made for communications within the risk management framework itself and should include those arrangements made for formal reporting. They should be in line with the governance structure and, ideally, integrated with internal management reporting for efficiency and effectiveness.

Openness of communication is one of the key requirements for organizations that have a positive culture, and it has been shown in the nuclear industry that 'individuals who report low accident experience have a high perception of risks' (Coote and Lee Employee perception of safety at Sellafield. Initial results of the safety survey carried out in 1991/92. BNFL, Risley, Warrington).

Communication has to be a two–way process, with management taking note and action, where appropriate, on those matters raised through the upward communication processes. Failure to do so will almost certainly damage, if not destroy, the culture that an organization needs to ensure it has risk management embedded within the organization. All too often there are well-developed communication channels down the organizational chain that ensure personnel know their responsibilities, but the upward channels are equally important. These should also be well established to gain employee buy-in. Formal reporting arrangements from staff meetings is an effective way that this may be achieved, and the practice that exists in many organizations for safety meetings and the minutes issued could be a successful formula to follow.

There may well be business sensitivity around certain risks and the risk management processes may operate on a restricted access basis, with only those specifically involved aware of the controls and arrangements that are in place. This does not preclude personnel from being made aware that in the 'event of', or if there is 'concern about', *X*, they should advise a designated person responsible for the area. For example, it would be unwise to advise employees of all the sophisticated arrangements that may be in place should there be a bomb threat, but key personnel should be able to activate a plan if advised of such an emergency without all personnel knowing the contingency arrangements.

Many risks, such as fire, emergency, safety and security, may have well-documented systems upon which everyone has received training and which are openly available. In such cases, feedback on performance areas where there is a need for improvement will have established routes for communication. If the risk is a sensitive issue, the policy of openness may not be sensible. Employees should be advised that, for security reasons,

the communication channels are not visible to all, but are in place and are effective, and any concerns should be routed via designated key personnel. Acknowledgement of any messages communicated upwards will also help to promote the active engagement of employees.

A worker finds that a particular spray polish is far better for his day-to-day cleaning work than the one supplied by the organization. He may not be aware that the silicone content can be very damaging to the electronic switchgear and is likely to cause major failure to a control system, which could have significant consequences.

The organization did not recognize the need to promulgate the information provided by the switchgear installers to its maintenance/cleaning personnel about the importance of using the specified product for essential maintenance. Failure to communicate effectively caused display panels to fail, which in turn led to major adverse consequences at a large transport arrival/departure centre.

Internal communication should not be seen as employee consultation. Consultation and, more importantly, participation of employees is vital. For some areas of risk, the employee is a valuable source of information, as a result of previous work experience, training or just by using plain common sense. They are a valuable resource and should be used particularly in the areas of operational risk, such as safety, food safety, quality, information security and fire. In some of these areas it is essential that workers are consulted on what 'will work' and what 'won't work'. If personnel find it difficult to follow a procedure they may well adopt a more convenient one, which may be better (which would be good and should be recognized) or which may create risks of which they and the organization are not aware.

Lack of internal communication in a railway organization had major consequences. One working party research group identified underutilization of vehicles, and put in major steps to significantly reduce the fleet size and to make the vehicles work four times as hard. A parallel activity was being undertaken on vehicle maintenance, which identified this fleet of vehicles as over-maintained for the work undertaken. They recommended a signification reduction in maintenance activity. Both recommendations were implemented, with disastrous consequences, in that there were major problems with vehicles breaking down in service and investigators looking for failures in components for erroneous reasons. In effect, the vehicles were working four times as hard with a quarter of the maintenance levels!

Two project groups were independently developing a risk opportunity for improving efficiency and reducing cost of operation by introducing new methods of working, without the essential internal communication channels.

Internal communications should provide specific information on risks and their management to enable those in receipt of the information to act in the manner required.

External communication

ISO 31000 identifies the following with respect to external communication:

> The organization should develop and implement a plan as to how it will communicate with external stakeholders. This should involve:
>
> - engaging appropriate external stakeholders and ensuring an effective exchange of information;
> - external reporting to comply with legal, regulatory, and governance requirements;
> - providing feedback and reporting on communication and consultation;
> - using communication to build confidence in the organization; and
> - communicating with stakeholders in the event of a crisis or contingency.

> These mechanisms should, where appropriate, include processes to consolidate risk information from a variety of sources, and may need to consider the sensitivity of the information.
>
> ISO 31000, Clause 4.3.7

The guidance is succinct and makes the relevant points on what is needed here. There is an obvious need to meet any regulatory requirements that apply and it should be remembered that these may vary from region to region and country to country, and local offices may have to take responsibility for any local enforcement issues. The sources of information will vary considerably, but a good place to start is websites provided by relevant government bodies, regulatory agencies and trade associations. Where organizations seek insurance to cover specific risks (an example of risk sharing) the insurance body would expect to be advised of the areas of risk to ensure the proper considerations are made and an appropriate premium levied.

It will depend very much on the nature of the organization and its risks, but consideration should be given to active communication to stakeholders over emergency and contingency arrangements. It is rare for an organization to be totally independent, such that it has no impact on others or reliance on other bodies.

The business continuity arrangements should be established and communicated, or activated in the event of an emergency, and such plans will almost certainly involve external bodies.

> *A small organization working in a unit on an industrial site processing/cleaning industrial oils poses a significant risk to its neighbours should there be a fire or explosion, because of polychlorinated biphenyl (PCB) and other chlorinated compounds on its premises. No matter what controls are in place, a lightning strike could have disastrous consequences.*
>
> The nature of the risk should be communicated to the emergency services and to neighbours so that they can establish contingency plans in the event of an emergency. In the absence of such communication the outcome could mean that a manageable incident may become a disaster.

When establishing communication links it is necessary to put in place reviews of the risk perceptions from external stakeholders. The customer requirements, social standards and societal expectations can change dramatically due to a specific event, political change or discovery of some previously unknown characteristic of a product or material. Early warning

of this possibility needs to be fed into the organization so that it can strategically respond should it be the sensible option.

The checklist below is provided to give some guidance of those communication processes that should be considered. There may well be more, depending on the organization, that should be added to this list.

Checklist — Communication

	Yes	No
Does the organization see internal communication as essential to success?		
Is there a mechanism for communicating to all levels in the organization that actually works?		
Is the organization willing to change things when necessary to improve internal communication?		
Does the organization have a policy on 'whistle-blowing'?		
Is senior management seen to be listening to the views of those involved in day-to-day activities on how risk can be more effectively managed?		
Is the organization prepared to invest in resources to enhance the effectiveness of internal communication?		
Does the organization ensure that those responsible for internal communication have access to all the right information at the right time?		
Does the organization have effective mechanisms for communicating with external stakeholders, including: suppliers, shareholders, customers, neighbours and regulators?		

Gillie's T 4 2

Rob and Gillie identified the internal and external context for their progressive expansion of Gillie's T 4 2 tea shop and café.

They recognized the risks that needed to be managed and recognized that communication was an important step towards minimizing any problems that might occur (in other words, to control the risks). The following were immediately identified as external and internal communication issues.

- It was essential to approach the owners of the site and establish whether the price and terms were right for Gillie to take on the lease.
- It would be necessary to make a planning application for change of use and to establish any covenants the council may apply about unloading, parking, and outdoor tables and chairs.
- The insurers would need to be contacted regarding the insurance premium.
- The local environmental health officer would need to be contacted to ensure a good working relationship is established.
- There was the important issue of taking the current staff into their confidence where this was practicable, as they would wish some of these to help with setting up the new facility and to train newcomers. Equally, others would have a more important role in the existing operation and would need to train newcomers for both existing and new operations.

So, one of the key stages would be to involve the workforce and communicate the plans for expanding the business with them collectively and individually. The timing for this and applications, etc. were also agreed.

Reporting

One of the key outputs of communication is reporting, both to internal and to external parties. The importance of general communication has been outlined already, but ISO 31000 highlights the issue of reporting as being an integral part of designing a framework for managing risk. This element is covered briefly here for completeness as it is a key part of the framework. However, the subject matter is dealt with in greater depth in Chapter 11.

Those organizations with formal management systems in place should have established monitoring and checking systems, together with audit programmes, that give senior management information on how the organization is performing and where improvements should be made. Auditing (see Chapter 10) is a proactive tool for establishing the robustness of how the risk management process is working, and the report should be viewed positively by management as a tool for continual improvement rather than one for apportioning blame. Similarly,

information on corrective and preventive action should be viewed as a learning resource on how to improve.

Other areas of risk may not have such formal systems in place. There is, however, merit in adopting approaches such as that specified in ISO 9001, which is used by more than one million organizations worldwide and defines the requirements for quality management but, in reality, is, in many ways, a business management standard. This approach should be integrated into the overall management system.

Risk appetite and risk profile

Neither of the terms 'risk appetite' and 'risk profile' is covered in any detail within ISO 31000 or BS 31100, although these terms are commonly used by those working in the field of risk management.

Risk appetite is defined as: 'amount and type of risk…that an organization is willing to pursue or retain' (from ISO Guide 73) and relates closely to risk criteria and risk tolerance.

> Risk criteria: 'terms of reference against which the significance of a risk…is evaluated'
>
> Risk tolerance: 'organization's or stakeholder's…readiness to bear the risk…after risk treatment…in order to achieve its objectives'

ISO Guide 73

The concepts are useful and some guidance is provided below for those who wish to embrace them within their risk management arrangements.

Organizations live with risk and manage aspects of their 'risk profile' in various ways. They insure against losses, implement safety, health and environmental management systems, lobby governments, hedge currencies, trade commodity futures, and protect their IT systems with firewalls, etc. Whilst some organizations are well aware of the need to manage elements of risk, the reality is often that, despite strong performance, there is a lack of real comprehension of some of the risks being taken. There is a lack of understanding of the 'appetite' the organization has for risk – a fundamental building block of any system designed to manage those risks.

> …executives are relatively comfortable in describing risk appetite in 'traditional' areas e.g. regulatory compliance. However they are less confident about describing risk appetite in more qualitative areas e.g. reputation.
>
> © KPMG 2008
>
> 'Understanding and articulating risk appetite'

The concept of 'risk appetite' is one that is difficult for organizations of all sizes to get to grips with, but the risk appetite of an organization goes right to the heart of how it does business, how it wishes to be seen by its various stakeholders. Naturally, this appetite will vary from organization to organization and each organization's own perspective will be influenced by its own unique circumstances – the context in which it operates. Put very simply, risk appetite is the amount of risk the organization is prepared to take in order to achieve its objectives.

The risk appetite has to be determined by the board (or equivalent) of an organization as it is linked very much to the overall strategic objectives for the organization, an area for which the board should have ultimate responsibility. If the board does not have a clear understanding of the organization's risk appetite, its ability to communicate this appetite to those in the organization responsible for the operational management of risk, and its ability to manage the risk management process, will be severely hampered.

When determining the risk appetite and the organization's tolerance to risk, the following considerations should be taken into account:

- the context of the organization and its understanding of its risks and associated management processes;
- whether the organization might be prepared to accept a higher than usual proportion of risk in one area rather than another;
- the need for guidance on the direction and boundaries of the risk that can be accepted at various levels of the organization;
- the controls, authorities, etc., including the delegation of authority, in relation to approving the organization's risk acceptance;
- what is stated in the organization's risk management policy and whether the risk appetite reflects this statement;
- possible limits of tolerance, including qualitative and quantitative statements for specific risks the organization is or is not prepared to accept.

Some organizations may choose to have a risk appetite statement that reflects the above and is a written guidance statement for relevant personnel.

In developing the risk appetite, the organization may wish to consider a number of areas, including:

- liquidity;
- cash flow;
- credit rating;
- reputation;
- new products;
- customers;
- technological developments;
- supply chain management;
- environmental impact;
- corporate governance;
- human resources;
- safety record;
- legislative requirements.

Risk appetite planning

A team approach is a good way to plan for the development of the risk appetite within the organization. If a team approach is possible, it should try to make sure that all parts of the organization are represented and there is visible commitment from senior management to this activity. The planning should take into account the business context in which the organization operates, and keep present strategies, business plans, etc. in view. Without the ability to ensure that the team understands the context in which the organization operates, the development of the risk appetite statement is much more difficult to achieve. The team should be able to assess the organization's capabilities in the management of risk.

A simple process for developing a risk appetite statement might be as shown in Figure 8.

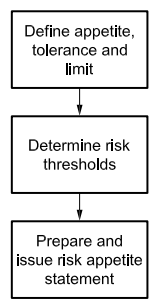


Figure 8 — Developing a risk appetite statement

Defining appetite and tolerance

The next stage should broadly identify the risks that the organization may face and the impact these risks might have upon the achievement of objectives. It can then decide what the appetite is for the various areas – which may be quantitative or qualitative.

Determine risk thresholds

It is most important that those risks that have zero tolerance are identified. Other areas of risk may have limits or targets defined and this will often depend not only upon organizational appetite but also upon external factors, e.g. customers and regulators in the electricity industry have virtually zero tolerance of supply interruptions. Professional services firms – lawyers and accountants – may have a low appetite for risk in the technical aspects of their work but may be very willing to take commercial risks in expanding to new markets.

Risk appetite statement

Finally, after preparing a risk profile for the organization, the outcome should be a formal statement of risk appetite, approved by the board, which can be effectively communicated throughout the organization. When preparing the statement of appetite the organization should ensure that it is consistent not only with the organizational culture but also with the capacity within the organization to manage risk, and reflects:

- owners/shareholders;
- external context;
- internal context;
- competition in the field of operation;
- culture of the country;
- regulation, etc.

Should a formal risk appetite statement be made, then it should not just be filed away and forgotten. The environment in which the organization operates will be constantly changing and it will need to react to these changes without delay. This may mean a review of risk appetite, limits and targets if the organization is not to be left behind in a competitive environment where other organizations achieve advantage through their ability to manage risk more effectively.

The organization should therefore determine with great care what its risk appetite is for its risk profile.

Risk profile: 'description of any set of risks…' (ISO Guide 73)

Development of a company's risk management profile can be a fairly elaborate process but it is possible to use a simple self-assessment process to identify the largest gaps.

A principle that can be used is to map out, at a high level, the processes that an organization uses to obtain its raw materials and/or services in order for it to deliver its business objectives, and then to determine the weakest links. By focusing on those that pose the greatest risk, an organization can mitigate against some of its vulnerabilities.

Some organizations use failure modes and effects analysis (FMEA), particularly in the engineering sector. FMEA can be used with good effect with the process approach used for quality systems to determine what could happen if certain stages of the process failed or did not fully work to specification. It is possible to identify those that are most critical and therefore determine the risk profile.

Guidance on this type of approach and many others that may be more appropriate for the operational sector of the business can be found in IEC/ISO 31010.

The risk profile may be for a few large groupings, as can be found for Severn Trent PLC – a large, international company operating in the water supply and treatment field. See its risk profile, provided below.

It is recommended that both the risk appetite and the risk profile are monitored by the board (or equivalent), and are formally reviewed as part of the organization's strategy and planning processes.

Gillie's T 4 2

In the discussions that took place between Rob and Gillie, Rob explained that they needed to agree the appetite for risk. 'We need to determine how willing we are to take on risks.' Gillie stated: 'Surely we might have different appetites for different types of risk? For example, we cannot take risks with the food safety side of the café and shop or else we will be closed down!'

They agreed to list, in broad terms, the areas and activities, and the appetite.

Both agreed that their appetite for risk was at the lowest level, 1, on a scale of 1 to 5, as far as compliance was concerned. Any deviation could lead to prosecution, loss of reputation and the closure of the facilities.

In contrast, they both agreed that, at the other end of the scale, they were prepared to invest money in a new outlet in a village some 10 miles away to see if the expansion programme was realistic and practicable, and gave this a value of 5.

They then determined their risk appetite for their risk profile, but Rob pointed out: 'We need to determine our risk criteria and risk analysis models before we can really move forward.' (For further details on outputs, see Chapter 7.)

Key learning points

The organization needs to understand its context and top management needs to mandate the organization to develop a risk management framework that is robust enough to manage its risks.

The framework and risk management processes should be integrated into the organization's overall management system. In order to do this, it should consider what it has in place that is operating effectively and try to integrate the processes to avoid duplication, conflict and unnecessary bureaucracy.

When designing the framework the key questions to consider are:

- Has top management mandated a risk management framework on the basis of the context of the organization and its risks?
- Has top management taken into account the resources and competencies needed?
- Are there effective processes for managing instances of risk already in operation?
- If so, are other instances being managed in a similar, effective manner?
- Have the best practices and approaches been used to develop the framework and processes for managing instances of risk?

Although not particularly recommended in the various standards, some organizations may benefit from having a strategy for developing and implementing their risk management framework.

It is essential that the competency needs are established so that any person performing risk management activities is competent. There is a need to build the capability throughout the organization so that people have the right experience, skills and knowledge to undertake their duties.

Clarity of responsibilities for risk management is important. Accountability and roles need to be clearly defined, and individuals need to know what is expected of them and what authorities they have.

Both effective internal and external communication channels are essential for risk management and should be addressed.

Communication should be aligned with the governance structure, and internal channels that enable upward communication should be equally as effective as those for communicating downwards.

A robust system is equally needed for two-way communication with all relevant external stakeholders.

It is essential that there is a reporting mechanism, both internally and externally, which utilizes information generated through the various feedback processes.

Use can be made of the outputs from any formal management system processes adopted by the organization, such as ISO 9001.

Determine risk appetite along with risk tolerance, have it agreed by the governing body in the organization, and then communicate it effectively.

Links with management systems standards

Those who have developed an integrated approach such as that in PAS 99 may find their structure will help in developing their framework.

Those with ISO 9001 will find the quality management policy addressed in its Clause 5.3 will help in developing the risk management policy. Similarly, policies addressed in Clause 4.2 of both ISO 14001 and OHSAS 18001 will help.

ISO 9001 deals with competence under Clause 6.2.2 and ISO 14001 and OHSAS 18001 deal with it under Clause 4.4.2.

Responsibility and authority is dealt with under Clause 5.5.1 in ISO 9001, and Clause 4.4.1 in both ISO 14001 and OHSAS 18001 deals with roles, responsibility and authority. OHSAS 18001 also deals with accountability.

Communication is dealt with in Clauses 5.5.3 and 7.2.3 in ISO 9001 and in Clause 4.4.3 in both ISO 14001 and OHSAS 18001.

There is no specific reporting clause in ISO 9001, ISO 14001 and OHSAS 18001, although there are some actions that require reporting.

There are no specific clauses in the management systems standards that refer to risk appetite although there is recognition in Clause 4.3.1 of OHSAS 18001 of acceptability of risks.

Severn Trent – Risk profile

Through its business operations the group is exposed to a number of commercial risks and uncertainties which could have a material impact on our businesses, financial condition, operations and reputation, as well as the value and liquidity of our securities. Not all of these factors are within our control and, in addition, other factors besides those listed below may have an adverse effect on the group.

