STANDARDS Australia

SA/SNZ HB 436:2013

Risk management guidelines—Companion to AS/NZS ISO 31000:2009

handbook

HB

This document is Standards Australia Ltd copyrighted material that is distributed by SAI Global Pty Ltd on Standards Australia Ltd's behalf. It may be reproduced in accordance with the terms of SAI Global Pty Ltd's Licence 1801-c086 to Sheridan College. All licensed copies of this document must be obtained from the Licensee. Standards Australia Ltd's material is not for resale, reproduction or distribution in whole or in part without written permission from SAI Global Pty Ltd: tel + 61 2 8206 6355 or copyright@saiglobal.com

STANDARDS® NEW ZEALAND
PAEREWA AOTEAROA

This Joint Australian/New Zealand Handbook was prepared by Joint Technical Committee OB-007, Risk Management. It was approved on behalf of the Council of Standards Australia on 29 November 2013 and on behalf of the Council of Standards New Zealand on 4 December 2013.
This Handbook was published on 16 December 2013.

The following are represented on Committee OB-007:

Attorney General's Department
Australian Chamber of Commerce and Industry
Australian Computer Society
Australian Industry Group
Australian Logistics Council
Dairy Companies Association of New Zealand
Department of Finance
Engineers Australia
Financial Services Institute of Australasia
Governance Institute of Australia
Institution of Professional Engineers New Zealand
Minerals Council of Australia
Ministry of Business, Innovation and Employment (New Zealand)
New Zealand Institute of Safety Management
New Zealand Society for Risk Management
Risk Management Institution of Australasia
Royal Australian Chemical Institute
Society for Risk Analysis, Australia and New Zealand Regional
The Institute of Internal Auditors - Australia
United Independent Pools

Keeping Standards up-to-date

Standards are living documents which reflect progress in science, technology and systems. To maintain their currency, all Standards are periodically reviewed, and new editions are published. Between editions, amendments may be issued. Standards may also be withdrawn. It is important that readers assure themselves they are using a current Standard, which should include any amendments which may have been published since the Standard was purchased.

Detailed information about joint Australian/New Zealand Standards can be found by visiting the Standards Web Shop at www.saiglobal.com.au or Standards New Zealand web site at www.standards.co.nz and looking up the relevant Standard in the on-line catalogue.

For more frequent listings or notification of revisions, amendments and withdrawals, Standards Australia and Standards New Zealand offer a number of update options. For information about these services, users should contact their respective national Standards organization.

We also welcome suggestions for improvement in our Standards, and especially encourage readers to notify us immediately of any apparent inaccuracies or ambiguities. Please address your comments to the Chief Executive of either Standards Australia or Standards New Zealand at the address shown on the back cover.

This Handbook was issued in draft form for comment as DR HB 436.

Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

Handbook

Risk management guidelines—Companion to AS/NZS ISO 31000:2009

Originated in Australia as HB 142—1999.
Originated in New Zealand as HB 142:1999.
Previous edition HB 436:2004.
Jointly revised and designated as SA/SNZ HB 436:2013.

COPYRIGHT

© Standards Australia Limited/Standards New Zealand

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher, unless otherwise permitted under the Copyright Act 1968 (Australia) or the Copyright Act 1994 (New Zealand).

Jointly published by SAI Global Limited under licence from Standards Australia Limited, GPO Box 476, Sydney, NSW 2001 and by Standards New Zealand, Private Bag 2439, Wellington 6140.

Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

ISBN 978 1 74342 633 3

PREFACE

This Handbook was prepared by the Joint Standards Australia/Standards New Zealand Committee OB-007, Risk Management, to supersede HB 436:2004, *Risk management guidelines—Companion to AS/NZS 4360:2004*.

This Handbook provides guidance on the implementation of AS/NZS ISO 31000:2009, *Risk management—Principles and guidelines* (hereafter referred to as 'the Standard').

AS/NZS ISO 31000:2009 (the Standard) defines the concept of risk, explains how it comes about, and describes the principles, framework and process that allow risk to be managed effectively. It also provides an internationally agreed terminology and criteria against which the effectiveness of risk management activity can be judged.

This Handbook expands on and explains these elements and provides advice about applying the Standard, including using it to evaluate and improve existing risk management practice.

The vocabulary in this Handbook is aligned with the defined terms in the Standard and other terms in ISO Guide 73:2009, *Risk management—Vocabulary*. These terms and their definitions are given in Appendix F of this Handbook.

The structure of the Handbook follows the structure of the Standard. Each Clause of the Standard, with the exception of Clause 2 (the terms and definitions) which is reproduced in its entirety in Appendix F, is replicated in a grey-shaded box and is followed by related guidance. Similar clause numbers are used for the guidance in the Handbook to the clause numbers of the Standard to which they relate. There are additional appendices—one providing a change methodology to assist organizations to transition from present risk management practices to practices aligned with the Standard, one providing examples of risk management policy statements, one providing guidance on qualitative and quantitative approaches to establishing risk criteria, one providing additional guidance for communication and consultation, and one providing guidance on integration. To avoid confusion between the 'appendices' of the Handbook and the single 'annex' of the Standard, the latter is replicated and explained in its own section (Section 6) of this Handbook.

To help explain the concepts and the application of the Standard, the Handbook has numerous examples and illustrative templates. However, these need to be used thoughtfully and care is needed before they are directly applied to any particular risk management activity. The setting of their intended use should be carefully considered and where appropriate modifications or adjustments made, provided that the amended technique is consistent with the Standard.

Audience for this Handbook

This Handbook is intended for those who are—

- responsible for tasks associated with establishing risk management in a new organization or aligning risk management in an existing organization with the Standard;
- responsible for the application of risk management and its components to support the decision making in the strategic and day-to-day activities of the organization; or
- seeking to acquire skills in risk management.

Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

Relationship of AS/NZS ISO 31000:2009 to AS/NZS 4360:2004

The introduction to the Standard explains that it is an international standard that has drawn on many aspects of the previous joint Australian and New Zealand Standard (AS/NZS 4360), first published in 1995 with revisions in 1999 and 2004. Users of these earlier documents will recognize the similarities.

Even so, there are important improvements that have resulted from the international collaboration and consultation that occurred in the development of the international standard, a standard that both Australia and New Zealand have adopted in place of AS/NZS 4360. Principal amongst these improvements are the following:

- Risk is now defined in terms of the effect of uncertainty on objectives.
- The principles that organizations need to follow to ensure they 'manage the risk associated with managing risk' have been made more explicit.
- There is much greater emphasis and guidance on how risk management should be implemented and integrated into organizations through continuous improvement of the framework that delivers both the mandate and capability to manage risk effectively.
- An annex that describes the outcomes that are achieved by effective risk management (in effect a critical test of success) and sets out key attributes by which the organization can judge the way it acts in relation to risk has been included. These attributes will ultimately determine success.

Companion documents

Progressively, Standards Australia and Standards New Zealand are revising and republishing companion guideline documents (whether these were Standards or Handbooks) that had been prepared to expand on the earlier Standards. The replacement documents will align with the new Standard. Examples that have been completed at the time of publication of this Handbook include the following:

AS/NZS
5050:2010 Business continuity—Managing disruption-related risk

HB
89 (2013) Risk management—Guidelines on risk assessment techniques

141 (2011) Risk financing guidelines

158 (2010) Delivering assurance based on ISO 31000:2009 Risk management—Principles and guidelines

203 (2012) Managing environment-related risk

246 (2010) Guidelines for managing risk in sport and recreation organizations

266 (2010) Guide for managing risk in not-for-profit organizations

327 (2010) Communicating and consulting about risk

Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

CONTENTS

Page

Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

Page

Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

STANDARDS AUSTRALIA/STANDARDS NEW ZEALAND

Australian/New Zealand Handbook
Risk management guidelines—Companion to AS/NZS ISO 31000:2009

S E C T I O N 1 S C O P E

1.1 SCOPE OF THE STANDARD

The scope of AS/NZS ISO 31000:2009, *Risk management—Principles and guidelines* (the Standard) is, as below, designed to assist organizations of all types to manage their risks effectively, irrespective of type or how they arise. It also is intended to be used to harmonize other standards that are concerned with managing risk.

The Standard is suitable for use by newly established organizations to guide the arrangements to be put in place to manage risk, and also by other organizations to evaluate and improve the effectiveness of their existing arrangements. The guidance in the Standard is generic, therefore enabling the varying characteristics of individual organizations to be taken into account. Because successful risk management ultimately depends on the application of the risk management process to individual decisions, it is neither intended nor suitable to be used for certification of either individuals or organizations.

Essential to understanding the scope of the Standard is an understanding of the broad meaning of the word ‘organization’ as used throughout the Standard (and this Handbook). It is used as a convenient term to describe any entity that is able to establish and pursue objectives, and therefore ranges from an individual to all forms of public, private and community enterprise,* association or group, to communities, governments and their agencies, and international bodies.

* This meaning of the word organization (on which this Standard is based) is similar to the definitions of organization used in some other ISO Standards such as ISO 9001 and ISO 38500:2008.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

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.

1.2 SCOPE OF THIS HANDBOOK

This Handbook provides guidance on the implementation of the Standard. As with the Standard, it applies to all types and size of organization and all types of risk. It applies to an organization as a whole, to parts of an organization or to its activities.

The Handbook is structured to explain the following:

- Key concepts and words that are fundamental to what follows.
- How to use eleven principles of effective risk management to shape the way that risk is managed.
- How to either set up or enhance the organization's existing framework for managing risk so as to express the intent of the organization and enable it to acquire the capability to manage risk more effectively.
- How to establish the context and then, based on this, identify, analyse, evaluate and, where warranted, treat risk. To support these processes, the Handbook explains how to communicate with and consult stakeholders, and how to use monitoring and review techniques to ensure ongoing effectiveness and to detect and assimilate change.
- The application of the tests of effective risk management that are described in Annex A of the Standard.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

SECTION 2 TERMS AND FUNDAMENTAL CONCEPTS

Certain words and concepts are central to understanding both the Standard and this Handbook. Some of these words (such as 'risk') are in everyday use, sometimes having several meanings. However, in both the Standard and this Handbook they have a particular (formally defined) meaning and are only used in that way. These core words and related concepts are explained below.

2.1 RISK AND OBJECTIVES

Organizations of all kinds face internal and external factors and influences that make it uncertain whether, when and the extent to which they will achieve or exceed their objectives.

The objectives being referred to in the Standard and this Handbook are the overarching outcomes that the organization is seeking. These are its highest expression of intent and purpose, and typically reflect its explicit and implicit goals, values, and imperatives or relevant enabling legislation.

Consequently, the Standard defines risk as the *effect of uncertainty on objectives,* and this meaning also applies throughout this Handbook.

Particular objectives may include a specific timeframe. Organizations might change their objectives from time to time (e.g. as a result of periodic strategic review of opportunities), however, any such changes could create a risk source in relation to the original objectives and so first should be subject to risk assessment.

NOTE: The objectives of organizations established by statute will normally be specified in the statute. The objectives of organizations that act on behalf of society or particular communities (such as governments or non-government interest groups) will reflect the objectives of those they represent.

The level of risk is expressed as the likelihood that particular consequences will be experienced. Consequences relate directly to objectives and arise when something does or does not happen (i.e. there is an event or change in situation or circumstances that might occur at some point in the future). Therefore, the likelihood being referred to here is not just that of the event occurring, but also the overall likelihood of experiencing the consequences that flow from the event.

Typically, there can be a range of possible consequences that can flow from an event and each will have its own likelihood. It is also typical that the mechanisms through which consequences arise will be complex rather than simple and can involve interactions between multiple risk sources. This means that it will usually be necessary to take a 'whole of system' approach in order to understand both how consequences can arise and the likelihood of them occurring.

A risk is not an event. Therefore, it is not correct to say that 'risk has happened' or, when there has been an event, that risk has 'occurred'. It is also not correct to describe a hazard or some other risk source as a risk nor is it correct to characterize a risk as 'positive' or 'negative', although it would be valid to describe the *consequences* associated with a risk as either positive (i.e. beneficial) or negative (i.e. detrimental) in terms of the organization's objectives.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

2.2 UNCERTAINTY

Objectives and uncertainty give rise to risk. Uncertainty is to be found in the internal and external environment* in which the organization operates (or will be operating) in pursuit of its objectives. This might be intrinsic uncertainty that is unavoidably associated with these environments (e.g. variability in natural systems) or might arise from information that, alone or in combination—

- is not available;
- is available but is not accessible;
- is of unknown accuracy;
- is invalid or unreliable;
- involves factors whose relationship or interaction is not known;
- is variable or subject to different interpretations;
- exceeds the organization's capacity to process;
- is random or is chaotic;
- is conflicting or inconsistent;
- involves a range of known possibilities, whether and when they could occur; or
- changes over time.

Assumptions and presumptions (e.g. with respect to how people or systems will behave or how events might occur) are a common source of uncertainty. It is necessary, therefore, that decision makers are aware of any assumptions made, and the nature and extent of the associated uncertainty.

The nature of uncertainty and its effect on objectives can change over time with the result that risk will change. What is true at a point in time might not be true in the future. That is particularly so in very dynamic operating environments. That is why ongoing 'monitoring and review' and therefore anticipation and detection of change are inseparable aspects of all steps of the risk management process.

2.3 RISK SOURCE, CAUSE AND EVENT MECHANISMS

Particular sources of uncertainty are sometimes referred to as risk sources. These are defined in Clause 2.16 of the Standard as tangible or intangible elements that alone or in combination have the intrinsic potential to give rise to risk. However, something that can be characterized as a risk source in one setting will not necessarily be a risk source in other settings.

For example, a discarded banana skin on a footpath, in combination with gravity, might provide a source of uncertainty for anyone stepping on it on their way to a destination that is their objective. On the other hand, if the banana skin is discarded into a waste bin, even though also in the presence of gravity, it is unlikely to provide a source of uncertainty and therefore would not be a risk source.

The application of the label 'risk source' to something tangible or intangible therefore requires careful consideration of the context.

Something can only be deemed a cause if either alone or in combination with other causes it has actually brought about the occurrence of an event. The expressions 'cause' (which relates to events) and 'risk source' (which relates to risk) are therefore not interchangeable.

---

* The 'internal environment' refers to internal conditions and characteristics.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

As has been explained in Clause 2.1 of this Handbook, risks are not events.

The cause of any particular effect might in fact involve a complex mechanism ('event mechanism') or sequence of occurrences, in which several things need to interact or occur in order to produce the effect of interest. This point can be illustrated with the earlier analogy of the discarded banana skin—together with gravity, the discarded banana skin might cause someone to slip, which in turn (perhaps due to the fragility of their bones) causes a fracture, which in turn causes them to delay their holiday plans. It is therefore quite wrong to refer to 'causes of risk' or 'risk causes' when describing what has caused an actual event.

2.4 HOW RISKS SHOULD BE DESCRIBED

Because risk is the effect of uncertainty on objectives, the description of risk needs to convey both elements, in other words firstly make clear which objectives are being referred to, and secondly identify the particular source of uncertainty and how it could lead to consequences.*

The process of defining the risk criteria (see Clause 5.3.5 of the Standard) involves considering the principal expressions of each of the organization's objectives that are important to the organization. Using the example of a retail business, two measures of a high level objective, which is 'to build shareholder value', could be 'margin on sales' and 'rate of customer retention'.

The risk identification process (Clause 5.4.2 of the Standard) examines sources of risk, the mechanism of how those sources could result in consequences, and the types of those consequences. Therefore, the risk description should include this information in sufficient detail to be useful in the next of the risk assessment steps.

An appropriate method of providing sufficient detail can be illustrated using the high level objective of a typical retail business referred to above. Most types of retailing depend on free access to the goods on sale by potential customers, without prior vetting of customers. Some people are dishonest but the retailer generally does not know (i.e. is uncertain) which customers are in this category. The staff within the store and perhaps the store's CCTV surveillance will detect (or deter) some thieves, as might electronic tags on goods, however the retailer will not know whether all thieves will be detected in this way. As such, there are several sources of uncertainty. While a single theft might have little impact, the retailer will need to be very attentive to cumulative loss, while also not making the security arrangement so unfriendly as to depress sales. Therefore, the risk associated with uncertainty regarding the honesty of shoppers could be expressed in this way—the margin on sales is reduced by more than 5% as a result of shoplifting.

In practice, much shorter risk descriptions are often used (e.g. 'shoplifting') but this insufficiently characterizes the effect of the uncertainty and later, when the risk is being analysed and evaluated and, possibly, risk treatments are being considered, there is insufficient information about the risk to allow sound decision making.

No universal 'formula' can be provided for risk descriptions, but as a general guide, the description should make clear—

- which objective is 'at risk';
- the source of the risk; and

* ISO Guide 73 defines a risk description as a 'structured statement of risk usually containing four elements: sources, events, causes and consequences'.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

- either the nature or the fact of uncertainty, and the sequence through which the effects on the objectives could be experienced (see box aside for guidance).

It is sometimes convenient or practical to collectively consider or refer to risks that have common or distinctive characteristics. Reasons for doing so might be to—

- consider the adequacy or effect of particular types of controls;
- develop suitable risk assessment techniques that are relevant to assessing particular consequences or forms of uncertainty; or
- draw attention to a particular group of risks.

Such groupings might relate to common risk sources (e.g. human dishonesty), common types of event that could result in consequences (e.g. 'fire'), particular types of consequence (e.g. disruption) or to particular objectives (e.g. security or safety).

Formula for describing a risk

A useful way of describing a risk is to describe an event or situation in terms of what could happen or not happen, or what is present and what it could lead to regarding the organization's objectives. The following is a general approach to describing risk:

[Something might occur or not occur or is present], which leads to [consequences with reference to particular objectives].

The description can be extended to say what causes the event or situation, and also how the consequences might come about.

In such cases, it is appropriate to use expressions such as 'fire related risk', 'disruption related risk' or 'safety related risk' to label these groupings, rather than 'fire risk', 'disruption risk' or 'safety risk'. That is because risk is the effect of uncertainty on objectives, and therefore irrespective of the source of uncertainty or the objectives under consideration, *risk is risk*.

Using the 'xxxx related' form of reference avoids misunderstandings and miscommunication as to the nature of risk. For example, to use one of the above examples, to refer to 'fire risk' could obscure the fact that the principal consequences could relate to loss of assets, disruption, injury or death, or reputational damage. Although controls aimed at fire prevention will be relevant to all such consequences, other controls such as insurance, contingency planning, evacuation schemes or public relations activity are not particular to fire, and each will be relevant to only some types of consequence.

2.5 CONTROLS AND RISK TREATMENT

Controls are used by organizations to modify risk. They might comprise a single element (e.g. a warning notice) or, more frequently, multiple elements that work together, sometimes in quite complex ways (e.g. the many components of a system for quality management, which includes customer consultation, specified methods of work, training, exception reporting and documentation control).

However, controls might not exert the modifying effect assumed, due to—

- defects in the control or deterioration over time;
- uncertainty associated with any assumptions on which controls are designed; and
- the fact that there has been change in the context in which the control operates.

Risk treatment is the process that is intended to change or create controls.

2.6 RISK MANAGEMENT FRAMEWORK

The risk management framework (framework) refers to the arrangements within the organization's system of management that enable risk to be managed. The characteristics and quality of the framework will ultimately determine how effectively risk is managed.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

The framework includes the expression by senior management of the organization's intent regarding risk management (described in the Standard as the mandate and commitment) as well as providing the necessary capacity to achieve this intent, keeping this under continual review to detect change, and improving efficacy and efficiency wherever possible.

This capacity does not exist as a single system or entity. It comprises numerous elements that might either be unique to the task of managing risk (e.g. a specialized information system), or are a component of or provided by other aspects of the organization's system for management (e.g. its human resource practices).

2.7 PRINCIPLES

The Standard lists 11 principles for effective risk management (see Clause 3 of the Standard). The role of the principles is to inform and guide all aspects of the organization's approach to risk management, as well as providing the basis for managing the risks associated with risk management itself. They should therefore influence all elements of the transition process described in Appendix A of this Handbook. They also provide an ongoing basis for evaluation of the adequacy of the risk management framework. The principles provide a diagnostic tool for the ongoing evaluation of the adequacy of the risk management framework, and of the applications of the risk management process.

Rather than implementing the principles, the organization should therefore give effect to them in all aspects of risk management.

2.8 THE MEANING OF 'CONTEXT' AS USED IN THE FRAMEWORK AND THE PROCESS

The expression 'context' is used in both Clause 4 (Framework) and Clause 5 (Process) of the Standard in different ways, although aspects of the context concerning the framework might also be relevant to the context being referred to in the process. To understand the difference, it is necessary to consider how the word is used in each setting.

Clause 4.3.1 of the Standard advocates 'evaluating and understanding' the external and internal context of the organization, and then goes on to enumerate numerous examples of what might fall within these categories, making clear that this is not an exhaustive list. Clause 4.3.1 of the Standard explains that the reason for doing so is because these issues can (and should) influence the design of the framework.

The following are two examples that illustrate this:

- One of the factors of the organization's external context (as listed in Clause 4.3.1 of the Standard) might be the 'regulatory' environment in which it operates. If the organization is strongly regulated, an obvious source of risk will be regulatory non-compliance. Part of the risk management framework could therefore include arrangements to obtain expert legal advice and subscribing to an updating service to be kept informed of all regulatory changes.
- An example of the organization's internal context is its system of corporate governance. This system might require regular reporting to the governing body (e.g. the board of directors) about any risks with levels that are found to be very high or any controls that are critical in that, alone, the control makes an otherwise very high risk level, medium. The organization will therefore need to ensure that the framework has the intrinsic ability to capture and report this information as required by the governance procedures.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

The reference to context under process is more wide ranging in scope and is specific to each application of the process. Clause 5.3 of the Standard requires that the process commences by establishing the context. As explained in Clause 5.3 of this Handbook, establishing the context has the following components:

- Articulating the organization's objectives.
- Considering the internal and external environment in which particular objectives are pursued.
- Identifying stakeholders
- Establishing risk criteria.
- Identifying the specific purpose and setting for the particular application of the process.

Of the elements involved in establishing the context, those concerned with considering the internal and external environment will inevitably give rise to at least some of the issues that will have been noted when evaluating and understanding the internal and external context of the organization in the design of the framework. However, the purpose of understanding the internal and external environment when applying the process is different. In the framework, the purpose is to tailor the framework to the organization. In the process, it is to reveal the sources of uncertainty that relate to the relevant objectives and the particular decision that the process is being applied to.

2.9 MANAGEMENT, RISK MANAGEMENT AND MANAGING RISK

Management involves coordinated activities that direct and control an organization in pursuit of its objectives.

Risk management is therefore a component of management, as it involves coordinated activities concerned with the effect of uncertainty on those objectives. That is why, to be effective, the elements of the risk management framework should be incorporated, as far as is possible, within existing aspects of the organization's systems of management, and the risk management process should be integrated into all decision making processes.

In this Handbook, as in the Standard, the expression risk management (noun) is generally used to refer to the architecture (principles, framework and process) for managing risk effectively, and managing risk (verb) refers to applying that architecture to particular decisions and risks.

2.10 THE RELATIONSHIP BETWEEN GOVERNANCE AND RISK MANAGEMENT

There are several dimensions to the relationship between governance and risk management. These are best understood by considering the meanings of the two terms.

Governance is the system, primarily including people and processes, for the direction and control of management. It encompasses the mechanisms by which the organization and those that manage it are held to account. If the governance arrangements are effective, it is more likely that the organization will function as intended and achieve its objectives. The converse is also true.

Risk management refers to coordinated activities to direct and control an organization with regard to the effect of uncertainty on its objectives (i.e. risk). Because the environment in which the organization operates (including its internal governance) includes many sources of uncertainty, there is risk associated with all decisions. Effective risk management is essential for the organization to understand its risks, modify them as appropriate, and thereby maximize its chance of achieving its objectives.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

Therefore, effective risk management is essential for there to be effective governance. In that sense, the risk management arrangements are a subset of governance. On the other hand, poor governance can be expected to increase uncertainty and thus can be a source of risk. Consequently, in some organizations improving the quality of governance (e.g. adopting clear policies concerning the monitoring of controls) can be an important and even critical risk treatment for some risks.

Governance and risk management are therefore highly interdependent. Good governance requires effective risk management, and effective risk management requires good governance.

An important role for the governing body for an organization is to monitor the effectiveness of the risk management arrangements. For example, it should ensure that at all times there is a risk management policy which it approves, there is an appropriate commitment of resources in support of the policy, the organization's risk criteria properly reflect its attitude to risk, risks are generally within its risk criteria, and there are clear delegations of responsibilities and accountabilities for managing risk.

2.11 THE RELATIONSHIP BETWEEN THE PRINCIPLES, FRAMEWORK AND PROCESS

These core elements of the risk management architecture are interdependent. The principles characterize the underlying concepts that are fundamental to effective management of any risk, and therefore need to inform and be reflected in the other two elements. They also serve as a diagnostic tool to gauge the efficacy of the framework and the manner in which the process is applied.

Through the framework, the organization clarifies its risk management intent, and ensures (through continuous review) that it has the capability to give effect to that intent.

The organization discovers and, as necessary, accepts or modifies its risks by applying the capability of the framework through a structured process.

The relationship between the three main elements of the ISO 31000 architecture is illustrated in Figure 1 below (replicated from the Standard) which summarizes the overall architecture of the Standard.

The horizontal arrows between the three elements demonstrate that the 11 principles should inform the organization's mandate for and commitment to risk management, and that the framework once implemented provides and facilitates application of the process to decision making within the organization.

Continual improvement is a key part of the framework (depicted by the familiar 'plan, do, check, adjust' cycle in the diagram). The organization's experience of applying the process will often demonstrate a need for improvements in the framework (e.g. difficulties at a risk assessment workshop could be indicative of a need for improvement in the skills of those applying the process, and difficulties in obtaining data from monitoring and review activities could demonstrate a need for improvement in the collection and availability of risk management information). This feedback component of the architecture is depicted by the double headed arrow between the framework and the process.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

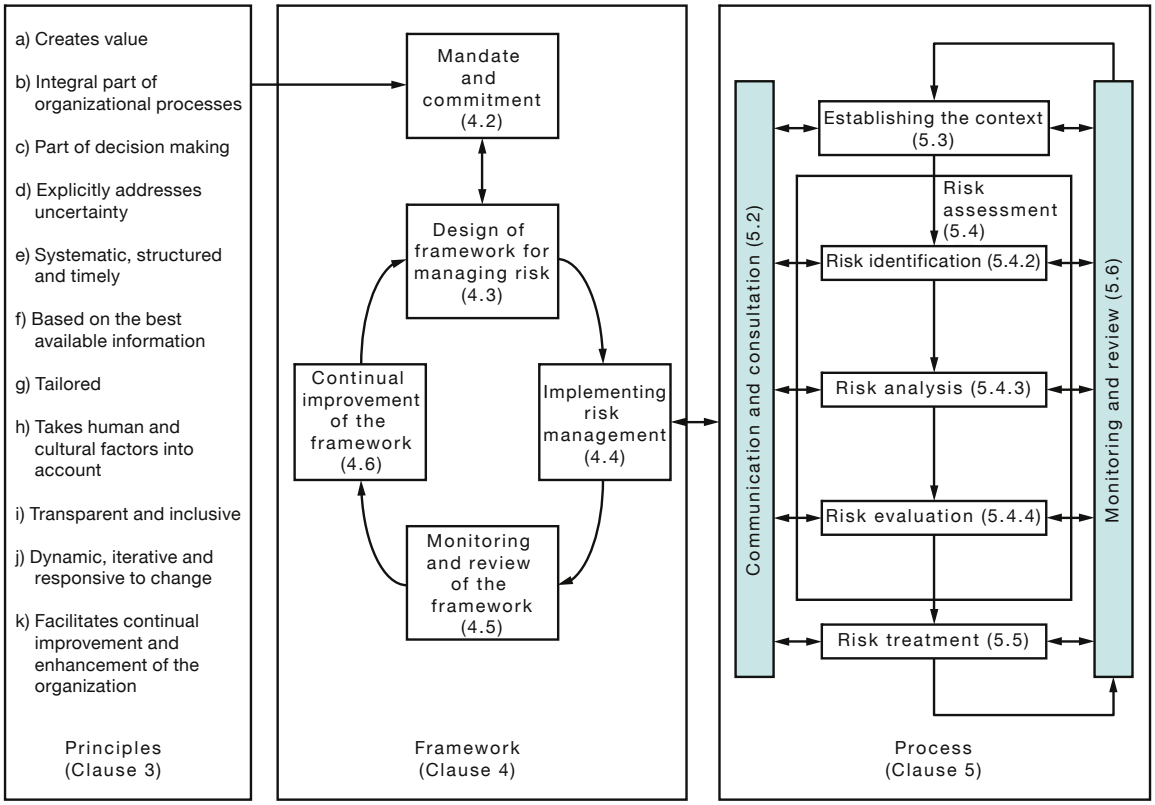

FIGURE 1 AS/NZS ISO 31000 ARCHITECTURE

(Source: AS/NZS ISO 31000:2009)

2.12 RISK MANAGEMENT PLANS

Managing risk inevitably involves making and implementing numerous plans, both written and unwritten. For example, within the risk management process, it will be necessary to plan how risks will be assessed. Supporting this will be a plan for communicating and consulting. Implementation of each risk treatment will inevitably need planning, as will the arrangements for ongoing monitoring and review.

However, in addition to these plans, many organizations find it of assistance to develop a master plan for a period of time (often a year) or for a specific activity such as a project. This plan is often called the risk management plan, with its main purpose being to ensure that the framework remains fit for purpose. Such a plan should be consistent with the risk management policy and can include the following:

- Detailed activities to transition the existing approach to risk management to one that aligns with the Standard (see Appendix A of this Handbook).
- Activities to monitor whether changes are occurring in the organization and its context (refer to Clause 4.3.1 of the Standard) that will be relevant to the ongoing adequacy of the framework (e.g. changes to relevant legislation or acquisitions or disposals that change the size, structure or activities of the organization).
- Activities to review whether the framework is enabling the process to be applied effectively to decision making across the organization.
- Activities to confirm whether risk management activity is still adequately reflecting the principles.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

- Development and implementation of improvements to the framework to take regard of the above.

The organization-wide risk management plan (as referred to in Clause 4.3.4 of the Standard) should—

- be developed in consultation with those who will be involved in its implementation;
- have a clearly expressed purpose and specific goals in support of that purpose; and
- be assessed for the risks associated with both the implementation and the end state of the plan, and establish accountabilities and performance measures for implementation.

In large organizations with a specialist risk management support function (e.g. a Chief Risk Officer) it will be usual for that function to have custody of the plan, but in smaller organizations responsibilities for implementation will be distributed across the management team according to the tenor of each action item. As part of the organization's governance arrangements, the governing body is responsible for evaluating the organization-wide risk management plan, monitoring progress and directing changes as required.

2.13 SILO-BASED APPROACHES TO RISK MANAGEMENT

Many organizations have historically managed various types of risk in silos, typically known by the name of the silo. Common examples are health and safety (which is concerned with managing risk related to personal injury and health), environment (which is concerned with managing environment-related risk) and continuity management (which is concerned with disruption-related risk). It is not unusual that these silos have adopted a distinctive vocabulary, in some cases being derived from relevant legislation.

Similarly, organizations in which there is an in-house legal function or a public affairs/corporate communications function might delegate to those functions (whether formally or informally) responsibility for managing liability-related risk and reputation-related risk respectively. In some organizations there can be an insurance function and also a risk management function, notwithstanding that insurance is a particular type of control that involves sharing particular types of risk with other parties in return for an agreed fee. There are many other such examples.

Nevertheless, all such specialist functions (or silos), whatever their name or descriptor, are specifically managing risk. Given that risk is the effect of uncertainty on objectives, and given that all such silos are part of the same organization and are therefore pursuing the same high level organizational objectives, risk is a common denominator. For these reasons it is more appropriate to refer to risks within the field of interest of these silos as 'xxxx-related risk' rather than 'xxxx risk'.

Although many of these silos are legacy arrangements that predate the Standard, they often persist for one or both of two reasons that are not mutually exclusive. The first is a very human one in which those accustomed to running the silos can be protective of their sphere of influence and status, and so resist change for that reason. The other reason relates to technical specialization, with the silo in fact being defined by the expertise needed to understand the risks being managed by the silo. Although the first reason has little worth in terms of effective risk management, the second reason can be an important and valid consideration.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

The Standard encourages organizations to integrate risk management activities into their other processes (refer to Clause 4.3.4 of the Standard). Some of the reasons for this take into account—

- organizations having a single set of high level objectives;
- the benefits of consistency of process, risk criteria and language;
- ownership of controls common to the risks associated with more than one silo; and
- particular consequences that can arise from risks associated with more than one silo.

However, the general goal of integrated practices does not necessarily preclude the continuation of some silos or other forms of organization-specific tailoring of the framework. Furthermore, it will usually be more efficient for the responsibility of the maintenance of the framework for managing all forms of risk to be the responsibility of a central function, and for that function to obtain such specialist technical advice as is needed from other functions within the organization.

In larger organizations, there can be good reasons to preserve clusters of expertise, provided that the risk falling within the responsibilities or expertise of each such cluster (silo) is managed in a consistent way across the organization in accordance with the organization's risk management policy. Therefore, across all such silos there should be a common language (specifically, the language of the Standard), common reporting mechanisms, and the same risk criteria applied to all silos.

Where there is an organization-wide risk management function, its responsibilities should be to overview, coordinate between clusters and give general direction to each cluster (or silo), so that there is consistency in the way risk is managed and there is an efficient framework (e.g. by having common training practices that incorporate risk management).

Transitioning from a silo-based approach of managing some forms of risk to one involving a fully common system, or modifying the practices within silos to conform to a common organization-wide approach, requires careful planning and execution. The requirement to make the change should be mandated by the governing body through senior management with clear communication and consultation around the benefits and implications of the change.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

SECTION 3 PRINCIPLES

3.1 GENERAL

Clause 3 of the Standard lists 11 principles that are relevant to all levels and activities of the organization that make risk management effective. The relationship of the principles to the other elements of the risk management architecture (framework and process) is depicted in Figure 1 of the Standard and of this Handbook.

The 11 principles provide guidance as to the—

- rationale for managing risk effectively [e.g. Principle (a). which specifies that risk management 'creates and protects value']; and
- characteristics of risk management that enable risk management to be effective [e.g. Principle (b) which specifies that risk management is 'an integral part of all organizational processes'].

In the Standard, each principle is summarized in a few words by its heading with the supporting text providing explanation and detail.

Not surprisingly, there are strong linkages between the principles and the attributes of enhanced risk management that are specified in Annex A of the Standard.

Unlike the components of the framework and the steps of the risk management process, the principles are not specified actions that need to be taken, but rather essential underlying concepts and drivers. The principles therefore provide guidance to both the way the framework is structured and the risk management process is applied, and indicators or characteristics can be used diagnostically to evaluate the effectiveness of the risk management arrangements. In other words, they enable an organization to assess and if necessary, treat the risk that it is not managing risk effectively.

Although the principles are expressed succinctly, the implications of each needs to be thoroughly understood in order to give effect to them on a continuing basis.

For example, Principle (c) states 'risk management is a part of decision making'. While an organization might entirely agree with and accept that this is an important principle, to give effect to the principle will require initially, careful thought about the following:

- How can this help create and protect value [Principle (a)]?
- How and where in the organization are decisions made?
- Who is involved in decision making?
- What knowledge and skill is needed for those who make decisions to make risk management a part of their decision making?
- How will decision makers acquire such knowledge and skill?
- What instructions and encouragements for existing staff are needed for this to occur?
- How will future staff be inducted to this method of decision making?
- How will external stakeholders be affected?
- What decision making processes in the organization would need to change?
- How would progress in applying this principle be monitored?

Thereafter, the results of such analysis should be reflected in the design or enhancement of the framework (e.g. in the allocation of accountabilities, provision of training, communication with stakeholders, and the design of ongoing monitoring and review of risk management performance).

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

The purpose of this Section of the Handbook is to provide guidance, in the form of a general method (see Clause 3.2) and some tips about each of the 11 principles (see Clause 3.3), to assist organizations to give effect to the principles and thereafter, periodically, to review and confirm that the principles continue to be satisfied. Each organization will need to tailor this general method to its 'organizational context' (refer to Clause 4.3.1 of the Standard).

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.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

(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.

3.2 HOW TO GIVE EFFECT TO THE PRINCIPLES

1 Become thoroughly conversant with each principle. Know the meaning of those words in the principles that are specifically defined in Clause 2 of the Standard and ensure that this meaning becomes part of the understanding of the principle. Recognize that several of the principles interrelate and keep such linkages in mind, for example, Principles (b) and (c), Principles (b) and (j), Principles (e) and (h), and Principles (h) and (i).

2 For each principle, consider in a general sense (in the context of the type of organization concerned) in what respects the principle would be likely to have application (the example in Clause 3.1 of this Handbook relating to Principle (c) is an illustration of this step).

3 For each principle, review the present situation. Consider which aspects of the organization's activities and processes generally, and risk management practices specifically, the principle applies to, and then consider to what extent the principle is already evident and in which ways it could be given greater effect.

Use a simple methodology to allow a structured approach, such as considering in turn (for each principle), the organization's—

- strategy;
- structure;
- methods (including internal risk management standards); and
- culture.

This need not be a comprehensive review across all parts of the organization of each of these four organizational characteristics. Usually, it will be sufficient to use a sampling approach that considers various levels and types of activities in the organization, as well as its formal systems of governance and management.

4 Initially record the results of this evaluation of each principle in a simple tool (see Table 1).

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

TABLE 1

EXAMPLE OF A TOOL TO EVALUATE THE EXTENT OF APPLICATION OF EACH PRINCIPLE

Organizational characteristic	Extent evident (1-10)	Main evidence (bullet points)	How to give greater effect (bullet points)
Principle x			
Strategy			
Structure			
Methods			
Culture			

5 Use the results of the evaluations for all of the principles to improve the framework and the way that the risk management process is applied. In some cases, the improvement might simply involve giving greater emphasis to the principle concerned, in others it might require significant modification of processes, documentation or even the organization's policy for risk management.

6 Incorporate these changes into the annual risk management plan. For organizations initially transitioning to align their risk management arrangements with the Standard (refer to Appendix A of this Handbook) the changes will be incorporated into the implementation plan (see Clause 4.4.2 of the Standard).

7 Use the same approach to evaluating present practice as part of the annual review of the organization's risk management framework.

3.3 EXAMPLES

As emphasized in Clauses 3.1 and 3.2 above, giving effect to the principles requires a thorough understanding of each principle and lateral thinking about where it is applicable throughout the organization. Table 2 below is intended to provide examples of the range of organizational characteristics to which each principle might have relevance. It is not a comprehensive list or tailored to any particular type or size of organization, and should only be regarded as illustrative of the extent to which the principles might have application. Every principle will be relevant to the organization's risk management policy, whereas some other principles will only be relevant to some characteristics. Some of the examples will be applicable to more than one principle.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

TABLE 2

EXAMPLES OF ORGANIZATIONAL CHARACTERISTICS TO WHICH EACH PRINCIPLE MIGHT APPLY

Principle	Examples of relevant organizational characteristics
All	• Policies • Applications of the risk management process
a Risk management creates and protects value	• Mission statement • Governance framework • Planning and budgets • Capital allocation and rationing • Selection of risk treatments • Organizational culture
b Risk management is an integral part of all organizational processes	• Governance mechanisms • Instructions for strategic and business planning rounds • Formal management processes (e.g. project management manuals) • Delegations • Management of change process
c Risk management is part of decision making	• Approval processes (plans, budgets, expenditure, investments, disposals, projects, system changes, resource allocation) • Design (products, services, organizational structures, systems, tasks) • Contracting • People appointments
d Risk management explicitly addresses uncertainty	• Context • Design of monitoring and review activities • Effectiveness of communication and consultation • Assumptions (planning, budgeting, forecasting, designing, controls and risk treatments) • Human factors (behaviour, culture, assumptions) • Research (markets, stakeholders)
e Risk management is systematic, structured and timely	• Decision making processes • Project timetables • Incident investigation • Reviews
f Risk management is based on the best available information	• Framework resourcing • Research • Data (collection, analysis, review, accessibility) • Monitoring (context statement, control performance, risk treatment implementation) • Incident investigation, analysis, reporting • Continual improvement (assurance methodology, remedial measures, updating)

(*continued*)

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

TABLE 2 (*continued*)

Principle	Examples of relevant organizational characteristics
g Risk management is tailored	• Organizational context (including changes such as acquisitions, mergers, restructuring) • Decision making • Risk criteria • Stakeholders (nature, needs, concerns, changes) • Delegations (expenditure, acceptance of risk)
h Risk management takes human and cultural factors into account	• Culture (organizational, societal, national, transnational) • Staff (behaviours, skills, attitudes, preferences, values) • External stakeholders • Trust • Communication and consultation (formal and informal) • Monitoring design • Control design (reliance on human actions, ergonomics, people/system/machine interfaces, predictability, cognitive bias, peer pressure)
i Risk management is transparent and inclusive	• Consultation and feedback • Clarity and integrity of communication • Risk criteria • Access to information and disclosure • Treatment design • Reporting
j Risk management is dynamic, iterative and responsive to change	• Change management • Framework review • Currency of information (risk registers, data bases, statement of context, monitoring and review methods) • Results of monitoring and review (ongoing validity of assumptions) • Global events with local impacts
k Risk management facilitates continual improvement of the organization	• Framework review • Application of results of monitoring (assurance system, routine data collection, incident investigation, root cause analysis, performance review) • Annual risk management improvement plan • Periodic external review • Decision making speed and efficiency • Ability to recognize and make use of opportunity

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

SECTION 4 FRAMEWORK FOR MANAGING RISK

An organization's ability to manage risk effectively depends on its intentions and its capability to achieve those intentions. This intent and capability is referred to as its risk management framework and is part of the organization's system of governance and management.

The quality of this framework is important because ineffective risk management inevitably can be linked to the following:

- Unclear or contradictory expectations from 'the top'.
- Lack of capability (skills, resources).
- Poor relationships with stakeholders.
- Failure to build in the necessary risk management practices to the day-to-day activities and accountabilities of the management team.
- No commitment to continually learn and improve.

Effective risk management is the opposite, providing clear intent and matching capability.

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 these processes is adequately reported and used as a basis for decision making and accountability at all relevant organizational levels.

This Clause (4.1) 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.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

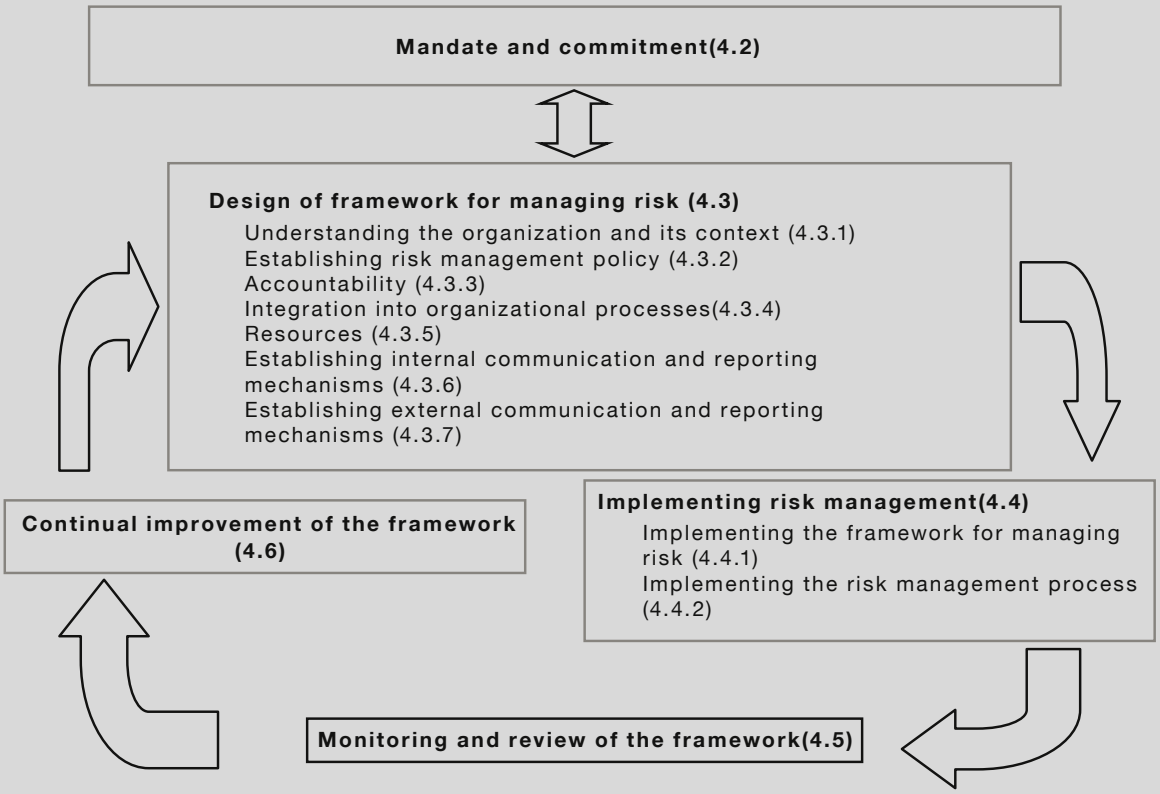

FIGURE 2 RELATIONSHIP BETWEEN COMPONENTS OF THE FRAMEWORK FOR MANAGING RISK

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.

4.1 SIGNIFICANCE OF THE RISK MANAGEMENT FRAMEWORK

All organizations manage risk to some extent and to varying degrees of effectiveness. As Annex A of the Standard explains, the management of risk is only truly effective when—

- the organization has a current, correct and comprehensive understanding of its risks; and
- its risks are within its risk criteria.

The risk management process in Clause 5 of the Standard allows an organization to achieve these outcomes. However, the organization needs both the intent and the capability to consistently integrate the risk management process into those management processes it uses to make decisions.

Consequently, the soundness of the organization's decisions (and therefore its ability to deal with the effect of uncertainty on its objectives) will be the direct result of the quality of its risk management framework.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

Although this intent and capability is referred to in the Standard as the risk management framework this does not imply that this framework stands alone or is separate from the other aspects of the system of management through which the organization operates. In fact, the opposite is the case. To be effective, the risk management framework as described needs to be fully integrated into the organization's everyday modes of operation.

The framework is what actually exists at any point in time, whether it is effective or ineffective. It has many tangible elements: it is not a single document such as a policy statement, nor is it just a particular procedure or a piece of risk management software or a risk rating method or a database, even though all these might form part of the framework.

Appendix A to this Handbook provides a structured transition process to identify and make any necessary changes to an organization's existing framework so that it aligns with ISO 31000.

4.2 THE INTENT COMPONENT OF THE FRAMEWORK

The intent component of the framework is the means by which the organization first determines and then signals to itself and its stakeholders, what it is intending to achieve in its management of risk. In the Standard, this is referred to as mandate and commitment.

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.

In practice, organizations and their people respond to a range of internal signals and other stimuli. Some of these, such as formal policies and plans, are explicit; others, such as the organization's general culture and brand, are implicit (but can take longer to evolve than developing and publishing a policy). Both can be equally powerful in influencing and directing the way that people in the organization behave and perform, but can undermine the other if not fully aligned. In fact, the implicit stimuli are usually more powerful and deeply embedded, and are always harder to change. In practice they often override the explicit stimuli.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

For example, the organization might have a policy statement explicitly requiring all decisions to be supported by risk assessment. However, if the Board or Executive are prepared to make major decisions (such as those involving organizational change or acquisitions) without a risk assessment, it sends a clear signal to the organization that in reality it is not committed to its own policy and that other practices are tolerated. This inevitably has the result that decisions lower in the organization will also be made without adequate risk assessment, despite the policy.

So establishing the intent is a matter of not just having a written mandate (e.g. policy statements) but also providing explicit and implicit demonstration of commitment in a strong and sustained manner. It should make clear what is entailed and how can it be achieved.

4.2.1 Implications of intentions

If the organization wishes to manage risk effectively it will aspire to achieve the attributes given in Annex A.3 of the Standard, namely the following:

- Full integration in the organization's governance structure.
- Application of risk management to all decision making.
- Full accountability for risks.
- Continual communications.
- Continual improvement.

The practical meanings of these attributes are expanded upon in Annex A.3 of the Standard, but in aspiring to achieve them, those responsible for the design or improvement of the risk management framework will need to be able to visualize what this would mean in practice.

For example, in broad terms at least the following questions will need to be answered:

- What would need to change or be enhanced?
- What resources/budget will be required?
- Who would lead the change?
- Who would need guidance and support?
- What would be an acceptable time frame in which to realize these aspirations?
- What will be the key milestones in each case that would provide evidence of progress, and how would successful achievement be monitored?
- What are the risks associated with these aspirations and their achievement, and how will these risks be treated?
- How will these aspirations be communicated?

4.2.2 Means of communicating the mandate and commitment

If the organization's intentions for the management of risk are not clearly communicated using the channels and forms of communication the organization normally uses for other important aspirations, those intentions are unlikely to be achieved. Whereas some organizations set norms and expectations with formal, written policies, others use verbal communication reinforced by performance-based remuneration. Consistency in approach is often more believable and has the effect of generating sustained engagement with the organization's intentions.

Whatever the method, the test of adequacy is whether, in practice, the intentions for the management of risk are clearly understood throughout the organization, are believed, and are evident in behaviour. Depending on the organization and its usual practices, written policy statements can therefore either reinforce or detract from meeting this test.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

Whatever mechanism or means are used to communicate the mandate and commitment, they need to be—

- clear and unambiguous;
- relevant to the organization's objectives;
- achievable;
- credible; and
- consistent with the organization's normal mechanisms or means for communications.

Potential means for communication, reinforcement and feedback include the following:

- Written policy statements (see Clause 4.3.2 of the Standard).
- Rules and instructions.
- Rewards and sanctions.
- Performance standards.
- Personal communication.
- Discussion and agreement.
- Consistent language.
- Consistent behaviour.
- Avoidance of ambiguous and contradictory behaviours.
- Induction, training and refresher programs.

Further advice on communication techniques can be found in Clause 5.2 and Appendix E of this Handbook, and in Standards Australia/Standards New Zealand Handbook HB 327:2010, *Communicating and consulting about risk*.

4.3 THE CAPABILITY COMPONENT OF THE FRAMEWORK

This Clause explains and gives advice with respect to Clause 4.3 of the Standard. It emphasizes the importance of there being a good fit between the framework, and the characteristics of the organization and its surroundings.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

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, 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 might 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.

4.3.1 Tailoring the framework to the organization

Improvements to the risk management framework need to be tailored to fit the organization. This tailoring will ensure that the resulting approaches are accepted, regarded as relevant, able to be integrated efficiently with minimum disruption, provide the necessary agility to support the business model, and responsive to ongoing change.

To achieve a good fit, the components of the framework need to reflect the following:

- The objectives of the organization.
- The environment (internal and external) in which the organization pursues its objectives.
- The general characteristics of the organization, including the pace at which change occurs or can be expected and the required speed of decision making.

External environmental factors that might require tailoring include the following:

- External stakeholders (e.g. the mix, location and expectations of external stakeholders might require changes to the organization's communications methods).
- Laws, norms and standards (e.g. the information required to meet regulatory reporting requirements might require changes to data collection methods).
- Markets and competitors (e.g. the frequency of change in either markets or competitors might warrant more regular reviews of the effectiveness of the risk management framework).