Changes in law or regulation in the countries and types of business in which we operate could have an adverse effect on our business and operations.

Regulatory decisions in relation to our businesses, e.g. on whether licences or approvals to operate are renewed, whether market developments have been satisfactorily implemented, on the level of permitted revenues for oand reur [sic] businesses, whether there has been any breach of the terms of a licence or an approval, could have an adverse impact on the results of our operations, cash flows, financial condition of our businesses and the ability to develop those businesses in the future.

The results of our operations depend on a number of factors relating to business performance, including the ability to outperform regulatory targets and deliver anticipated cost and efficiency savings.

Earnings from our regulated water business will be affected by our ability to meet or better our regulatory targets set by Ofwat, the Environment Agency, Drinking Water Inspectorate and other regulators. To meet these targets, we must continue to improve management processes and operational performance. In addition, earnings from a regulated business also depend on meeting service quality standards set by regulators. To meet these standards we must improve service reliability and customer service. If we do not meet these targets and standards, both our results and our reputation may be adversely affected and fines could be imposed.

Various government environmental protection and health and safety laws and regulations govern our businesses.

These laws and regulations establish, amongst other things, standards for drinking water and discharges into the environment which affect our operations. In addition, our businesses are required to obtain various environmental permissions from regulatory agencies for their operation. Environmental laws and regulations are complex and change frequently. These laws and their enforcement have tended to become more stringent over time, both in relation to their requirements and in the levels of proof required to demonstrate compliance. While we believe we have taken account of the future capital and operating expenditure necessary to achieve and maintain compliance with current and foreseeable changes in laws and regulations, it is possible that new or stricter standards could be imposed or current interpretation of existing legislation amended, which will increase the group's operating costs or capital expenditure by requiring changes and modifications to its operations in order to comply with any new environmental laws and regulations.

The failure of our assets or our inability to carry out critical operations could have a significant impact on our financial position and our reputation.

We may suffer a major failure in our assets which could arise from a failure to deliver the capital investment programme for our businesses or to maintain the health of our systems. Any failure could cause us to be in breach of a licence or approval and even incidents that do not amount to a breach could result in adverse regulatory action and financial consequences, as well as harming our reputation.

Severn Trent Water's regulated business controls and operates water and sewerage networks and undertakes maintenance of the associated assets with the objective of providing a continuous service. The failure of a key asset could cause a significant interruption to the supply of services, which may have an adverse effect on the group's operating results or financial position. In addition water supplies may, inter alia, be subject to contamination from the development of naturally occurring compounds and pollution from man made sources and these may have an adverse effect on our operating results or financial position.

> The group could also be held liable for human exposure to hazardous substances or other environmental damage.

www.severntrent.com/content/ConWebDoc/386

Chapter 7 - Risk management and implementation

Risk assessment and risk management are two of the key stages for implementing the framework. Risk assessment is the process that provides information and analysis on the risks faced by the organization and enables informed decisions to be made with respect to how it manages its risks.

The process for risk management now needs to be developed to operate within the framework.

In this chapter we cover:

- implementation of the framework;
- risk identification;
- risk criteria and analysis;
- risk evaluation.

Implementation of the framework

In order to progress, the organization needs to determine the risks it needs to manage, including any legal and regulatory requirements. Only when it has done this can it really make sound decisions on its strategy, its policy, objectives and the appropriate processes it needs to implement for managing the risks. Communication and consultation with stakeholders and managers can follow in order to determine the risk appetite. This is very much an iterative process.

ISO 31000, Clause 4.4.1 recommends that the organization should:

- define the appropriate timing and strategy for implementing the framework;
- apply the risk management policy and process to the organizational processes;
- comply with legal and regulatory requirements;
- ensure that decision making, including the development and setting of objectives, is aligned with the outcomes of risk management processes;
- hold information and training sessions; and

- communicate and consult with stakeholders to ensure that its risk management framework remains appropriate.

It further expands on this, stating that risk management should be implemented '…at all relevant levels and functions of the organization as part of its practices and processes.' (ISO 31000, Clause 4.4.2).

This clause is all-embracing and covers many parts of the standard. It very much links with the implementation of the process, which is covered in Chapter 6 through to Chapter 8. The bullet 'ensure that decision making, including the development and setting of objectives, is aligned with the outcomes of risk management processes' identifies that it is essential that the risk management process is implemented, and this will then determine much of the risk management infrastructure.

A first step in the risk assessment process is to determine the tools that may be needed to:

- help implement risk management in practice;
- ensure the organization's risk management framework is aligned with the overall management system and the process it uses to develop maturity;
- ensure the organization's risk management framework is in keeping with its nature, scale, complexity and culture; and
- assist in the development of risk management knowledge and expertise within the organization.

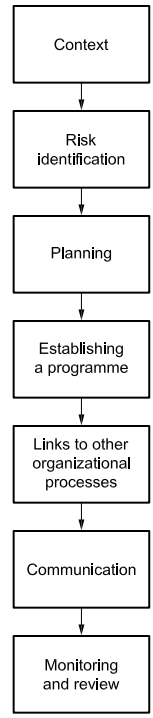
Whatever is developed should be approved by the relevant parties and those intimately involved should be trained in the process and the methodology adopted for risk assessment. (Extensive guidance can be found on risk assessment in IEC/ISO 31010.)

This is a significant task and needs greater resourcing in the early stages than when the system has matured and is operating effectively. Ideally, a team approach should be adopted even if most of the development work is done by a few people or only one person. There needs to be a wider forum within the organization supporting and reviewing the risk assessment programme and determining the strategy and timing for implementation. Each of the recommendations made in ISO 31000, Clause 4.4.1 is considered in turn below.

'define the appropriate timing and strategy for implementing the framework'

This is an activity that should be led by top management. Only by establishing the context and the risks will it be possible to fully determine the organization's overall strategy, define the policy and objectives, and define the appropriate framework. The implementation strategy for delivering the framework and the risk management process

can then begin. The implementation of the framework is best tackled by having a plan with phased stages, as outlined below:



Ideally, the framework and organizational processes will have been developed, and consultation and training completed, before implementation of the framework.

'apply the risk management policy and process to the organizational processes'

A policy in respect of risk management will have already been established (see Chapter 6) and this policy should be:

- relevant to the size and complexity of the organization;
- relevant to the risks the organization has to manage.

These requirements of the policy will need to be applied to organizational processes, enabling objectives to be set that will deliver this policy and will help define the process(es) needed to deliver the specified outcomes.

'comply with legal and regulatory requirements'

The identification of all legal requirements can be challenging. In some of the technical areas, such as environment, food safety, occupational health and safety, and commercial law, there is a labyrinth of laws, regulations and codes of practice that can be extremely difficult for smaller organizations to identify and subsequently apply in their activities. The difficulty is multiplied when working in many countries and having to meet the obligations of one country that might conflict with requirements in another.

For smaller organizations that do not have direct access to legal advisers or specialist help, there are some options for gathering information:

- trade associations;
- suppliers of goods to the organization, who may provide some warning or guidance;
- government agencies – for example, in the United Kingdom:
  - Environment Agency;
  - Health and Safety Executive (HSE) – has a website with search facilities to identify any guidance, code of practice, regulation, etc.;
  - Food Standards Agency (FSA) – provides guidance according to sector and good practice information;
  - Foreign & Commonwealth Office (FCO) and the Department for Business, Innovation and Skills (BIS) [formerly the Department of Trade and Industry (DTI)] – can provide information on practices and requirements when working overseas;
  - British Chambers of Commerce;
- independent specialists.

'ensure that decision making, including the development and setting of objectives, is aligned with the outcomes of risk management processes'

There has to be visible commitment from the top and an embedded culture for managing risks if the organization wants to manage its risk effectively in line with its stated strategy, policy and objectives. It is not uncommon for disasters to occur where the CEO thought that everything was in place and the workforce was committed to delivering the 'vision'. In such cases, there can be a layer of management/line management/supervisors who believe their only role is to deliver output – no matter what the consequences. They can seem to be oblivious to the consequences of mismanaging a risk that they perceive (incorrectly) to be someone else's task. The attitude of 'I manage production' and 'we have

a quality manager/adviser for sorting out quality', etc. is not an unusual situation. To overcome this common problem requires active involvement from top management and one effective solution can be the use of facilitated sessions, using an independent person, that bring together cross sections of the workforce. Each attendee should be able to freely question management's role and, in particular, their manager's role, and the expectation that is placed upon them as an individual, and to identify gaps in the plan and its implementation.

'hold information and training sessions'

If the framework for managing risk is to be successfully implemented, it is necessary for all personnel to be aware of the organization's overall policies and strategies for the structure for managing risk in accordance with ISO 31000. Not only is this a matter of good management practice, but also ensuring that details of the organization's approach to risk management are known will go a long way to developing an appropriate risk management culture in the organization, and will help ensure that all staff are aware of their responsibilities in meeting the organization's aims.

Information and training should also inform staff about the risks they are required to manage and the importance of doing so for both the organization and themselves. This can be done as part of the normal induction process where new employees are introduced to how they should respond to emergencies, occupational health and safety, etc. This information and training should be reinforced by on-the-job training and formal reinforcement training, as and when deemed necessary. The training should not be seen as a one-off event; it should be regularly followed up to ensure that changes in the organization and its policies or strategies are communicated.

'communicate and consult with stakeholders to ensure that its risk management framework remains appropriate'

A mechanism for identifying appropriate stakeholders should have already been developed as part of the development of the context of the organization (Chapter 5). When implementing the framework, communication with the identified stakeholders should take place.

Change can have a significant influence on the framework and, in the same way that the risk management policy cannot be 'cast in stone', reviews will need to take place in the light of changes in circumstances such as:

- new markets;
- new products;
- acquisitions/mergers;
- new partnerships;

- new countries of operation;
- new regulations and/or requirements;
- customer/stakeholder demands;
- workforce expectations;
- insurers;
- incidents;
- public/societal expectations;
- outcomes of internal audits and (management) reviews;
- political changes.

The list is not meant to be exhaustive but serves to illustrate that there is always a need to be proactive and to recognize that what is acceptable today may not be appropriate tomorrow.

Over a period of time the risk profile may change and there may also be a need to review the risk appetite.

Risk identification

One of the most challenging steps is the identification of risks. As stated by Donald Rumsfeld:

> '…as we know, there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns – the ones we don't know we don't know.'

Donald Rumsfeld, www.rumsfeld.com/about/page/authors-note

The organization can only deal with foreseeable risks. However, a robust system may help in developing strategies quickly for risks that emerge where no direct provision has been made for their control or treatment.

ISO 31000, Clause 5.4.2 states:

> The organization should identify sources of risk, areas of impacts, events (including changes in circumstances) and their causes and their potential consequences. The aim of this step is to generate a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives. It is important to identify the risks associated with not pursuing an opportunity. Comprehensive identification is critical, because a risk that is not identified at this stage will not be included in further analysis.

> Identification should include risks whether or not their source is under the control of the organization, even though the risk source or cause may not be evident. Risk identification should include examination of the knock-on effects of particular consequences, including cascade and cumulative effects. It should also consider a wide range of consequences even if the risk source or cause may not be evident. As well as identifying what might happen, it is necessary to consider possible causes and scenarios that show what consequences can occur. All significant causes and consequences should be considered.
>
> The organization should apply risk identification tools and techniques that are suited to its objectives and capabilities, and to the risks faced. Relevant and up-to-date information is important in identifying risks. This should include appropriate background information where possible. People with appropriate knowledge should be involved in identifying risks.

The standard makes it quite clear — that it is crucial to identify all the risks otherwise those omitted will not be considered for treatment. In reality, as the Rumsfeld quote above illustrates, this is, indeed, difficult. For instance, many large organizations probably had not made provision for ash generated by a volcano, so when, in 2010, an Icelandic volcano erupted, it affected delivery of contracts, goods and personnel, and caused chaos in many quarters. This was a known risk but it would appear that not many organizations had made provision for such an eventuality on their risk register.

Some of the higher level risks should have been identified when considering the context of the organization and identification of stakeholders. The risks are best identified from a review in broad areas such as:

- external;
  - strategic;
  - supplier;
  - customer;
- internal.

Trying to catalogue all the possible risks an organization might face can be a daunting task and, typically, takes some time. Where organizations already have existing management systems in place, for example, identifying processes (ISO 9001), identification of environmental aspects (ISO 14001) or safety requirements for control of hazards (OHSAS 18001), these could form the basis for the development of a risk register.

In the absence of any formal systems a simple approach will often work well. As a first step, it can be useful to consider all the company's internal processes, in order to isolate the most relevant and critical risks.

Examination of process maps in a questioning way can identify the most significant vulnerabilities by asking, at various stages, a 'What if?' question. For example, the 'Structured What if Technique' (SWIFT) is commonly encountered as a simple tool that people can start with.

- Identify the systems/processes being considered.
- Brainstorm possible risks.
- Create hierarchy of risks.
- Consider each risk in turn examining:
  - possible causes of the risk;
  - frequency and possible consequence;
  - options for treatment or control.
- Record outcome.
- Reconsider whether any hazards have been omitted.
- Review.

The SWIFT technique is an iterative process and should be reviewed from time to time, particularly at crucial times of change in organization's structure or activities.

There are many sophisticated techniques for risk assessment and not all are appropriate for every organization and situation. Further guidance on the techniques available can be found in Annexes A and B of ISO/IEC 31010.

After this stage the organization can determine where there are risks that should be included in the risk register for treatment and/or control.

In addition, consideration should be given to the critical infrastructure, the relationships, people, regulations, plant and equipment that support the organization's ability to generate earnings. This step might include brand reputation, which could be dependent on product quality control processes.

The following checklist is provided as an aide-mémoire for identifying generic risks that may be applicable to your organization. Tick (1) if it is applicable and (2) if it is not relevant.

External risks

1	2	
☐	☐	Strategic importance of the organization in the marketplace
☐	☐	Public image and reputation
☐	☐	Stakeholder relationships and engagements
☐	☐	Political
☐	☐	Commercial
☐	☐	Suppliers and supply chain
☐	☐	Contractors
☐	☐	Security – including protection of intellectual property

- ☐ ☐ Technology
- ☐ ☐ Legal liability and compliance
- ☐ ☐ Cultural/heritage/environment
- ☐ ☐ Opportunity cost – by not taking opportunity

Internal risks

Leadership and commitment:

- ☐ ☐ Commitment by managers
- ☐ ☐ Resources to deliver objectives and treatment/control
- ☐ ☐ Competence to support decision making
- ☐ ☐ Leadership behaviours
- ☐ ☐ Consistency in communication
- ☐ ☐ Adequacy of planning
- ☐ ☐ Alignment of organizational culture to risk management framework

Employee commitment and competency:

- ☐ ☐ Competency
- ☐ ☐ Ongoing training
- ☐ ☐ Motivation
- ☐ ☐ Opportunities for development
- ☐ ☐ Adequate resources to support activities

Internal communication:

- ☐ ☐ Adequacy of communication systems
- ☐ ☐ Clear directions on implementation
- ☐ ☐ Effective participation of employees with management in decision making
- ☐ ☐ Effective reporting systems from employees to management

Resources and support

- ☐ ☐ Ability to meet deliverables
- ☐ ☐ Delivering customer and stakeholder expectations
- ☐ ☐ Adequate staff support systems
- ☐ ☐ Adequacy of control systems
- ☐ ☐ Structured monitoring and review systems

The above list is obviously not meant to be exhaustive as it would be impossible to cover all the risks faced by all organizations in the world. Every organization is different and the local circumstances may generate risks that are very specific to them. The above list may therefore serve as a series of prompts, and trigger questions about related risks, if the list is used in a group set-up to determine the enterprise risks. Once the risks have been identified, there is a need to record them and show how they are to be managed. Table 5 shows one way of doing this. The records

and prompts for action can be managed electronically but the stage of identifying the applicable risks has to be done by the organization manually.

Gillie's T 4 2

With just one operation, the internal and external risks have all been, in effect, managed informally by Gillie, partly through developing and maintaining good relationships with stakeholders. Now that an expansion of the business is on the horizon she needs to take a more structured approach. When sitting down with Rob to identify the risks that apply to her existing operation, a number of points arise:

- review identified risks;
- the need for a mechanism for formally recording the details, including what are in place as controls;
- whether the controls currently in place will continue to be appropriate once the expansion programme is under way;
- new risks particular to the new context.

The development of a formal risk register focuses their attention, and it becomes clear that existing controls cannot be relied upon, without modification, to deliver the risk protection needed to support the new business model. Gillie, in particular, has concerns about the ongoing resilience and quality of supply to an expanding network of cafés.

The following extract from Gillie's T 4 2 risk register (Table 5) is one example of the manner in which risk can be formally recorded.

Table 5 — An example of the manner in which risk can be formally recorded

1. Risk identifier (number and title)	T 4 2 R1 — Resilience of supplier
2. Nature of risk (possible events: their size, type and number)	Risk of non-supply and/or quality of cakes, etc.
3. Risk analysis	Only one source of supply with unreliable vehicles
4. Stakeholders	Customers and current supplier
5. Risk evaluation	Impact on shop would be significant if product not delivered
6. Loss experience (lessons from previous events)	Only previous problem has been vehicle breakdown. No poor quality issues have ever been experienced
7. Risk tolerance, appetite	The risk of non-delivery is not acceptable
8. Risk treatment	Invest in own new vehicle, which could be used for other purposes
9. Potential for risk improvement	Likelihood of breakdown low and supplier could fill gap in case of such an eventuality
10. Strategy and policy	Look at longer-term solution with respect to supplier and delivery when T 4 2 expands

1. Risk identifier (number and title)	T 4 2 R5 — Food hygiene
2. Nature of risk (possible events: their size, type and number)	Risk of food poisoning
3. Risk analysis	Lack of effective hygiene control
4. Stakeholders	Customers and employees
5. Risk evaluation	Impact on shop would be significant and would possibly lead to closure

6. Loss experience (lessons from previous events)	No previous problems at current shop because of adequate training and supervision
7. Risk tolerance, appetite	The risk of food poisoning is not acceptable
8. Risk treatment	Ensure all equipment is fully maintained and strict cleaning processes are in place All staff to be trained and food safety team leader to be appointed Manager to be given extra training on hygiene and supervisory skills
9. Potential for risk improvement	Likelihood of problem low
10. Strategy and policy	Ensure effective systems are developed, which can be transferred when T 4 2 expands

Risk criteria and analysis

Once the risks have been identified, there is a need to gain a better understanding of each risk and its implications with respect to the organization. For instance, you may have identified that you have a vulnerability in your supply chain and this may need to be analysed in more depth to determine the likelihood of an interruption or delivery failure occurring. This is what is meant by risk analysis. It is about understanding the risk, and the output of the analysis is used in the evaluation of the risk (see 'Risk evaluation', below). In order to be able to make such an analysis the criteria have to be established for making judgements and comparisons.

Risk criteria

As a starting point, the organization should define the risk criteria that it intends to use when analysing the risks. By risk criteria we mean the terms of reference that are to be used when evaluating the significance of the risk. It should help in identifying the significance of each risk with respect to its effect and the likelihood of the event occurring. Such a tool is needed to enable comparisons to be made of the various risks, which should help the organization in determining its priorities and cost justifications when deciding what treatment it is going to adopt. It is quite possible that some controls selected for a specific risk may impact on another risk or the controls selected for that risk. The organization will need to balance one risk against others and determine its course of action, but should have established risk criteria for assisting in the decision making.

The risk assessment tool based on these criteria should enable the benefits of different courses of action to be seen, such as reducing the likelihood or effect of the risk.

ISO 31000 gives the following guidance:

> When defining risk criteria, factors to be considered should include the following:
>
> - the nature and types of causes and consequences that can occur and how they will be measured;
> - how likelihood will be defined;
> - the timeframe(s) of the likelihood and/or consequence(s);
> - how the level of risk is to be determined;
> - the views of stakeholders;
> - the level at which risk becomes acceptable or tolerable; and
> - whether combinations of multiple risks should be taken into account and, if so, how and which combinations should be considered.
>
> ISO 31000, Clause 5.3.5

In practice it is often quite easy for the organization to determine the worst-case scenario with respect to the consequences, but determining the likelihood is often more difficult. For instance, consequences of losing a particular contract can be determined with relative ease. The likelihood may be difficult to determine because of unknown factors affecting the customer, new product/methodology developed by a competitor that the customer will favour, or failure to deliver on the organization's part for some reason that had not been considered in the risk register.

Each of the recommendations from ISO 31000 is considered below, in turn.

'the nature and types of causes and consequences that can occur and how they will be measured'

There is no comprehensive list of causes and consequences as they are both extremely large and relate very much to the organization and its context. There may be advantages in having broad categories of consequences, such as financial, reputational, business continuity, regulatory and loss of life, although this poses problems in itself as an environmental disaster, for instance, may bring regulatory, financial and reputational costs to the organization. There is a very useful model provided in AIRMIC//Alarm/IRM's *A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000* (2010), which proposes that risks can be broken down into four areas. See Figure 9.

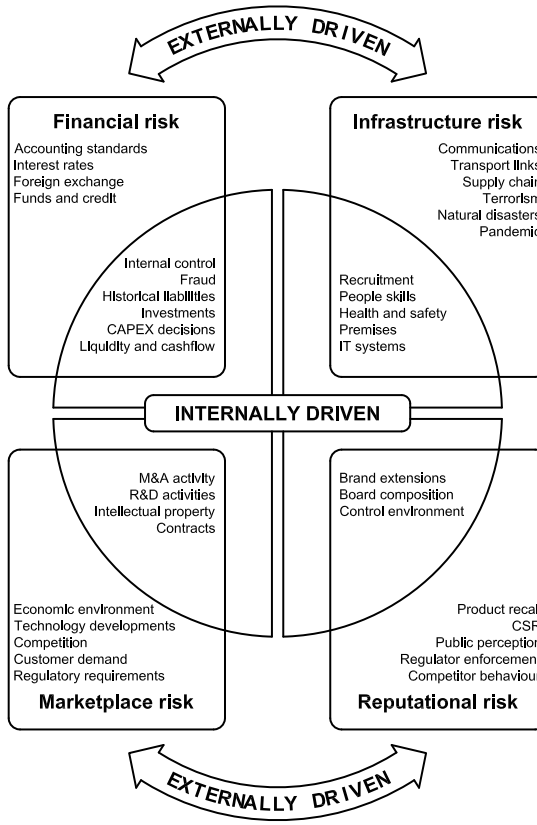


Figure 9 — Drivers of risk management

A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000

There are benefits to classifying the consequences in a comparative way. One way of doing this is to assign a monetary cost, as shown in Figure 10.

Severity	Frequency: Once per day	Once per week	Once per month	Once per year	Once per 10 years
Multiple fatalities or >$10 million loss	1	2	3	4	5
Fatality or $1-10 million loss	2	3	4	5	6
Reportable injury or $100k-$1 million loss	3	4	5	6	7
Lost time injury or $10k-$100k loss	4	5	6	7	8
Minor injury or <$10k loss	5	6	7	8	9

Figure 10 — Risk ranking matrix example

The organization needs to have a feel for how one risk relates to another one by some comparative means, when it is making decisions on priorities.

'how likelihood will be defined; the timeframe(s) of the likelihood and/or consequence(s)'

The variable of timeframe needs to be agreed after some consideration. One way is to rank likelihood on a scale with increasing factors of approximately 10 (logarithmic). The highest likelihood would be once in a month, for instance, and the next level would be, for example, once in a year, followed by once in 10 years and then once in 100 years. Such approaches need to be fully understood by the decision makers when interpreting the significance. An incident that could occur once in 100 years could happen in the first year, as one of the authors experienced when advising on the likelihood of fire occurring on road-carrying vehicles in the Channel Tunnel (the fire occurred within the first year of operation, with a 1-in-100-year risk). So, great care needs to be taken in defining the criteria and in ensuring the understanding of the users and decision makers.

'how the level of risk is to be determined'

This is an equally important issue and covers a great number of approaches and options, which are discussed in detail under 'Risk analysis', below.

‘the views of stakeholders’

Relevant stakeholders should be canvassed on their views. How their views are weighted is something the organization should determine. A local government department seeking guidance from the public on whether to use landfill sites or incinerators could probably conclude the best option is not to collect waste at all (as it is quite likely there will be no consensus for any specific scheme). A process of consultation may well have to be developed in order to gather a balanced view of stakeholders, remembering that there are internal stakeholders as well as external ones.

‘the level at which risk becomes acceptable or tolerable; whether combinations of multiple risks should be taken into account and, if so, how and which combinations should be considered.’

What is acceptable or tolerable to one will be unacceptable for other organizations. It will very much depend on the sector, the stakeholders, the importance of reputation, the company’s risk appetite, etc. For example:

> A low cost food retailer may be prepared to accept imported meat products at an attractive price, without fully checking the full supply chain and determining the original source of the meat and the processes it undergoes. In contrast, an established supermarket chain may be far more cautious, recognizing that the quality of its products and its ethical stance are too important to put at risk and has processes in place to control every stage of its supply chain.

BS 31100, Clause 3.3.12.2 provides additional advice to help in making decisions on risk criteria and includes the following guidance:

> Risk criteria should state the following.
>
> *1) The consequences to be considered in judging the importance of risks* (such as lives lost, financial gain or loss, legal penalties or awards, reputation effects and environmental impact). This should include guidelines for deciding the time periods over which consequences are to be considered.

2) Measures of the level of risk, taking into account the likelihoods of different levels of the consequences. These should combine the different consequences and simplify distributions of effects into a level of risk. They should include guidelines for deciding which expectations to use in assessing the effects of risks.

3) The importance of different levels of risk, for use in decision-making. This may be demonstrated using thresholds that determine when action has to be taken to manage risk, and/or by defining scales of importance linked to level of risk.

In some cases an activity may be quite complex and decisions on multiple risks may need to be taken. The approach may need to vary depending on the nature and consequences of the risk involved. Some techniques are offered in IEC/ISO 31010 for those who work in complex and high-risk environments.

Risk analysis

Once the risks have been identified and the criteria determined, the risks need to be analysed individually. Those that are unlikely to occur and will have very little impact may be discounted in order that the organization focuses on those that are critical. The risks can then be evaluated (see 'Risk evaluation' below) and the treatment determined (see Chapter 8).

ISO 31000 gives particularly good advice in the area of risk analysis:

> The way in which consequences and likelihood are expressed and the way in which they are combined to determine a level of risk should reflect the type of risk, the information available and the purpose for which the risk assessment output is to be used. These should all be consistent with the risk criteria. It is also important to consider the interdependence of different risks and their sources.
>
> The confidence in determination of the level of risk and its sensitivity to preconditions and assumptions should be considered in the analysis, and communicated effectively to decision makers and, as appropriate, other stakeholders. Factors such as divergence of opinion among experts, uncertainty, availability, quality, quantity and ongoing relevance of information, or limitations on modelling should be stated and can be highlighted.
>
> Risk analysis can be undertaken with varying degrees of detail, depending on the risk, the purpose of the analysis, and the information, data and resources available. Analysis can be qualitative, semi-quantitative or quantitative, or a combination of these, depending on the circumstances.
>
> ISO 31000, Clause 5.4.3

A process should be developed, as stated above in 'Risk criteria', which allows the balancing of one risk against another, etc., particularly where different types and levels of risk occur, as part of the risk management decision-making process. In some cases, there is a need to analyse those risks that are interrelated. Examples of this are self-evident in the supply chain, where there are many inputs to the manufacture of a product. In some cases, it makes sense to analyse risks in groups, where they are interrelated or where they have many common features.

The aim is to try to understand the source of the risk and the causes – which may be positive or negative – and the likelihood and consequences of the risk occurring. Understanding the factors that relate to the foregoing may help in determining the strategy to be adopted for treatment. Where there are existing controls in place, it can be useful to analyse the risk with, and without, the control in place and to determine whether the control is robust enough.

As stated before, although each risk needs to be analysed, the depth of analysis should depend on what the likelihood and consequences are likely to be should the risk be exploited or the threat realized. Those that would have minimal impact with regard to consequences, or are extremely unlikely to happen, should be put on hold when first developing the system; the main focus should be on those that would have greatest impact. If care is not exercised at this stage, the risk register will be seen as being almost too large to manage and this can have a demotivating effect. As the system matures the lesser risks may be re-evaluated.

Risk analysis can be very complex and there are many methods in use for analysis and evaluation. The reader should look at IEC/ISO 31010 if they are seeking to identify the most appropriate methodology to apply. In some cases, possibly because of regulatory requirements, there is a need to use complex, scientific approaches, e.g. for chemical plants, petroleum and gas operations, and nuclear plants. Methods such as hazard and operability studies (HAZOPS) are widely used in some of these industries. Even in those cases, it is not uncommon to use a simplified approach in the first instance, as a method of filtering out which risks should be evaluated in greater depth.

Examples of risk matrices are given below in this section (see Figure 10 and Figure 11). The principles are very similar. They show, in simple terms, a method of ranking risks which will reflect the organization's risk appetite and risk criteria. The unacceptable zone has to be determined by the organization. There has to be recognition though, that, as Tony Blair, the former British Prime Minister, stated: 'A risk-averse business culture is no business culture at all' [Blair, A. (2005) 'Risk and the State' speech delivered at University College London, 26 May 2006]. In the case of injuring employees, no organization would wish to be responsible for the death of a worker, yet the HSE recognizes with its ALARP (as low as

reasonably practicable) model that it is impossible to function without risk, and the aim is to minimize risk of harm without incurring unreasonable cost. For example, it is possible to ensure that railway workers do not get killed on the track by passing trains if they work only when trains are not operating. This situation is very difficult to achieve except at scheduled weekends and nights, but, often, events occur during the daytime that require immediate attention and that necessitate track working and the inevitable risk to workers.

One example of a simple risk ranking tool can be seen above in Figure 10.

Gillie's T 4 2

Rob was well aware of the various sophisticated tools available for risk analysis but decided to use a simplified model at this stage of developing T 4 2. He used a 3x3 matrix as shown below (see Figure 11).

This less complex model allowed Gillie and Rob to make decisions on what risks were acceptable and to prioritize actions.

Figure 11 — Simplified risk ranking matrix

	Slightly harmful	Harmful	Extremely harmful
Highly unlikely	1	2	3
Unlikely	2	4	6
Likely	3	6	9

Risk evaluation

There is a need to agree how risk should be evaluated, and to ensure that the process prioritizes the risk in an order that makes good business sense to the organization.

ISO 31000 states:

> 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.
>
> Decisions should take account of the wider context of the risk and include consideration of the tolerance of the risks borne by parties other than the organization that benefits from the risk. Decisions should be made in accordance with legal, regulatory and other requirements.
>
> In some circumstances, the risk evaluation can lead to a decision to undertake further analysis. The risk evaluation can also lead to a decision not to treat the risk in any way other than maintaining existing controls. This decision will be influenced by the organization's risk attitude and the risk criteria that have been established.
>
> ISO 31000, Clause 5.4.4

Although there may be a matrix in use such as one of the ones given in 'Risk criteria and analysis', above, that provides answers on risks, based on the criteria the organization has defined, it is good practice to consider each risk carefully in the evaluation process. The decision makers may take a view, for instance, that a risk that is not very likely to happen would have far-reaching effects above what can be accepted, and prioritize this risk for treatment above others that may seem to be greater in numerical terms on the risk estimator (see Chapter 6, 'Risk appetite and risk profile'). The matrix should be used as an indicator and to highlight areas that need to be considered and addressed in some manner. The evaluation should be against the risk appetite defined by the organization (see Chapter 6, 'Risk appetite and risk profile'). Often, the process of risk evaluation is linked to mitigation (treatment), which is covered in Chapter 8.

It is important that the organization does not feel overwhelmed by the risks it has identified and evaluated. There may be some specific risks that can be addressed quickly that can bring swift benefits at little or no cost. There may be some that have legal implications that have to be addressed or the failure to comply could impact on the organization's reputation, as well as reduce customer confidence.

The organization should, therefore, focus on those risks it cannot tolerate without treatment. The output of this stage, as stated in 'Implementation of the framework', above, will determine to some extent the strategy, policy and framework.

For those who need more complex approaches there are many sources of information, including those referenced in BS 31100, which provides more information in Annex A on risk management tools, and IEC/ISO 31010, which provides some summary and references to many techniques.

Key learning points

In 'Implementation of the framework', the guidance outlines what is basically needed for implementing risk management and the framework, and provides advice on how the various recommendations might be achieved.

Risk identification is one of the foundations of risk management and 'Risk identification', above, recommends that organizations establish a process that includes:

- identifying the sources of risk;
- considering how they might impact; and
- considering what events might occur, and their causes and potential consequences.

'Risk criteria and analysis' deals with risk criteria and its importance, and provides guidance for:

- determining the likelihood of an event/action;
- the consequences of such an event;
- ranking risks so that an organization can evaluate them.

The organization has to develop its own approach to risk assessment that reflects the nature, size and complexity of the organization and its context.

The guidance on evaluation of the risk ('Risk evaluation') aims to help an organization to make informed decisions on which risks should be controlled (treated).

The aim should be to develop a process that allows the various risks to be compared in a similar manner, and then judgements can be made as to which risks are to be prioritized.

Links with management systems standards

Only OHSAS 18001, Clause 4.3.1 deals with risk assessment.

Chapter 8 - Risk treatment and implementation

This chapter deals with:

- risk treatment;
- selection of risk treatment options;
- implementing risk treatment/control plans.

Chapter 6 covered the framework and the process for risk management and Chapter 7 covered the identification of risks and prioritization for treatment. The next stage deals with how to treat the risk, in other words, the process of selecting and implementing measures to modify the risk. Depending on the strategy adopted, the policy and the risk appetite, the organization has to determine how it is going to deal with the risks it has identified.

Risk treatment

ISO 31000, Clause 5.5.1 states:

> Risk treatment involves a *cyclical* process of:
>
> - assessing a risk treatment;
> - deciding whether residual risk levels are tolerable;
> - if not tolerable, generating a new risk treatment; and
> - assessing the effectiveness of that treatment.

The standard is, in effect, advocating a cyclical plan–do–check–act (PDCA) process (Figure 12) for its implementation of treatment.

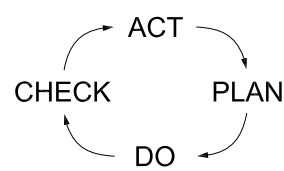


Figure 12 — The cyclical 'plan–do–check–act' (PDCA) process taken from the Deming Cycle

The whole risk assessment process is shown as a PDCA process in Figure 2 of ISO 31000 (see Figure 13), but the element entitled 'Risk treatment' in Figure 3 of the standard is a PDCA process in its own right for those processes that use the management systems standards approach, such as ISO 14001 (environment), OHSAS 18001 (occupational health and safety), ISO/IEC 27001 (information security) and ISO 22000 (food safety).

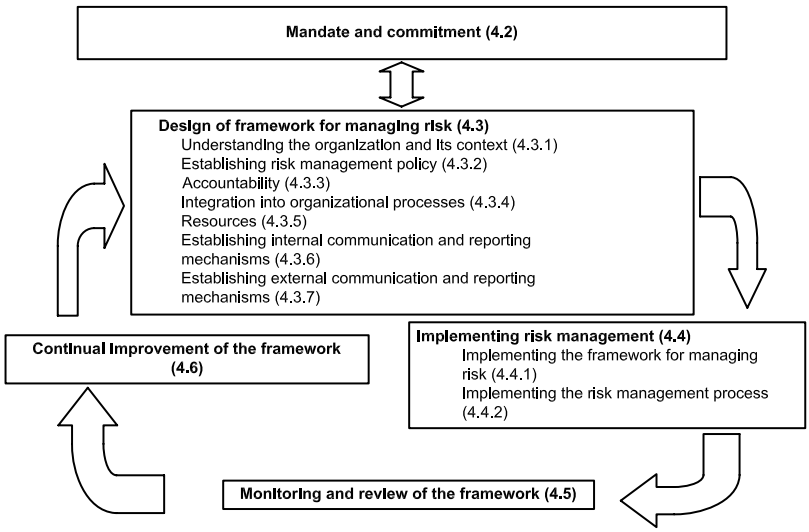


Figure 13 — Relationship between the components of the framework for managing risk

ISO 31000, Figure 2

In brief, the PDCA approach involves the following (this list is not exclusive but indicative and more detail can be found in Chapter 12):

- plan – involves determining the policy and planning for the identification of risks, their evaluation, etc.;
- do – involves the application of the treatment (controls) selected at the planning stage, and such issues as:
  - accountabilities;
  - responsibilities;
  - competence;
  - training;
  - communication;
  - documentation;
  - and the application of the treatment;

- check – involves:
  - monitoring;
  - measuring;
  - compliance;
  - correcting; and
  - audit;
- act – this considers the success of the treatments and the outputs of the 'check' process, and evaluates opportunities for improvement.

The earlier chapters have largely dealt with policy and the risk assessment aspect of the risk management process, which is the 'P' (planning element). Options for dealing with an individual risk or a number of risks, and determining what treatment should be selected, follow a similar PDCA pattern within this planning phase of risk selection. It should be recognized that there are rarely simple treatments that do not have knock-on consequences and generate new risks (see 'Implementing risk treatment/control plans', below, for more information on this). The identification, possible treatments, knock-on consequences and residual risk after treatment should be assessed as part of the selection programme of treatments (controls), before implementation (the 'do' stage) of the treatment is considered.

The 'do' stage will require that the roles, responsibilities and accountabilities are assigned, and appropriate resources are allocated, and that personnel have the necessary competencies. When determining risk treatment options, the aforementioned capabilities should be considered. For example, there is little purpose in identifying a very technical solution unless the resources and appropriately trained personnel are available or can be found. Such a solution may not be immediately practicable in a developing country if there are limited skills or resources available.