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

- Societal and political characteristics of the location where the organization operates (e.g. operating in foreign countries might require obtaining regular independent political assessment as an input to the organization's general statement of context).
- Natural events (e.g. the effects of extreme weather events, and how their frequency and intensity will increase due to climate, change might require the revision of risk criteria).
- Financial markets (e.g. increased market volatility might require a change in risk management policy).
- The economic climate (e.g. macro changes in the economic climate might require changes in risk management policy).
- Technology and trends (e.g. developments and trends in social media might lead to changes in external reporting and communications protocols).

Irrespective of the size, type and domicile of the organization, each of these should be considered from a local, regional, national and even international perspective. As the 2008 global financial crisis illustrated, even the smallest, locally-based organization can be severely and rapidly affected by international events.

The general characteristics of the organization to be considered in the design of the framework include the following:

- Structure (e.g. the functions and divisions of the organization, how they relate, and their reporting lines).
- Internal stakeholders (e.g. key reporting or oversight functions such as the legal department, and how they need to be involved in decisions or informed of activities).
- Governance practices and requirements (e.g. the organization's obligations under corporate governance requirements such as the *ASX Corporate Governance Principles and Recommendations,* * and how the governing body such as a board wishes for these to be satisfied).
- Policies, internal standards and models (e.g. the policy for capital expenditure and how this is allocated and approved, or the approach that will be taken to ensuring safety in the workplace).
- Organizational culture (e.g. the results of recent staff satisfaction surveys and how management is responding to these).
- Contractual requirements (e.g. the contracts the organization has to follow with its customers or suppliers).
- Strategic and operational systems (e.g. the methodology for business planning or for planning the maintenance of equipment).
- Capability and resources (e.g. financial and reputational capital, time, people, processes, systems, and technologies).
- Knowledge, skills and intellectual property (e.g. how the organization's IP is protected, or how the organization 'learns' from its successes or failures).
- Information systems and flows (e.g. formal reporting requirements, informal communications and liaisons, and working relationships).

---

* Australian Securities Exchange (2010) *Corporate governance principles and recommendations with 2010 amendments* (2nd ed.). Available at http://www.asxgroup.com.au/media/PDFs/cg_principles_recommendations_with_2010_amendments.pdf (retrieved 1 October 2010).

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

- Other organizational priorities and imperatives that can be perceived to compete with the organization's intentions for managing risk (e.g. priorities that may occur as a result of its financial position, or the specific requirements of lenders or regulators).

These characteristics should be recorded so that they can be referred to subsequently, in order that any change that might require the framework to be adjusted can be adjusted. For example, if the organization is restructured, this might require revised policies and a reallocation of resources; if there were new legislative requirements for record keeping, changes to accountabilities and training for information capture might be needed.

4.3.2 Policy about managing risk

As noted in Clause 4.3.1 of this Handbook, improvements to the risk management framework should be tailored to the general characteristics of the organization. This Clause explains how to express the policy and what to take into account when deciding how to communicate it.

The purpose of making policy is to clearly and consistently communicate what is required. Therefore, two issues need to be considered:

- What is required?
- How it is to be communicated?

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.

A written statement can be an effective way to clearly express the intentions and requirements of the organization, but the way that the statement is distributed and publicized will affect how successfully it is communicated.

To be effective the statement should express the organization's motivation for managing risk effectively, and explicitly set out what is required and by whom. The tenor of such statements of policy therefore should therefore clearly signal—

- the necessity of taking risk;
- that managing risk effectively is proactive and a core part of business as usual; and
- that managing risk effectively creates and protects value by supporting decision making at all levels.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

Other key ingredients include statements that—

(a) link effective risk management to the achievement of the organization's objectives and therefore the preservation and creation of things the organization values;

(b) give requirements and express commitment to managing its risks effectively;

(c) define the process that will be used for the management of risk;

(d) allocate responsibilities and accountabilities including those for setting risk criteria and for accepting risk;

(e) make commitment on resourcing;

(f) link this policy to other relevant policies;

(g) describe how risk management performance will be monitored and reviewed; and

(h) specify when the policy will be reviewed and what will cause it to be reviewed.

Policy statements are normally more effective if they are succinct and expressed on one page. The language used in the policy statement should be readily understandable by those to whom it applies and terminology should be consistent with the Standard.

The style and title of the policy statement will depend on the type of organization and its normal format for such statements. For example, some organizations express their risk management policy as a Chief Executive Instruction, others do so as part of general organizational policies or as a standalone policy. Four illustrative examples of policies are given in Appendix B to this Handbook, selected to show a range of styles and organization types.

Writing the policy statement is only the start of the communication process. In deciding how the policies will be promulgated, explained and consistently reinforced, the organizations should take into account the general characteristics described above. For example, a small enterprise might explain the policy at a staff meeting, whereas a global organization might distribute it in an email broadcast to every employee and then reinforce the policy in each workplace through road shows or seminars.

Effective communication also requires confirmation that the information has been understood and is truly believed to reflect the organization's intent. Inevitably this requires tangible and consistent evidence that the organization has changed its behaviours, and that those changes persist over time. Otherwise, the effect of the policy on the organization will be either neutral or negative.

For example, if an organization announced a zero harm policy for safety-related risks and immediately after the announcement, a senior manager walked past a tripping hazard without comment, there will be immediate doubts about the organization's commitment to the policy and it might not be believed. If a bank has clear policies for trading currency but in the interests of producing optimistic monthly reports these are regularly ignored with tacit acceptance by management, the policy will not protect the organization and will have no value.

For these reasons, at least as much effort should be applied to the planning of how policies will be communicated as to their formulation. That plan should also contain clear processes to monitor and review the uptake and effectiveness of the policy.

For example, if the policy required all proposals for capital expenditure to be supported by risk assessment, internal audit should be required to assure that this is taking place to the required standard; if the policy required managers to be responsible and accountable for the correct functioning of controls, review of this should be part of annual personal performance assessment and salary review and monthly management reporting.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

Further advice on effective communication and consultation can be found in Standards Australia and Standards New Zealand Handbook HB 327:2010, *Communication and consulting about risk*.

4.3.3 Accountability

As with every other aspect of organizational management, managing risk effectively requires people to have specific accountabilities, authorities and delegations, and appropriate competence according to their role in the organization.

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.

Accountabilities for risk management are of two kinds:

1 Accountabilities of those who are responsible for tasks associated with establishing, enhancing or maintaining the risk management framework. These tasks include planning, resourcing, monitoring and the review of the effectiveness of and therefore continual improvement of its components. In many large organizations, some of these people will be specialists in risk management theory and practice, some will have supporting technical expertise such as in quantified risk analysis, information systems or independent assurance, and others will have particular framework responsibilities as part of their general responsibilities (e.g. in finance or information technology). In smaller organizations several members of staff, managers or the CEO might undertake these roles.

2 Accountabilities of those who are responsible for the application of the risk management process or elements to support decision making in the strategic and day-to-day activities of the organization. These people are both managers who own particular risks* and others who own particular controls or treatments, as well as those who are responsible for the completion of any specific task.

The accountabilities need to be clearly expressed in terms of what is required, how performance will be measured, and how this will count in the overall assessment of an individual's performance. These accountabilities should therefore be part of a particular role, and be specified in formal role or position descriptions.

As well as this formal allocation of accountability, as with policy, the organization should continually reinforce accountabilities through the informal systems of management, such as in the discussions and the agendas of internal meetings, and through the positive reinforcement of good performance.

---

* The Standard defines the risk owner as a person or entity with the accountability and authority to manage a risk.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

Because an organization's success is strongly linked to how effectively it manages risks, the most powerful personal stimuli—promotion, recognition and remuneration—should be used to reinforce risk management accountabilities.

For the same reason, recruitment criteria should take into account the intended risk management accountabilities. Candidates should be required to demonstrate their proficiency in fulfilling such accountabilities as well as the other attributes of the role.

Accountabilities without matching skills are unlikely to produce the required performance. As formal tertiary qualifications seldom include risk management in their curricula, organizations of all sizes should expect to invest in training to build skills and competence in this area (see Clause 4.3.5 of the Standard). This could also include continuing professional development through mentoring, networking and participation in suitable professional bodies and societies, as well as formal training.

4.3.4 Integration

All organizations manage risk in some way or other. The methods and behaviours used to do so might be effective or ineffective, efficient or inefficient, formal or informal, and explicit or implicit, but they will already be integrated and embedded in the strategic and day-to-day activities of the organization, and reflective of the organization's culture. Therefore, this Clause of the Handbook is concerned with the task of ensuring that as far as is possible, the elements of the framework (including any improvements to the framework) are fully integrated into the organization's processes.

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.

Many organizations have sought to improve their risk management practices without appreciating that the only risk management approaches that will have an enduring effect are those that are an integral part of the organization's system of management, supported and reinforced by actual accountabilities.

Such embedded practices cannot be changed simply by the promulgation of policies, procedures or requirements unless these are deliberately and thoughtfully integrated into the system of management, replacing or enhancing those that are already there.

However, as with change of any type, integration of different approaches will not occur unless the objectives are clear, it is properly planned, after careful analysis of the present situation, and the approaches have been clearly communicated and suitably resourced. As is sometimes said, effective change is dependent on establishing where the organization is now, what it wants to achieve and what it needs to change to get there.

Plans for integrating changes to the framework need to be explicit, and should contain actions, timelines and accountabilities. A realistic plan will secure the necessary resources, and take into account competing priorities and any risks created by the plan. More information on planning for integration as part of a transition process is given in Appendix A and methods for achieving integration are described in Appendix D of this Handbook.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

As well as integrating the risk management framework into the organization's overall system of management, it will considerably enhance effectiveness and efficiency if the framework also integrates the approaches for managing all forms of risk. This can be challenging for some organizations (and even individuals) that are accustomed to managing risk of different types in separate silos, but is likely to be worth the effort.

4.3.5 Resources needed for managing risk

As with any aspect of management, resources are needed to achieve the benefits that flow from managing risk effectively. These include, but are not limited to, people with skills and competencies, information systems, systems of assurance, specialist advice, and time and effort generally. Such resources, whether additional or existing, need to be of the requisite quality and quantity, otherwise they might undermine rather than enhance the framework.

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 risk processes, methods and tools to be used for managing risk;
- documented processes and procedures;
- information and knowledge management systems; and
- training programmes.

Whether it is a new organization that is establishing its framework for managing risk or an existing organization that is seeking to enhance its existing framework, it is to be expected that greater resources will be needed initially. There might be a delay on the return from this initial investment and hence the importance of there being a clear level of commitment from the outset. Even so, it can be useful to look for opportunities (especially quick wins) that demonstrate the early benefits of investing in a sound framework.

By fully integrating the risk management framework into the organization's overall management system it quickly becomes apparent that very few additional or distinctive resources are needed over and above those needed for management generally. As is often said, 'risk management is management'—an observation that is entirely consistent with the definition of risk management in the Standard.

For example, for risk management accountabilities to be meaningful, it is necessary to monitor and review individual performance. However, rather than establish a separate performance review process, risk management performance can be integrated into the general system of performance review. As well as being efficient, this also reinforces the intent that managing risk is part of business as usual and not something that is separate.

One of the two supporting activities of the risk management process is monitoring and review. Its purpose is to detect change and provide ongoing confirmation and confidence (i.e. assurance) that—

- risks have not changed;
- the level of risk remains acceptable; and
- the controls continue to perform as intended and continue to modify the risk in the manner and to the extent assumed in the risk assessment.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

The organization's system of assurance (through which it monitors and reviews all aspects of organizational performance) will therefore be part of the risk management framework, modified as necessary to include risk management requirements. Monitoring and review should include both lead and lag indicators and therefore include, for example, both inferred and direct monitoring of controls.

For example, in a manufacturing company variations in production data from those expected can be used to infer whether process controls are working. Assurance regarding process controls can also be directly achieved by routine inspection of those controls.

Although most organizations will use both internal or external assurance providers who are independent of the operational parts of the organization, the system of assurance provided by the framework should also include routine monitoring and review by control owners (i.e. those responsible for the correct functioning of each control).* This is sometimes called control self-assessment.

As noted at Principle (a) in Clause 3 of the Standard (risk management creates and protects value) the benefits of effective risk management will invariably offset any additional resource costs and generate a net gain as a result of improved organizational outcomes.

For example, the costs of training managers to effectively assess the risks associated with capital projects (and rewarding good performance in this regard) are easily offset by avoiding project delays or budget overruns that commonly result from unrevealed and untreated risks. Similarly, the simple inclusion by the organization's human resources section of a background check on the risk management performance of position applicants as part of a recruitment process can avoid costly errors, expensive retraining, or even the eventual dismissal of an underperforming employee and the costs of further recruitment.

To implement revisions to the risk management framework through a risk management plan does itself require the allocation of some dedicated resources, provision of which should be included in the plan. Such resources might include the time and effort of employees of the organization supplemented, as is necessary, by external specialists. Typical revision tasks that might need to be resourced include the following:

- Drafting of policy statements and procedures.
- Developing methods and tools for elements of the risk management process.
- Working with functional experts to integrate the risk management process into existing organizational processes.
- Developing a risk management plan to achieve the transition.
- Sourcing and configuring a suitable database system to hold risk management information and to produce required reports.
- Developing a strategy for training of people at all levels of the organization (from the governing body downwards) as part of existing general or specialist training. (e.g. as part of induction training or in relation to a process for managing projects).
- Developing a plan for communicating with stakeholders about how the organization manages risk.
- Re-scoping audits of the framework by assurance providers.

4.3.6 Communication, consultation and reporting capability of the framework

Managing risk effectively requires engagement with people both inside and outside the organization, and requires the capture and flow of information to track progress.

---

* Further advice may be found in Standards Australia and the Institute of Internal Auditors Handbook, HB 158: 2010, *Delivering assurance based on ISO 31000:2009 Risk Management.*

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

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.

The framework will need to include the capability to permit engagement with people within and outside the organization. That is, it will need to do the following:

- Consult internal stakeholders (such as managers) who will be expected to undertake specific accountabilities, for example to ensure that the necessary supporting resources are provided.
- Communicate the organization's policy about risk management, both internally and externally.
- Conduct the communication and consultation activities that are part of the risk management process (see Clause 5.2 of the Standard) in a way that achieves the purpose while avoiding undesirable outcomes.
- Capture, store and manage information that is required to internally monitor and review the performance of the framework.
- Capture, store, analyse and report any aspect of risk management information that either needs to be reported to stakeholders (including regulatory agencies) or which, if shared with particular stakeholders, would assist in implementing the organization's risk management intent.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

Providing this capability requires the following:

- Training in the skills of communication and consultation (as explained in more detail in Standards Australia and Standards New Zealand Handbook HB 327:2010) to enable unambiguous, truthful, succinct and respectful communications.
- Procedures and infrastructure that facilitate stakeholders obtaining or requesting legitimate information (e.g. websites or toll-free inquiry numbers).
- Templates, search algorithms and related policies and tools to enable the capture, consolidation and analysis of information, preservation of confidentiality, verification and reporting.
- Software that assists in communication and with consultation.
- Procedures for handling suggestions, commendations and complaints.

To ensure there is the capability within the framework for effective interface with other people, the communication, consultation and reporting needs of each stakeholder should be determined by stakeholder analysis. This should be reviewed periodically as those needs can change.

4.4 IMPLEMENTING RISK MANAGEMENT

Once improvements to the risk management framework have been designed, it is necessary to plan and execute their implementation so that the risk management process is routinely and competently applied to decision making across the organization.

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.

4.4.1 Implementing the framework for managing risk

Having expressed the intent and designed improvements in the capability to manage risk, the organization, whether new or existing, needs to actually implement these components of the framework. As far as possible, this should be achieved through modifications or additions to existing elements of the organization's systems of management with the action list incorporated into the organization-wide risk management plan (refer to Clause 2.12 of this Handbook).

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

Paragraph D2 in Appendix D provides further explanation and advice on implementation that applies to new and existing organizations, including those that have adopted standardized management systems, such as those prescribed, as in ISO 9001, to manage particular groups or types of risk.

A new organization will be able to integrate these components from the outset into the design of its general systems for management, such as those concerned with the following:

- Business and strategic planning.
- Budgeting.
- Safety.
- Recruitment and remuneration.
- Delegations of authority for both expenditure and acceptance of risk.
- Performance management.
- Procurement.
- Project management.
- Capital raising and expenditure.
- Marketing.
- Stakeholder engagement.
- Legal compliance.
- Assurance.
- Management reporting.

For existing organizations, existing organizational functions such as those above will need to be examined to identify where required changes or enhancements are best implemented.

Because risk arises when the organization makes and acts on decisions, implementation of the framework needs to take into account where and when, in the organization's activities, decisions are actually made and acted on. In that way, appropriate aspects of the framework (such as training of the decision makers and the design of each decision making method) can be incorporated at those points.

One way of identifying where decisions are made is to map the organization's processes. Paragraph D3 of Appendix D includes some methods for doing so for both structured and ad hoc types of decision making. The appendix also addresses the issue of making managers and others aware that decisions are being made, particularly those decisions that deal with apparently small operational matters.

Implementing some changes to the framework might encounter resistance or be unsuccessful, unless they are supported by a properly applied organizational change management process that—

- clearly explains the reasons for the change;
- has a realistic timetable;
- provides suitable training and support;
- allocates responsibilities for implementation; and
- measures progress, including by means of a post-implementation review that helps the organization learn from its successes and failures.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

In short, implementing a new or revised risk management framework in a new or existing organization requires careful planning and a methodical approach. Appendix A of this Handbook provides such a process based on a conventional change management approach for making the transition to aligning an organization's framework for managing risk with that anticipated in the Standard.

4.4.2 Implementing the risk management process

Subject to its quality, once implemented, the framework will ensure that the risk management process described in Clause 5 of the Standard is routinely applied to decision making at all levels, so that risk associated with decisions is effectively assessed and treated as necessary, and that controls are routinely monitored and reviewed. Detailed advice for applying the risk management process to decision making is provided in Paragraph D3 of Appendix D of this Handbook.

An improved framework will ensure that any parts of the risk management process that have been conducted poorly (with the result that the organization does not have a current, correct and comprehensive understanding of its risks and its risks are not within its risk criteria) are improved. However, this is an ongoing issue and (as explained in Clause 4.5 of the Standard) ensuring that the process is being applied consistently and correctly is a key function of the arrangements for monitoring and review of the framework.

The following examples of common poor practice in applying the risk management process will probably indicate that some adjustment to the framework is required (such as additional training or improved tools):

- Incomplete establishment of the context. For example, a failure to—
  - (a) clearly articulate the organization's objectives;
  - (b) have a sufficiently comprehensive view of the external and internal environment in which those objectives must be pursued; or
  - (c) set appropriate risk criteria.
- Commencing risk identification without having adopted a systematic approach.
- Inconsistent risk management language and terminology across the organization.
- Inadequate risk analysis resulting in an insufficiently deep understanding of the risk.
- Using risk criteria that are inconsistent with the organization's objectives.
- Not considering multiple options for risk treatment.
- Not placing sufficient emphasis on the use and quality of the two supporting elements of the risk management process (i.e. communication and consultation, and monitoring and review in support of each of the five core steps).

Remediation of such deficiencies is achieved through appropriate adjustments to the organization-wide risk management plan.

4.5 MONITORING, REVIEW AND CONTINUAL IMPROVEMENT OF THE FRAMEWORK

Effective risk management is so fundamental to the success of the organization that any weaknesses (whether through design or application) can be expected to degrade performance against the objectives.

Clauses 4.5 and 4.6 of the Standard explain both why and how the effectiveness of the framework should be continually monitored and reviewed, and improved where appropriate.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

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.

The outcome and attributes tests set out in Annex A of the Standard provide simple but revealing indicators for the effectiveness of the organization's approach to risk management (see Section 6 of this Handbook). Each set of tests serves as an indicator of the other, for example, weak performance on the attributes tests will inevitably result in poor outcomes, whereas the explanation of poor outcomes will be found in all or some of the attributes. The results of structured monitoring and review of the other elements mentioned in Clause 4.5 of the Standard will also provide useful diagnostic advice.

The organization's existing performance management system can be used to monitor and drive the continual improvement of its risk management framework. This can involve the following:

- Setting performance indicators for risk management (see Table 3), that are aligned with organizational performance indicators and reviewed periodically for appropriateness.
- Measuring risk management performance against the performance indicators.
- Periodically reviewing whether the risk management framework, policy and plan are still appropriate.
- Reporting on the effectiveness of the risk management framework, progress against the risk management plan and any major deviations from it.
- Reviewing how well the organization's risk management policy is being followed.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

TABLE 3

EXAMPLES OF PERFORMANCE INDICATORS FOR RISK MANAGEMENT

Indicator type	To show
Success indicators	• The extent to which organizational objectives are being achieved
Process indicators	• The extent to which the risk management process is being applied to decision making • The effectiveness of monitoring and review actions
Outcome indicators	• Risk treatment action completion • Controls are functioning as assumed

Even when the framework is operating as intended, if it can be improved (e.g. by the emergence of new techniques or knowledge) it can be expected that performance against objectives will be enhanced. For example, gaining greater competence in assessing and treating risk or improving the way that risk information is made available to decision makers can make the organization more agile, and therefore more able to quickly, confidently and efficiently realize transient or emergent opportunities. This is also likely to make it more resilient* in the face of unexpected change or developments and, indeed, enable it to achieve the level of resilience it requires.†

Although the evaluation of the performance of the framework should be ongoing, formal review should occur when the organization makes or revises its strategic plan. This is necessary to ensure that the framework is capable of supporting the new plan. For example, if the organization decided to expand through the acquisition of another organization, additional resources might be needed to assess the risk associated with both the acquisition and the subsequent assimilation of the new capacity.

* Resilience—adaptive capacity of an organization in a complex and changing environment (ISO Guide 73:2009, *Risk management—Vocabulary*, Clause 3.8.1.7).

† Although there is an increasing advocacy for organizations having ‘resilience’, the above definition makes clear that resilience exists across a continuum. It is in setting its risk criteria that an organization is able to determine where on that continuum it aspires to be.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

SECTION 5 PROCESS

5.1 WHY A RISK MANAGEMENT PROCESS NEEDS TO BE APPLIED

Annex A of the Standard explains that to manage risk effectively, the organization must achieve the following outcomes:

(a) Have a current, comprehensive and correct understanding of its risks.

(b) Ensure that those risks are within its risk criteria.

To achieve this consistently, a systematic process is needed to reveal and understand risks, and to modify them where necessary. A properly designed framework will both enable and ensure that it will be routinely applied as part of day-to-day management.

This Section of the Handbook describes this process in more detail, providing examples and illustrations of each of its steps.

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.

5.1.1 Design of the risk management process

The risk management process described in the Standard, as illustrated in Figure 2 below, comprises five core steps that although shown sequentially, in practice are applied in an iterative way. These steps allow risk to be detected and understood, and to be modified (treated) if necessary against criteria that are set as part of the process. The effectiveness of these five steps depends on the application to each of those steps of the two supporting steps (communication and consultation, and monitoring and review), as illustrated in the horizontal arrows in Figure 2.

The following considerations explain the design of the risk management process:

- Because risk arises from an organization pursuing its objectives against the uncertainties created by its internal and external environment, a very clear understanding is needed from the outset of both the objectives and these environments.
- Risk is created by and experienced by people, and people are inevitably involved in modifying risk. People also have relevant knowledge and experience, and so need to be part of the process.
- The environment in which the organization pursues its objectives is constantly changing, as indeed can the objectives, and therefore the process needs to both detect such changes and be dynamic if its results are to remain ‘current’.
- There is inevitably some uncertainty about the effect of those things (controls) that are relied upon to modify risk, so ongoing scrutiny is needed to provide both evidence of their actual effects and confidence in their dependability.
- Decisions about risk (particularly whether or not to modify risk) should take into account the efficiency of the options to avoid wastage (of effort and resource).

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

The process illustrated in Figure 2 below has been in wide use in Australia and New Zealand for many years, and has shown itself to be effective and systematic for all types of organization and all types of risk.

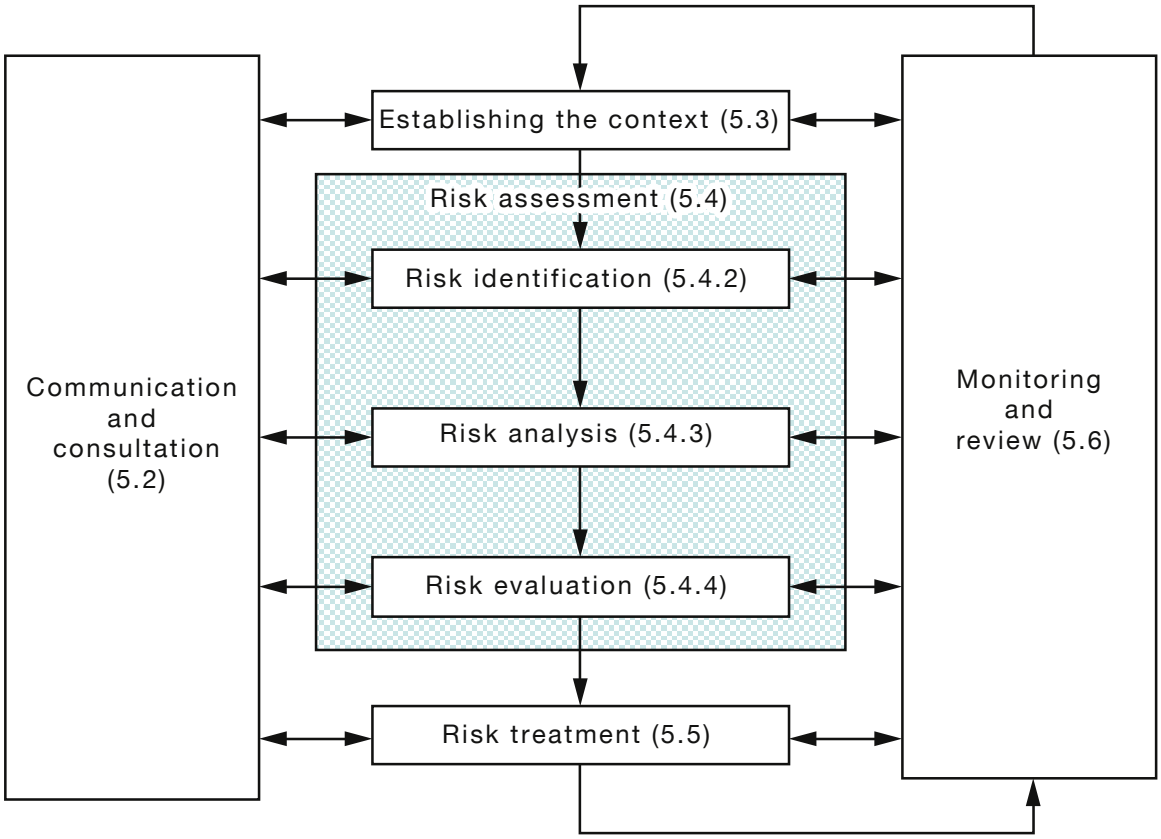

FIGURE 2 RISK MANAGEMENT PROCESS (RELEVANT CLAUSES OF AS/NZS ISO 31000 SHOWN IN PARENTHESES)

5.1.2 Application of the risk management process

The risk management process should be applied whenever—

- someone in an organization makes decisions (to ensure that the risks created or modified by the decision are understood and are within the organization's risk criteria);
- there has been a change to objectives;
- there have been material changes in the internal or external environment; and
- assurance is needed that the present understanding of risks is correct, comprehensive and within the risk criteria.

The process might also be used to fulfil or support compliance with regulation or contract.

The risk management process is applicable to decisions at all levels in an organization including the organization as a whole, departments, teams and individuals and within any activity or function.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

The process must be applied in a way that is fit for purpose. Therefore, the scope, the level of detail and the tools used should be tailored to its end use in each case. The following are brief descriptions of these:

- **Scope**: Within projects there are decisions that might require the project team to make narrow and focused risk assessments that only address the project methods, schedule or budget parameters (e.g. which contractors to use). However, board approval of a new project will require assessment of the risks of the project itself to the organization's overall objectives (e.g. whether the revenues expected to be generated by the project once complete are sustainable).
- **Level of detail**: A decision about approving release of a pharmaceutical item into the market place requires a high level of rigor and detail in the risk assessment, whereas risk assessment to support a decision about which supplier to obtain fuel from can probably be done more quickly and simply.
- **Tools**: Consulting stakeholders in the workplace might be achieved through face-to-face meetings, whereas obtaining the views of the community in which the organization operates might require establishing a website and using sophisticated survey techniques.

The success of the risk management process is dependent on the application of all of its steps. Therefore, if the purpose of a particular activity is focused on one step, this must still be undertaken in a way that has regard to the other steps and so is coherent. For example, in the course of risk analysis, a person with particular analytical skills might be modelling the range of possible consequences. However, that work will only have validity if the modelling task has been informed by the preceding steps of the process, even though the modeller might not have been involved in those steps.

Although the process is shown as a sequence of steps, in reality to be efficient there must be iteration between all the steps as the arrows on Figure 2 attempt to show. It is often necessary to apply the process more than once either as more information becomes available or as decision making becomes more detailed.

Depending on the purpose (including any obligations), the complexity of the issues, the dynamic nature of the operating environment and the time available to make the decision, the process might be applied in a visible way involving, for example, several people at structured meetings or as part of a train of thought (intuitive or otherwise). In either case the process must be fully applied.

The following are examples:

- A military special forces section leader might have a split second in which to make a tactical decision on which personal wellbeing and that of the subordinates as well as the success of the mission, might depend. In that time the leader must recall the objectives, appreciate the external and internal environment, assess the risks, consider the options, review those against the objectives and take the appropriate action. Despite the very short decision making window, the quality of each of these steps must be of the highest standard.
- Senior managers of a university examining disruption-related risks arising from failure of their IT systems will need to consult representatives of IT users, IT system experts, financial experts and external suppliers, examine the sources of risk and the business impacts, and at a series of meetings choose the best combination of making the IT systems more robust and developing contingency plans for their failure.

The risk management process will generally be applied most effectively if there has been appropriate preparation and planning (including preparation for any decisions that need to be made quickly) and the participants have adequate skills. As the process is part of a wider management activity, its timetable needs to have regard to the timetable of that activity.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

5.2 COMMUNICATION AND CONSULTATION

Managing risk necessarily involves people because of the following:

- The interests of people are part of the organization's objectives.
- People will need to take (or not take) particular actions in order for risk to be managed effectively.
- People have some of the knowledge and information on which effective risk management relies.
- Some people might have a right to be informed or consulted.

Communication and consultation are therefore key supporting activities for all parts of the risk management process. The mechanisms set up for communication and consultation and the resources to implement them, are a necessary part of the risk management framework (see Clauses 4.3.6 and 4.3.7 of the Standard).

Communication and consultation are processes and not outcomes. They normally take place with stakeholders (i.e. those persons or organizations that can affect, be affected by or perceive themselves to be affected by a decision or activity). The beneficial effects of communication and consultation are based on exchange of information and persuasion rather than the exercise of power or authority.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

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 analysing 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.

5.2.1 Purpose

The purposes of communication and consultation in the risk management process are to—

- access knowledge and views;
- fulfil obligations of disclosure and transparency (e.g. public bodies are generally expected to act in a transparent way);
- explain what is required of others and obtain their cooperation;
- inform stakeholders.

Communication and consultation therefore helps, for example, to—

- identify risks;
- improve understanding of risks;
- overcome misconceptions;
- ensure that the varied objectives, views, values and other perspectives of stakeholders are both better understood and considered;
- enable stakeholders to understand the views and perspectives of the organization;

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

- ensure that all participants are aware of their roles and responsibilities;
- expedite implementation of decisions;
- strengthen working relationships and partnerships based on trust;
- build confidence in the decisions that are made; and
- bring about any necessary changes in the organization's culture.

In some cases decisions might be improved by involving appropriate stakeholders in the decision making if they will have to take or support actions as a result. Their involvement can lead to ownership of the decisions and the outcomes.

Consequently communication and consultation are an inseparable and indispensable part of the risk management process, and so they should be an explicit part of each of the five core steps.

Communication can also, of itself, be a control (e.g. by providing the public through television advertisements, with knowledge and skills that will make them better able to act optimally in the face of earthquake shaking, flooding or other dangers).

5.2.2 How to communicate and consult effectively

Although the general purpose of communication is to provide others with information, and the purpose of consultation is to seek information, both processes should preferably involve a two-way exchange.

In the case of communication, a two-way exchange helps to ensure that the message has been successfully transmitted. In some cases, such as providing information on websites or in reports, this might require a feedback number or contact point to be provided for those needing more information or clarifications.

In the case of consultation it is necessary to ensure that the party being consulted correctly understands what is being asked and how their response will be handled or taken into account. If an opinion is sought, the party being consulted should be provided with contextual background to facilitate fully considered views. Feedback should be provided to show that responses have been correctly understood and taken into account.

As with any activity, communication and consultation will be more effective if it is planned. A different plan might be needed for different steps in the risk management process or for different activities within each step (e.g. different risk assessments).

Factors to take into account in communication and consultation plans are—

- the objectives and scope of the specific communication or consultation;
- who is to be involved in the process;
- the knowledge, experience, perspectives and capabilities of the other party;
- the intended method and timing; and
- how feedback and evaluation about the plan will be achieved.

To build and maintain trust, communication and consultation should be designed and implemented in a way that will facilitate truthful, relevant, accurate and understandable exchanges of information, taking into account confidential and personal integrity aspects.

The following are examples of common tools for communication and consultation:

One-way

- Distribution of printed material such as letters, leaflets and letterbox drops.
- Newspaper notices, advertisements or articles.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

- Billboards or notices posted at the site of some intended activity.
- Information posted on websites or distributed via social media.

Two-way

- Facilitated workshops (face-to-face or online).
- Focus groups.
- Public meetings.
- Webinars.
- Questionnaires and other forms of survey (via interview, telephone poll, news media, post or online).
- One-on-one discussion and interviews.
- Social media discussion groups.

Standards Australia and Standards New Zealand Handbook HB 327-2010, *Communicating and consulting about risk*, describes in more detail some of the matters that need to be considered when planning communication and consultation. Appendix E of this Handbook discusses some frequently encountered challenges to communication and consultation and provides a range of practical solutions.

5.3 ESTABLISHING THE CONTEXT

5.3.1 General

A key aim of the 'establish the context' step in the risk management process is to identify the organization's objectives, and those external and internal factors that could be a source of uncertainty, so that risk can be identified.

Establishing the context also provides the information that allows the other steps of the risk management process to occur. It therefore involves articulating the following components, having regard to any anticipated changes over time:

(a) Objectives.

(b) Internal and external environment.

(c) Stakeholders.

(d) Purpose, scope and circumstances of the particular risk management activity.

(e) Risk criteria.

If this step is not done thoroughly and competently it will affect the value and validity of the rest of the process, and will lead to an unreliable assessment of risk and, possibly, the selection of inappropriate risk treatments. Establishing the context should consider the best prediction of the future situation (and specifically take into account uncertainty about the future). Monitoring and review is required to ensure that the predicted aspects of context remain valid.

Clause 5.3 of the Standard specifies the requirement for establishing the context as part of the risk management process.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

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.

The parts of establishing the context are shown in Figure 3. The numbers refer to the clauses in the Standard.

FIGURE 3 PARTS OF ESTABLISHING THE CONTEXT (CLAUSES OF THE STANDARD ARE SHOWN IN PARENTHESES)

5.3.1.1 *How to articulate objectives*

The objectives of an organization, as referred to in the Standard, are the highest expression of its intent and purpose. The objectives are the outcomes that it is seeking in all it does. They might take into account the interests of stakeholders and will usually include compliance with the law.

Objectives typically reflect the organization's explicit and implicit goals, values and imperatives. The objectives should not be confused with the plans (strategic, project or operational) through which the organization pursues its purpose.

In the case of statutory organizations, high-level objectives are typically set by the relevant enabling legislation.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

Divisions or departments of complex organizations might have subordinate objectives that need to be considered in conjunction with those of the organization as a whole. However, if the subordinate objectives are not consistent with the organization's overarching objectives, this in itself will give rise to risk, as sometimes occurs with projects where those responsible for the execution of the project either lose sight of or are unaware of the big picture.

In order to assess risks, objectives need to be expressed clearly and unambiguously so that risks (i.e. the effect of uncertainty on these objectives) can be assessed.

Most organizations have more than one objective and so must make their decisions (which usually affect more than one objective) taking into account the risk that is created by each objective. This might require a decision to be adjusted if the resulting risks that would be created for one set of objectives are unacceptable, even though those for another objective are acceptable.

Example

A manufacturing organization includes among its high level objectives the following:

(a) To grow its revenue and profit by 20% per annum.

(b) To protect and enhance its reputation as an ethical and nationally owned business.

It is exposed to strong competition and is operating in a country with high levels of national employment and high employment costs.

In pursuit of Objective (a) it proposed to relocate its customer service and new business call centre to another, unregulated market with lower employment costs. Assessment of the risk of this tentative decision shows in the short term this strategy would present a relatively low level of risk in terms of Objective (a) but, through onshore competitors providing disinformation to the media, there was a relatively high likelihood that its carefully nourished reputation would suffer badly almost immediately and in time this would negatively affect revenue. To treat this latter risk, it decided to revise its decision by also implementing some safeguards concerning protection of privacy, establishing detailed quality procedures, creating an independent call centre complaint service with transparent reporting, and beginning a publicity campaign to explain the benefits to its customers of the improved efficiencies. Risk assessment showed this revised approach would slightly increase the level of profit-related risk and substantially lower the level of reputation-related risk.

5.3.1.2 *How to identify stakeholders and their objectives*

Establishing the context also involves identifying key stakeholders who might be affected by a decision, both external and internal to the organization, and developing an understanding of their objectives and characteristics.

The views of stakeholders can also be an input into the development of risk criteria.

External stakeholders might include the following:

- Legislators and regulators.
- The people in the community in which the organization operates.
- Special interest groups.
- Contractors and suppliers.
- Customers and clients.
- Emergency services organizations.
- Creditors.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

- Providers of funding.
- The media.

Internal stakeholders include managers and staff at all levels and shareholders, members or, in statutory organizations, the relevant ministers or cabinet officers.

As with the external and internal environment, stakeholders are normally identified using some systematic method, often brainstorming, that employs the experience and knowledge of a group people. Each stakeholder is recorded in the statement of context (see Clause 5.3.6 of this Handbook) together with note of those of their objectives that are relevant to the decision being made.

Often the communication needs of each stakeholder are also identified at this time to help with planning communication and consultation.

5.3.1.3 *How to articulate the external and internal environment*

Central to this essential preparatory step is a clear understanding of its purpose and the relevance of the external and internal environment to later steps in the risk management process. Together with the previous step involving articulating the organization's objectives, this step reveals and enables the assessment of the risks associated with particular decisions (and of any resulting actions). The information will also be of great importance, subsequently, in the design of risk treatments should these be necessary, and will guide the way in which risk management activity is structured and implemented.

The internal and external environments are therefore described by the factors within and outside the organization that might influence how particular decisions (or resulting actions) could affect the organization achieving its objectives. Such factors will be the source of certainty or, for those elements that the organization is not necessarily able to control or predict how they will perform, uncertainty.

Illustrative examples of these factors are given in Clauses 5.3.2 (external context) and 5.3.3 (internal context) of the Standard, but no such list can be exhaustive. For this reason, a systematic approach is needed that is tailored to both the organization and its objectives, and the particular decision that is to be subject to risk assessment.

Systematic approaches that draw on the experience and knowledge of a group of internal (and sometimes external) stakeholders are usually the most effective.

Although there will be many external and internal factors that will be relevant to all decisions, because of the variability of organizations, objectives and decisions, there is no rule of thumb that can be followed to identify the external and internal context in all cases. Furthermore, what might work well for one type of decision will not be appropriate for others. Usually, however, starting with simple tests can help to focus thinking. These tests can be questions such as the following:

- What will constrain us?
- What will enable us?
- What will we be relying on?
- What will we encounter?
- What might change?

This list of questions can be expanded or amended as necessary.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

Using questions of this nature, an understanding of the relevant factors of external environment can be gained by applying common knowledge and also reviewing a wide variety of information sources, from government and scientific documents to commercial information and experts. Possible sources of information include the following:

- Laws and regulations.
- Newspapers.
- Electronic media.
- Newsletters, magazines, journals and books.
- Reports and presentations.
- Interviews with experts or specialists.

The relevant internal factors may be similarly identified through discussions with experts and managers familiar with the subject of interest or type of decision under consideration, and through the examination of relevant documents.

Documents from which relevant information on the internal environment might be obtained include the strategic plan, business plans and budgets, annual reports, economic analyses, organizational charts, and any other documentation expressing the organization's values, ambitions, obligations, vision and purpose. Data from the organization's information system provides useful information regarding its operations and supply chain.

Another technique that can, in some cases, improve awareness of the elements of both the external and internal environment is to prepare a flow chart of the activities of the organization relevant to the decision in question, noting inputs, constraints, dependencies, outputs and opportunities along the path.

Strategic analyses such as the SWOT method (strengths, weaknesses, opportunities and threats), the PEST method (political, economic, social and technological) or value chain analysis might also be valuable, as they assist in revealing some relevant aspects of the external and internal environment. Care should be taken, however, that these methods are only used to define relevant factors from the external or internal environment, and not to attempt to identify risks.

The outputs of this part of establishing the context should be two lists of relevant factors (external and internal), and for each factor, the related sources of uncertainty (i.e. the 'so what' consideration).

Furthermore, any factors (such as the organization's management structure legal obligations or culture) that will need to be taken into account when conducting risk assessment, designing treatments or planning monitoring and review, and communication and consultation, should also be noted.

These lists will form part of the statement of context referred to and described in Clause 5.3.6 of this Handbook.

5.3.2 The external environment

Unlike many features of the internal environment, those in the external environment can often not be controlled by the organization (e.g. the weather, the law, the currency exchange rate or the behaviour of competitors). At most, the organization might only be able to influence them (e.g. making submissions about government policy, vetting the quality practices of suppliers or maintaining influence over their quality practices through contractual obligations).

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

To ensure that it obtains the earliest possible warning of change, the organization should regularly monitor those features of the external environment that provide significant uncertainty. Depending on the expected volatility, such monitoring could be undertaken either monthly or semi-annually. While the relevant features will typically be different for each organization, what is relevant might also change over time.

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 The internal environment

The internal environment characterizes the way that the organization is structured and operates, including the resources it has available and the people in it. Although many of these features can be directly controlled by the organization, their effect and the manner in which they operate in practice is not always predictable, and therefore can still be a source of uncertainty.

Understanding the internal environment is also important because any application of the risk management process needs to align with the organization's culture, processes, structure and strategy if it is to be effective. Also, internal factors might be risk sources and the internal environment will need to be taken into account when subsequently deciding how risks are treated.

The organization's culture is an important aspect of the internal environment. It includes a range of attitudes and beliefs that can either contribute to or hinder the application of risk assessment decision making and the ongoing effectiveness of controls. It can, therefore, constitute a risk source and either help or frustrate attempts to treat risk.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

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 Articulating the context of the risk management process

The risk management process might be applied to decisions of the organization as a whole, to those of particular sections or in relation to particular projects or activities. It can also apply to all processes affecting the organization's objectives or to just those of particular interest at the time.

The Standard uses the term 'context of the risk management process' to refer to a particular application of the risk management process, and this therefore will vary from task to task. For example, one use of the process might be to update the organization's overall understanding of its risks. Another, at the opposite end of the scale, could be to examine the risks associated with a change in legislation or a small change in operational practices.

Making sure that the exact purpose and scope of each particular risk management activity is clear, coordinated with the overall risk management arrangements, and suitably structured and resourced is an example of tailoring, as per Principle (g) of the Standard (see Clause 3.2 of this Handbook).

There are three elements to this part of establishing the context, these determine the following:

(a) The purpose, scope and circumstances of the risk management activity.

(b) A structure and approach for the risk management activity.

(c) The resources, techniques and tools needed for the risk management activity.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

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.

5.3.4.1 *How to articulate the purpose, scope and circumstances*

The exact purpose and scope of each particular risk management activity should be defined before it takes place. The risk management activity should be planned consistent with its scope and purpose, and this should include suitable structuring and resourcing of the activity.

Whatever the purpose and scope of the activity, it should be clearly articulated so that all who will be involved are clear as to what is to be done. The scope should include any decisions that will be supported or influence by it. For example, the purpose might be to assess the risks associated with outsourcing in order to decide whether to outsource, the controls that should apply or whether to retain the activity in house.

Although aspects of the risk management process might occur in isolation (e.g. the statistical analysis of relevant data) the way in which this occurs should be informed by the preceding and subsequent steps in the process. Therefore the following should be defined:

- **The purpose of the particular application of the process.** For example, the purpose might be to assess risks associated with outsourcing in order to decide whether to outsource or retain an activity in house, or the setting might be that this decision has been made and the purpose is to decide how risks should be treated.
- **The decisions which are to be made.** For example, whether or not to treat the risk, or whether the risk is within the organization's risk criteria.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

- **Who will make the decision.** This will affect the scope of risk management activities to be carried out, the resources needed, the tools and techniques which are applied, and the way in which results are communicated.
- **The particular risk criteria that are to be applied.** These might be a more detailed expression of the overall criteria set by the organization, for example, they might be specific legislative criteria which apply to the particular setting or criteria defined by the organization for specific projects.
- **What is to be achieved, and by when**. For example, the assessment of the risks of the organization's draft strategic plan, or a particular project or task, or a review of the ongoing adequacy of existing controls.
- **What is included or excluded.** For example, only risks arising from particular risk sources or of a particular type, or relating to a particular division of the organization.
- **Who is responsible for the implementing this activity.**
- **The circumstances in which it takes place.** That is, a description of the parts of the organization involved and the processes affected, service or product under consideration.

5.3.4.2 *How to define the structure of the risk management activity*

It is less likely that risks will be overlooked and the process will prove more practicable if whatever is being examined is considered logically in smaller parts (often called key elements). The level of subdivision applied (which might be hierarchical) will depend on the purpose, scope and setting of the application of the process.

The following are examples:

- If the risks associated with an organization as a whole are to be considered, this could be done by looking at either each organizational unit or each location separately.
- A project might be divided into its elements (e.g. via a work breakdown structure or by contract structure).
- A process might be divided by considering the blocks of a flow chart.
- Areas of responsibility as defined by an organizational chart.

Subdivision will also help show whether special expertise is needed to understand particular elements. Suitable experts can then be involved in appropriate parts of the risk management activity.

One simple way to create key elements is by grouping together (or chunking) the external and internal environmental factors that were identified when the context was established.

After examining the pieces, the whole should also be considered to ensure that the big picture is not lost.

5.3.4.3 *Deciding on the resources, techniques and tools*

The resources, techniques and tools needed for the risk management activity should also be planned and available to ensure that it is successful. This planning requires consideration of the following:

- The methodologies to be used (e.g. whether to use workshops in order to capture collective knowledge or judgement, or whether to use individual desk study, and whether quantitative or qualitative approaches are to be used).
- The resources required (e.g. venues, projectors, access to the organization's risk management information system, technical specialists, drawings, documents, and incident or performance data).

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

- The timing and logistics of the each session.
- How the output will be captured, recorded and, where required, communicated.

Advice on the general nature and selection of risk assessment techniques is contained in Standards Australia and Standards New Zealand Handbook HB 89:2013.

Importantly, such planning should include a method for determining whether the risk management activity was successful or not and the lessons learnt.

5.3.5 Defining risk criteria

The expression 'risk criteria' is used in two ways in the Standard. It provides both the means to determine and express the magnitude of risk, and to judge its significance against predetermined levels of concern. They comprise internal procedural rules selected by the organization for analysing and then evaluating the significance of risk, and are also used when selecting between potential risk treatments.

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

The fundamental role of risk criteria in the risk management process means that they should be determined or endorsed at the highest levels of the organization (i.e. the governing body or top management) and once established, applied throughout the organization whenever the risk management process is being applied.

More detailed or specific expression of these criteria might be required for a particular application of the process (e.g. for assessing the risk related to a project). However, any such amplification must be consistent with the overarching criteria.

The form of risk criteria will depend on the nature of the organization's objectives and the needs of decisions makers when the risk management process is applied in support of particular decisions. In all cases, the description of the organization's risk criteria has three elements:

- The method(s) to be used to express and measure consequence and likelihood (whether qualitative or quantitative).
- The method(s) to be used to combine consequences and their likelihoods and then to express the resulting level of risk.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

- The organization's internal rules for accepting (or tolerating) particular risks as well as risk in the aggregate.

The risk criteria may also specify who in the organization is authorized to accept risk of a particular type or level.

Risk criteria are derived from an organization's objectives, its risk management policy and strategic intent (which form part of the internal context) and take into account the organization's risk attitude (see box aside), the views of its key stakeholders as well as requirements of any external regulations with which the organization intends to comply. Criteria are, therefore, unique to the organization, and so normally it is not possible or appropriate for one organization to copy its criteria from another organization.

Risk attitude and risk appetite

The term 'risk attitude' (defined as the *organization's approach to assess and eventually pursue, retain, take or turn away from risk*) is used in the Standard rather than 'risk appetite' for two reasons—it is a wider term (risk appetite is defined in ISO Guide 73 as *the amount and type of risk that an organization is willing to pursue or retain*) and also translates better into some other languages, a necessary consideration in the drafting of ISO 31000. However, some organizations are subjected to external requirements or recommendations to prepare a risk appetite statement. As a general rule, the underlying intent of any such requirement will be met by clearly expressing its risk criteria, as explained in this Handbook.

As with the other parts of establishing the context, risk criteria will need to be developed before risk assessment takes place, although insights subsequently gained through risk assessment might require the risk criteria to be revisited and expanded, or adjusted in keeping with the iterative nature of the risk management process.

Risk criteria should be documented, and in some cases communicated to relevant stakeholders to facilitate understanding and consistent application. However, in some cases the communication of risk criteria to all stakeholders might be sensitive for commercial or other reasons.

Risk criteria should be reviewed periodically and updated to ensure that they continue to reflect the values and objectives of the organization and its key stakeholders.

Detailed advice on a selection of methods for developing risk criteria is given in Appendix C of this Handbook but in all cases, when setting risk criteria the following general steps should be followed.

Tips

To set risk criteria, follow these steps:

1. List the sought after outcomes for each objective
2. Select measures and scales for each outcome to characterize consequences
3. Decide how likelihood will be expressed
4. Decide how consequences and likelihood will be combined to derive the level of risk
5. Decide how the level of risk will be expressed;
6. Establish the rules for evaluating risk.

1 List outcomes for each objective

In forming the criteria the desired outcomes for each of the organization's objectives should be specifically identified (in some cases these might already be expressed through key performance measures).

For example, if one of an organization's objectives is continual growth, it is necessary to consider which categories of performance would, for that organization, best characterize growth. A university's outcomes might include any of student enrolments, percentage of foreign students, extent of social inclusion, research income, or academic success. For a farm, these outcomes might include how many vegetables it sells, the annual increase in income, or the proportional increase in the number and diversity of its customers.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

If an objective includes a timeframe, this should be reflected in the associated outcomes.

2 Select measures and scales for each outcome to characterize consequences

For each outcome it is necessary to consider meaningful measures, whether quantitative or qualitative, which reflect the degree of success in achieving the underlying objective. There must be an appropriate scale on which to express each measure. These are then used to express consequences.