The next section looks at risk treatment, the options and the 'do' implementation stage in more detail.

Selection of risk treatment options

The selection of options should be a carefully considered process, and is not a one-off exercise. The structured approach used in BS 31100 (Clause 4.5.2) is useful in determining the way forward when considering the risk options (see 'Implementing risk treatment/control plans', below).
ISO 31000, Clause 5.5.1 is more elaborate and states:

> Risk treatment options are not necessarily mutually exclusive or appropriate in all circumstances. The options can include the following:

a) avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
b) taking or increasing the risk in order to pursue an opportunity;
c) removing the risk source;
d) changing the likelihood;
e) changing the consequences;
f) sharing the risk with another party or parties (including contracts and risk financing); and
g) retaining the risk by informed decision.

Ways of treating risk are identified above and the thinking is expanded below.

The options

'a) avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk'

One of the best ways of avoiding a risk is to stop the activity that gives rise to the unacceptable risk. If there is a new development proposed and the risk is not considered acceptable, then do not start. Although this makes obvious sense, in practice it may be a difficult treatment option to adopt. For example, an oil exploration company may decide not to start deep-sea exploration for oil if there has been a huge leak from a similar activity in another part of the world – and which led to international outrage and criticism of a competitor. It would fear that its exploration would come under very strict surveillance and possible actions by pressure groups. The problem is that such a decision stops the very activity that the company does as its daily business.

On the political front, if there is likely to be a change of government and the possibility of new policies that could significantly affect a new development or impose new controls in the area you were hoping to explore, then the answer may be not to start, or to discontinue, exploration in that area. An airline operator would not necessarily open a new route if it thought the government was going to impose a new, heavy tax on new air routes.

'b) taking or increasing the risk in order to pursue an opportunity'

Not all risks are negative and this should not be forgotten. If there is an opportunity, then it may be worthwhile taking, even if it increases the adverse risk, providing the benefits are judged to justify the course of action to be taken. There may be means of mitigation that can be taken to minimize some of the adverse risks.

Gillie's T 4 2

Rob and Gillie were prepared to try out expanding by opening a new outlet in Reptune. By opening the shop as a separate venture the risk to the existing operation is minimized, whereas expanding the current operation could lead to it becoming non-profitable. If the new venture failed they recognized they would lose money, but the existing business would still be there.

'c) removing the risk source'

There can be risks that relate to the source itself. If, however, the source is changed, the overall activity may not pose an unacceptable risk to the organization. For example, the organization could be at risk from using materials or goods from an unreliable source, or the source is not operating to the organization's ethical standards. In the case of the latter example, organizations have overcome such problems by sourcing from suppliers, countries and markets that are deemed to be ethical, sustainable, etc.

Gillie's T 4 2

Gillie proposed to reduce the risk at the new operation with respect to quality by using the same sources for supplies of tea, bread and cake. As some of the key personnel who already worked for her would be setting up and operating the new shop, the risk of using completely new personnel, who were not fully aware of the standards she expected, was not a risk she needed to take. Had the new operation been set up at a town some distance away, these risks would have required new sources of supplies and personnel, and would have posed a greater risk.

'd) changing the likelihood'

This is a very appealing option in many cases, particularly when dealing with supply chains. If the organization is dependent on one source of supply for its base materials and service, there is the risk that the organization could be put at risk by the failure of the supplier. The likelihood of failure can be reduced in such cases by:

- identifying and establishing alternative suppliers that provide, say, 30 per cent of the organization's needs, but have the capacity to meet the full demand should there be a need;

- setting up your own source;
- buying a share in, or buying the whole of, the organization that poses a risk;
- installing your own IT/financial management system rather than relying on another organization to manage the accounts.

Gillie's T 4 2

Gillie was very happy with the local bakery but was concerned about punctual deliveries as the van driver and vehicles were not so reliable. Gillie and Rob thought that investment in their own vehicle would help and it could be used for delivery services as they expanded. This enabled them to reduce the likelihood of delivery problems and negotiate a better financial deal with Jane Lovecake's bakery, and another supplier.

'e) changing the consequences'

There are two dimensions to risk (likelihood and consequences) and point d) above deals with changing the likelihood. An equally attractive option may be to remove, or change, the consequence should risk be realized. There is always the prospect of some failure occurring through service problems, equipment failure or personnel losses, and it is quite possible to change the consequences so that the effect is minimized or the consequence is such that the effect is not as critical.

A process involving chemicals could have significant environmental consequences should there be a leak, if it has close proximity to a watercourse. By bunding (secondary containment for escaping material) the process, any leak would be contained and could be more easily managed than a leak that has entered the drainage system, for instance.

The location of a tank containing material that could be a source of toxic fumes could be changed, so that any escaping fumes do not affect personnel, or to reduce or eliminate any unpleasant consequences.

Swimming pools often use chlorine to make the water safe for swimmers. By using chemicals in another form (that generate chlorine in solution) than tanks of neat chlorine, the consequences of serious harm from malfunction is significantly reduced.

Some business continuity provisions can also fall under this umbrella. A stand-alone backup system for IT systems, should power or network systems fail, is a good example of reducing the consequences of this event occurring.

'f) sharing the risk with another party or parties (including contracts and risk financing)'

The meaning of this statement is clear and there are a number of examples. For instance, if there is an opportunity that requires investment and you do not wish to put a large amount of your capital at risk, then seeking partners helps in reducing the consequences individually. Another solution may be to take out insurance against an adverse event that would put a project or an operation at risk.

Gillie's T 4 2

By partnering with Rob, Gillie reduced the risks she was exposed to when expanding the operation. The investment in the operation at Reptune was being jointly financed with Rob.

'g) retaining the risk by informed decision'

In some cases it may be decided that a risk should be accepted. This decision will obviously be made after due consideration as to the likelihood and consequence of the risk, and the cost of control. It may be, for instance, that the organization relies on goods being shipped on a regular basis by air through European airspace, and there is recognition that a volcano could (and did) become active in Iceland, which could prevent flights over parts of Europe. The organization might take the view that taking measures for all sorts of natural disasters is too costly and the insurance premiums prohibitive, thereby justifying acceptance of the risk, recognizing that the likelihood is extremely small.

Selecting the most appropriate option

Chapter 7 provides guidance on analysing and evaluating the identified risks. The first section in this chapter ('Risk treatment') provides guidance on risk treatment and 'The options' section, above, provides guidance on the options that should be considered, but, before we move on, we need to determine whether the option makes sense in terms of money and effort. If it requires a lot of effort and finance, it may be that the organization reviews its tolerance to the risk and revises its risk appetite. In some cases it may be appropriate to have intermediate solutions. For example, a transport operation identifies a new route that it believes will generate substantial revenue. The cost of buying a new fleet in order to achieve this goal may be significant, but the option of leasing buses for a year would still enable the opportunistic risk to be explored whilst minimizing cost. The long-term plan of investing in a fleet for the route can then be made on data that has a firmer foundation.

The opening paragraph of ISO 31000, Clause 5.5.2 states:

> Selecting the most appropriate risk treatment option involves balancing the costs and efforts of implementation against the benefits derived, with regard to legal, regulatory, and other requirements such as social responsibility and the protection of the natural environment. Decisions should also take into account risks which can warrant risk treatment that is not justifiable on economic grounds, e.g. severe (high negative consequence) but rare (low likelihood) risks.

The selection of which risk treatment option to choose depends on a number of factors including:

- likelihood of the threat being realized and the impact;
- consequence of the threat being realized and the impact;
- potential cost (not only financial) of not seeking an opportunity;
- financial costs and effort of implementation of any specific treatment;
- financial cost of non-implementation of treatment;
- financial benefits derived from compliance, social responsibility, protection of environment.

It is recommended, then, that a number of treatment options are considered and the option or combination of options that offers the best 'value' in terms of outcome, costs and effort be identified.

Gillie's T 4 2

One of the senior members of Gillie's T 4 2 tea shop and café was approached, because of her recognized competence, with a view to moving her to the new operation. She was happy at the initial prospect of this new opportunity and increased wages, but had serious misgivings:

- How do I get there?
- What happens if the business fails? I need to work and prefer my current security and convenience of living 500 metres from my workplace.

Gillie and Rob recognized that they needed to involve everyone in their decision-making process before they could assume they could reduce the risk of their investment in the new operation by using existing employees.

Gillie and Rob agreed that should the new venture fail the senior member of staff would be able to return to her old job, and made a financial allowance for the transport issue.

ISO 31000, Clause 5.5.2 recommends that 'A number of treatment options can be considered and applied either individually or in combination. The organization can normally benefit from the adoption of a combination of treatment options.'

For example, in the case of the transport operation, it has accepted the opportunistic risk [see 'The options', b), above], but has also shared the risk by leasing the additional bus fleet [see 'The options', f), above].

ISO 31000, Clause 5.5.2 goes on to state:

> When selecting risk treatment options, the organization should consider the values and perceptions of stakeholders and the most appropriate ways to communicate with them. Where risk treatment options can impact on risk elsewhere in the organization or with stakeholders, these should be involved in the decision. Though equally effective, some risk treatments can be more acceptable to some stakeholders than to others.

Establishing what the key stakeholders think is an important way of ensuring that the decisions an organization makes on risk treatment are accepted. It could be foolhardy to select a particular treatment without some consulting of relevant stakeholders – for instance, making a decision to invest in a new process or product that conflicts with the interests of some of the major investors would be ill-advised, as they may sell their shareholding and put the organization at risk. For competitive reasons, the details of what is planned and who is consulted depends on who needs to know, as there may be commercial sensitivities.

It is not only important to satisfy some of the external parties, but also essential that those in the organization who are expected to manage the risk in the proposed manner recognize the value of the approach and think it is workable.

In some cases it would be best to have direct discussions with parties, such as employees, encouraging ideas and feedback. In other cases, the communication may need to be far more formal and documented, to avoid ambiguity and to ensure that all parties have time to give due consideration to what is being proposed.

There may also be significant importance in scheduling the implementation plan. Some good opportunities have been lost, or not fully realized, by not sequencing the introduction of the implementation.

Relocating an organization into a new building can produce significant issues unless the various risks are managed in an order of priority to ensure a smooth transition.

Implementing risk treatment/control plans

The word 'control' is used in some disciplines, rather than 'treatment', but for consistency with ISO 31000 the word 'treatment' is used here.

As stated in 'Risk treatment', above, there is no comprehensive guidance given in either ISO 31000 or BS 31100, used as the main reference documents for this book, as to how to implement a risk management process, although the framework itself is covered in some detail. In some areas there are recognized processes for managing specific risks, such as in the fields of quality, environment, and occupational health and safety (a regulatory requirement in the EU). There may be specified 'management representatives' at top management level who are, in effect, risk owners of specific disciplines and the appropriate processes for risk management. Having stated this, risk management processes can have many common elements, making it possible to integrate them (see Chapter 12) and for one nominated person to be the risk owner.

There is clear guidance on what should be covered in the plan for controlling risks (ISO 31000, Clause 5.5.3):

> The information provided in treatment plans should include:
>
> - the reasons for selection of treatment options, including expected benefits to be gained;
> - those who are accountable for approving the plan and those responsible for implementing the plan;
> - proposed actions;
> - resource requirements including contingencies;
> - performance measures and constraints;
> - reporting and monitoring requirements; and
> - timing and schedule.

For the purposes of implementation, this needs some expansion. For the sake of simplicity, and bearing in mind that many organizations will have some processes in place for managing some areas of risk, it is thought better that treatment plan implementation is dealt with on a common management system theme. The management systems standards can be usefully used to provide the detail needed.

Those with specific management systems in place may draw on what has been established as a framework for management systems. The framework based upon the PDCA approach is particularly appropriate for risk management and is compatible with the approach being adopted for

future standards and those that are being revised. [*ISO/IEC Directives, Part 1: Consolidated ISO Supplement — Procedures specific to ISO*), 'Annex SL (normative) Proposals for management system standards', 'SL.8 Guidance on the development process and structure of an MSS' plus Appendices 2–4]. For smaller organizations it would be more efficient to combine at least some of the components of the process with the framework.

In essence, the risk-based management systems standards comprise key elements (clauses), illustrated as follows by ISO 31000:

1. general requirements – dealt with in Clause 4.1 of the standard and Chapters 4, 5 and 6 of this book;
2. policy – dealt with in Clause 4.2 of the standard and Chapter 6 ('Risk management policy') of this book;
3. planning – dealt with in Clause 4.3 of the standard and Chapters 7 and 8 ('Risk treatment' and 'Selection of risk treatment options') of this book;
4. implementation – dealt with in Clause 4.4 of the standard and Chapter 8 ('Implementing risk treatment/control plans') of this book;
5. checking (monitoring, correcting and auditing) – dealt with in Clause 4.5 of the standard and Chapters 9 and 10 of this book;
6. review – dealt with in Clause 4.6 of the standard and Chapter 9 of this book.

Typically in the implementation ('do') clauses the following areas are covered:

- roles, resources, accountabilities and responsibilities;
- competence and training;
- communication to external parties and internal parties (including consultation, etc.);
- documentation and document control;
- operational control.

More guidance on integrating your management systems is provided in Chapter 12.

ISO 31000 provides good guidance for effective implementation:

> The treatment plan should clearly identify the priority order in which individual risk treatments should be implemented.
>
> Risk treatment itself can introduce risks. A significant risk can be the failure or ineffectiveness of the risk treatment measures. Monitoring needs to be an integral part of the risk treatment plan to give assurance that the measures remain effective.

> Risk treatment can also introduce secondary risks that need to be assessed, treated, monitored and reviewed. These secondary risks should be incorporated into the same treatment plan as the original risk and not treated as a new risk. The link between the two risks should be identified and maintained.
>
> ISO 31000, Clause 5.5.2

Any new risk management activity creates new risk. Modification or implementation of new systems inevitably creates new issues that need to be analysed and evaluated.

Changes to a process to improve the quality of the surface coating of a car, which may be highly desirable from a sales point of view, can have other serious risks. In such cases the customer may be enthusiastic, but if the workers find the fumes and processes are unacceptable from a workplace point of view, or there is inadequate environmental control, there are then two new risks that will need to be carefully managed. It is self-evident that delivery of the treatment plan should extend to deal with additional risks generated, in order to ensure a smooth outcome and avoid disillusionment.

Part of the plan should be monitoring (see Chapters 9 and 10 for more information) to establish the effectiveness of the controls implemented, and for any secondary risks that have been underestimated.

Although not explicitly identified in the standards, it is recommended that the model given in points 1 to 6 in the list above, and expanded upon in Chapter 12, is used for implementation.

Roles, resources, accountabilities and responsibilities

In Chapter 4 the importance of leadership and commitment was stressed, together with a positive culture. Chapter 6, 'Accountability, roles, responsibility and authority' identified the needs in this area for the framework and provided a checklist for evaluating whether the personnel know their roles, etc.

Risk management is unlikely to be fully effective and efficient without these aspects being addressed, and it is self-evident that for this to be the status quo everyone needs to understand what is expected of them. Successful organizations will typically have:

- roles clearly defined;
- accountabilities assigned;
- responsibilities clearly stated and understood by all those who have management responsibility with respect to a particular risk(s);
- sufficient resources to enable and to ensure that management of risks can be undertaken efficiently and effectively.

Everyone has some part to play and this should not be forgotten. Even those employees with the most basic tasks can have a significant impact by doing the wrong thing. Involving them in understanding the importance of what they do and how they do it can help to promote the culture needed. No one willingly wants to put their job at risk and cause problems for their colleagues and so awareness training is crucial.

What is perhaps understated in Chapter 6, 'Accountability, roles, responsibility and authority', is that there has to be the resources in both personnel terms and time to undertake risk management roles, as well as the infrastructure to deliver what is required by the risk management framework. Some managers can be focused very much on output and lose sight of their risk management responsibilities.

BS 31100 provides some further guidance on what is needed, in Clause 3.3.7.1:

> The risk management framework should identify the resources of all kinds to be applied to:
>
> a) develop risk management over time; and
> b) manage instances of the risk management process.
>
> The risk management framework may identify the resources to be applied to operate instances of the risk management process already in place or planned.
>
> The framework may also provide estimated resource requirements for:
>
> 1) operating additional instances of the risk management process (e.g. for projects not yet planned); and/or
> 2) implementing and operating risk responses.

Competence, training and awareness

This is a standard clause in management systems standards such as ISO 9001 (quality) and many others. The requirements for competency with respect to the framework have already been spelt out in Chapter 6, 'Building capability and competence'. This extends to the process and is linked to training needs.

It is recognized that personnel should be competent for the task(s) that they are expected to carry out. Training in itself may not be sufficient. The aim should be to establish the competency needs for the job, which may be gained by education, on-the-job experience or training, or a combination of these facets. It is not uncommon nowadays for a skills matrix to be developed to serve this purpose. Any training is accompanied by some means of assessing its effectiveness and it may need to be reinforced from time to time. Railway track workers have to

undergo training and demonstrate their competence for a certificate that allows them to work on the railway track. They are retested to ensure the understanding is maintained.

Apart from the above, there is a need for some sort of appreciation training, in order to make sure personnel are generally aware of the organization's risks and their role in the general day-to-day operation of the organization. For instance, most employees will receive training on what to do in an emergency.

Communication

This is a key topic and has been already dealt with in Chapter 6, 'Communication' with respect to the framework.

Arrangements need to be in place for interacting with stakeholders, including internal stakeholders. As previously stated, involving personnel in understanding the risks they have to manage in their day-to-day duties helps in promoting the culture needed, particularly if they are party to the decision making on what controls/treatments are adopted.

Documentation and document control

ISO 31000 (Clause 5.5.3) recognizes the importance of documenting the plans, as proposed below:

> The purpose of risk treatment plans is to document how the chosen treatment options will be implemented. The information provided in treatment plans should include:
>
> - the reasons for selection of treatment options, including expected benefits to be gained;
> - those who are accountable for approving the plan and those responsible for implementing the plan;
> - proposed actions;
> - resource requirements including contingencies;
> - performance measures and constraints;
> - reporting and monitoring requirements; and
> - timing and schedule.
>
> Treatment plans should be integrated with the management processes of the organization and discussed with appropriate stakeholders.
>
> Decision makers and other stakeholders should be aware of the nature and extent of the residual risk after risk treatment. The residual risk should be documented and subjected to monitoring, review and, where appropriate, further treatment.

It is recognized that what should be in place from a documented point of view should be an integral part of the overall processes (management system) of the organization. In the absence of such embedding, there is the danger that risk management treatment is seen as a peripheral activity. Care should be taken to ensure that the documentation (either paper or electronic) is kept to the minimum, as overburdensome systems can be a barrier to the effective and efficient operation of the operational processes that have been prescribed. Many organizations find that process maps are a simple way of gaining understanding, and are useful for communication purposes. Bearing in mind the multicultural world that is present in many organizations, and the fact that the national language may not be the first language of some employees, it is important that documentation can be understood by all.