The consequence measures are not necessarily the same for each outcome. Therefore, when outcome measures are expressed on scales (for both consequences and their likelihoods) the graduation of the scales should reflect the nature of the objective and the tolerance for variation in that outcome.

In the example above, in terms of its growth objective, a university might see a percentage increase in student numbers as being more significant than a comparable percentage increase in revenue. A farm might view the increased diversification of its income as more significant than a simple increase in revenue.

Any uncertainties in the measurement of consequence (e.g. if it has been estimated) should be made clear. In some cases, it might be more appropriate to characterize consequences as a distribution rather than a single value (refer to Paragraph C3 of this Handbook for guidance about the use of distributions).

The scales used to represent the extent of consequences must be designed carefully. If not, then either the level of risk is not assessed properly or incorrect choices are made to accept or treat the risks.

The necessary attributes of a consequence scale include the following:

- The range of the scale includes the upper values that could possibly occur and even beyond to ensure that rare high-consequence conditions are not missed in risk assessment;
- The granularity (i.e. the number of steps and the interval between steps) of the scale is—
    - finest at the point where the consequences from most events are expected to occur;
    - precise enough to discriminate between acceptable and unacceptable levels of risk; and
    - useful in determining which treatments should be implemented.

The above may mean that the intervals represented by a scale may not be regular.

3 Decide how likelihood will be expressed

Likelihood of experiencing the particular consequences may be measured in terms of probabilities or frequencies or by using descriptive scales. The latter will be appropriate where reliance must be placed more on judgement and experience than solely on data.

Probability is always expressed as a number between 0 and 1 for a particular condition or situation. For example, we can say that a consequence has a probability of 0.5 of occurring during a particular activity over a particular time frame. However, for there to be risk, probability cannot be either 0 or 1.

Any uncertainties in the measurement of likelihood (e.g. if it has been estimated) should be made clear. In some cases, it might be more appropriate to characterize the likelihood as a range rather than a single value.

Even where data is available, the characteristics of the stakeholders might mean that descriptive scales (even if based entirely on quantitative data) are more useful.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

Stakeholder interests and perceptions should also be considered when selecting likelihood scales. For example, it may be more helpful to express likelihood in terms of a return period (i.e. every 'n' years) rather in terms of chances per year.

Different measures of likelihood might be appropriate for different types of consequence. The choice of likelihood measure will depend on the availability of data and the resources available for the subsequent analysis. In all cases, the relevant time frames of interest will need to be considered.

4 Decide how consequences and likelihood will be combined to derive the level of risk

To determine the level of risk, measures of consequence and their likelihood have to be combined in a way that reflects the organization's risk attitude and the way in which the risk assessment is to be used in decision making. Deriving the level of risk may be done qualitatively (descriptively), semi-quantitatively (using ordinal scales) or quantitatively (using ratio scales).

Often quantitative risk analysis is not justified unless the significance of the decision to be made is substantial (e.g. a major acquisition or release of a new drug), the data to support the analysis is available and reliable, and most importantly decision makers need and are able to utilize quantitative results. If these requirements are not satisfied, qualitative analysis might be more appropriate. Notwithstanding these considerations, the form of analysis might be specified through external requirements, such as in regulations or supply contracts.

When the level of risk is expressed quantitatively units must be specified. For example, the level in a criterion of 'increase in student numbers' should be expressed as 'more than 5000 full time equivalent enrolments in the academic year'.

The nature and limitations of each of the possible types of scales are described in Table 4. These limitations are important to take into account when determining risk criteria (and later risk assessment). For example, where ordinal scales are used to estimate consequences or likelihoods, combining them by multiplying them will produce unreliable or illusory results. The same limitation also applies to interval type scales where certain types (decile or logarithmic) can only be added and cannot be multiplied.

If quantitative measures are involved, they can be combined arithmetically as a product expressed in absolute terms as an estimated value. They can also be plotted on a graph or combined through some other more complex computation.

Alternatively, where ordinal scales are involved a matrix can be used to display the combination of measures of consequences and their likelihoods. Further advice on this is given in Appendix C of this Handbook.

Whatever method of combination is chosen, the reason for that choice should be understood. In other words, the method should reflect the purpose and the intended uses.

If the organization wishes to consider risks in the aggregate (e.g. the level of risk to which a particular business unit of the organization is exposed for several objectives) then the aggregate level of risk can be obtained from summing the appropriate form of combination of each consequence likelihood pair for each risk. However, this is only valid if these individual combinations form proper interval or ratio scales and the consequences are expressed in units commensurate over the individual scales.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

5 Determine how the level of risk will be expressed

The level of risk can be expressed in several ways. For example, using a simple scale from high to low, by a precise numerical result, on a colour-coded matrix, or by presenting the results as a distribution of values. The following factors should be considered:

- Simple labels such as 'high', 'medium' and 'low' are suitable in many cases provided that all people who use them have the same understanding of what they mean, including whether they represent a linear progression. If such labels are not properly defined they might be perceived differently by different people, and this will lead to inconsistency in decision making and risk treatment.
- Colour coding the level of risk in diagrams such as matrices can help if the users of the diagram understand the meaning, on that particular matrix, of each of the selected colours, and therefore the relative levels of risk represented by each colour. For example, if the highest level of risk is coloured red some people, by drawing analogy with traffic lights, might assume that this means that the activity concerned must stop immediately. Others might conclude the red simply means danger and that high levels of risk are not acceptable under any circumstances. Neither of these might be true.
- Often, simple numerical or alphabetical labels together with keys and clear explanations can overcome these problems of perception and understanding.
- In most cases, a level of risk will be linked to both an authority to accept such a level of risk (including the seniority of those authorized to make such a decision on behalf of the organization) and to some priority for treatment if the risk exceeds the criteria.
- There is little point having many levels of risk (and labels for these) if the organization cannot meaningfully resolve and respond to that level of resolution. On the other hand, too few graduations means that within one level (or colour) there can be quite a wide range of values making it more difficult to realistically portray the risk, especially if there is significant uncertainty in the analysis. In practice, this normally will mean that four or five levels are sufficient although the number of graduations of consequences and likelihood need not be symmetrical.
- Distributions (such as 'S' graphs showing cumulative distributions, FN curves, etc.) are useful to represent an aggregated set of risks subject to them being expressed on the same ratio scale, as well as for specific risks. Inference may be drawn from the shape of the curve and the points at which it intersects or becomes parallel to axes. This information and the position of the curve relative to a criterion line or lines may then be used in risk evaluation and to inform risk treatment.

6 Establish the rules for evaluating risk

A rule set for evaluating risk (including by whom and when evaluation should be undertaken) should be developed in order to determine whether to accept (tolerate)* or treat risk. The rule set should provide decision-support that helps determine the following:

- Whether all or some risks are to be considered in the aggregate with other risks.
- Whether the risk is insignificant or otherwise acceptable and needs no further consideration (other than ongoing monitoring and review).
- Whether, irrespective of the level of risk, the organization would obtain benefit overall from treating the risk, either to lower or raise the level of risk or to introduce additional risks.
- Any preferred priorities for treatment.

---

* The definitions of 'risk acceptance' and 'risk tolerance' in ISO Guide 73 are substantially the same, even though there is a common perception that the latter implies reluctant acceptance. In practice, the result is the same—the organization will experience the risk concerned.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

- The relative urgency for completion of treatment plans (i.e. for implementation of a risk treatment) and continued tolerance of a level of risk pending completion.
- The potentially valid forms of treatment.
- Whether an action that is generating or would generate particular levels of risk can be proceeded with.
- Whether more information is needed in order to make decision.

Such considerations should, in all cases, be directed to obtaining greater certainty that the organization's objectives will be achieved.

The rule set may also include specific authorities to accept risk based on level or type of risk, or in some cases, where the level of risk would otherwise be much higher were it not for a single control, dependency on critical controls. (In such cases, the risk management framework should include a system of formal delegated authorities for acceptance of risk arranged in a similar manner to the common practice of delegated authorities to incur particular levels of expenditure.)

The evaluation rule set is developed as part of the risk criteria to ensure they are compatible. For example, if the risk criteria include restrictions on authority to accept risk according to the level of risk, the risk evaluation should only be performed or approved by a person with such authority.

The risk evaluation rule set might also stipulate when in a specified decision making process, risk is to be evaluated. (For example, in a project there might be a requirement for risk related to financial viability and ethical veracity to be evaluated at particular stages before the project can proceed to the next stage.)

If the risk criteria include prohibitions on acceptance of particular types of risk if the level of risk is above particular limits (e.g. as is implicit in the ALARP* concept) the evaluation rule set might specify what is to happen (e.g. immediate cessation of the risky activity) if the risk analysis detects such levels.

* ALARP is the acronym for as low as is reasonably practicable. See Paragraph C2.6, Appendix C.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

TABLE 4

TYPES OF MEASUREMENT SCALES AND APPLICABILITY

Type of scale	Description	Limitations/freedoms	Level of risk example	Conceptual explanation
Nominal	Assigns data into categories	No mathematical operation can be performed.	Lists or classifications of wildlife, cultural patterns, land use, etc.	Colour (classification), texture, plant genus.
Ordinal	Comparative scales—can be judged as more than or less than a given level	Not measures of absolute magnitude, only relative. Summation is arbitrary in absence of zero points. Ordinal scale of likelihood cannot be combined with ordinal scales of consequence in any way.	Rankings such as high, medium, low or 1, 2, 3, 4, 5 where numerical value does not relate to value or quantity (i.e. level 2 might not be twice as big as level 1).	Cold, warm, hot.
Interval	Quantitative intervals between units of measurement are constant (10 exceeds 9 as 2 exceeds 1)	Can add/subtract or divide/multiply by a constant only. Amalgamation possible only if defined equal points on all scales (e.g. a deficit of 2 is not twice 1, since redefining the zero point could transform value 2 to 5 and value 1 to 4.	A scale such as 1, 2, 3...9, 10, where numerical value has some meaning but zero point is arbitrary.	10° of temperature. 20° of temperature. 30° of temperature (but set point [0°] is not defined).
Ratio	Quantitative—similar to interval scale, but with set or non-arbitrary set point.	Measures magnitude or significance. Can be mathematically combined provided units are same or suitable conversion applied.	A measure of effect where zero point is set as no effect.	A scale such as ‘no loss’, $1 loss’, ‘$2 loss’, etc.

5.3.6 The statement of context

The output from the establishing the context step of the risk management process will need to be captured in a way that the output can be consistently applied and also monitored for change. This is best achieved by preserving it in a statement of context. This statement provides the principal input to the risk assessment process, as well as demonstrating that important issues for the organization as a whole were understood and have been taken into account in the way the risk management process is applied.

Although each application of the risk management process requires a statement of context, there will be many components of the statement that will be common to all such applications across the organization, unless, of course, changes to objectives or the internal and external environment have occurred, or there are new stakeholders or the organization has changed its risk criteria. That is why some organizations provide a common core statement of context (updated from time to time as necessary) leaving its branches or divisions to add additional (non-conflicting) information to suit each particular risk management activity.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

Apart from providing the source document on which the remaining steps of the process are based, the statement of context also records and makes transparent, the basis on which risks were assessed and decisions were made whether and how to treat the risk at any particular time. It also records with whom communication and consultation occurred and why the monitoring and review step was followed.

The statement of context should identify the following:

- Organizational objectives and success measures.
- Important factors within the internal and external environment, including the velocity at which change can be expected.
- Relevant stakeholders and their objectives.
- Risk criteria.
- Documents and people consulted in establishing the context.
- The date the statement was developed and recorded, the author(s), and (depending on the purpose) the scope and setting of the particular risk management activity.
- A structure for the risk management activity.
- The resources, techniques and tools needed for the risk management activity.

If any elements of the context subsequently change, it can be expected that risks will also change as will the actual effect of controls and validity of risk treatments. A statement of context dated with the time at which it was established facilitates ongoing monitoring and review and adjustment of the risk assessment.

5.4 RISK ASSESSMENT

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.

5.4.1 General

Risk assessment enables an organization to—

- find or recognize its risks;
- understand its risks so that subsequently their significance can be judged and the level of risk can be evaluated in terms of the organization's risk criteria;
- appreciate whether the risk should be accepted or modified; and
- consider the relative modifying effect of different risk treatment options.

Risk assessment requires that the context is established beforehand. For example, unless risk criteria have been defined (Clause 5.3.5 of the Standard) before risk assessment there is no basis for risk analysis and risk evaluation.

Effective risk assessment will normally involve iteration between its three steps and the other steps of the risk management process. It might also be necessary to conduct risk assessment or one or other of its individual steps more than once, either as more information becomes available or as decision making requires greater resolution and accuracy. Iteration between risk analysis and risk treatment when treatment options are being considered and evaluated will help reveal the actual effect of each candidate treatment.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

The outputs from risk assessment then support decisions on whether risks should be treated and the best ways that this can be achieved.

The structure of risk assessment and the resources, techniques and tools needed are determined when the risk management context is established (Clause 5.3.4 of the Standard). Decisions will therefore be required on the following examples:

- What, if any, prior research will be required (e.g. obtaining statistical data that might help in the determination of likelihood)?
- Who will lead or facilitate any workshops or meetings?
- Who will attend workshops or meetings?
- Which specialist staff will be involved?
- Which (if any) internal and external stakeholders will be consulted, and might be involved in workshops and meetings?
- How the results of the risk assessment will be communicated to internal and external stakeholders?

An important resource for risk assessment is up to date and reliable data and information as required by Principle (f) in Clause 3 of the Standard. Risk assessments can be undertaken with varying degrees of detail that depend on the purpose of the assessment, and the information, data and resources available. A comprehensive assessment should be undertaken to allow the organization to identify the following:

- If the characteristics of the risk, when compared with criteria, will be acceptable or tolerable or will need to be modified (i.e. treated).
- The actual modifying effect of existing controls.
- Those risks where more detailed risk analysis is required so that the risk can be better understood, and so that appropriate treatment can be planned and implemented.

Confidence in the estimates of the level of risk, and their sensitivity to preconditions and assumptions, should be considered in the assessment 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 the limitations on modelling, should be stated and can be highlighted. Sensitivity testing should be used to demonstrate the sensitivity of the level of risk to sources of uncertainty.

The following sections consider each of the three steps of risk assessment in greater detail.

5.4.2 Risk identification

Carried out thoroughly, the risk identification step will reveal what, where, when, why and how something could happen or occur and the range of possible effects on objectives. In some cases, these effects (i.e. consequences) might only occur at some future point or will be experienced, at a fixed or variable rate, over time. Such considerations should form part of the risk identification.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

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.

Although risk identification should be comprehensive (and therefore consider all significant causes and consequences), it does not have to describe every possible outcome or every stage of every possible sequence of cause and effect. Its purpose is to identify sufficient events to characterize the risk so that there is a reliable basis for risk analysis, then evaluation and, if required, risk treatment.

To ensure that risk identification is efficient and the outputs are reliable it should be—

- systematic;
- based on the best available information;
- collaborative; and
- properly recorded.

These criteria are described in more detail below.

1 Systematic

Adopting a system for risk identification will help ensure that it is comprehensive and repeatable, and produces reliable output. A system will also help counteract any cognitive bias and also ensure that this step in the risk management process is efficient.

Using the key element structure developed when the risk management context was established can help ensure that the method used is comprehensive.

The method selected for risk identification should take into account the following:

- Complexity of the scope and setting for the risk assessment.
- Resources available for risk identification.
- Purpose of the risk assessment.
- Needs of decision makers.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

Standards Australia and Standards New Zealand Handbook HB 89:2013 contains a list of techniques for risk identification together with advice on how these should be selected and applied. These techniques include the following:

- Data-based techniques, such as analysis of historical data, modelling or simulation.
- Structured techniques that stimulate a group of people to apply their knowledge and experience of what can happen, why it can happen and what it can lead to. Examples of this type of methodology are HAZOP, failure mode and effects analysis, and scenario analysis.
- Eliciting information from stakeholders through techniques such as brainstorming and structured interviews.
- Research and testing such as reviewing literature or testing whether a component or process might fail.

2 Based on best available information

As required by Principle (f) in Clause 3 of the Standard, risk identification should be based on the best available information. In preparing for risk identification, relevant historical data should be compiled and analysed. The experience of similar organizations might also be useful. Stakeholders can provide useful information based on their experience, and they should be involved through communication and consultation.

Normally much of the information and data required for risk identification will have been gathered as part of establishing the context (Clause 5.3 of the Standard).

The sources of the information that form the basis for risk identification should be recorded so that they can be checked if required. This will also allow any future changes to this information to be detected as part of monitor and review so that the risk can be reassessed.

3 Collaborative

Stakeholders should be involved in risk identification because they will—

- have a wide range of relevant experience of what can happen and what it can lead to;
- have views, values and other perspectives that will help overcome bias;
- gain a better understanding of risks and be able to overcome any misconceptions;
- appreciate the need for risk treatment if this is required and help expedite this; and
- build their confidence in the decisions that are made.

4 Properly recorded

The risks identified should be recorded in a suitable form so that the output from this step can be preserved, accessed and reviewed.* The minimum information required for the subsequent steps of the risk management process is the following:

- What could happen or occur.

---

* Sometimes, because it is perceived that necessary risk treatments are beyond the power of the organization to implement, the risk is not recorded. This practice should not occur. In other cases, for reasons of internal or external sensitivities, risks that are revealed or known about are not documented (e.g. risks associated with incompetency of senior managers). This practice may be valid provided that senior management are made fully aware of the risk. The guideline always is that risk is risk and therefore should be known to the organization.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

- What it could lead to in term of the range of possible effects on the organization's objectives.
- The reasons why these effects might occur, including the risk sources and any necessary preconditions or event sequences.

As with all steps of the risk management process, risk identification should be iterative and repeated until a level of resolution and accuracy is obtained that is sufficient for the decisions concerned.

A different method of risk identification might be needed for subsequent risk assessments with a different or narrower scope. For example, an organization that wants to decide on whether it should invest in large capital project might initially use brainstorming to identify a broad range of risks. If this shows that uncertainty arising from the performance of a contractor could seriously affect the organization's objective to protect and enhance its brand, then a subsequent assessment involving a form of HAZOP might be used to more precisely recognize the risks caused by the terms of the draft contract.

Sets of risks can also be collated or combined where a lower level of resolution is required. The basis for the collation can be those associated with a particular objective or a common risk source.

A record should be made and preserved that identifies the date of the statement of context from which the risks were identified and describes the following:

- Risk identification method or methods used.
- People involved.
- Data and information sources consulted.
- The risks.

Tips

For effective risk identification—

1. Ensure that the context is fully established;
2. Chunk up the subject matter into key elements and adhere to these when identifying the risks;
3. Gather, consolidate and analyse relevant historical information and data beforehand;
4. Involve people with wide ranges of experience;
5. Adopt a systematic method to ensure that all risk sources that could affect the achievement of objectives are identified;
6. Ensure that risks are clearly described and there are no unintended gaps or overlaps between risks;
7. Take into account the potential for and effect of the failure of existing controls;
8. Use broad and general methods first and then more detailed methods if greater resolution is required for effective risk analysis; and
9. Record the output fully and preserve the record for future reference.

5.4.3 Risk analysis

Risk analysis investigates and draws upon—

- the information on risks generated during risk identification;
- the effect and reliability of controls;
- additional information from the statement of context;
- supporting statistical data, results of predictive modelling or expert judgement; and
- the risk criteria developed during establishing the context.

This is to gain an understanding of the nature of the risk including the magnitude of consequences and their likelihoods, and therefore to derive the level of risk.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

This analysis enables each risk (or group of risks when considered in the aggregate) to be evaluated in order to determine whether risk treatment is needed. The same methods are useful later in the risk management process to gauge the effect of risk treatment options.

When considering whether risks that have been identified during the risk identification step should be considered in the aggregate, a useful technique is to use the bowtie diagram (refer Figure 4) to first focus on the range of consequences and then work back to the event and post-event mechanisms that can interact to produce those consequences. This is particularly useful in safety applications.

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 analysed 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.

Risk analysis requires continual awareness of sources of uncertainty including those implicit in assumptions. An iterative approach to risk analysis and risk evaluation enables the effect of differing assumptions, situations and inputs to be examined. Sensitivity analysis is a useful tool for examining the effect of making changes in assumptions.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

Factors that affect consequences and likelihood that are not already evident from the risk identification step should be specifically explored. This includes specific consideration of the controls that are in place and the way in which they modify the risk (e.g. whether and how they modify consequence or likelihood or both), and whether controls function individually or in combination. Any assumptions about the actual effect and reliability of controls should be recognized, with particular focus on individual controls or specific combinations of controls that are assumed to have a major modifying effect.

This crucial aspect of risk analysis can be enhanced by consideration of information gained through routine monitoring and review of controls, for example through the organization's system of control assurance (see Clause 5.6.2.2 of this Handbook). As well as facilitating a more accurate analysis of the risk, the information gained through examining how controls operate and their actual or likely effect can be useful later in the design of treatments aimed at improving controls.

This consideration of the potential for control failure also enables the scale of the consequences should failure occur to be estimated. Such estimations are often used in the insurance industry as a means of enabling the insurer to understand the maximum amount that could be payable by way of claim. Expressions such as 'potential exposure' or 'foreseeable maximum loss' are often used for this purpose, although these are not terms used by the Standard or defined in ISO Guide 73. Of course, each such consequence will have its own likelihood.

Recognizing the effects of control failure has the added advantage of highlighting those controls that are being relied on to significantly modify risk, and therefore warrant intense monitoring and review (see Clause 5.3.4.1 of this Handbook and HB 158:2010, *Delivering assurance based on ISO 31000:2009 Risk management—Principles and guidelines*).

The way risk is analysed, the approaches used, and the level of resolution and detail obtained should be consistent with the risk criteria developed as part of establishing the context (refer to Clause 5.3.5 of the Standard). They should also be consistent with the decisions that have to be made. This further explains the importance of establishing the purpose of the risk analysis when establishing the context (refer to Clause 5.3.4 of the Standard).

The level of risk might be expressed as a likelihood of a particular consequence, or where appropriate, a distribution of probabilities, or ranges of likelihoods for a type of consequence. The way in which consequence and likelihood are expressed and the way in which they are combined to determine a level of risk should all be consistent with the criteria used to evaluate risk (see Clause 5.3.4 of the Standard).

In some cases the exact events or situations that lead to consequences might be uncertain, and the risk sources and events can be outside the control of the organization.

Complex forms of analysis might be needed where cause and effect chains have to be understood. These will use techniques such as event tree or failure analysis, or the behaviour and performance of multivariable systems. These are discussed in detail in Standards Australia and Standards New Zealand Handbook, HB 89:2013.

5.4.3.1 *Analysing controls*

Controls can take many forms including tangible devices (hardware or software), minimum design criteria, specified skill sets, rules, specified methods of work, other specified procedures, or mandated processes. Some features of an organization, including its people and its systems of management, although not specifically designed as a control, might have such an effect. Some controls will depend for effect on the correct operation of interrelated controls.

A single control might sometimes act on more than one cause or more than one consequence (see Figure 4).

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

The functionality and reliability of many controls will depend in part on the cultures within the organization, general management policies, general operational practices, and the actual skills and motivations of those involved in any way in the correct functioning of the control. These factors should be a part of an analysis of the control.

Because there is always some level of uncertainty about the reliability of any single control, an analysis should examine the likelihood that controls will function as intended and whether there is more than one control providing a similar type of modification. That is particularly so if the level of risk is so high that a substantial amount of modification is required. If there are overlapping (but independent) controls, the overall reliability will usually be higher (provided that there are not common points of failure).

Irrespective of the form of controls, in all risk assessments it is necessary to consider the extent to which controls modify risk and the level of risk that is being modified. This is done as part of risk analysis and includes consideration of the following:

- The nature and level of risk being modified.
- How the control (or a particular group of interrelated controls) exerts its modifying effect on the mechanisms by which events and resulting consequences can occur (refer guidance below).
- The extent of the modification.
- The expected reliability of the control (i.e. to what extent can it be relied upon to function as intended or assumed).
- Availability of the control in practice (i.e. is the control only in place for some of the time or in particular circumstances).
- Whether there are other (overlapping) controls that exert the same or similar modifying effect.

These considerations also assist in understanding the relative importance of each control (or group of interrelated controls), so that the appropriate level of attention can be given to the regime of monitoring and review that is to be applicable to the control.

If a particular control (or group of interrelated controls) is having a major modifying effect on the risk (particularly a risk having a high level of risk) a more active monitoring regime of that control might be warranted together with closer scrutiny of it by more senior levels of management. Some organizations might, therefore, find it useful to use the forgoing analysis of controls to create a simple system to rate (high, medium, low) the relative importance of controls. Table 5 can be used to record the factors that influence judgements of the relative importance of each control (or group of controls). It is not based on any mathematical combination of these ratings.

TABLE 5

METHOD FOR CONSIDERING THE RELATIVE IMPORTANCE OF CONTROLS

Control (description)	Level of risk being modified	Relative extent of modifying effect (H, M, L)	Reliability (H, M, L)	Availability (H, M, L)	Other overlapping controls? (Yes No)	Relative importance (H, M, L)

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

Analysis of the expected effect of controls on consequences or likelihood can be simulated using techniques such as fault tree analysis and event tree analysis. The effect of controls can also be represented on bow tie diagrams such as that shown in Figure 4 which can highlight, for example, how some controls have the effect of modifying more than one risk.

Bow tie diagrams also can be used later in the risk management process to design risk treatments, either to provide additional controls, or to enhance, replace or improve existing controls. These can be created to reveal the path(s) through which an event with consequences can occur (left hand side) and the range of consequences which could result (right hand side). The bowtie is useful for analysing the specific effect of individual controls, and the extent to which there is dependency on a single control or whether there is control redundancy. It can also reveal knock-on cascaded effects. Events, causes, risk sources and mechanisms are discussed in more detail in Clause 2.3 of this Handbook.

These analysis techniques are described in more detail in Standards Australia and Standards New Zealand Handbook HB 89:2013.

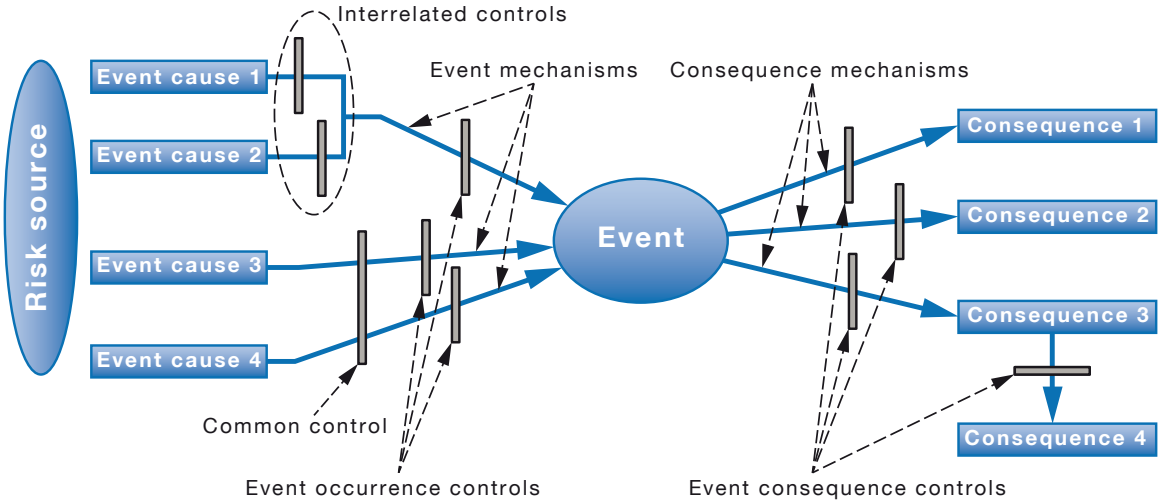

FIGURE 4 EXAMPLE BOW TIE DIAGRAM

In some sectors and for some types of risk, either custom or regulation might designate that some types of control are preferred over others (e.g. controls that don't require human intervention might be institutionally preferred over those that are human reliant and controls that involve the addition of energy in order to function might be assumed to be less reliable than those that are passive).

However, such rigid hierarchies might not reflect the inherent reliability of each type in a particular case (and or the cost effectiveness of the control). Therefore, when analysing the effect and reliability of controls (or when designing new controls during risk treatment) the fact that the controls might conform to such a designated hierarchy does not remove the need for rigorous analysis of the *actual* effect and *actual* reliability.

When considering reliability and availability, the arrangements in place to monitor the ongoing functionality of each control and to review its ongoing effect should be taken into account as part of the analysis.

This might be informed by the results of monitoring (e.g. the results of routine tests or audit reports), which might indicate the extent to which the control is available. If subsequent risk evaluation shows that the risk requires further treatment, in some cases this could involve improving the reliability of existing controls by improving the monitoring regime.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

Reflecting Principle (a) of the Standard (risk management creates or protects value), the foregoing analysis of controls, as part of risk analysis, might reveal opportunities to improve the efficiency of controls, for example, by replacing or amending controls with alternative arrangements that are more cost effective (such as automating a manual procedure). Such information should be considered during the risk evaluation step.

5.4.3.2 *Determining consequences*

Events can lead to either a specific or range of consequences (each linked to particular objectives) of either different types or magnitudes, each with its own likelihood.

Determining the type and range of consequences requires collecting, collating and considering relevant available data (including that held by stakeholders). Techniques to generate such information might include the following:

- Experimentation.
- Research of past events (although the past might not be indicative of the full range of consequences that are possible).
- Modelling to determine the way in which consequences develop following an event and how consequence modifying controls will operate.
- Considering both immediate consequences and those that might arise after a certain time has elapsed.
- Considering secondary consequences, such as those affecting other objectives, associated systems, activities, equipment or organizations.

5.4.3.3 *Determining likelihood*

Analysing risk also requires determination of the likelihood of experiencing consequences. This determination involves combining both the likelihood of an event occurring that is able to generate consequences of interest and the likelihood that such consequences will occur. This can be represented by the expression:

$$L_c = f(L_{E,c}, L_{a,c})$$

The simplest form of which is:

Likelihood of the consequences of interest = *the likelihood of an event occurring that can generate consequences of interest* × *the likelihood of that event actually generating those consequences*

Of course, the actual likelihoods of both the event ($L_{E,c}$) and of this leading to particular consequences ($L_{a,c}$) are each influenced by the likelihood of relevant controls functioning as intended.

In the absence of complete data, likelihood might in part involve an expression of informed belief based on available data or other information.

The method of expressing likelihood should be consistent with that used in the organization's risk criteria. The time period concerned should be explicit and consistent with the scope of this particular application of the risk management process (e.g. per year, per life of a plant item, per operating cycle or within the project duration). Even if comparative terms (such as likely or rare) are used to label bands of likelihood, these need to be defined in relation to a time period. This is discussed in detail in Clause 5.3.5 of this Handbook.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

There are three general methods to estimate likelihood. These might be used individually or in combination. The methods are the following:

- Using historical data based on similar events that have occurred. The data used should be relevant to the scope and purpose of the assessment, and to the decisions that need to be made. This approach can only be used if there is sufficient historical data for the analysis to be statistically valid. This especially applies for zero occurrences, when one cannot assume that because an event or consequence has not occurred in the past it will not occur in the future, particularly if the non-occurrence was the result of controls which might or might not function equally well in future. In the case of zero or very few observed events, special statistical techniques should be used to predict likelihood.
- Synthesis from data relating to parts or components of systems. Numerical data for the performance of equipment, people, organizations and systems can be obtained from operational experience, published data sources or experimental measurement. These can be combined to produce an estimate of likelihood using techniques such as fault tree and event tree analysis. Due allowance should been made within the analysis if common mode events involving separate but coincidental events can arise from the same cause.
- Structured opinion of subject matter experts. Experts can be asked to express their opinion on likelihoods taking into account relevant information and historical data to arrive at an opinion. A systematic approach should be adopted to minimize bias and to ensure that the experts are provided with the same information. There are several methods for this given in Standards Australia and Standards New Zealand Handbook HB 89:2013 including the Delphi technique or applied probability judgements. The method used should make clear the information used by the expert to arrive at a decision and any assumptions he or she made. The sensitivity of the level of risk to these assumptions should be tested.

5.4.3.4 *Outcomes from risk analysis*

The main outcome from risk analysis should be a level of understanding about risks so that they can be effectively described, taken into account in decision making, evaluated against the organization's attitude to risk and, if necessary, efficiently treated. This understanding will comprise an appreciation of, for each risk, the following:

- The source(s) of risk, and the causes and sequences that lead to events.
- The consequences that could occur (expressed in terms of the organization's objectives), their nature, range and magnitude.
- The associated likelihood of those consequences occurring.
- The effect and reliability of the controls that are modifying the risk.
- The level of risk and its sensitivity to assumptions made in relation to consequences and likelihoods.
- Where any subsequent risk treatment should be directed and with what effect.
- Uncertainty in the foregoing.

The record of risk analysis should provide the following:

- The specific statement of context on which it is based.
- The names/roles of those involved.
- Sufficient insight into the inputs and assumptions on which the analysis relies.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

- Such details of the results of the analysis that will be required elsewhere in the risk management process as well as those needed to meet any external recording or reporting obligations.

Further guidance about recording the risk management process can be found in Clause 5.7 of the Standard.

5.4.4 Risk evaluation

Risk evaluation uses the information generated by risk identification and risk analysis to make decisions about whether the risk falls within the organization's risk criteria and, therefore, whether it requires treatment.

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.

Although the need for risk treatment will be very clear in some cases (e.g. if the risk analysis reveals 'very high' level of risk), in others the case for treatment will depend on the ratio of treatment costs to benefits. The latter is determined in the risk treatment step of the risk management process, but the decision of whether or not to proceed with further risk treatment will require that the risk evaluation is revisited. For this reason, risk evaluation and risk treatment will typically need to occur in an iterative way.

The risk evaluation step might also provide an input to determining the priority of risk treatments (assuming that from a practical perspective, it is necessary to establish such priorities) and to identify the seniority of management that is authorized (in terms of the risk criteria) to tolerate the continued exposure of the organization to a certain level of risk without further risk treatment. This can be part of the organization's delegation of authority system and should be reflected in the risk criteria. Also see Appendix C, Paragraph C2.7 of this Handbook for guidance on establishing a rule set for risk evaluation.

5.5 RISK TREATMENT

5.5.1 General

At its simplest, risk treatment involves a process to modify a risk by changing the consequences that could occur or their likelihood. This process requires creative consideration of options and detailed design, both inputs being necessary to find and select the best risk treatment.

Once implemented, risk treatments will either create a new control or amend an existing control.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

Risk treatment takes place in two distinctive contexts:

1 In the *proactive* context, in organizations that have successfully integrated risk management into their general systems of management, risk treatment will be integral to and effectively indistinguishable from decision making. Therefore, at the time a decision is finalized, the risk created by the decision will be within the organization's risk criteria.

2 In a *reactive* context, the organization will be looking retrospectively at the risk created by decisions previously taken and implemented and so any risk treatments found necessary will be remedial in nature.

In both contexts, those risks that the organization judges are unacceptable will require treatment so that they fall within the organization's risk criteria.

There are often several ways to treat a risk or group of risks. In some cases, careful design of treatments can have the efficient effect of modifying more than one risk. This step requires identification of the options and a rational process to select those that are practical, compliant with any legislative obligations, will not generate unacceptable risk during implementation and provide the best return on investment.

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.

The statement of context and the risk assessment steps that precede risk treatment provide much of the information needed to develop and select risk treatments, supplemented where necessary by published technical Standards and first-principle design methods, such as morphological analysis, to ensure that they will be fit for purpose.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

This Standard provides a list of broad options that should be considered when risk treatment is designed. These options are not mutually exclusive and often a combination of measures is required to bring the risk within the organization's risk criteria. These options are discussed below:

1 Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk

This provides the simplest form of risk treatment, but might involve foregoing any benefits that come from that activity and could even make an objective unattainable. Careful analysis is therefore needed. If this technique is applied, the reasons should be recorded to ensure that the activity is not restarted inadvertently in the future.

2 Taking or increasing the risk in order to pursue an opportunity

Exposing an organization to new risks or higher levels of risk can be beneficial, both to make more things possible or, in some cases to reduce the costs of controls that are not providing a comparable level of risk modification.

3 Removing the risk source

This method is particularly suited to risk sources that have little or no intrinsic value, or are incidental to the organization's activities (e.g. accumulation of rubbish within the organization's premises). However, it might also be used where the potential for adverse effects clearly outweighs the benefits (e.g. using cheap untrained staff in customer contact environments).

4 Changing the likelihood

Both pre-event and post-event treatments can be used to change likelihood of experiencing a particular consequence. Pre-event treatments might also involve altering (increasing or decreasing) the number of risk sources (see above) that can give rise to an event, or altering the number, reliability or effectiveness of controls intended to prevent or modify the frequency or magnitude of events. Post-event treatments alter or supplement the controls that determine whether particular consequences are more or less likely to occur.

Having a clear understanding of the sequences involved in bringing about particular consequences is necessary to reveal all of the opportunities to change likelihoods. Fault trees, event trees and other flow-charting techniques are useful methods for doing so.

Examples of methods for changing likelihood include the following:

- Changing the predictability of human behaviour through more careful staff selection, training, public education, or the setting and enforcement of rules.
- Modifying the design or timing of project elements.
- Quality assurance to prevent unintended variance.
- Repricing products.
- Maintenance practices.
- Modifying the strategic plan.
- Protection systems.
- Market research.
- Contractual requirements.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

5 Changing consequences

This form of treatment concentrates on actions that have an effect after an event has occurred to change the nature and size of particular consequences.

Examples of this type of risk treatment include the following:

- Contingency plans and additional contingent capability to modify the effects of potentially disruptive events.
- Protection systems such as fire sprinklers and sea walls.
- Diversification of business.
- Hedging.
- Sharing risk (see point 6 below).
- Tort actions.
- Product recall.
- Customer complaint lines.
- Quality assurance to detect unintended variance.

6 Sharing the risk with another party or parties (including contracts and risk financing)

Sometimes (incorrectly) described as risk transfer, this form of risk treatment is a particular way of changing the consequences experienced by one organization by agreeing to share the consequences with one or more other organizations.

Insurance or other forms of risk financing (whereby at least some aspects of the financial losses of the few are shared by the many who participate by way of the insurer, through payment of their premiums) fall under this type of risk treatment,* as does the more general approach of using a contract to allocate responsibilities.

Risk sharing will always involve the exposure of the first organization to some reciprocal risk from the other organization(s), so recognizing how and where this occurs is an important consideration in the design of risk sharing arrangements. This is also why the term risk transfer is not appropriate, as there is always transfer in both directions.

Although the intention of an organization might be to transfer all or a specific component of the risk, in practice this is seldom possible, as inevitably some risk will remain. The following are examples:

- A contractor might be legally liable for remedying their work, but the principal might have to endure delay and legal costs to enforce the obligation.
- The terms of an insurance policy might oblige the insurer to indemnify a particular loss, however, the insured might have difficulty in proving, when the loss occurs, that the circumstances match the policy wording.
- If insured events affect many policy holders (e.g. as occurs with floods and earthquakes), the insurer's reinsurance arrangements might not be sufficient to meet all claims.
- A manufacturing company might contractually bind component suppliers to meet the cost of any product recall as a result of defective components, but it is likely to be the reputation of the manufacturer that suffers if the final product is defective rather than that of the component manufacturer with whom the end consumer has no relationship.

---

* See Standards Australia and Standards New Zealand HB 141:2010 Risk Financing for further information.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

7 Retaining the risk by informed decision

If an organization, having assessed the risk, determines that the risk is within its current risk criteria and that no (further) treatment is required, it is said to retain the risk, and that decision is usefully regarded as a form of risk treatment. In this way, the decision and the basis of it will be recorded, the risks associated with the decision will be assessed, and the decision will be subject to ongoing monitoring and review.

5.5.2 Selecting risk treatment options

The risk treatment step of the risk management process involves searching for and considering the comparative merits (including costs and benefits) of various options for risk treatment. This produces the optimal set of treatments.

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.

When selecting risk treatments the direct and ancillary costs, and the disadvantages of the proposed treatment should all be considered. Similarly both the direct and ancillary benefits should be taken into account. These considerations can be quantitative, however, often disadvantages and ancillary benefits cannot be easily quantified, in which case a qualitative consideration should be used.

The potential for particular risk treatment options to replace a less efficient existing control should also be considered. This is true for all organizations, but is particularly important for regulators where other parties will be incurring the cost of compliance.

Where there is a large disparity between the timescales during which costs are incurred and benefits are gained, those costs or benefits that occur over the longer timescale should be discounted to enable valid comparison.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

In examining options for risk treatment the organization should apply a systematic approach to consider the following:

- The degree to which the treatment option will modify the risk.
- Whether the treatment could replace (or enhance) existing controls.
- Cost and affordability.
- Costs and benefits.
- Whether the treatment acts alone or in combination with other treatments or existing controls.
- The expected reliability of the option.
- Any ongoing costs associated with the option (e.g. training, testing, maintenance).
- Whether the treatment will result in the risk being within the organization's acceptance criteria.
- The views of internal and external stakeholders on the preferred form of treatment.
- Whether a particular form of treatment is required by legislation.
- Whether particular treatments will also modify other risks.
- The level of reliance on the treatment (having regard to the consequences of failure).
- Whether the treatment itself will create new risks or will affect other risks.
- Whether the treatment will affect the performance of existing controls.
- The practicality of the risk treatment and the resource requirements for detailed design and implementation of the actions.
- Competing priorities and resources within the organization, and the timing of other related projects that could affect the timing of implementation.
- Whether the risk treatment or the resulting control is capable of being checked and assured and the on-going maintenance requirements.

Figure 5 shows a summary of the entire risk treatment process.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

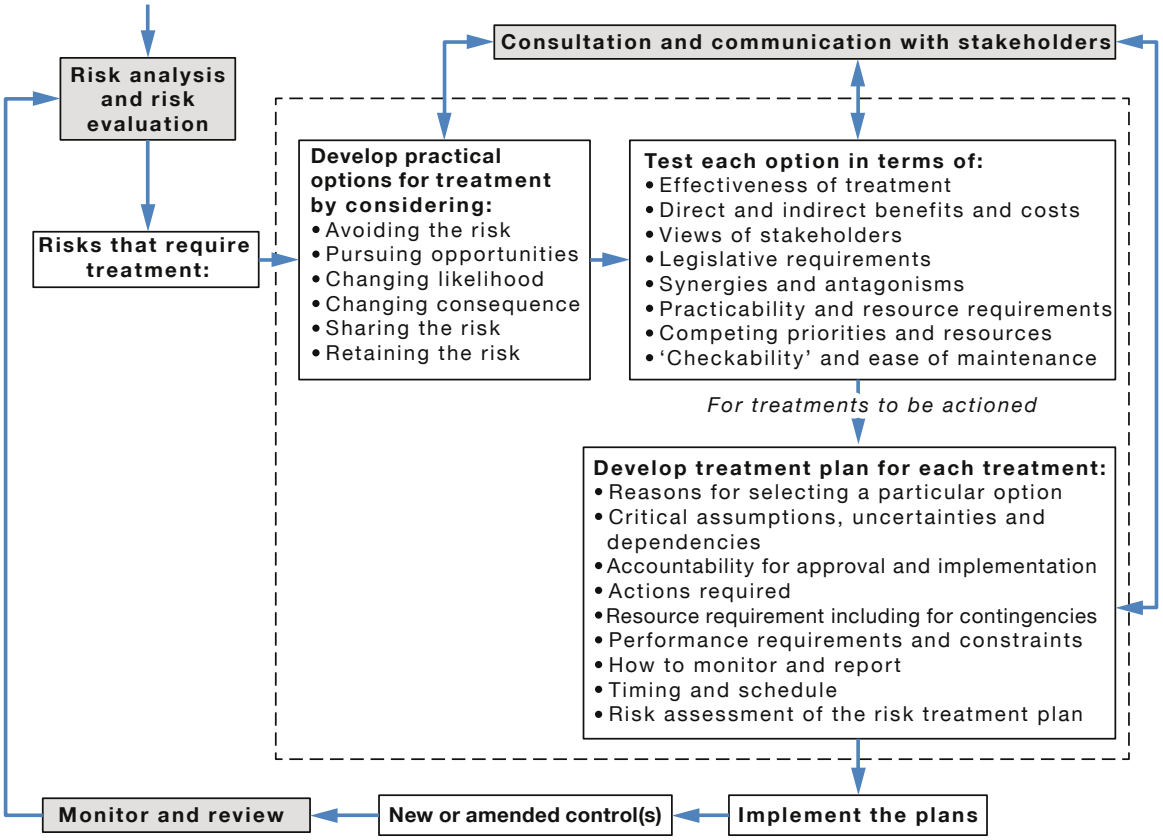

FIGURE 5 THE RISK TREATMENT PROCESS

5.5.3 Preparing and implementing risk treatment plans

Risk is not modified until risk treatments are implemented. Risk treatment implementation requires a plan that specifies tasks, responsibilities, timing and monitoring arrangements, and provides any necessary expenditure authorities.

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.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

The implementation plan might generate risk, particularly if it involves physical or procedural modifications to existing arrangements or has implications for stakeholders. It should therefore be subject to risk assessment and modified if necessary.

The scale of the work involved in some risk treatments might warrant the development of a fully-fledged project plan, complete with milestones, cash flows, tendering, contracts, progress reporting and commissioning activity. In large organizations with central support functions (such as training departments) it may be necessary for one section of an organisation to arrange for the implementation of a selected risk treatment (e.g. a program of training) to be conducted by the central function, which might also have wider benefits to the whole organization.

It will often be appropriate to keep stakeholders informed of progress with implementation of the risk treatment plan. This includes making monitoring information generated as part of the implementation plan available to stakeholders (e.g. the results of noise monitoring during any construction work taking place close to neighbours, or reports to regulators if the risk treatment involved mandated remedial actions).

Once implementation is complete, the resulting controls should be documented together with an appropriate scheme for ongoing monitoring and review.

5.6 MONITORING AND REVIEW

5.6.1 General

Monitoring and review are two distinctive techniques intended to detect change and determine the ongoing validity of assumptions. Both are necessary in order to ensure the organization maintains a current and correct understanding of its risks, and that those risks remain within its risk criteria. Both require a systematic approach integral to the organization's general management systems which reflects the speed at which change occurs within the internal and external environment.

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;
- analysing 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).

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

5.6.2 Monitoring

Monitoring involves the routine surveillance of information and actual performance, and comparison with that which is assumed or required. Its purpose is to generate information needed to ensure that risk is managed effectively on an ongoing basis but its risk management effect depends upon the significance of that information being understood and applied.

Examples of things to be monitored include the following:

- The factors in the internal and external context as this enables the organization to determine whether its risks remain as previously assessed and therefore within the organization's risk criteria.
- Whether controls continue to function as intended as this enables the organization to know whether they continue to modify the risk in the manner assumed in their design and thus whether the present understanding of the risk remains correct.
- Data from the organization's usual performance measurement system, as these might indicate if the current risk assessment is still valid or controls are still effective (e.g. an unexpected fluctuation in the rate of rejected product might mean that controls aimed at quality-related risk are not functioning as intended).

Understanding the significance of the results of monitoring can be complex. Although sudden deterioration in indicators will usually attract attention, progressive deterioration can be equally problematic (but can be detected by monitoring trends).

Monitoring therefore requires a systematic approach involving the following:

- Establishing the procedures for continual checking, supervising, critically observing, or otherwise determining the status of information or systems.
- Having a means of detecting variance or change from what has been assumed or is expected (including detecting and reporting incidents).
- Incorporation of the organization's general performance indicators.
- Determining how resulting information is to be captured, analysed, reported, considered and acted upon—otherwise it has no value.
- Providing necessary resources and expertise.
- Allocating responsibilities for various risk management monitoring activities and incorporation of those responsibilities in the individual's performance review criteria.

An aspect of effective governance is assurance that risk is managed effectively. Monitoring is critical to this responsibility. Although monitoring should be a routine aspect of management, some organizations might also insist that the most critical monitoring activities are also conducted by persons independent of those with day to day responsibility for the system being monitored. The selection of the things to be monitored independently should be risk-based with a strong focus on the performance of the *management* monitoring systems.

5.6.3 Review

Review involves periodic investigation of the current situation or a particular type of activity or system, usually with a specific focus. It is, therefore, an occasional rather than continuous activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives.

The frequency of review might be influenced by the level of risk, the business planning cycle, or a decision by a governance body.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

To ensure that monitoring is operating effectively, line management (or someone independent) should review processes, systems and activities periodically to ensure that new risks have not arisen as a result of undetected changes, and that controls and risk treatments are still suitable and effective. Involvement of those not directly involved in the operation of the processes might provide a more objective analysis.

If problems are found, the review should also consider how these came about and why they were not detected by routine monitoring.

The performance of controls should be an embedded process not reliant on internal audit or any other review function. Internal audits are responsible for the assurance of the control assurance processes and not on the assurance of controls generally. If audits become or are seen as being the primary system of assurance, then it is often the case that the assurance regime will be weak.

5.6.4 Assurance

The monitoring and review activities, and the actions taken in response to findings, are often characterized as a system of assurance because as well as the potential to detect and remedy weaknesses before adverse effects occur, these processes also serve to help those with responsibility for organizational outcomes to fulfil governance obligations, including obtaining an alternative view.

As noted, assurance processes should be continuous and dynamic and primarily conducted by those with day-to-day responsibility for the relevant risk management activity. It follows on from this that it is not sufficient to rely only on occasional, third party reviews and audits for assurance. The absence of any outstanding items arising from audits (which take place only at a point in time) is not in itself assurance that risk is continuing to be managed effectively.

5.6.4.1 *Independent audit*

Audit is a type of assurance activity (and therefore a part of monitoring and review) that comprises a process of systematic review against predetermined criteria. Auditors might be internal or external. If appointed by and responsible to a part of the organization higher than or separate from that which is being audited, the auditor will be independent and can provide a greater measure of objectivity and perspective.

Audits need not be conducted with prior notice or consent, although generally they should be anticipated and planned as a transparent part of the risk management process.

Audits are only truly effective if their principal role is checking that those with the routine responsibility are discharging it effectively, and if the results are made known to those being audited.

Advice on the scope and planning of audits and other forms of assurance is given in the Institute of Internal Auditors, Standards Australia Handbook HB 158—2010, *Delivering assurance based on ISO 31000:2009 Risk management—Principles and guidelines*.

The internal audit function in organizations also has the specific role of providing assurance to senior management and, in particular, to the board or oversight body of the organization, so that—

- its risk criteria are aligned to its objectives and the context in which it is operating;
- the method used to assess and treat risks is consistent with the risk management process and there is confidence that this will continue to operate;
- controls believed to be modifying otherwise unacceptable risks are effective; and
- the organization’s processes for monitoring and reviewing risks and controls are effective.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

5.6.5 Post-event analysis

Incidents, accidents and successes provide a valuable occasion to review risks and controls, and to gain insight into whether and how the risk management can be improved. A systematic process should be used to review the causes of successes, failures and near misses to learn useful lessons for the organization. The process should include the following:

- Establishing and recording the exact purposes of the review and the methods to be used.
- Communicating the purpose.
- Collecting and preserving evidence.
- Accurately recording the observations and recollections of witnesses.
- Creating accurate time-lines of occurrences.
- Initiating any supplementary studies to obtain additional information.
- Conducting analyses to determine the root causes of any successes or failures.
- Preparing draft findings.
- Identifying possible improvement actions.
- Seeking comments.
- Finalizing the report.
- Implementing improvements.