It is also important that there is a document control system that ensures documents are kept up to date and that those that are redundant are withdrawn. Those organizations with ISO 9001 and other management systems standards operating will already have well-developed systems that meet these requirements. Those organizations that do not have such systems would be well advised to look at what is recommended in ISO 9001, and select what is appropriate for their organization to use in order to manage their risks.

The documentation needs to extend, as stated in Chapter 6, 'Reporting' (and ISO 31000, Clause 5.5.3), to the monitoring and reporting activities as well as to implementation activities.

Operational control

Once the treatment (control) of the risk has been identified, the arrangements selected should be implemented (as per this chapter) and operated as specified (ISO 31000, Clause 5.5.1).

The treatment options will necessitate certain actions, or continuing control, in order to deliver the mitigation required or to achieve the opportunistic objective.

Auditing the operational control element is an important, proactive component of management systems requirements (see Chapter 10). It enables the organization to determine whether its existing risk responses are adequate and efficient. Clause 4.4.3 (in BS 31100) states: 'Residual risk reflects inherent risk and the effect of all relevant controls, but residual risk levels may be estimated directly from evidence of past risk occurrence'. Data gathering from assessing the effectiveness of controls (see Chapter 9) should help to determine weaknesses and lead to improved operational controls. If there is residual risk the need for vigilance to determine effectiveness is even more acute.

The controls that may be covered under this area will depend very much on the nature of the risk treatment and can include control of:

- suppliers;
- logistics;
- use of limited resources;
- customers;
- market forces;
- investment and investment strategy;
- finance;
- political impacts;
- environmental impacts;
- IT and infrastructure security;
- occupational health and safety;
- social responsibility;
- emergency/contingency preparedness;
- reputation.

All the above sections under 'Implementing risk treatment/control plans' have dealt with the aspects of the process that should be implemented to deliver the declared objective of the organization with respect to its management of risks. There is a need to monitor what is implemented and to determine what improvements are needed, if any, and to review the arrangements from time to time. These aspects of the framework and the process are covered in Chapters 9 and 10.

Key learning points

Risk treatment should be a cyclical process of assessing risk treatment options, deciding whether the residual risk levels are acceptable and, where necessary, determining a more appropriate treatment.

There should be an assessment of the effectiveness of the treatment selected.

When deciding how to control (treat) a risk there can be a number of options, which all need to be considered.

The decision process is very much one the organization itself has to make in the light of its tolerance to risk.

Risk treatment (control) plans should clearly identify the priority order in which risks are to be treated.

Care needs to be taken because risk treatment may create secondary risks that need to be assessed before treatment is implemented.

It is recommended that practices used in management systems standards that can help organizations with the implementation of effective processes for controlling risks are considered when implementing treatment or controls.

For the effective implementation of risk treatment everyone needs to know their role and responsibilities and be competent to undertake their duties.

Links with management systems standards

Risk treatment and implementation is dealt with to some extent in Clauses 4.3.1 and 4.4.6 of both ISO 14001 and OHSAS 18001.

Chapter 9 - Monitoring and review

This chapter covers:

1. introduction – an introduction to the area of monitoring and review;
2. monitoring and measurement – arrangements that should be put in place to establish that the measures that have been put in place are operating;
3. compliance – with any legal, customer or internal control requirements;
4. corrective action – measures taken to correct any deficiencies found in the current arrangements;
5. internal auditing (dealt with in detail in Chapter 10) – a formal internal process for evaluating the arrangements;
6. review – processes carried out by the organization to look at outputs from points 2 to 5 above and consider changes;
7. management review – formal management process to review the performance of points 2 to 6 and the need to develop strategies, changes, etc. in the future.

Points 2 to 7, above, are essential stages in the risk management process for evaluating the effectiveness of what is in place and for improving performance over time.

Introduction

The organization should develop and implement effective ways of monitoring the performance of the framework and the process it has selected for managing risks. There should also be a review process, by management, to identify the strengths and weaknesses of what is in place for delivering the strategy and policy. This process should also determine what action should be taken to deal with any risks that may arise from future activities and products/services, to remedy any deficiencies, and to identify opportunities for improvement. One way of determining how the framework and system is working is to carry out internal audits, a topic that is covered in the next chapter. Organizations with formal management systems will already have processes in place for undertaking internal audits and management reviews, and the approach used for reviews here follows that advocated for management reviews in management systems standards (see 'Management review' below).

Risk management is about being proactive. It is about determining risks and either taking advantage of opportunities or treating those that pose a threat. Monitoring should be focused on checking that everything is in place and is working as planned. The aim should be to prevent incidents rather than reacting to problems and trying to prevent a recurrence.

ISO 31000 and BS 31100 give some guidance on monitoring and review in several parts of the two standards. ISO 31000 proposes that the framework be monitored and reviewed, in Clause 4.5, and that there should be a similar exercise for the risk management process (Clause 5.6). The guidance is consistent in ISO 31000 but in practice there may be an overlap in the two activities/processes and, for those organizations that only need simple systems, the monitoring and review stages may be combined. The processes employed for any formal management system, such as ISO 9001 and ISO 14001, that an organization already has in place could be modified for monitoring and review of the risk management framework and risk management process. For simplicity, the guidance here and the recommendations found in Clauses 4.5 and 5.6 in ISO 31000 are dealt with as one subject. BS 31100 recognizes the overlap to some extent in Clause 3.5.1 by stating that the review process should be undertaken annually to determine whether 'the framework and processes are fit-for-purpose'.

The standards provide useful prompts but there is little detail of what should be included under these headings. There is far more informative guidance given in the various management systems standards and their appropriate guidance documents. This guidance can be applied in a generic fashion to risk management. The sections below outline what the organization can do to help improve the risk management framework and processes.

Combining the monitoring and review processes for the framework and the risk management processes has the benefit of avoiding duplication for those who have established management systems standards in place (with existing arrangements for monitoring and review), and builds upon the existing processes, instead of creating new ones. This approach should reduce the possibility of confusion, redundancy and possible conflict.

Monitoring and review activities should be planned as part of the risk management process and, ideally, the various aspects should be undertaken periodically as well as on an ad hoc basis. The responsibilities for the various activities should be clearly defined. Specifically, ISO 31000, Clause 5.6 states:

> The organization's monitoring and review processes should encompass all aspects of the risk management process for the purposes of:

- ensuring that controls are effective and efficient in both design and operation;
- obtaining further information to improve risk assessment;
- analyzing and learning lessons from events (including near misses), changes, trends, successes and failures;
- detecting changes in the external and internal context, including changes to risk criteria and the risk itself which can require revision of risk treatments and priorities; and
- identifying emerging risks.

Other management systems standards have a number of clauses to cover these areas, which have been developed over many years to help organizations monitor their specific management systems and improve them. Useful parallels can be drawn and the common requirements can be identified and made generic, where needed. On this basis, a framework for monitoring performance of the process is provided below:

- monitoring and measurement;
- compliance with regulations and requirements;
- corrective action for failures in the system or for identified areas of improvement;
- internal auditing (see Chapter 10);
- management review.

The topics are thus dealt with in this order, as given at the beginning of the chapter.

Monitoring and measurement

In order to be able to monitor effectively, the performance for risk management should be measured against indicators that have been set, possibly as SMART objectives, measuring progress against existing plans.

There are many activities that can fall into the monitoring category. It can be simple inspections, such as checking the security fence, ringing into the 'helpline' to check it is performing as required, checking customer feedback reports and looking at trends from incident reports, or it can be via the more formal internal audit route (see Chapter 10).

The monitoring activities should reflect the organization's needs, including:

- the nature of the risks and any uncertainty about them;
- any incidents that have occurred;
- any changes that have occurred in management/the organization/processes.

There are a number of activities that should be considered, which may be formal or informal, when monitoring. A manager walking around the location and observing day-to-day activities may not be a formal activity as such, but may provide information on the way risks are being managed. The aim should be to determine that any plan and objectives set have been delivered or are on course, and that processes are being followed:

- Has the *plan* been fully implemented?
- Have the *objectives and targets* been achieved?
- Are they still relevant?

In addition, to maintain effective control of specific risks:

- Are risk controls continuing to be *effective*?
- Are lessons *being learned and acted upon* from any risk management deficiencies?
- Is the information obtained used in reviewing and improving the practices and arrangements?

Proactive activities help to ensure things are working as planned, and modified or corrected where you can see potential areas for improvement. Reactive measures are measures that need to be acted on because a failure has been identified that needs to be corrected to prevent a recurrence.

Some of the monitoring activities are proactive, such as:

- management walkabouts/tours;
- inspections of equipment and records;
- staff attitude surveys;
- assessing effectiveness of training and briefings;
- calibration and checking of equipment for contingency situations;
- monitoring performance with respect to following processes/procedures/rules, etc. (e.g. what happens when the fire alarm goes off?);
- use of reactive measures of performance, such as monitoring near miss reports;
- monitoring occupational health and safety performance to ensure objectives and targets are being met;
- keeping, results of audits and reviews, etc., particularly those relating to compliance with legal and other requirements.

Equally there are reactive monitoring activities, such as:

- incident investigations;
- statistical trends in performance;
- breakdowns in systems/communications, etc.;
- complaints from stakeholders.

A checklist is provided after 'Corrective action', below, which gives some more indicators.

Compliance

A mistake that can be made is to establish a system/process for compliance reasons when first putting in the risk management process and failing to check that it is still effective. For example, a particular accountancy procedure may have been established to satisfy a certain regulation, but a change of personnel/structure may have led to changes in operational procedure that are no longer sufficient to meet the organization's needs. Alternatively, the requirements may have changed and the process should be re-evaluated to establish its continuing suitability. An environmental example would be where a system of filtration for discharges that may have met prescribed limits when installed five years ago needs to be checked to see whether it still operates as specified, five years later.

It is not only regulatory requirements that need to be checked for compliance. Your customer may insist that you vet your supply chain for socially responsible behaviour with respect to the labour used. The supplier may have been operating to the required standards when the contract was agreed, but the organization should ensure that the supplier is checked from time to time to ensure it is still meeting the requirements.

Corrective action

Inevitably, things will not always work as planned or perhaps some circumstances will not be fully foreseen. There will also be complete failures.

It is essential that the root cause of failure is determined through in-depth investigation, particularly when the outcome was, or could have been, of great significance. If the root cause is not identified, then it is possible that a similar or related failure will occur. From safety studies it is estimated that 80 to 90 per cent of accidents are due to management failure in some way, and that only a very small percentage is due to the individual. It is easy to blame the individual and often time-consuming to investigate the real cause, particularly when the cause is down to

management failure, which may be culturally difficult to accept. Any investigation should be conducted in a climate in which reporting is made without the fear of blame and retribution, and in such a way that facts are established without personnel being intimidated.

The action taken to remedy the defect or make improvement should be monitored to establish that the measures taken are working. The aim is to prevent recurrence. The checklist provided below can be used to establish what the organization has in place and what it might adopt. Score (1) if there are arrangements in place and they are implemented effectively, score (2) if they are in place but are not fully implemented and score (3) if they are not adopted.

Checklist – Performance monitoring

Examples of performance indicators

1	2	3	
☐	☐	☐	Progress in achieving the plans, targets and objectives that have been set
☐	☐	☐	Attitude surveys of perceptions about management commitment to risk management
☐	☐	☐	Appointment of a director with management responsibility for risk management
☐	☐	☐	Appointment, where necessary, of a risk management specialist
☐	☐	☐	Progress on reviewing and publishing a relevant risk management policy
☐	☐	☐	Progress on communicating the policy – responses and feedback
☐	☐	☐	Number of personnel trained in risk management
☐	☐	☐	Monitoring the effectiveness of training
☐	☐	☐	Staff understanding of risk control
☐	☐	☐	Staff attitudes to risks and risk controls
☐	☐	☐	Regular reviewing of the risk assessment programme
☐	☐	☐	Monitoring compliance with risk treatments/controls
☐	☐	☐	Monitoring compliance with statutory requirements
☐	☐	☐	Awareness of new standards and legislation that affect the business
☐	☐	☐	Monitoring the number and effectiveness of audits, tours, inspections/surveys
☐	☐	☐	Monitoring staff suggestions for risk management improvements
☐	☐	☐	Progress on completing and closing out audits
☐	☐	☐	Progress on implementing audit recommendations
☐	☐	☐	Monitoring the frequency and effectiveness of meetings on risk management
☐	☐	☐	Monitoring the frequency and effectiveness of staff briefings
☐	☐	☐	Progress on implementing actions as a result of complaints and suggestions

☐ ☐ ☐ Reported near misses
☐ ☐ ☐ Reported incidents
☐ ☐ ☐ Reportable dangerous occurrences
☐ ☐ ☐ Complaints made, e.g. by members of the public
☐ ☐ ☐ Criticisms made by regulatory agency staff
☐ ☐ ☐ Regulatory agency enforcement action
☐ ☐ ☐ Fatal accidents

Internal auditing

Internal auditing is a very powerful, proactive tool that should help in ensuring the system is effective and is continually improved. Chapter 10 deals with this in great detail.

Review

A review of the framework, processes or internal arrangements should naturally occur when there is a need, because of changes in the organization, systems or processes, or some failure. These may be formal, depending on their nature, and it is normally good practice to note such events.

They may not necessarily be scheduled, but occur as circumstances change. In contrast, there are benefits in having a more formal 'management review' process (see below), on the lines of those advocated in management systems standards, that defines what should be covered and the form of the outputs. The inputs listed in the next section may be tailored and used for such reviews.

Management review

Reviewing management systems is a fundamental requirement in any organization. Reviews ensure that the framework, processes and procedures are being applied effectively, as intended, and continue to meet the needs of the organization. Most importantly, they provide the mechanism to drive the continual improvement required of the risk management system. It is a live process within the business.

The management review is the opportunity for top management to carry out a strategic review of the system over a previously set period of time, and to decide whether any improvements need to be made. This should take place at least once a year. It should consider any feedback from interim reviews, audits, incidents, inspections and employee consultations,

as well as information from external sources (such as neighbours, customers, shareholders, regulators, trade associations and insurers), as well as any new opportunities or threats. Where improvements are to the benefit of the system and can sensibly be made, these need to be taken on board and any required actions communicated.

Many of the management systems standards require a management review process that identifies specific inputs to the management review and what is expected in the form of outputs. These inputs and outputs are consistent with the general guidance given above and can provide a useful template for any organization, reinforcing the vital role of these reviews in driving the continual improvement cycle required for an effective management system. BS 31100 gives recommendations that are helpful and consistent with general management systems guidance. The review process should be undertaken, as a minimum, on an annual basis, but if significant changes are occurring then the review should be held more frequently. Any changes to the context, or to other factors affecting the suitability or cost of risk management, should be identified and addressed. It is recommended that the input to management reviews includes information on:

- whether the framework and processes are fit for purpose, and are aligned to the objectives and priorities of the organization;
- the extent to which business risk objectives have been met;
- whether relevant stakeholders are receiving adequate information and reports to enable them to discharge their roles and responsibilities;
- whether personnel across the organization have the necessary skills, knowledge and competence, in line with the risk role/risk element of a role they are required to perform;
- whether the resources are adequate;
- whether lessons have been learned from actual losses, near misses and opportunities that were not acted upon soon enough;
- the results of audits;
- follow-up actions from previous management reviews;
- whether the current risk management maturity and capability achieve the objectives set out in the organization's risk management strategy;
- changes that could affect the risk management system;
- recommendations for improvement;
- any change in circumstances, including developments in legal and other requirements related to the business performance (this could be both internal and external factors, such as takeovers or mergers, reorganizations, new technology, new projects and new competition).

The output from the management review should include any decisions and actions related to:

- the framework and process(es) and their constituent elements;
- performance;
- resources;
- improvements to the risk management arrangements.

To be truly effective, a management review of the organization's processes should be structured around areas of delivery and involve all parts of the organization. This can run from line managers/supervisors periodically reviewing operational management within a department or over a process, to the senior management team considering the business performance against the organization's strategy, policy, objectives, targets and risk management requirements.

The management review differs from the audit in that it is more strategic in its focus. For example, the audit may conclude that everything is in place to meet the policy and objectives, but the management review may show, for example, that internal or external considerations justify a change.

As well as seeking to remedy deficiencies, the management review offers the opportunity for a more proactive approach: to consider where the organization wishes to be in managing its risks and how it can maximize the resulting benefits to improve business performance.

The organization should define the frequency and scope of periodic and management reviews of the management system, according to its needs. The following is a checklist of the key issues involved in reviewing the risk management system. A tick box is provided for you to identify those issues you are already addressing (1) and those you need to consider (2).

Checklist — Management review

1	2	
☐	☐	Top management periodically reviews the risk management framework and process.
☐	☐	Business units within the organization undertake reviews within their sphere of responsibility.
☐	☐	Management considers the outputs of any review to identify opportunities for improvement.
☐	☐	The review considers the adequacy, effectiveness and suitability of the framework and process(es).
☐	☐	The review considers the performance against annual and local objectives and targets.
☐	☐	The review considers the overall performance of the framework.
☐	☐	The review considers the performance of the individual elements of the framework and process.
☐	☐	The review considers the findings of audits.
☐	☐	The review considers internal factors affecting risk management.
☐	☐	The review considers communications from relevant external parties to the organization.
☐	☐	The review is forward-looking, adopting a proactive approach towards improving the risk management process.
☐	☐	The review considers changing circumstances and recommendations for improvement.

Key learning points

Monitoring and review are essential elements of risk management. The many facets within monitoring and review all contribute to understanding how well the risk management framework and processes are working.

Organizations with formal management systems in place should find their existing processes for monitoring and review useful for improving risk management within the organization.

Links with management systems standards

Monitoring and review is dealt with in all management systems standards and, in particular, in Clauses 5.6 and 8 of ISO 9001, and Clauses 4.5.1, 4.5.2 and 4.6 of both ISO 14001 and OHSAS 18001.

Chapter 10 - Internal auditing

Introduction

ISO 31000 does not mention the word 'audit' in the text and talks generally about monitoring and review. In contrast, BS 31100, along with management systems standards in general, recognizes that auditing plays an important role in monitoring the effectiveness of management arrangements. BS 31100 devotes a section (Clause 3.3.4.4) to the role of the audit function, should there be one, and the role audit can play. Its use is referenced many times in AIRMIC/Alarm/IRM's guidance on risk management, *A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000* (2010), where it is seen as an important management tool. In larger organizations, it is not unusual to find an audit function that reports to the board.

Where an organization has committed itself to a formal risk management system, it is only sensible that it should periodically reassure itself that the risk management system is effective. In order to do this, arrangements should be put in place for a formal internal audit programme. Auditing is a powerful, proactive tool for determining whether the organization is actually carrying out in practice what it has stated it will do, and internal audits should be viewed positively – a way of ensuring that all is working well and determining where improvements can be made. They should not be viewed as a means of finding fault and apportioning blame.