Generally, post event analysis will seek to illuminate the following:

- Whether the risks involved were properly understood.
- Whether people acted as anticipated or assumed.
- Whether the prevailing conditions were as assumed.
- Whether the controls operated as had been assumed or intended.
- Whether monitoring and review processes were effective.
- The required remedial or improvement actions, who should implement them and by when.
- How any lessons that arise for the event should be ‘learnt’ and codified by the organization.

5.6.6 Planning monitoring and review

The primary responsibility for planning monitoring and review activities lies with those who are accountable for the management of risk, not with assurance providers such as internal audit. Quality assurance functions, independent review functions and regulatory monitoring are only useful adjuncts to the process of line management reporting because they provide an alternative view.

Monitoring and review activity plans should include all of the following:

(a) Continuous (or at least frequent) monitoring through routinely measuring or checking particular parameters (e.g. pollution levels or cash flows).

(b) Periodic line management reviews of risks, controls (sometimes called control self-assessments) and implementation of treatment plans, and other routine supervisory activities (such as reconciliations). These are often selective in scope (based on risk weighted criteria), but typically routine and regular.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

(c) Auditing reviews using both internal and external audit staff, and generally aimed at testing systems rather than conditions. These audits will be more selective in scope and of lower frequency than the above measures.

Figure 6 illustrates these as a hierarchy with the regime at the top comprising the greatest level of activity and, if properly designed, providing the most powerful level of assurance.

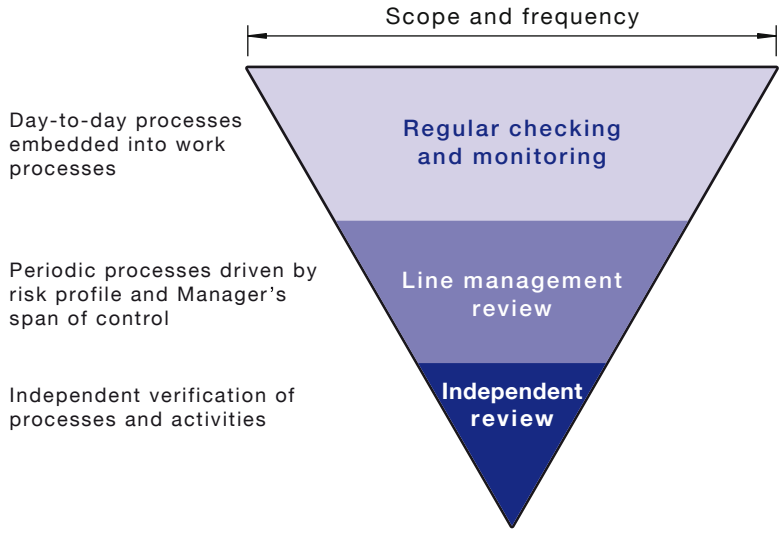

FIGURE 6 HIERARCHY OF MONITOR AND REVIEW ACTIVITIES

5.7 RECORDING THE RISK MANAGEMENT PROCESS

5.7.1 General

Appropriate levels of documentation of the steps of the risk management process and their outcomes will be necessary to record decisions and the basis on which they are made, so that this information is available on an ongoing basis. Record keeping should be fit for purpose and thus not unnecessarily burdensome. Clause 5.7 of the Standard provides insight into the factors to be taken into account as to the content and form of the records.

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.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

5.7.2 General purposes of records

The purposes for making records are typically to—

- record what and how decisions were made so that these might later be justified;
- preserve the views of stakeholders;
- enable reporting;
- facilitate subsequent amendment if circumstances change;
- assist the organization to defend itself against legal actions (it provides evidence of due care in decision making and discharge of accountability for risk management);
- show whether the process has been conducted in a planned and systematic manner;
- fulfil any external obligations (e.g. regulatory compliance);
- enable information about the process and its outcomes to be communicated; and
- provide an audit trail.

This organizational memory of the risk management process is also needed to support decision making and facilitate ongoing application of the risk management process, particularly if there are changes in personnel, as in the following examples:

- Providing a record of the context statements so that changes can be detected that would lead to a reassessment of risk.
- Enabling risk management communication plans to be monitored for progress.
- Enabling risk treatment plans to be monitored for progress.
- Enabling assumptions to be checked and analysis methods to be reviewed and quality assured.
- Providing information about the purpose and scope of controls, so that their performance and suitability can be assured by checking, inspection and audit.
- Facilitating continuous improvement of the risk management process. The outcomes of earlier applications of the process can be critically reviewed to identify opportunities for improvement and enhancement.

5.7.3 Making records

5.7.3.1 *General*

Records can take any form or use any type of medium that is fit for purpose, provide ready access for those who require the information for decision making or other purposes, and provide sufficient security. Holding risk management information in a computer system can enable it to be searched, compared, correlated and reported upon, but only by those with access to it.

Records generated by risk management processes should follow accepted information security protocols to ensure the protection and ongoing integrity of information. This includes ensuring the confidentiality, integrity, authenticity, availability and reliability of the information, and complying with any legislation that concerns the privacy of individuals or freedom of access to information.

If specialist software systems are used, these should be chosen and configured to align with the organization's framework for risk management, and its current and future needs for access at various levels of the organization.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

Whether risk management information is stored in paper form or electronically, it should be protected against potential loss or corruption and, depending upon its criticality, interruptions to accessibility. The organization should therefore develop contingent capability and plans to protect the information, and preserve its integrity and availability.*

5.7.3.2 *Risk registers and risk logs*

Although the Standard stipulates that risk management activities should be traceable, it is not always necessary, practical or of benefit to prepare a comprehensive, or even selective, register or log of risks.

Indeed, a common risk management error is for organizations to regard the generation of a register of risks as either the main purpose or end goal of risk management activity, whereas, as explained in Annex A of the Standard, the actual purpose is to ensure the organization understands its risks and that the they are within its criteria.

Consequently, deciding whether to invest resources to generate and maintain risk registers and logs should reflect a clear and beneficial need for future use of the information. Furthermore, the method of doing so should have regard to how each component of the information is to be used, by whom, and in what circumstances.

Various pro forma templates for risk registers are available (some in the form of software applications). They often provide tables or schedules of risks with columns for the relevant objective or decision, consequence, likelihood, level of risk and planned treatments, and so on. However, there is no universally suitable technique. Care is needed when using risk register software that purports to generate a level of risk. Users should ensure that algorithms in the software that generate the level of risk are consistent with the advice given in Clause 5.4.3.3 of this Handbook.

It could be sufficient for some organization to only keep a register of final decisions involving risks that exceed (or are below) the selected thresholds determined by its risk criteria or those associated with controls that individually have a major modifying effect (refer to Clause 5.4.3.1 of this Handbook). The reason for such a register might be a desire to apply a higher level of monitoring of such controls and periodic reassessment of such risks to see whether additional treatments have become available.

Alternatively, it might be sufficient to only maintain a register of those risks for which there are treatments still to be implemented, with the target date for completion. The reason, in this case, might be to monitor timely completion of the treatments.

Even where there is a need for more comprehensive records to be kept (e.g. to fulfil an external obligation), it does not necessarily follow that the best way of doing so will be through use of a central register. In the case of substantial projects that have a discreet set of project files, it might be more useful for the organization to record the risks associated with the final decisions of a project in the project files.

With the above points in mind, the best way to design a system for registering or logging risks is to start with the specific end-user needs (which may be several and varied) and work back to the design of the register rather than starting with a data recording template or adopting one developed for other organizations or other circumstances.

Whatever the form of registers or logs of risks, the following attributes should always be evident:

- The dates of the activity that generated the information are included (otherwise, there is no easy reference point for determining whether change may have occurred subsequently)

---

* See AS/NZS 5050:2010 for further detailed advice on contingent arrangements.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

- The output of risk assessments and the selection of risk treatments are directly linked to the statement of context on which they were based. This linking could be done, for example, by providing a space in the register to document the statement of context or by providing a specific cross-reference in the register to another accessible document containing the statement. Without this linking, there will not be traceability of the basis to the assessment or treatment selection, ability for later verification, or a basis for monitoring and reviewing to detect any subsequent change in the context.
- The identity of the person responsible for entering the information in the register.

5.7.4 Planning documentation

A documentation plan should be produced which specifies the following:

- Which records should be kept?
- How long they should be kept for and how will their destruction be ensured?
- Which format they should be stored in?
- Which technologies should be used?
- Which legal or regularity requirements have to be complied with?
- Who has access to them and how is it controlled?
- What are the indexing and cross-referencing requirements?
- How are the records protected, and what are the arrangements for access in contingencies?

This plan might be a subset of the organization's record management plan. For more information on the proper management of records see AS ISO 15489.1—2002, *Records management—General*.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

SECTION 6 HOW TO USE ANNEX A OF AS/NZS ISO 31000 TO MAINTAIN AND IMPROVE RISK MANAGEMENT EFFECTIVENESS

6.1 INTRODUCTION

Annex A of the Standard sets out attributes of enhanced risk management. The preceding sections of the Standard explain what is involved in managing risk effectively. Annex A therefore provides both a basis against which an organization can evaluate the extent to which it is conforming to the Standard and guidance as to how, if risk management is not as effective as possible, it can be improved. However, the Annex is not intended and should not be used for the purposes of certifying that an organization is in conformance with the Standard.

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.

Annex A provides two sets of indicators of effective risk management.

The first set (outcomes) describes the end result of effective risk management, namely that the organization at all times is aware of and understands its risks, and that the risks are within its risk criteria. If an organization is to manage its risks effectively, it must know what they are.

The second set (attributes) describes particular characteristics of the way in which the organization goes about risk management that make it more likely that it will achieve the above outcomes.

In that sense, therefore, the attributes are lead indicators and are predictors of actual risk management performance, whereas the outcomes are lag indicators of what is actually being achieved. It follows from this that if the outcomes are not being achieved, the explanation will probably lie in shortcomings in one or more of the attributes. The converse also applies.

For organizations seeking to confirm or improve the effectiveness of their risk management activities (or as is sometimes said, improve maturity), these two sets of criteria (contained in Paragraphs A.2 and A.3 of the Standard), together with the principles in Clause 3 of the Standard, provide a useful basis for assessing performance and planning improvement.

As part of the monitoring and review requirements of the framework (Clause 4.5 of the Standard and Clause 4.5 of this Handbook) the organization should establish surveillance methods for both the outcomes and the attributes.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

6.2 METHODS FOR USING ANNEX A TO MAINTAIN AND IMPROVE PERFORMANCE—OUTCOME TESTS

There are two components of the outcomes criteria.

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**.**

The first outcome is that the organization has a 'current, correct and comprehensive' understanding of its risks.

Each of these three adjectives is important, and sets powerful and challenging requirements not only to achieve, but also to monitor its achievements. That is particularly so when it is appreciated that all decisions, and the actions taken as a result of decisions, will have risk implications, and that risks can change if there is a change in the context. Each decision or action might introduce risk, terminate risk, modify risk or leave risk unchanged. Any change in the organization's risks might be large or small.

Organizations make many decisions, and so a range of techniques and indicators should be used to see if this outcome is being achieved. It can be expected that this first test will be met if the following is enacted:

- **Risk management is a part of decision making.** This will be largely determined by features of the risk management framework and so can be tested in several ways, including examining whether the organization's policies about risk management require this to occur, or examining position descriptions and performance evaluation criteria to see if this obligation is specifically included in the accountabilities of individuals. It can also be tested by examining any formal processes for decision making (e.g. the process for approving capital expenditure to see whether risk is assessed, and arranging for the organization's system of assurance to systematically test day to day practices).
- **Key components of the framework that are a necessary part of applying the risk management process are in place and current.** For example, whether high level, organization-wide statements of context, including risk criteria (see Clause 5.3.6 of this Handbook) exist, if there are procedures for ongoing monitoring of both the context and the effectiveness of controls (together with procedures that respond to change when this is detected), and whether there are established methods for communicating and consulting with stakeholders.
- **Those involved in applying the risk management process have the necessary experience and skills so that they can to apply the process knowledgeably and competently.** This might mean that they also have access to supplementary and specialist skills where necessary.
- **There is ready evidence in recent decisions made by the organization that risk management has been a part of the decision making.** One way of checking this is to examine risk management records for various parts of the organization and for projects. Particular attention should be given to whether risk management is an intrinsic part of the decision making process (which is generally more efficient and better reflects Principle (c) in Clause 3 of the Standard) or whether it is applied after the decision has been made thus necessitating in some cases, changes to be made to the decision.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

- **The organization's governance body is itself applying this practice routinely in the decisions that it makes, and is specifically monitoring whether this occurs elsewhere in the organization.**

The second outcome test relates to whether risks are within the organization's risk criteria. This can be tested by:

- **Examining risk management records** (see Clause 5.7.3 of this Handbook)**.** This is, firstly, to determine whether for those risks that would otherwise be outside the criteria, risk treatments have been developed and, secondly, to determine whether, having selected risk treatments, there are then plans (and associated resourcing) to ensure implementation including follow up and sign off. Unless a risk treatment has been actually implemented, it has no effect on the risk.
- **Checking the results of monitoring of controls, including the timeliness and completion of actions taken if controls are found not to be effective.**
- **Establishing whether top management and the governing body are requiring reporting of risks that are outside the risk criteria.** This should also investigate what happens on receipt of such reports so that risks are modified accordingly.

A fairly common but unhelpful activity is to report the 'top ten risks' to top management or a governing body. There is no logical reason why reporting should be limited to 10 risks (or any other number), as the next ranked risks might also be well outside the organization's risk criteria. The more appropriate action would be to require reporting of all risks that are outside the risk criteria (by some material amount), for example, all risks with a high or very high level of risk. The sometimes stated objection to this practice that there would be too many risks in this category would be in itself an indicator that the organization is either falling far short of managing risk effectively, or that there are problems within the risk assessment or risk treatment implementation process.

6.3 METHODS FOR USING ANNEX A TO MAINTAIN AND IMPROVE PERFORMANCE—ATTRIBUTES TESTS

Each of the five attributes (numbered A.3.1 to A.3.5 in the Standard) are well explained in the Standard, and include specific indicators through which organizational performance can be assessed. This Section contains additional advice about each, as shown below.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

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 All decision making involves application of risk management

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.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

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 Fully integrated 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.

6.3.1 Continual improvement

If an organization finds at any point in time that it is not meeting the outcome tests, it will need to identify why the normal practices for continuous improvement, which should be part of the framework, are not bringing about the desired result. It will then need to not only plan and implement the improvements that are needed to achieve the particular outcome (either Paragraph A.2.1 or A.2.2 or both), but also examine its routine arrangements for continuous improvement.

The underlying problem will usually be found to be one of the following:

- The arrangements for monitoring and review of the framework are not effective. For example, they might not be detecting the implications of organizational change, change of personnel or changes in the external environment, or the monitoring arrangements might not be monitoring individual performance (e.g. through the organization's normal performance monitoring arrangements).
- There are no effective procedures for responding to change when it is detected. For example, responsibility and ownership of the framework has not been properly allocated to someone with appropriate authority, skill and knowledge.
- The response when problems are detected by the monitoring and review arrangements is merely to respond to the issue rather than regard it as a symptom and look more deeply for, and once found remedy, root causes.
- Top management is sending mixed signals about the importance of managing risk. Well-written and explicit risk management policies will have no effect if they are not supported by matching behaviours (this is the commitment aspect of mandate and commitment).
- Resources have not been made available to implement continual improvement.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

6.3.2 Full accountability for risks

The overall focus of this attribute is that risk management activity within the organization should not be left to chance. It places emphasis on what are described in the framework as accountabilities but if accountabilities are to be discharged effectively, they must be expressed clearly, be understood and be believed to rank alongside any other accountabilities that that their holders might have.

To achieve this, the organization might—

- express accountabilities in writing using language that is consistent with the Standard;
- not only specify what is to be done, but when it is to be done and also, where possible, include performance criteria;
- explain and discuss the accountability with the person concerned, to ensure they know what is needed of them, have the opportunity to ask for training if that is required and understand how their performance will be assessed;
- include performance of risk management accountabilities in general performance reviews (such as in 'balanced scorecard' systems of evaluation); and
- require those with such accountabilities as an example to other employees.

6.3.3 Application of risk management in all decision making

It is the decisions and related actions that create or modify risk. This attribute highlights that the obvious and most efficient point at which to assess (and if necessary treat) risk is as a part of the process that brings about the decision. If this is not occurring, then it can be expected that either the organization will not have a comprehensive understanding of its risk or risks will not be within its risk criteria.

As noted elsewhere, organizations make many decisions and these typically occur across the organization. Therefore, a review of the effectiveness of this attribute should make use of the guidance in Paragraph D3 in order to consider the following:

- Risk assessment is a part of decision making at all levels and in all parts of the organization.
- There is a consistent appreciation of the fact that a decision has been made. This is particularly relevant to considerations that leave the status quo undisturbed, because doing so is as much a decision as is changing the status quo.
- The risk management process is being applied in an informed way and at a level of granularity that is appropriate to the decision and its complexity—for example, by reviewing documentation, finding out who was involved in the assessment, and establishing which stakeholders were communicated with and consulted.
- There are incentives and disincentives that influence whether risk assessment is part of decision making. For example, whether proposals for new investments or changes in operating methods can be accepted without being supported by an assessment of the associated risk, or whether in the discussions that are often a part of decision making, there is explicit discussion of the organization's objectives, uncertainty, assumptions and, therefore, risk.
- The general approach to decision making allows adequate time for risk assessment to occur. For example, whether risk assessment is shown as a specific item in a project plan and appropriate resources are allocated to this in the plan.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

6.3.4 Continual communications

All aspects of managing risk involve people. People need to be informed and, if they are stakeholders, consulted. Communication and, as appropriate, consultation are necessary supporting activities for the core steps of the risk management process, as they involve and engages stakeholders. This provides access to their views and knowledge and can encourage a sense of ownership. It also can give stakeholders confidence that the organization is managing risk effectively. This can be particularly important in relationships with—

- customers and suppliers;
- employees or members of the organization;
- regulators;
- investors; and
- neighbours.

The organization can make effective use of communication to inform internal and external stakeholders through the following:

- Publishing articles about the organization's risk management efforts in staff or member publications, and in external publications likely to be read by external stakeholders.
- Providing information about the results of risk management on staff noticeboards. For example, injury or wellness statistics and trends, achievement of quality goals and performance against project schedules and completion dates.
- Providing information about risk management performance in routine (e.g. monthly) internal management reports.
- Routinely including risk management topics in the agenda of internal meetings.
- Specifically reporting on risk management performance in annual reports or investment prospectuses.
- Making reference to risk management expectations in contracts with third parties. This includes representations to insurers regarding the nature of risks and the state of controls.

6.3.5 Full integration in the organization's governance structure

All organizations are governed. The governance structure (which might be explicit or inferred) is the expression used to describe the system, primarily including people and processes through which the organization authorizes, directs and controls the management team, and holds itself accountable to the ultimate owners and stakeholders.

The most common example of a governance structure will comprise the following:

- A board of directors or, in the government sector, a chief official.
- Formal delegations of authority. This is from the governing body, usually via a chief executive with specific constraints as to the scope.
- A monitoring regime so that the governing body can monitor continual improvement.
- A regime for reporting to the governing body, top management, owners and other stakeholders.

This attribute recognizes that risk management cannot be effective if it is a standalone activity—it must be fully integrated into the day-to-day workings of the organization. This is because all parts of the organization are constantly making decisions and thus creating or modifying risks.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

The method for satisfying this attribute lies in the design of the framework. The framework should reflect the principles, several of which directly relate to this attribute. For example, Principle (a) in Clause 3 of the Standard is that risk management has the ability and purpose of creating and protecting value. However, if risk management is not effective, the opposite is true and value might be destroyed.

To determine how well risk management is integrated into the governance structure for an organization, the components of that structure should be identified. Then, for each component of the structure and for the structure as a whole, the following questions should be asked:

- Does the governance structure reflect the risk management principles given in the Standard?
- Does the mandate and commitment component of the framework enable the outcomes in Annex A of the Standard to be achieved?
- Do other elements of the framework enable the risk management process to be applied in a competent way to decision making?
- Are there clear accountabilities specified for managing risk?
- Are there the capability and practices to monitor risk management performance?

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

APPENDIX A

HOW TO TRANSITION THE FRAMEWORK FOR MANAGING RISK TO ALIGN WITH AS/NZS ISO 31000

A1 HOW TO MAKE THE CHANGE

Although the Standard explains how to manage risk effectively, it does not explain how to make the changes that are needed to existing approaches, which will ensure that they align to it. Even though organizations are different and their starting points might differ widely, the generic and systematic process described in this Appendix is applicable in all cases.

The approach is top down, commencing with senior management making its intent and requirements clear. This ensures that the purpose of the alignment is understood throughout the organization and the necessary accountabilities, and resources that are needed to make the transition as efficiently and effectively as possible are available. This is consistent with the requirement for clear mandate and commitment in Clause 4.2 of the Standard, and follows accepted approaches to managing change in organizations.

Even though alignment activities might be organized within the parts of the organization (such as within a subsidiary business) the approach should still be top down and include the governance body and the organization's head office functions.

Having established the intent, the change method involves the following:

- Determining what changes are needed to its existing framework for the management of risk.
- Planning, resourcing and implementing those changes.
- Monitoring the ongoing effectiveness of the amended framework.

The detail of these activities should be developed so as to give effect to each of the principles for effective risk management in Clause 3 of the Standard and satisfy the attributes of enhanced risk management in Paragraph A.3 of the Standard. In this way, the outcomes of effective risk management descried in Paragraph A.2 of the Standard will be achieved.

This approach continues to be applicable once organizations are aligned to the Standard as a means of continually improving their framework as required by Clause 4.6 of the Standard.

All aspects of transition might be assisted by drawing on the experience of other organizations who manage similar types of risks or who have gone through a similar process.

A2 THE TRANSITION PROCESS

A2.1 General

To transition to alignment with the Standard, the organization should follow the steps described below in the sequence illustrated in Figure 7.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

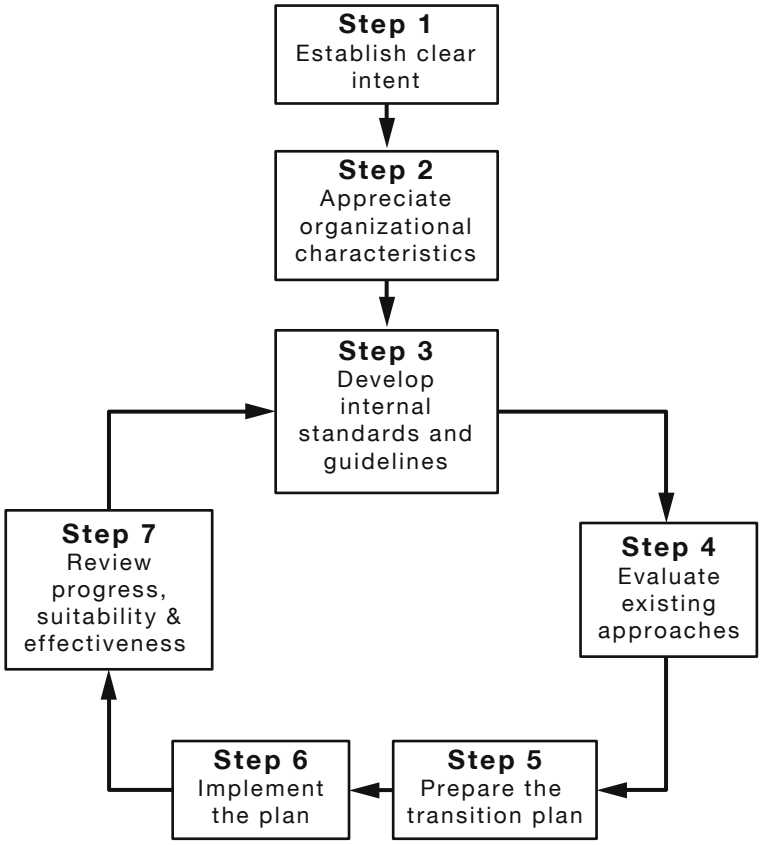

FIGURE 7 STEPS IN IMPLEMENTATION PROCESS

Step 1: Establish clear intent for the transition

Top management clearly communicates to employees and relevant stakeholders the following:

- The reasons for the changes.
- The expected benefits (e.g. to improve the organization's ability to achieve its objectives through an approach that achieves the outcomes and attributes described in the Standard, Annex A).
- The end goal.
- The consequences of failure to complete the transition.
- The organization's commitment to complete the changes within the selected timeframe.

This might involve revisiting and revising any existing policy about risk management in accordance with Clause 4.3.2 of the Standard.

Step 2: Appreciate the characteristics of the organization to be taken into account in making changes to its existing risk management framework

This step ensures that the transition process and plan is tailored to the organization and will be a good fit with the structure, culture and general system of management of the organization and therefore consistent with Principle (g) in Clause 3 of the Standard. For example, the plan will have regard to the speed of change to which the organization is exposed and whether it is orderly or unavoidably chaotic.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

This step is conducted according to the process described in the Standard, Clause 4.3.1, and the guidance given in Clause 6.3.1 of the Standard. It includes consideration of any legal obligations and certification requirements arising from any management system standards that the organization has chosen to adopt.

Step 3: Develop or amend internal standards* and guidelines

The organization documents the methods to be used within the organization to manage risk in a set of within-organization standards. These should be consistent with the Standard and the organization's policy regarding risk management, and also be supported by appropriate guidance material.

The extent and content of the organization's internal standards and guidelines should reflect the characteristics of the organization (refer to Step 2), including its size. Even very small organizations will need to document what employees are expected to do and provide them with sufficient guidance as to how it should be done.