BS 31100, Clause 3.3.4.4 states:

> If the organization has an internal audit function, this may provide independent assurance on:
>
> a) the design, operation and effectiveness of the risk management framework and instances of the process;
> b) management of key risks, including the effectiveness of the controls;
> c) reporting of risk and control status; and
> d) the reliability of assurances provided by management relating to risk management.

In organizations where the risk and internal audit functions are independent, it also shows what information may be usefully shared between the two functions (see below).

A system for routinely monitoring risk management performance is insufficient in itself to ensure that the process implemented for managing risk is effective. There needs to be a procedure for auditing the system to make sure that it is being followed throughout the organization. Only in this way will it be possible to judge whether the system is adequate to meet the requirements expressed in the stated policy of the organization. If it is found that the policy and objectives are not being met, then the organization cannot be sure whether it is the system or its implementation that is responsible for the shortfall, unless an audit confirms that the system is, in fact, being followed. The output can be used to improve the process or to provide feedback for improving the framework.

BS 31100 does not give detailed guidance on auditing, but comprehensive guidance can be found in ISO 19011:2011. This standard is now being issued as a generic audit document for those who wish to audit any management system and the approach can equally be used for risk management.

An organization may have a large department that fulfils the internal audit function, or it may be fulfilled simply by one individual. Irrespective of size, the internal audit 'function' may be responsible for:

- the assessment of the risk management processes, including design, and how well they are working;
- the assessment of key risks and the effectiveness of controls;
- assessment of risk, and reporting of risk and status of controls.

Whilst the audit function will operate independently, it should share information with other parts of the organization, particularly if there is a function devoted to risk management.

> The information shared may include:
>
> 1. each function's annual activity plans;
> 2. key risks;
> 3. methods of managing risks effectively;
> 4. key control issues;
> 5. output from risk management process activity and audits; and
> 6. reporting and management information.
>
> BS 31100, Clause 3.3.4.4

An audit programme should be planned, and the frequency and depth of audits will depend on the organization, its complexity and the nature of the risks, and any assurance it may need to make to its stakeholders.

In addition, there are an important number of matters that need to be addressed when planning such audits, such as the depth and nature of

the audit, the scope and the competencies needed. For example, in Clause 9.2 of ISO 22301 (business continuity management) it is required that:

> The organization shall
>
> - plan, establish, implement and maintain (an) audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting. The audit programme shall take into consideration the importance of the processes concerned and the results of previous audits,
> - define the audit criteria and scope for each audit,
> - select auditors and conduct audits to ensure objectivity and the impartiality of the audit process,
> - ensure that the results of the audits are reported to relevant management, and
> - retain documented information as evidence of the implementation of the audit programme and the audit results.

To achieve these requirement, in practice, requires that the operation of the system is checked in all areas and applications by auditors who are not directly involved in the work area and/or processes.

The term 'auditing' is frequently misinterpreted by those who are going to be audited, largely because of the association with financial auditing, which is quite different. It is important that the purpose of auditing is made clear to all who are going to be involved, as otherwise there may be discomfort when the auditors ask questions about how a system is being operated. The object is to help, not to criticize. It is about identifying improvements and recognizing what is being achieved, as well as identifying where the system is not working properly and establishing the reasons behind it. Is the system itself at fault, making it unworkable in some way? Has the manager or operative not understood what is being asked, possibly through lack of training? The auditor is rather like a coach who is trying to identify strengths and weaknesses, to find out what is wrong in order to put it right.

Although the primary purpose of auditing is to check that the system is being followed and is effective, it is also a means of achieving continual improvement of the system, another essential requirement.

Where the internal audit is undertaken by employees of the organization (which can have many advantages), they need to be selected with care and given the training they need. This training should consist of systems auditing in general, and ISO 31000 and the risk management framework and process in particular. It may be that the organization already has experienced management systems auditors – e.g. experienced quality systems auditors – who may be suited for the task after training on the specialist risk management aspects. It is important that those performing

the audit do not themselves have direct responsibility for the function being audited; otherwise the integrity of the audit may be compromised.

All parts of the system need to be audited regularly – customarily, during the course of a year – but not all parts of the system need to be audited at the same time or at the same frequency. Those areas where the risk is greatest should be audited more frequently than those where the risk is lower, and the audit programme should recognize this requirement. Organizations in which the risks are inherently high should audit their systems more frequently. Where there have been changes to the system, it is a matter of good practice to arrange an audit soon after the changes have been fully implemented, in order to identify and resolve any problems that may have arisen as a result of the changes.

In addition to maintaining auditors' independence and integrity, it is important that auditors feel they have the full support of senior management and can make the findings known to the local manager (if that has been agreed at the commencement of the audit) without fear of intimidation. The outcome should be confidential to the manager but given freely as a guide to where the system has weaknesses or could be improved. In the absence of such openness, auditors may feel their job is vulnerable if they deliver bad news. Audits are for the benefit of the organization, to help it improve, and should not be seen as the justification for finding fault.

Ideally, the results of audits should be communicated to all relevant personnel on completion of the audit, so that any necessary corrective action can be taken and improvements made. These results will be an important input to the management review. If the auditor finds a serious problem in the course of the audit, this should immediately be raised with the appropriate manager without waiting for the formal report.

The following is a checklist of the key issues involved in auditing the risk management system. A tick box is provided for identifying those issues that are already being addressed (1) and those that need to be considered (2).

Checklist — Auditing in the organization

1	2	
☐	☐	Regular, periodic audits of the risk management system are taking place.
☐	☐	Staff conducting audits are competent to perform this task.
☐	☐	Staff conducting audits are independent from the activity being audited.
☐	☐	T Audits verify that the organization is fulfilling its risk management obligations.
☐	☐	Audits identify strengths and weaknesses in the risk management system.
☐	☐	Audits verify that the organization is achieving its risk management performance objectives.
☐	☐	Audit results are communicated to all relevant personnel.
☐	☐	Audit results are the basis for corrective action.
☐	☐	Audit results are monitored to ensure risk management improvement, i.e. there are no repetitions of failures revealed by previous reports.
☐	☐	Audit results are seen as a benefit to managers rather than a threat.

Auditing methodology

Auditing is an essential element of the risk management system. All personnel should appreciate its importance and all managers must be fully committed to it, co-operating in its execution, and acting reasonably and promptly on any findings and recommendations. Staff must recognize that it is not a threat, but a means of seeing how the system is working and where it needs to be improved. Everyone must co-operate fully and be open and honest with the auditor. In summary, the audit must be seen as an integral part of the process of maintaining and improving the risk management system

Planning an audit

The audit process should be a structured activity and requires careful planning. To ensure that the audit process is effective, top management should:

- demonstrate its commitment to it;
- authorize the internal audit programme;
- ensure adequate resources are available;
- encourage all personnel to be positive towards the internal audit activity;
- accept the audit outputs in a positive manner (both positive and negative findings);

- review the outputs at the management review.

Objectives

There are some general principles and methodology described in ISO 19011 that are applicable, such as:

- objectives should be established for an audit programme, to direct the planning and conduct of audits;
- these objectives can be based on:
  - management priorities;
  - risks to the organization;
  - statutory, regulatory and contractual requirements;
  - commercial intentions;
  - stakeholder requirements;
  - structural and operational changes;
  - risk management failures;
  - framework and management system requirements.

Extent of audit

In order to plan an audit, the following issues should be considered:

- Will the audit look at the whole or just part of the organization, or focus on a specific activity, location or issue?
- Will the audit look solely at risk management or will it involve technical areas?
- Is the audit intended to:
  - establish the effectiveness or otherwise of the risk management system (it could sometimes be a validation audit for management system audits); or
  - verify whether the organization is complying with its own standards and procedures (a compliance audit against rules and procedures, etc. that have been issued); or
  - both?
- Will the audit only assess elements of the management system?
- Will the audit, as proposed, require any special skills of the auditors?
- Should the audit be carried out by internal or external auditors, or a combination, to ensure objectiveness?
- When is the audit to be carried out and over what timescale?
- How frequently will the audits be conducted?
- What are the concerns of interested parties (regulators and customers, for instance)?
- What were the outcomes of previous audits?
- What are the areas where there have been significant changes in the organization or its operation that may impact on the risk management arrangements?
- Have the competence needs of audit teams been identified?

Gathering the information from the above exercise should ensure that the audit is focused and allows careful preparation of the audit programme.

Establishing an audit programme

When determining the audit programme for the organization, the plan should take into consideration the frequency, criteria and depth of the audit. There may be a need to have a particular focus on those areas that are perceived to be of a higher risk for, say, business continuity or insurance reasons, but it should be remembered that the audit is simply a snapshot of arrangements and practices on a particular day.

Once the objectives and the extent of the audit programme have been established, those responsible for managing the audit programme should establish the procedures, secure the resources and implement the audit programme. Following that, it should be ensured that it is maintained, monitored and reviewed and, where necessary, improvements are made.

Resources

Audits cost time and money and, therefore, a suitable budget and resources should be allocated for the task. There is a need for:

- competent auditors;
- an adequate timeframe for them to undertake the audit;
- budgeting of costs associated with management and workforce time (of those being audited);
- budgeting of costs incurred for travelling, materials, etc.
- budgeting of costs incurred in training auditors;
- budgeting of costs associated with securing external resources to assist.

Audit programme procedures

A procedure(s) should be established for the programme, taking into account such items as:

- schedule;
- auditor competence;
- audit team availability;
- conducting the audit and following up, where necessary;
- records and reporting the output; and
- monitoring the performance of the programme (note: this is to evaluate the effectiveness of the audit programme itself).

The competency of the auditor is an important issue in its own right and guidance on this is given below. In some cases there may be a need to ensure that auditors are acceptable to the auditee and/or manager being audited, as there may be particular sensitivities that need to be observed.

Audit programme implementation

The implementation of an internal audit programme should address the following:

- communication of the audit programme to relevant parties;
- establishing and maintaining a process for the selection of auditors and audit teams;
- providing the resources necessary for the audit programme;
- planning, co-ordinating and scheduling audits;
- ensuring that audit procedures are established, implemented and maintained;
- control of records of audit activities;
- the following up and reporting of audit results.

The audit programme should be based on the results of the risk assessments and needs identified in the audit programme implementation list above and the results of previous audits. The input of this information will help the organization in determining what the frequency of audits of particular activities, areas or functions should be, and what parts of the risk management system should be given attention.

The internal audits should cover all areas and activities within the scope of the risk management system, and should assess conformity to the policy and objectives set by the organization.

The frequency and coverage of internal audits should be related to:

- the risk of failure associated with the various elements of the system;
- available data on performance;
- the output from management reviews; and
- the extent to which the risk management system or the organization itself is subject to change.

Audit records

Arrangements need to be established for recording the various elements of the audit programme, to demonstrate conformance with audit requirements. These arrangements need to record the plans, schedules and details of the audit team, and the outputs of individual audits and nonconformity reports and the actions taken.

Audit activities

Internal audit activities

Normally, risk management audits should be conducted according to the determined (agreed) audit programme, but additional audits might be necessary for a number of reasons, e.g. where organizational changes,

new operations, new processes and/or risks are introduced. If there are incidents in a particular area, there might be an immediate need to audit the affected activities in order to ascertain why the system failed or needs improvement.

One way of planning the audit process is proposed in Figure 14.

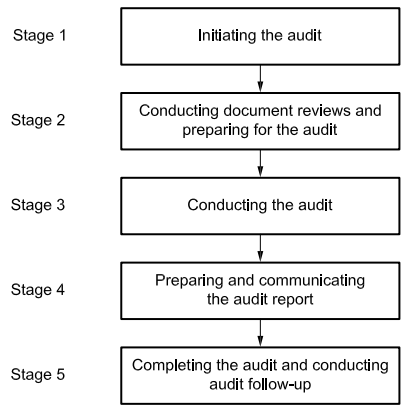


Figure 14 — One way of planning the audit process

BS 18004, Figure L.1 Audit process

Where there is a team approach for the audit programme, a team leader (commonly called the lead auditor) should be appointed. This person should be designated well in advance in order to prepare for the audit.

The lead auditor needs to determine the following:

- What essential information is needed for the audit in terms of measurement criteria (specification, customer requirements, etc.) and internal documentation?
- Has the necessary authority been sought and arrangements with local managers made?
- What elements of the management system are to be assessed, if the scope is to be limited?
- What competency skills are needed for the audit team?
- Is there a need for briefing the employees?
- Do any special precautions need to be taken?
- What representative sample of activities are to be included?
- What auditing aids, e.g. checklists, aides-mémoire and inspection procedures, are needed?

Stage 1 Initiating an audit

Planned risk management system audits should be carried out by personnel from within the organization and/or by external personnel selected by the organization, to establish whether the arrangements for risk management have been properly implemented and maintained. Competence and impartiality are important considerations in the selection of auditors.

The following activities are typically done to initiate an audit:

- selecting the appropriate auditors and audit team for the audit, taking into account the need for objectivity and impartiality;
- defining the objectives, scope and criteria for the audit;
- determining the audit methodology; and
- confirming audit arrangements with the auditee and other individuals who will take part in the audit.

The determination of any applicable workplace risk management rules is an important part of this process (e.g. are there security, information security or safety issues that need to be taken into account?).

In some cases, auditors might need additional training and/or be required to conform to additional requirements (e.g. the wearing of specialized personal protective equipment).

Stage 2 Conducting document reviews and preparing for an audit

Auditing involves obtaining evidence from interviews, documents and worksite visits, and checking for consistency. The auditors should review appropriate risk management documents well in advance, including the results of prior audits. This information should be used for planning the on-site audit.

The documentation that may be reviewed includes that with information on:

- roles, responsibilities and authorities (e.g. an organizational chart);
- the risk management framework;
- the risk management policy (e.g. the risk management policy statement);
- the risk management strategy;
- the risk management objectives and programme(s);
- the risk management system audit procedures;
- the risk management procedures and work instructions;
- risk assessment and risk control results;
- any stakeholder, applicable legal and other requirements; and
- any incident, nonconformity and corrective action (e.g. reports on these).

The amount of documentation to be reviewed and the detail provided in the plans for the audit should reflect the scope and complexity of the audit. The plans for the audit should cover the following:

- audit objectives;
- audit criteria;
- audit methodology;
- audit scope and/or location;
- audit schedule; and
- roles and responsibilities of the various audit parties.

The audit planning information may be contained in more than one document. The focus should be on providing adequate information to implement the audit.

It is quite common for auditors to devise a set of questions for checking compliance with a standard such as ISO 31000, even though these standards are guidance documents and have no requirements. However, this approach can be less effective, particularly when the same question set is used on every audit. It is often found more effective if an open approach is used. Such an approach starts with very general, open questions and then allows auditors to steer the subsequent questions towards those areas that they are particularly focusing upon.

Questions should preferably encourage those being questioned to explain in their own words what their understanding is, what they are doing and any concerns they have about the current arrangements.

Stage 3 Conducting an audit

The lead auditor should explain to the manager of the department or function being audited exactly what the purpose of the audit is, and confirm the plan and any local arrangements that apply. The auditee should be advised that the auditors' findings will be reported back to them in confidence.

For a team approach, individual auditors should be assigned tasks and the lead auditor should co-ordinate the overall activities, review the findings and report back at the closing meeting.

The following activities are typically part of the audit:

- communication during the audit;
- collecting and verifying information;
- generating audit findings and conclusions.

Depending on the scope and complexity of the audit, it may be necessary to make formal arrangements for communication during the audit. The audit team may need to communicate the status of the audit activities, any concerns raised during the audit and any preliminary conclusions.

Communication of the plans for the audit may be achieved through the use of an opening meeting. Audit findings and conclusions should be reported during a closing meeting.

During the audit, information relevant to the audit objectives, scope and criteria should be collected as appropriate. The methods for collecting this information will depend on the nature of the risk management audit being undertaken.

The audit should ensure that a representative sample of the important activities is audited and that relevant personnel are interviewed. Apart from talking to senior managers and supervisors, interviews may need to encompass individual workers or, in some cases, contractors.

Documentation, records and results should be examined to assure the auditor that what they are being told is consistent with the information provided. Wherever possible, checks should be built into the risk management audit procedures to avoid misinterpretation or misapplication of collected data, information or other records.

Audit evidence should be evaluated against the audit criteria to generate the audit findings and conclusions. Audit evidence should be verifiable. The audit will aim to determine whether:

- a comprehensive system exists;
- employees and those working on behalf of the organization are fully aware of the requirements and their duties with respect to risk management;
- the documentation system reflects the practices;
- the procedures, work instructions, etc., are being worked to and satisfy those they are supposed to protect;
- there areas that are deficient and are nonconformities;
- there are areas where improvements can be made.

Stage 4 Preparing and communicating the audit report

The audit findings from all the audit activities should be reviewed collectively by the audit team. Where there is objective evidence that there is a deficiency in the risk management system, the audit finding should identify the area of ISO 31000 with which the organization does not comply. It should provide the objective evidence of this deficiency. The audit team should not involve itself in resolving the deficiency, but should ask those audited for their proposals.

The results of the risk management audits should be recorded and reported to management, in a timely manner. The final risk management audit report content should be clear, precise and complete, and be dated and signed by the (lead) auditor.

The following elements should be covered in the report:

- the audit objectives and scope;
- information about the plans of the audit (identification of the members of the audit team and the audited representatives, dates of audit and identification of the areas subject to audit);
- the identification of reference documents used to conduct the audit (e.g. BS 31100, risk management procedures);
- details of identified nonconformities;
- information relating to the ability of the risk management arrangements to achieve the stated risk management policy and objectives;
- a list of recipients who are to receive the audit report.

The results of risk management audits should be communicated to all relevant parties as soon as possible, to allow corrective actions to be taken.

Stage 5 Completing the audit and conducting the audit follow-up

A review of the results should be carried out and effective corrective action taken, where necessary.

Follow-up monitoring of prior audit findings should be established to ensure that identified nonconformities are addressed.

Top management should consider risk management audit findings and recommendations, and take appropriate action, as necessary, within an appropriate timescale.

Where deficiencies are identified, the audit team should agree with those audited the corrective action needed and timescale for implementation, and then reassess the effectiveness of the actions taken. Depending on the gravity of the nonconformity, the reassessment should be undertaken within a timeframe that is consistent with the risk.

Selection of auditors

One or more persons may undertake risk management audits. A team approach, involving managers, workers and employees, can widen involvement and improve co-operation, and allow a wider range of specialist skills to be utilized.

The people chosen as auditors should be competent on the basis of training, experience and education.

In order to maintain independence, objectivity and impartiality, auditors should not audit their own work; wherever possible, they should be independent of the part of the organization or the activity that is to be audited. The nature and extent of the audit will determine whether it is

to be undertaken by employees from another part of the organization or by external auditors. Other factors to be taken into consideration include:

- the availability of auditors for the length of time necessary to undertake the audit;
- the availability of auditors with the necessary skills;
- the level of audit experience required;
- the requirement for specialist knowledge or technical expertise;
- any requirement for training;
- the danger of an internal auditor being overfamiliar, or satisfied, with the organization's arrangements, compared with the benefits of the pair of fresh eyes and a possibly more questioning approach of an external auditor; and
- the danger of unfamiliarity or lack of understanding, particularly where complex technical issues or processes are involved.

Where an audit team is used, as opposed to an individual auditor, the composition of the team depends on the nature and scope of the audit. It may be possible to address any concerns about competence through the selection of a multi-skilled team, but consideration should be given to whether:

a) in-house auditors, external auditors or a combination of both should be used;
b) specialist knowledge, experience, skills or technical expertise are required; and
c) agreements have been reached about the involvement of employee representatives.

Auditors need to have the experience and knowledge of the relevant standards and systems against which they are auditing them to enable them to evaluate performance and identify deficiencies. They should be familiar with the risk management hazards and risks of the areas they are auditing, including any applicable legal or other requirements.

Key learning points

Audit is a key process for establishing that the risk management system is working and to identify opportunities for improvements. Key points are:

- the important role that auditing has as a means of assuring management that risk management is working as it would wish;
- how to plan an audit and establish an audit programme so that opportunities for improvement are identified and acted upon;
- how the selection of auditors is very important. They need to have the necessary skills, be independent of the areas they audit, and feel empowered to probe and question management about its duties. The audit team needs to be balanced appropriately.

Links with management systems standards

Internal auditing is dealt with in Clause 8.2.2 of ISO 9001 and Clause 4.5.5 of both ISO 14001 and OHSAS 18001.

Chapter 11 - Recording and reporting

This chapter covers two topics:

1. recording;
2. internal and external reporting.

Recording

All management systems standards have requirements about records that provide sound direction on what should be done. Standards such as ISO/IEC 27001 and ISO 9001 provide the minimum requirements that should be met for an effective record system. For example:

> The organization shall establish a documented procedure to define the controls needed for the identification, storage, protection, retrieval, retention and disposition of records.
>
> Records shall remain legible, readily identifiable and retrievable.
>
> ISO 9001:2008, Clause 4.2.4

There needs to be a formalized approach to recording information, and to its storage and retrieval.

> A not uncommon problem is where an organization has slavishly stored its records on disks that are no longer compatible with its current hardware or software and are therefore not easily retrievable.

Organizations need to learn and develop from the learning process. They also need to show that they have systems in place for managing risks, and record what treatment has been applied and its effectiveness, and any actions taken to improve performance. Not only does this make good business sense, it can also be important should litigation be taken against the organization.

There should be a knowledge management system (see below) and easy access to the records as well. This is because the treatment/control in place may seem to be too restrictive or unnecessary and, unless the background is known, some inappropriate decisions might be made. In a

simple case, it may be thought that production could be increased by raising the temperature of a curing process by a few degrees (thereby shortening the production time); however, such a change may have other consequences that are not desirable, such as a reduction in the life of the product (this may well be known from development trials carried out years ago). Access to information on variations in production processes and development need to be recorded and made available to ensure the validity of the database of knowledge that is in the organization.

A knowledge management system is a system for retaining and using knowledge. It is used by an organization for identifying, creating, distributing and enabling the adoption of *insights* and *experiences*. Such insights and experiences comprise *knowledge*, either embodied in individuals or embedded in organizations as *processes* or practices.

One key post in a railway maintenance activity was removed because there was only one day's work per week at the particular outpost. The task took about one hour per day. The time and motion assessment of the activity resulted in the task being assigned to just one working day per week at the outpost.

What the reviewer had missed is that the activity was critical and had to be carried out daily because, in its absence, vehicles regularly caught fire through inadequate axle box lubrication. Only when there was a series of fires on vehicles was the situation identified and rectified.

ISO 31000, Clause 5.7 states:

> Risk management activities should be traceable. In the risk management process, records provide the foundation for improvement in methods and tools, as well as in the overall process.
>
> Decisions concerning the creation of records should take into account:
>
> - the organization's needs for continuous learning;
> - benefits of re-using information for management purposes;
> - costs and efforts involved in creating and maintaining records;
> - legal, regulatory and operational needs for records;

- method of access, ease of retrievability and storage media;
- retention period; and
- sensitivity of information.

The points are all well made and are consistent with management systems requirements that will be in place for those organizations with certified management systems in place. Those without such formal systems in place may be having to manage in disciplines in which well-defined controls exist in international or national management systems standards, and should refer to these, in the absence of other sources, to determine effective practices (e.g. information security).

It is worth emphasizing that records should not just be kept for the sake of keeping them. There may be a time limit for some records, whereas others, such as environmental records, may need to be kept in perpetuity.

The bullet 'method of access, ease of retrievability and storage media' is very important. Are the records easily retrievable even if they are electronic? Can the files be opened with current software? There are records needed for regulatory purposes, which need to be carefully maintained to demonstrate ownership of a licence, etc.

One final point to be made is that records, such as those containing confidential information, may need to be kept secure. Also, there is the need for some records to be kept secure for sensitivity reasons, such as security or health records.

As stated above, it is important that the organization learns from risk events, which should be reviewed in a timely fashion. There may be emerging trends that need to be acted upon. A one-off event involving loss of data could show there is a vulnerability to wider problems and requires prompt action. The reporting system, if configured well, should enable trends to be detected.

A review should consider such issues as:

- What actually happened?
- What were the underlying causes?
- What action has been taken?
- What is the likelihood of the risk occurrence happening again?
- Is there a need for any additional measures?
- Are there any key learning points and to whom should they be communicated?

Information from external sources should be utilized when reviewing risk events and there is a need to review other internal processes in place, and incidents, to learn from them and incorporate any changes needed to make the risk management framework more resilient. Questions such

as 'Have similar events occurred to others in the sector and, if so, how did they deal with them?' should be asked.

Internal and external reporting

The importance of reporting about the framework for managing risks, both internally and externally, has been covered in Chapter 6, 'Reporting'. However, reporting is also a key feature for managing individual instances of a risk management process. The output from such a risk process should be input (reported) to those responsible for the risk management framework, and may be a key element in the reporting aspect of the framework. For this reason reporting is dealt with more holistically here than in Chapter 6, 'Reporting'.

Much of what has been said in Chapter 6, 'Reporting' is equally applicable to the risk management process. The internal reporting very much links with recording (see previous section) and the need for the organization to learn and improve. It is also good for employees to recognize how successful they have been in achieving objectives.

The need for external reporting and the level to which this is done will very much depend on where the organization sits in the marketplace and its external context. Listed companies strive to improve their performance and recognize the value of reporting, as this encourages higher ranking with investors (on, for example, the Dow Jones Sustainability™ Indices).

> The Dow Jones Sustainability™ Indices were the first global indices that tracked the financial performance of the leading sustainability-driven companies worldwide, which provided asset managers with reliable and objective benchmarks to manage sustainability portfolios.

Some of the larger international organizations use the framework of the Global Reporting Initiative (GRI) (www.globalreporting.org) for external reporting and, whilst this is a fairly generic process, it does provide a framework that is internationally accepted. It will almost certainly be necessary to have more formal reporting arrangements for regulators and some stakeholders, e.g. to comply with the requirements of the Sarbanes–Oxley Act of 2002, the *UK Corporate Governance Code* (formerly known as the *Combined Code*). Such reports will need to meet specific requirements and these should be determined so that appropriate data is collected for this purpose.

> GRI has pioneered and developed a comprehensive Sustainability Reporting Framework that is widely used around the world. The Framework enables all organizations to measure and report their economic, environmental, social and governance performance – the four key areas of sustainability.
>
> www.globalreporting.org

BS 31100 provides more guidance on reporting than ISO 31000 that should be considered. In essence, reporting should:

- reflect the stakeholders' needs – including:
  - their priorities;
  - timescales;
  - alignment with their responsibilities;
  - conciseness;
  - specificity;
  - reliability;
- be written so that the stakeholder can understand the key issues;
- be integrated, where practicable and appropriate, with other reporting processes;
- be provided in sufficient time to allow recipients to consider and review the content and respond;
- be independently reviewed periodically to validate its content;
- provide assurance that the risk management process is operating effectively;
- provide assurance that risks are being managed.

Additionally, internal reporting should be aligned with the governance requirements of the organization in order that information on risks can be effectively communicated to those who need to know. There is a requirement in formal management systems standards that the output from management reviews should be presented to top management by the appointed top management representative, and this practice would seem to be equally sound for reporting on the performance of the framework and risk management processes.

The process for these internal reports should be documented, with a timetable detailing responsibilities and timescales for the reporting process.

A checklist for reporting is provided below:

External reporting	
Does the risk report reflect an understanding of stakeholder requirements?	
Does the risk report reflect an understanding of stakeholder timescales?	
Is the risk report written so the stakeholder can understand the key issues?	
Is sufficient time given to allow recipients time to review and respond?	
Is the risk report independently reviewed?	
Are reports tailored to reflect the needs of the individual stakeholders?	
Does the report clearly demonstrate that risks are prioritized and managed accordingly?	
Does the report demonstrate that the risk management process is operating effectively?	
Internal reporting	
Does the report provide a mechanism for the identification of new and emerging risks?	
Does the report reflect the organization's stated appetite for risk?	
Does the report assist in the identification of internal and external changes that might impact upon the organization?	
Does the report identify new and emerging opportunities for improvement?	
Does the report assist in the prioritization of risks?	
Does the report assist in identifying where additional resources may be required to manage risks effectively?	

Key learning points

- Records and recording information are important features of risk management.
- Records can provide traceability and justification for actions taken.
- Records can also help in knowledge management, which ensures information is not lost that may assist in decision making on risk treatment.
- Both internal and external reporting are important with respect to the risk management framework and the individual instances of the risk management process.
- Following the requirements of formal management systems can be beneficial.

Links with management systems standards

Keeping records is dealt with in Clause 4.2.4 of ISO 9001 and Clause 4.5.4 of both ISO 14001 and OHSAS 18001.

Chapter 12 - Integrating your management systems

ISO 31000 is about establishing a risk management framework for managing the organization's risks through processes it has established for this purpose. It has been traditional in some organizations to manage some risks as separate entities, particularly those management systems that have been developed to meet formal management systems standards, where certification is sought. The difficulty experienced by organizations operating in this manner is to ensure that these separate systems, such as those for managing quality, environment and occupational health and safety, are fully embedded into their operations. Too often they appear as a peripheral attachment when each one of these systems should be operating as an integral part of the overall business of managing the organization.

ISO has now established a high-level structure, common core text and terms and definitions that should be adopted by all new management systems standards, and those undergoing revision. ISO 9001, ISO 14001 and OHSAS 18001 are the most predominantly used management systems standards by organizations, and all will take on this common framework. This means that all the common processes found in management systems standards will have the same core text, and it is very evidently inefficient to duplicate these processes for each discipline when implementing multiple systems. This common framework will facilitate the integration of many of the requirements of management systems standards, whilst allowing the specific controls that are discipline-orientated to be managed as entities in their own right, where this makes operational sense. PAS 99 has been developed to assist in the integration of common requirements and overcome the duplication of common requirements.

The new core text also has additional requirements that have not been present in management systems standards, which should, if applied properly, affect the way they are implemented. For instance, there is a requirement of 'ensuring the integration of the XXX management system requirements into the organization's business processes' (PAS 99:2012 – 5.1).

There are, therefore, benefits to be achieved by ensuring some of the management systems standards processes are incorporated as part of the risk management framework, particularly for those smaller, less complex, organizations.

If the decision is made to manage all the significant risks in a more holistic fashion, then there are many benefits to be gained. For instance, identifying an opportunity for a new product without considering, say, the environmental impact may be foolhardy. An integrated approach should make sense to the organization.

The basic framework is provided in Table 6 below to assist those with existing specific risk management systems, such as quality, environment, information security, business continuity, and occupational health and safety systems, to migrate towards integration.

It is suggested here that this model (the integrated approach) could be used as the process for risk management in its own right. Adopting such an approach will enable an organization to remove large parts of existing systems where there is duplication. As stated above, PAS 99:2012 will help in this respect as it provides the template and guidance on integrating the common requirements.

For those organizations wishing to adopt the integrated approach, it is suggested that they use one of their existing systems as a starting point. This would normally be the system most established and understood and, perhaps, already subject to certification. This system's framework should be reviewed against Table 6 (framework), and any deficiencies identified and rectified. The output from this gap analysis will become the foundation upon which the other management systems are integrated, using the common processes, documentation, etc. as appropriate.

The approach is best followed against a structured timeframe and a set of deliverable targets. There may be resistance to the integrated approach, usually from those wishing either to protect or to promote the design of their own system. The transition process should be handled with care. The culture developed through implementing effective quality or safety systems should not be destroyed by trying to bludgeon through changes. It should be made clear that all elements are working to achieve the same overall aim. The effective and efficient management of the organization is the ultimate aim, by removing bureaucracy and duplication whilst building on the good practices that exist.

The links with the ISO High Level Structure (see *ISO/IEC Directives, Part 1: Consolidated ISO Supplement – Procedures specific to ISO*, Annex SL, Appendix 3) for managing risks in line with the structure proposed in ISO 31000 and the PAS 99 model are shown in Table 6, together with the correspondence to specifications ISO 9001, ISO 14001 and OHSAS 18001. There are gaps in ISO 31000 where little is said about some parts of the

process where the authors felt the reader may need some further guidance. The matrix includes cross references to this book's chapters to help. For instance, there is a requirement for internal audit in the ISO High Level Structure but this is absent in ISO 31000. Chapter 10 deals with this area and is shown in the matrix.

It should be recognized that a manager assigned as the figurehead responsible for risk management cannot be expected to manage risk in isolation. This role should be seen as a support resource to the management team. All managers and supervisors have many issues that they need to manage and the risks that they need to control or influence should be seen as an integral part of the overall management duties.

Table 6 — Links between PAS 99, other specifications and this book

PAS 99:2012	ISO 31000 clause	Book chapter	ISO 9001 clause	ISO 14001 clause	OHSAS 18001 clause
	3. Principles	Chapter 3			
4 Context of the organization	4.3.1	Chapter 5			
4.1 Understanding the organization and its context	4.3.1; 4.3; 5.4; 5.5	Chapter 5	4.1*	4.3.1*	4.3.1*
4.2 Understanding the needs and expectations of interested parties	4.3.4	Chapter 7	5.2	4.3.2	4.3.2
4.3 Determining the scope of the integrated management system		Chapter 6	4.2.2a	4.1	4.1
4.4 Integrated manage system (IMS)		Chapter 6	4.1	4.1	4.1
5 Leadership		Chapter 4			
5.1 Leadership and commitment	4.2	Chapter 4	5.1	4.4.1	4.4.1
5.2 Policy	4.3.2	Chapter 6, 'Risk management policy'	5.3	4.2	4.2

PAS 99:2012	ISO 31000 clause	Book chapter	ISO 9001 clause	ISO 14001 clause	OHSAS 18001 clause
5.3 Organizational roles, responsibilities and authorities	4.3.3	Chapter 6, 'Accountability, roles, responsibility and authority'	5.5.1	4.4.1	4.4.1
6 Planning			5.4; 7.0	4.3	4.3
6.1 Actions to address risks and opportunities	4.4.2; 5.4	Chapter 8	4.1; 5.4.2	4.3.1	4.3.1
6.2 IMS objectives and planning to achieve them	5.5.3	Strategy: Chapter 6, 'Risk management strategy'	5.4.1; 5.4.2; 7.2–7.5	4.3.3	4.3.3
7 Support			6		
7.1 Resources	4.3.5	Chapter 6, 'Communication'; Chapter 6, 'Building capability and competence'	6.1; 6.2; 6.3	4.4.1	4.4.1

PAS 99:2012	ISO 31000 clause	Book chapter	ISO 9001 clause	ISO 14001 clause	OHSAS 18001 clause
7.2 Competence	4.3.5	Chapter 6, 'Communication'; Chapter 6, 'Building capability and competence'	6.2	4.4.2	4.4.2
7.3 Awareness	4.3.5	Chapter 6, 'Communication'	6.2	4.4.2	4.4.2
7.4 Communication		Chapter 6, 'Communication'	5.5.1; 5.5.3; 7.2.3	4.4.3	4.4.3
7.5 Documented information			4.2	4.4.4	4.4.4
7.5.1 General			4.2.1		
7.5.2 Creating and updating	4.3.6; 4.3.7		4.2.2	4.4.5	4.4.5
7.5.3 Control of documented information	5.7		4.2.3; 4.2.4	4.5.4	4.5.4
8 Operation			7		

PAS 99:2012	ISO 31000 clause	Book chapter	ISO 9001 clause	ISO 14001 clause	OHSAS 18001 clause
8.1 Operational planning and control	4.4.1; 4.4.2		7.1	4.4.6; 4.4.7	4.4.6; 4.4.7
9 Performance evaluation			8		
9.1 Monitoring, measurement, analysis and evaluation	4.5; 5.6	Chapter 9	8.2; 8.2.1; 8.3; 8.4	4.5.1; 4.5.2	4.5.1; 4.5.2
9.2 Internal audit		Chapter 10	8.2.2	4.5.5	4.5.5
9.3 Management review	5.6	Chapter 9	5.6	4.6	4.6
10 Improvement			8.5		
10.1 Nonconformity and corrective action			8.5.2; 8.5.3	4.5.3	4.5.3
10.2 Continual improvement	4.6		8.5.1		

* there is no direct correlation in PAS 99:2012 but some clauses contribute to this requirement.

Key learning points

Some organizations, depending on their context, size and complexity, may find benefit in integrating their management system arrangements for efficiency reasons and to overcome duplication and conflict. This chapter has proposed a way that this may be achieved using the model developed for PAS 99.

Chapter 13 - Self-assessment questionnaire

How to use the questionnaire

The following is a series of questions covering the various aspects of the risk management arrangements in your organization. It enables the organization to determine the maturity of the system as it develops from little or no commitment or arrangements in place. Each of the questions is answered by two statements (1) and (4), which describe two extreme positions. Numbers 2 and 3 should be ticked if your organization occupies the 'middle ground', nearer to 1 or to 4. Tick one number for each question. The clause(s) in ISO 31000 are given after each question to indicate how the question relates to what is recommended in the standard. Also listed is where to find the guidance and relevant checklists within this book that may identify additional recommendations.

Once you have answered each question, add your score to the box at the end of this chapter. Total the score and see how your organization rates, using the performance rating system also provided there. The assessment should be completed impartially and without exaggerating the situation in order to determine genuine progress.

a. Risk management principles

Has management identified the risk management principles that should be satisfied by the risk management strategy and policy through the framework and process(es) it has implemented?

(Relates to Clause 3 of ISO 31000 – see Chapter 3 *to assess whether you have fulfilled requirements, to score more than 1.*)

1. No firm principles have been established.

4. The top management appointee has reviewed the guidance provided by ISO 31000, BS 31100 and other sources of information, and the output of his findings were presented to the top management team. It reviewed the summary and committed to a set of principles over and above those found in the standards, and has committed to delivery of the principles through the strategy, policy and framework.

a.	1	2	3	4

b. Mandate for implementing the system

Has the organization at the most senior level given a mandate for the implementation of a risk management system?

(Relates to Clause 4.2 of ISO 31000 – see Chapter 4 and Chapter 6, 'Design of framework (and the process for managing risk)' *to assess whether you have fulfilled requirements, to score more than 1.*)

1. There has been no clear mandate and a manager has decided on their own initiative to look at implementing such a system.

4. Management at the most senior level of the organization has mandated the development and implementation of a risk management framework, and the operation, maintenance and continual improvement of it. It has appointed a member of top management as the person with ultimate responsibility for the system, and has allocated resources to ensure its effective implementation, operation and continual improvement.

b. 1 2 3 4

c. Management commitment

Does your organization recognize risk management as an integral part of business performance by allocating responsibility at the most senior level for ensuring continual improvement in performance?

(Relates to Clause 4.2 of ISO 31000 – see Chapter 4 *to assess whether you have fulfilled requirements, to score more than 1.*)

1. There is no clear management responsibility.

4. Management has defined and documented roles, responsibilities and authority for risk management. Ultimate responsibility is allocated to a manager at the most senior level, but all managers and staff are actively involved and encouraged in the continual improvement of risk management where they are in a position to impact upon it.

c. 1 2 3 4

d. Compliance

Does your organization identify all legal, compliance and other requirements (such as shareholder or customer requirements) that apply to it?

(Relates to Clauses 3a) and 4.2 of ISO 31000 – see Chapter 9, 'Compliance' *to assess whether you have fulfilled requirements, to score more than 1*.)

1. We have some knowledge about legislation that might apply to our activities, but have not actively determined all the requirements that might apply to the organization.

4. We operate procedures and implement controls to ensure regulatory compliance as a minimum, but seek to work towards excellence and identify the needs of our stakeholders, and ensure that these requirements are communicated within the organization to those functions that are required to implement treatment/controls.

d.	1	2	3	4

e. Framework

Has a framework been established for risk management?

(Relates to Clause 4.3 of ISO 31000 – see Chapter 6, 'Risk management strategy' to 'Accountability, roles, responsibility and authority' *to assess whether you have fulfilled requirements, to score more than 1*.)

1. There has been no agreement on the framework. A junior member of staff was told to get on with developing something as best they can.

4. The business management system was reviewed and revised in order that it could accommodate the comprehensive requirements needed for our management of risks, and enable the organization to manage all its business risks cohesively. A framework has been established to deliver the strategy and policy, and the risk management process is operating effectively.

e.	1	2	3	4

f. Context

Has the organization determined its internal and external context?

(Relates to Clause 4.3.1 of ISO 31000 – see Chapter 5 *to assess whether you have fulfilled requirements, to score more than 1*.)

1. Very little has been done to establish the environment within which the organization works and to understand, in particular, its external context.

4. The organization has carried out an extensive evaluation of all its operations and locations where it works, and has considered all the

processes undertaken by the organization, in order to gain a full understanding of its context. This evaluation has been undertaken on behalf of top management and has been reviewed by it.

f. 1 2 3 4

g. Objectives

Does your organization set objectives and targets to ensure continual improvement of risk management arrangements?

(Relates to Clauses 3a), 3h), 4.3.1 and 4.3.2 of ISO 31000 – see Chapter 6, 'Risk management policy' – 'links between the organization's objectives and policies and the risk management policy' *to assess whether you have fulfilled requirements, to score more than 1*.)

1. We do not set formal objectives or targets.

4. We set and agree objectives and targets consistent with our strategy and policy to ensure continual improvement of our risk management arrangements, and these are regularly reviewed. Risk owners are consulted and participate in determining the objectives and targets, and these are realistic.

g. 1 2 3 4

h. Policy

Does your organization define and document its risk management policy?

(Relates to Clause 4.3.2 of ISO 31000 – see Chapter 6, 'Risk management policy' *to assess whether you have fulfilled requirements, to score more than 1*.)

1. We do not have a risk management policy.

4. We have a comprehensive and documented policy that clearly defines the organization's commitment. It links clearly to the organization's strategy, objectives and other policies. It commits to making the necessary resources available. It is communicated to employees and other relevant, interested parties. It expresses a clear commitment by top management to continual improvement of performance.

h. 1 2 3 4

i. (Management) review

Does your organization carry out management reviews of its business activities?

(Relates to Clauses 4.3.2, 4.3.4, 4.5, 4.6 and 5.6 of ISO 31000 – see Chapter 9, 'Management review' *to assess whether you have fulfilled requirements, to score more than 1*.)

1. We do not carry out management reviews.

4. We undertake regular reviews involving top management to ensure that the efficiency and effectiveness of our management of risk is continually improving. The reviews consider audit results, performance and other relevant internal/external factors, including overall business performance. At least one top-level management review is undertaken every year, and other reviews are carried out when issues arise or it is felt necessary to do so.

i. 1 2 3 4

j Accountability, roles, responsibility and authority

Has the organization defined the accountability and authority for risk management, and ensured that personnel understand their roles and responsibilities?

(Relates to 4.3.3 of ISO 31000 – see Chapter 6, 'Accountability, roles, responsibility and authority' *to assess whether you have fulfilled requirements, to score more than 1*.)

1. No formal structure or arrangements have been implemented that define the accountability, roles, responsibilities and authority within the organization.

2. The organization has ensured that from top management down within the organization everyone is aware of the part they play, and it ensures that they are competent to undertake their roles. Accountability, authority and responsibilities have all been defined for each person responsible for ensuring the delivery of the risk management policy and objectives.

j. 1 2 3 4

k. Assignment of responsibility for risk management throughout the organization

Does the organization assign responsibility to its employees for those aspects of the management of risks that impact upon them in their day-to-day duties?

(Relates to Clause 4.3.3 of ISO 31000 – see Chapter 6, 'Accountability, roles, responsibility and authority' *to assess whether you have fulfilled requirements, to score more than 1*.)

1. Risk management responsibility is assigned to our compliance manager and they are expected to manage all risks.

4. Every employee is aware of their responsibility within their field of operation with respect to the risk management arrangements and the potential impact should there be failures in controlling risks.

k. 1 2 3 4

l. Competence and training

Does your organization determine the competency needs of the personnel assigned as risk managers, and carry out training to increase the awareness and knowledge of employees about the relevant issues?

(Relates to Clauses 4.3.3, 4.3.5 and 4.4.1 of ISO 31000 – see Chapter 6, 'Building capability and competence' *to assess whether you have fulfilled requirements, to score more than 1*.)

1. We do not carry out any specific training in this area.

4. We have established a competency matrix for the organization as a whole and have a well-developed training programme to ensure our employees are fully skilled, are aware of relevant business issues, and are competent for all the tasks they have to undertake.

l. 1 2 3 4

m. Integration

Is the risk management system embedded in the overall management system?

(Relates to Clause 4.3.4 of ISO 31000 – see Chapter 6, 'Design of framework (and the process for managing risk)' *to assess whether you have fulfilled requirements, to score more than 1*.)

1. Risk management is seen as a stand-alone system very much like the quality system.

4. Risk management is embedded in such a way that it is relevant, effective and efficient and is part of the organizational processes, rather than independent, ensuring there is no conflict with other operational processes. Risk management is an integral part of the overall management system.

m.	1	2	3	4

n. Operational control

Does your organization embrace relevant business treatment/controls in its operational control system?

(Relates to Clause 4.3 and 5.5.3 of ISO 31000 – see Chapter 8, 'Implementing risk treatment/control plans' *to assess whether you have fulfilled requirements, to score more than 1*.)

1. We focus exclusively on 'business' issues, e.g. products, processes or services, and do very little about risk control until it all goes wrong.

4. We integrate the controls necessary for risk treatment into every procedure and instruction covering our activities, processes and tasks, as appropriate. We believe that it is essential we have an integrated approach for efficiency and consistency, and to avoid duplication and confusion.

n.	1	2	3	4

o. Business continuity

Has the organization established a business continuity system?

(Relates to Clause 4.3.4 of ISO 31000 – see Chapter 8 *to assess whether you have fulfilled requirements, to score more than 1*.)

1. We do not have any formal procedures for dealing with contingencies other than the fire alarm.

4. We have a fully fledged business continuity plan, which is regularly exercised to either prevent and/or mitigate any business interruption. Employees are aware of their role and responsibilities in implementing the plan. The system is certified to BS 25999.

o. 1 2 3 4

p. Resources

Does your organization provide adequate resources for effective risk management?

(Relates to Clause 4.3.5 of ISO 31000 – see Chapter 6, 'Building capability and competence' and Chapter 7 *to assess whether you have fulfilled requirements, to score more than 1*.)

1. We do not allocate any resources other than specific roles for such matters as occupational health and safety.

4. We allocate resources and make budget provisions to ensure continual cost-effective improvement in risk management arrangements and in programmes, to ensure the culture of risk management is embedded in the organization.

p. 1 2 3 4

q. Documentation

Does your organization have a system for gathering relevant business information and keeping relevant records?

(Relates to Clauses 4.3.5 and 5.5.3 of ISO 31000 – see Chapter 8, 'Documentation and document control' *to assess whether you have fulfilled requirements, to score more than 1*.)

1. We do not have a formal system.

4. We maintain a comprehensive system, appropriate to the organization. It includes a risk management system manual, and documents, documentation management arrangements and records, to ensure the risk management arrangements are effective.

q. 1 2 3 4

r. Internal communications and participation

Does your organization provide information about relevant business risk matters to employees, and ensure that employees participate in developing appropriate risk management treatment/controls?

(Relates to Clause 4.3.6 of ISO 31000 – see Chapter 6, 'Communication' *to assess whether you have fulfilled requirements, to score more than 1*.)

1. Employees are not normally provided with information on any business issue.

4. We have an established communications system to keep employees informed and involved in discussions about relevant issues, including policy, risk treatment/controls, objectives, performance, remedial actions and future plans.

r.	1	2	3	4

s. External communications

Has the organization determined how it should engage with external stakeholders and provide effective exchange of information?

(Relates to Clause 4.3.7 of ISO 31000 – see Chapter 6, 'Communication' *to assess whether you have fulfilled requirements, to score more than 1*.)

1. We do not disclose information as we believe this will put us at risk.

4. We have established procedures to inform all relevant interested parties about the organization's business-related matters. They, in turn, participate, where relevant, in our decision making about risk response and treatment.

s.	1	2	3	4

t. Strategy

Has the organization determined its strategy with respect to risk management?

(Relates to Clause 4.4.1 of ISO 31000 – see Chapter 6, 'Risk management strategy' *to assess whether you have fulfilled requirements, to score more than 1*.)

1. We do not have an overall strategy for risk management.

4. The board (or equivalent) has developed a strategy for risk management. It has also developed a comprehensive strategic plan for implementing its policy, through a framework and process that are embodied within the organization's overall business plan and management system.

t. 1 2 3 4

u. Monitoring

Does the organization carry out monitoring, measurement, inspection, etc. on a regular basis, in order to determine whether the arrangements are in place and working, and also to establish the progress on implementing the strategy, policy, objectives and targets?

(Relates to Clause 4.5 of ISO 31000 – see Chapter 9, 'Monitoring and measurement' *to assess whether you have fulfilled requirements, to score more than 1*.)

1. We have no formal or informal monitoring practices in operation.

4. We have scheduled audits and inspections, and undertake monitoring and measurements as necessary, in order to deliver objectives.

u. 1 2 3 4

v. Audits

Does your organization carry out risk management system audits? (See Chapter 10 *to assess whether you have fulfilled requirements, to score more than 1*.)

1. We do not carry out any audits.

4. We have a programme of regular audits undertaken at intervals appropriate to the risks in the various functions and areas of the organization. Internal audits are seen by employees as a positive tool for improving the performance of the organization and adding value.

v. 1 2 3 4

w. Risk identification

Has the organization implemented a risk management system that is appropriate for the risks that it needs to manage?

(Relates to Clause 5.4.2 of ISO 31000 – see Chapter 7 *to assess whether you have fulfilled requirements, to score more than 1*.)

1. We have not established a risk identification system, although we have a very basic system for occupational health and safety as required by law.

4. We have a risk management programme in place in order to proactively identify emerging risks, covering all activities and processes undertaken by the organization and those in the external environment in which the organization operates. A risk management system has been embedded to control the risks that we have determined need to be managed in order for the organization to sustain itself.

w.	1	2	3	4

The above assessment should be used at various stages of implementation and assessed against a Gantt chart such as the one given below, to establish progress over time.

Performance assessment

- The maximum score is 92 and this should be the target for an organization to achieve, demonstrating commitment to risk management and resilience.
- The organization should not score less than 2 in any particular category.
- Scores of less than 50 are indicative of either poor management commitment or that the organization is in an early stage of development of its risk management framework.
- A score of over 70 is indicative of an organization that has made great strides and has the possibility of implementing a sound risk management framework.

Day 1

4																							
3																							
2																							
1																							
	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w

Day x

4																							
3																							
2																							
1																							
	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w

Day y

				w
				v
				u
				t
				s
				r
				q
				p
				o
				n
				m
				l
				k
				j
				i
				h
				g
				f
				e
				d
				c
				b
				a
4	3	2	1	

Appendix A

Table A.1 — Examples of risk management tools (including techniques)

Tool	Risk Identification	Risk analysis and evaluation	Risk treatment and decisions
Types of meeting/collaboration: interviews, focus groups, scenario analysis and planning, horizon scanning, brainstorming, Delphi technique, nominal group technique, SWOT (strengths, weaknesses, opportunities and threats) analysis, risk questionnaires	✓	✓	✓
For exploring and visualizing the context: stakeholder engagement matrices, PESTLE (political, economic, sociological, technological, legislation and environment) analysis, Boston grid, gap analysis, Pareto analysis	✓		
Structural guidance for risk analysis: risk checklists/prompt lists, project profile model (PPM), risk breakdown structure, risk taxonomy	✓		

Tool	Risk Identification	Risk analysis and evaluation	Risk treatment and decisions
Modelling styles: process mapping, flow charts, cause-and-effect diagrams, hazard and operability study (HAZOPs), failure mode effects analysis (FMEA), fault and event tree modelling, probability trees, critical path analysis (CPA), cash flow analysis, portfolio analysis	✓	✓	✓
Data analysis: descriptive statistics, model fitting		✓	✓
Model analysis methods and tools: risk simulation (Monte Carlo/Latin Hypercube), sensitivity analysis, stress testing		✓	✓
Risk recording and visualization techniques and tools: heat maps, RAG status reports, graphs of distributions, bar chart/radar chart, risk mapping, risk profiling, probability and consequence grid, risk indicators, risk register/database	✓	✓	✓
Decision bases: expected value, utility theory, cost-benefit analysis			✓

BS 31100:2011, Annex A

References

BS 18004, *Guide to achieving effective occupational health and safety performance*

BS 25999, *Business continuity management*

BS 31100, *Risk management — Code of practice and guidance for the implementation of BS ISO 31000*

IEC/ISO 31010, *Risk management — Risk assessment techniques*

ISO 9001:2008, *Quality management systems — Requirements*

ISO 14001, *Environmental management systems — Requirements with guidance for use*

ISO 14031, *Environmental management — Environmental performance evaluation — Guidelines*

ISO 19011:2011, *Guidelines for auditing management systems*

ISO 22000, *Food safety management systems — Requirements for any organization in the food chain*

ISO 22301, *Societal security — Business continuity management systems — Requirements*

ISO 31000, *Risk management — Principles and guidelines*

ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

OHSAS 18001, *Occupational health and safety management systems — Requirements*

PAS 99:2012, *Specification of common management system requirements as a framework for integration*

SA 8000, Social Acountability

ISO Guide 73, *Risk management — Vocabulary*

ISO/IEC Directives, Part 1: Consolidated ISO Supplement – Procedures specific to ISO, Annex SL (the ISO High Level Structure)

AIRMIC, Alarm, IRM (2010) *A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000*, London and Devon: AIRMIC, Alarm, IRM (available as a free download from http://www.theirm.org, http://www.airmic.com and http://www.Alarm-uk.org)

Cabinet Office (2010) *National Risk Register of Civil Emergencies,* London: The Stationery Office Limited

Coote and Lee Employee perception of safety at Sellafield. Initial results of the safety survey carried out in 1991/92. BNFL, Risley, Warrington

Global Reporting Initiative (GRI) – http://www.globalreporting.org

Great Britain (1974) Health and Safety at Work, etc. Act 1974, London: HMSO

KPMG (2008) 'Understanding and articulating risk appetite', Advisory, Australia

Marsh/Ipsos (2009) *New risk management insights for financial institutions*

Mazars (2009) 'Review of the effectiveness of the combined code – Summary of the main points raised in responses to the March 2009 call for evidence', London: Financial Reporting Council, July

Turnbull, et. al. (1999) *Internal Control – Guidance for directors on the combined code*, London: The Institute of Chartered Accountants in England and Wales

Financial Reporting Council (FRC) (2012) *UK Corporate Governance Code*

USA, Sarbanes–Oxley Act of 2002

Managing Risk the ISO 31000 Way

David Smith and Rob Politowski

All organizations face the challenge of managing their risks and opportunities effectively. Some risks and opportunities might be well understood and managed. Others might be less well understood, inadequately managed or simply ignored.

The aim then for organizations should be to create a framework that enables the management of identified risks whilst affording a structure for dealing with unidentified risks as they emerge.

Managing Risk the ISO 31000 Way sets out a practical and clear approach to achieving just that. Building upon the framework set out in the international standard for risk management, ISO 31000, and making use of extensive case studies, examples, hints and tips, this essential new book provides a step-by-step solution to effective risk management for any organization, regardless of sector or size. It also includes highlights and links that will enable those with existing formal management systems to integrate their risk management framework quickly and easily.

About the Authors

David Smith and Rob Politowski are directors of iMS Risk Solutions, providers of world class integrated risk management services in a wide range of risk areas relevant to modern day business, including Health & Safety, Environment and Governance.

As well as playing a leading role in the drafting of PAS 99, they have authored a wide range of guidance books on management systems standards also published by BSI. Additionally, David Smith represents the UK on a variety of international standards committees and is chair of the BSI committee on Health & Safety management systems standards.

BSI order ref: BIP 2153

bsi.

BSI Group Headquarters
389 Chiswick High Road
London W4 4AL

www.bsigroup.com

ISBN 978-0-580-67512-6

9 780580 675126

The Risk Management Standards and Guidance Collection

An interactive and searchable Risk Management system collection, featuring the full up-to-date text of ISO 31000, BS 31100, BS EN 31010, ISO Guide 73, plus the best-selling book Managing Risk the ISO 31000 Way.

This easy-to-use package provides the framework and guidance to enable an organization to put in place a standards-based system for risk management that is effective but not burdensome.

BSI order ref: BIP 3093

BSI Group Headquarters
389 Chiswick High Road
London W4 4AL

www.bsigroup.com

ISBN 978-0-580-71024-7