The standards can specify the following:

- How accountability for managing risk is expressed in position descriptions.
- Specific duties of risk owners and control owners.
- The training and support to be provided to those with risk management responsibilities.
- How risk assessment is to be conducted and any standard tools or templates to be used.
- How expenditure for treatment of pre-existing risk is to be requested and approved (risk treatments forming part of new decisions should be part of the decision).
- Where in the organization's various decision making processes risk assessment is required (e.g. prior to submission of capital expenditure proposals for approval).
- How internal and external stakeholders are to be engaged through comprehensive communication and consultation.
- How information about risks and the output from all applications of the risk management process are to be recorded (preferably in one information system or database) and made available to decision makers.
- How assurance and other monitoring and review practices are to be conducted, and the feedback reported and utilized.
- What is to be reported to the governance body and when.

Guidelines in support of the internal standards can then be used as the basis for training or skills development as well as for ongoing reference.

Although this step precedes the evaluation of present approaches against these standards, in practice, the evaluation might suggest a need for some aspects of existing internal standards or guidelines to be amended or expanded upon. This then would be an element of the transition plan.

---

* Such standards can take several forms such as chief executive instructions, formal protocols, processes or rule. Whatever they are called, their function is to specify to the whole organization how risk management activities are to be done.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

As with all aspects of risk management, the development of these documents should include communication and consultation with those who will be involved in their implementation. There also should be provision for periodic review of standards and guidelines if there are subsequent changes in the organization and its context, or if ongoing monitoring and review identifies weaknesses or inefficiencies. Such periodic reviews are thus a part of the arrangements for ongoing monitoring and review of the risk management framework.

Step 4: Evaluate existing approaches for managing risk

The organization undertakes an objective evaluation of its existing approaches to the management of all types of risks by comparison with its internal standards and guidelines. This includes both the process used to manage those risks and the aspects of the existing risk management framework that enable this process to be applied (e.g. relevant training and delegations). Specifically it should evaluate the following:

- **Process:** the evaluation of process should compare both the elements of the existing processes against those in the Standard, Clause 5, as well as the underlying principles that drive and provide the rationale for the process with the principles set out in the Standard, Clause 3 (e.g. whether the process is integrated into routine management practices and actually applied to decision making at all levels).
- **Framework:** the evaluation of the framework should particularly compare the present practices with the requirements of the following Clauses of the Standard:
    - 3 (principles).
    - 4.3.2 (policy).
    - 4.3.3 (accountabilities).
    - 4.3.4 (integration into organizational processes).
    - 4.3.5 (resources).
    - 4.3.6 and 4.3.7 (communication and reporting mechanisms).

From these evaluations, the organization determines which aspects of the current approaches—

(a) could continue to be used in future (with, possibly, extension to other types of decision making);

(b) need amendment or enhancement; and

(c) are no longer suitable and their use should cease.

The actions needed to give effect to these decisions need to be incorporated into a coherent and resourced implementation plan (refer to Step 5) with appropriate milestone dates for completion. It can be expected that for reasons of coherency, some components of the plan will need to occur before others (e.g. if the risk management process is to be changed, the relevant training will need to be first completed).

Evaluation of the present arrangements, selection of transitional actions, sequencing and planning implementation might be assisted by the use of a tailored evaluation sheet such as the example shown in Figure 8.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

Item for review	**Current status** (% compliance)	**Actions required & by whom? Stand-alone or combined?**	**Related stakeholders**	**Resources** (Additions & changes)	**Accountabilities** (New or changed)	**Priority/ Sequence**
Clear & communicated Policy						
Consistency with the eleven ISO 31000 "Principles"						
etc.						

FIGURE 8 ILLUSTRATIVE EXAMPLE OF A TOOL TO ASSIST THE EVALUATION OF EXISTING APPROACHES TO RISK MANAGEMENT AND TO IDENTIFY AND PRIORITIZE NECESSARY IMPLEMENTATION ACTIONS

Step 5: Prepare the transition plan

A detailed transition plan for implementation of the outcomes of Step 4 is needed to ensure that the necessary changes occur in a coherent order, and so that the necessary resources can be provided and applied. The plan should be supported by the resources required for its implementation and this might require specific budget allocations, the development of which should be part of the planning process.

NOTE: This transition plan is the risk management plan as required in Clauses 4.3.4 and 4.4.2 of the Standard.

The plan should be aligned with and integrated into the organization's overall management and development plans. This will be more efficient and will enhance appreciation of the value of integration. This also reinforces perceptions that the transition is an organizational requirement. This is discussed in detail in Appendix D of this Handbook.

Because the organization as a whole cannot suspend its need to manage risk effectively and because they do not test essential organization-wide elements of the transition, pilot studies—in which transition is trialled in a small section of the organization—should be avoided. Pilot studies can create difficulties at the interface between those parts of the organization in transition mode and those that are not, and thereby generate delay and confusion. Pilot studies also create uncertainty about senior management's intent as they inevitably imply that the organization can successfully achieve its objectives without fully understanding its risks and ensuring those risks are within its risk criteria.

The plan itself should be subject to risk assessment in accordance with Clause 5.4 of the Standard and any necessary risk treatment action incorporated into the final version of the plan to maximize the likelihood of its success.

The plan should both require and allow progress to be tracked and reported to senior management and the board, and for there to be periodic reviews of the plan if its implementation is likely to be spread over more than one year or if there are changes in the organization's context.

The plan should therefore enact the following:

- Detail the specific actions to be taken and the timeframe for completion—these will include any further amending of the internal standards and guidelines, explaining and training to build capability, and making adjustments in accountabilities.
- Identify any actions that are to be implemented as part of some wider actions associated with organizational development or which are otherwise linked (e.g. development of training material and engagement of trainers).

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

- Define responsibilities for transition.
- Incorporate a reporting mechanism for reporting completion, progress and problems.
- Identify and record any criteria that are to trigger a review of the plan.

Unless the organization is small or simple in function, the transition might take some time to complete. The usual practice of wherever possible giving priority to those changes that have the biggest impact on achieving the end purpose should be adopted.

An important element of the plan will be the strategy to explain the role of the internal standards and related guidance documents to employees, and to train both existing and new employees in the content and application of these documents to achieve adequate proficiency.

In some cases, explanations and training will need to be extended to external contractors and consultants.

Step 6: Implement the transition plan

Top management should assign accountability for elements of the plan or specific tasks as specified in Clause 4.3.3 and Paragraph A.3.2 of the Standard, and should review the performance of individuals against those accountabilities as part of general performance review (see Paragraph A.3.1 of the Standard).

To reinforce their importance, the organization's reward and recognition system should acknowledge these accountabilities. Completion of actions should become part of the performance measures for the managers concerned.

Step 7: Periodic review of progress, suitability and effectiveness

Progress against the plan and the performance measures should be tracked, analysed and reported to senior management. If the changes are scheduled to be spread over more than a month, it will be prudent to use the organization's normal system of management reporting to track progress, as this further reinforces that completing the transition is a necessary part of the organization's core business.

Reports of progress against plan and performance against measures should be validated periodically by independent review. This can be by an internal audit function.

These monitoring and review activities should include escalation provisions that apply if slippage against the plan milestones is detected. This is particularly important for those parts of the plan that need to be completed before other parts in order to achieve coherency. If such slippage results in amendments to the plan, the draft revisions should also be subject to risk assessment.

If the transition extends over more than one year, the overarching strategy for the transition and the elements of the implementation plan should be reviewed in terms of ongoing suitability and effectiveness. Such reviews should also occur should any of the other review criteria specified in the plan be triggered (e.g. expansion of the organization through a major acquisition or amalgamation).

Changes to the strategy and plan might occur as a result of these reviews.

A2.2 Continual improvement

For organizations that have aligned their approach for managing risk to the Standard, this process, and Steps 3–7 in particular, can be used as the basis for continual improvement in accordance with Clause 4.6 and Paragraph A.3.1 of the Standard.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

APPENDIX B

EXAMPLES OF POLICY STATEMENTS

B1 EXAMPLE OF RISK MANAGEMENT POLICY ANNOUNCEMENT—SMALL ORGANIZATION

NOTE: Even though the risk management policy might be expressed less formally in smaller organizations, the terminology and concepts should be consistent with those in the Standard to facilitate interaction with other organizations and to avoid misunderstandings of what is required.

Memo to all staff: Risk management

We are changing the way we manage risk to ensure that we always understand what risks we are creating when we make decisions and that the level of risk is acceptable and remains acceptable to us. This will help us avoid wasted effort, better achieve what we are trying to do and help ensure our personal wellbeing. Accordingly we are going to place more emphasis on:

- Involving staff and our other stakeholders by getting their input to help us understand and control risk.
- Being more aware of the assumptions we make when we are making decisions and how certain we are about those assumptions.
- Considering risk as part of making decisions, rather than doing so after the decision is made.
- Being more aware of changes of any type that occur, both inside and outside the organization because such changes can result in risks changing.
- Making sure that risk controls that we rely on, continue to operate as intended.

We will be progressively changing some of our procedures to give effect to this approach.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

B2 EXAMPLE OF POLICY STATEMENT—LARGE ORGANIZATION—SET BY DIRECTORS

Policy number	**XXXX**
Subject	**Risk management**
Background	There is always some uncertainty associated with the decisions and actions we take to achieve our objectives. We call the effect of uncertainty on objectives 'risk'. We will accept risk in order to pursue our objectives, but before doing so, we will set criteria about the levels and types of risk that are acceptable, understand the nature of the risks that are created by the decisions we make, and ensure that the level of risk is within our criteria, adjusting it as necessary. To enable us to do this in an efficient way we need to incorporate high quality risk management practices into all of our systems of governance and management. In this way, we are better positioned to take advantage of opportunities and to achieve our objectives.
Policy	We will accept risk in order to achieve or exceed our objectives, provided that we first understand the risks and have modified those risks as necessary so that they are within our risk criteria. We will therefore assess and treat risk as part of planning and decision making at all levels of the company. To provide consistency and confidence, we will undertake these risk management activities in accordance with our internal standards that shall reflect best national and international practice.
Responsibility	We will ensure we have the resources, delegations and organizational arrangements to make this possible, and we will establish an assurance program to confirm that this has been achieved. The Board is responsible for approval of the risk management policy, determining our risk criteria, ensuring the policy can be implemented and, assisted by its Audit and Risk Committee, for monitoring 'Very High' risks, the correct functioning of critical controls and the effective implementation of the policy. The Chief Executive is accountable to the Board for approving our risk management standards and ensuring they are applied in a consistent manner across the organization and to all forms of planning and decision making. The CE may delegate specific accountabilities and responsibilities for risk management but shall monitor the performance of those concerned. The Chief Risk Officer is responsible for developing and maintaining our risk management standards, providing technical risk management support and associated tools and practices. Managers are responsible for applying our standards to assessing and treating risks in their business areas, and monitoring the correct functioning and ongoing applicability of controls. All personnel shall fulfil their specific risk management functions.
Stakeholders	We recognize the legitimate interests, knowledge and experience of our internal and external stakeholders, and will regularly communicate and consult with them.
Assurance and improvement	We recognize that the internal and external environment in which we operate is constantly changing, and that we must recognize and adapt to those changes, improving wherever possible. Accordingly we will monitor and review all aspects of our risk management using risk-based assurance processes, and improve whenever we can.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

B3 EXAMPLE OF POLICY STATEMENT—LARGE ORGANIZATION—SET BY THE CEO

RISK MANAGEMENT POLICY STATEMENT

The effective management of risk is central to **[the organization]** achieving **[its purpose]**. This means that **[the organization]** must have a current, correct and comprehensive understanding of its risks and that those risks are of a type and at a level that are desirable to **[the organization]**.

By understanding its risks and treating its risks, **[the organization]** can provide greater certainty and security for its clients, its members, its cause, its employees, its volunteers and all its stakeholders. **[The organization]** will be better informed, more decisive and function with increased confidence to achieve **[its purpose]**.

[The organization] will adopt a structured and consistent approach to assess and treat all types of risk, at all levels and for all activities in the organization. **[The organization's]** approach to risk management will be consistent with the risk management standard AS/NZS ISO 31000:2009, *Risk management—Principles and guidelines,* and the organization's guidelines and procedures based on the Standard **[reference the organization's related guidelines and procedures]**.

[The organization's] aim is for high-quality risk management activities to be integrated with all its critical processes, so that before events occur or there be a change in circumstances that might enhance or prevent **[the organization]** achieving its purpose and objectives, the organization is able to recognize and respond to the risks in a consistent, proactive way. Equally, when events occur, **[the organization]** will use systematic processes to learn the lessons from its successes, failures and near misses. In this way **[the organization]** will drive operational excellence and organizational learning and growth.

Responsibility for managing **[the organization's]** risks rests with the managers and heads of all programs, projects and functions. This includes accountability for ensuring that the necessary controls modifying (enhancing or reducing) the risks are in place and are effective at all times, and for ensuring that control assurance activities also are effective. Assurance of good governance will be achieved through the regular measurement, reporting and communication of risk management performance.

As CEO, I will make certain that the necessary resources are available to ensure that the organizations risks are managed effectively.

[The organization's] senior management committee **[committee name]** will monitor and review the organization's risk management activities and performance (including being consistent with AS/NZS ISO 31000 and with **[the organization's]** guidelines and procedures) and report this to the Board Committee responsible for the oversight and review of the organization's risk management framework and process.

This policy is to be reviewed at least every two years.

[Name], Chief Executive Officer

DD/MM/YYYY

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

B4 EXAMPLE OF POLICY FOR MANAGING RISK—GOVERNMENT DEPARTMENT—SET BY CHIEF EXECUTIVE (DIRECTOR GENERAL OR EQUIVALENT)

Chief Executive Instruction # xxxx

Subject: Risk Management

1 Introduction

In this CEI, 'risk' means effect of uncertainty on objectives. The objectives are those set out in [the Department's] annual Statement of Intent.

'Risk management' refers to coordinated activities applied to:

(a) Strategic and operational planning.

(b) Service delivery.

(c) Engagement with stakeholders.

(d) Planning and execution of projects and initiatives.

(e) Learning lessons from operational successes and failures.

(f) Developing new policies.

2 Commitment

[The Department] is committed to using risk management principles and techniques to ensure all internal and external factors and influences impacting on the achievement of objectives are recognized, understood and appropriately managed. In doing so, it is expected that [the Department] will have:

(a) A reliable basis for sound decision making.

(b) Increased likelihood of achieving objectives.

(c) A basis for prudent risk taking.

(d) An understanding of the risks associated with each decision as well as an understanding of the level of risk to which it is exposed in the aggregate.

(e) Avoiding adverse outcomes while seizing beneficial opportunities.

(f) Improved accountability and control assurance.

(g) Improved operational effectiveness and efficiency.

(h) A culture based on reasonable foresight and responsible hindsight.

[The Department] will monitor and measure performance against this CEI.

3 Risk management method

[The Department] will manage risk in accordance with ISO 31000:2009.

4 Risk attitude and risk treatment

[The Department] has developed a process for the analysis and evaluation of risks. This is based on a set of risk criteria that reflect its critical success factors and its risk appetite. In general [the Department] will always treat a risk if:

- It involves a breach of legislation or of a contractual condition.
- It concerns the health and safety of an employee or member of the public.
- It is reasonable and cost effective to do so.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

Selection of treatments generally involves considering:

- Whether the risk is being controlled to a level that is reasonably achievable.
- Whether it would be cost-effective to further control risk.
- [The Department's] willingness to tolerate risks of that type.

The likely effectiveness of risk treatment will be considered. Wherever possible there should not be reliance on a single control. The range of types of risk treatment considered will include:

- Avoiding risk.
- Taking or increasing risk.
- Changing the consequences of the risk.
- Changing the likelihood of the consequences.
- Risk sharing.
- Tolerating the risk without further treatment.

Determining the cost effectiveness of further treatment will generally involve the application of cost benefit analysis that will include the consideration of all costs and ancillary costs (disbenefits) as well as all the benefits and ancillary benefits (opportunities). If most of the costs or the benefits are unlikely to be experienced within the first year or so, then it will be necessary to discount the benefits and costs to allow the assessment to be made in today's money.

If risk requires treatment, this should generally be done as soon as possible, but should also have regard to [the Department's] concurrent priorities and the level of risk that is being treated. Authority to accept the continuation of untreated risk over the period in which treatments are being implemented will reflect the level of the risk concerned. Timing and authorities shall be consistent with the following table.

Priority for attention

Risk	Indicative timing for implementing risk treatment	Authority for continued toleration of residual risk
Very High	Immediately if possible, but not more than one month	Director General
High	As soon as possible, no more than three months	Directors
Medium	No more than 1 year	Managers
Low	Ongoing implementation as part of normal management practice	All staff

6 Reporting

Risks and controls will be reported to the Executive team based on severity and criticality. Risks assessed to be very high are to be reported monthly and those that are high, three monthly. Critical controls are to be reported monthly. The state of conformance with this CEI will be reported on 6 monthly by [position].

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

APPENDIX C

USE OF QUALITATIVE AND QUANTITATIVE TECHNIQUES TO DEVELOP RISK CRITERIA

C1 SCOPE OF THIS APPENDIX

Determining risk criteria is an essential part of establishing the context, the first step of the risk management process. That is because risk criteria are needed to assess risk and, subsequently if required, to select risk treatments.

Clause 5.3.5 of this Handbook explains that the risk criteria have three components:

- The method(s) to be used to express and measure consequence and likelihood (whether qualitative or quantitative).
- The method(s) to be used to combine consequences and their likelihoods, and then to express the resulting level of risk.
- The organization's internal rules for accepting (or tolerating) particular risks as well as risk in the aggregate.

Clause 5.3.5 of this Handbook provides six generic steps for developing risk criteria. Table 4, which is part of that clause, describes four types of measurement scales and the limitations and applicability of each.

The purpose of this Appendix is to provide practical guidance to the use of qualitative techniques in the application of the six generic steps (Paragraph C2) and for those using quantitative risk analysis, some guidance in relation to expressing the level of risk as a mathematical distribution (Paragraph C3). Both paragraphs take into account the guidance in Table 4.

Attention is again drawn to the direct application of the detailed information in illustrative examples, such as that provided in Table C2, to real-life situations. In such cases, the purpose of the Handbook is solely to illustrate the conceptual approach because in each case, metrics relevant to the context will be required.

C2 DEVELOPING RISK CRITERIA FOR QUALITATIVE RISK ANALYSIS

C2.1 General

Qualitative risk analysis techniques rely on descriptive and or comparative characterization of consequence, likelihood and the level of risk comparative (rather than using numerical measures). However, qualitative descriptors should still be based on the best available information [refer to Principle (f) of the Standard], and so should take into account available numerical data and other evidence, as well as reflecting informed judgement.

Some scales can be used that have the appearance of being quantitative (e.g. 1, 2, 3) but they are actually nominal or ordinal. As arithmetic manipulation of such scales is not valid (see Table 4), care must be taken in establishing and using them.

Level of risk, as determined by combining consequence and likelihood (of both the event occurring and of the consequences occurring if the event has occurred), is not always suitable for use in definitively comparing treatments or in determining whether a treatment should be implemented when compared with accepting the risk. The scales can suppress meaningful difference between the treatments (see the example in the box below). These scales, even the concept of level of risk, should be used only when guiding managers to taking action to design and evaluate treatments.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

Example

If the consequence scale included a scale level range '$10M–100M' (as illustrated for Level 5 of Table C2) then it would be probably incorrect to assume that a treatment that reduces loss by $99M deserves the same consideration as one that reduces it by only $11M, if the likelihood of the consequence is the same.

C2.2 Step 1: Select outcomes for each objective

The organization's objectives (i.e. its highest expression of intent and purpose) will have been articulated as the preliminary step of establishing the context (organizations typically express their explicit objectives in their strategic and business plans but might also describe them in mission and vision statements—in very small organizations, the objectives might amount to a shared, but well understood purpose).

However, the organization expresses its objectives, developing the risk criteria requires there to be a clear understanding of the specific outcomes it will need to achieve to attain each objective, how such outcomes will be measured and an understanding of the likely range of performance for each outcome. In the risk management process, these outcomes and the manner in which they are measured become the method of expressing consequence.

For example, the hypothetical company, MineRight Limited is committed to successful realization of its mission to obtain the maximum value inherent in its property. To do this, it will need to be highly responsive to its markets and process its mineral reserves most efficiently in order to generate high returns for its shareholders.

However, MineRight Limited also has a vision of being the leading mining company of its peers in terms of growth, productivity, safety, environmental management and stakeholder relationships.

Consequently, the current, three-year strategic plan describes its objectives as shown in Table C1 below, the outcomes it seeks and the way it will measure its achievements. The measures in the third column are also used to express consequences.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

TABLE C1

OBJECTIVES, OUTCOMES AND MEASURES FOR MINERIGHT LIMITED

	Objective	Outcomes	Measures
1	Optimize shareholder value through decisions on the allocation of capital and resources across the portfolio of assets (including core and non-core)	Maximize shareholder value	Return on investment (net present value)
2	Achieve world class safety performance	Minimal injury to employees. Zero fatalities Avoid prosecutions and enforcement action	People impacts (using levels of injury and number of people affected) Legal actions
3	Mine in a sustainable way that minimizes the impact on the environment	Avoidance of irreparable damage to ecosystems and communities Minimize the cost of cleaning up after damage to ecosystems Avoid prosecutions and regulator actions	The severity and extent of environmental impacts The duration and cost of cleanup activities Legal actions
4	Maintain a constructive relationship with local communities who treat the company with respect	Regular engagement; Minimal complaints, balance of positive to negative media reports	Reputational impacts such as media attention and complaint trends
5	Maximize income from existing operational assets through better working methods	Income	EBITDA
6	Operate a lean business and improve our position on the cost curve for comparable mining companies	Reduction in mining cost ($ per tonne)	EBITDA
7	Grow the company through value creating acquisitions that are symbiotic and consistent with our existing assets	Increase in shareholder value	Return on investment (NPV)
8	Optimize the returns from the allocation of capital (sustaining and growth types)	Increase in shareholder value	Return on investment (NPV)

C2.3 Step 2: Select and define scales for consequences

It is necessary to define scales for each consequence type. These scales should enact the following:

- Have end points on the scale corresponding to outcomes that are regarded as extreme for the organization (including extremely good or extremely bad). If the consequences were detrimental, they would represent a level where radical action would be taken—often by external agencies—that would involve closure or substantial change to the organization. If the consequences are beneficial, they would be regarded as remarkable and highly unusual, and are also likely to trigger radical change in the business.
- Have the lowest levels corresponding to what the organization regards as trivial or extremely poor and at the limit of materiality.
- Contain descriptions or measures that are objective and, where possible, tangible.
- Avoid relative measures such as proportions and percentages.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

- Either be phrased to represent both detrimental and beneficial outcomes, or give descriptions for both.

The number of intermediate levels given for consequences should reflect the range between the highest and the lowest levels, and the level of resolution required in risk analysis and evaluation. This will often indicate the optimal number of levels and spacing between them.

It is common practice to use a logarithmic scale for those consequences that are measured in numerical terms. This practice provides good resolution for lower and middle parts of the scale. However, the corollary is that the intervals between levels at the top of the scale are large and the resolution is poor. Clause 5.3.5 of this Handbook provides more information about the granularity of scales.

A further consideration is the organization's existing delegations and how these relate to different types of consequence.

In general, most organizations find that five, six or seven levels are suitable with the upper and lower levels being 'greater than' or 'less than'. Unless the organization is very large, any more levels than this provide an unnecessary level of resolution and might be cumbersome to use. Unless the organization is very small, any less than five levels will probably not provide sufficient useful resolution.

A key consideration in developing scales for several types of outcome is the implied or perceived relative severity of one type of consequence compared with another. For example, if there are consequence scales for both financial outcomes and, say, human wellbeing outcomes (such as safety) the juxtaposition of the two scales reflects how seriously different degrees of human injury are regarded, compared with financial outcomes. When scales are developed it is important to check the equivalence of significance between the same level of different types of consequences. In that these equivalences can be regarded as one way the organization expresses its risk attitude, then draft scales should be considered and approved by the organization's governing body.

Table C2 shows an example of consequence criteria for a hypothetical not-for-profit organization.*

Table C3 shows some illustrative consequence scales for the hypothetical company, MineRight Limited based on the objectives, outcomes and objectives given in Table C3.

NOTE: The examples in Tables C1, C2, and C3 are illustrative only. In order to manage risk effectively, each organization will need to develop its own scales using the processes and guidance described above.

* Taken from Standards Australia and Standards New Zealand Handbook HB 266.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

COPYRIGHT

TABLE C2

EXAMPLE CONSEQUENCE SCALES FOR A NOT FOR PROFIT ORGANIZATION BASED ON FIVE LEVELS OF CONSEQUENCES
(Illustrative example only: Derive actual scales and metrics from Paragraphs C2.2 and C2.3)

Consequence Level	Financial impact	People effects (employees, volunteers and clients)	Reputation	Service outputs	Legal and Compliance	Management impact
5	>$3m	One or more fatalities or severe irreversible disability to one or more people	National media coverage; attracts substantial new funds OR CEO departs and Board restructured Organization may close or be split up Significant impact on funding for several years Long-term loss of clients	Positive transformation of organization OR Total cessation of multiple services for many months	Major litigation costing >$3m Investigation by regulatory body resulting in long term interruption of operations Possibility of custodial sentence	Restructuring of organization with the loss of many senior managers Complete suspension of normal management activities for many months
4	$1m–$3m	Extensive injury or impairment to one or more persons	State media coverage; attracts a moderate level of new funds OR CEO departs, affecting funding or causing loss of clients for many months	Distinctive enhancement or change of organization OR Disruption of multiple services for several months	Major breach of regulation with punitive fine, and significant litigation involving many weeks of senior management time and up to $3m legal costs	Significant event or disruption that will require considerable senior management time over several weeks or a month or so
3	$300k–$999k	Short-term disability to one or more persons	Local media coverage over several days; generates interest from potential funders OR Senior manager departs; Noticeable loss of clients or funding for several months	Major improvement in scope of organization OR Total cessation of one service for a few months/multiple services for several weeks and subsequent disruption	Breach of regulation with investigation by authority and possible moderate fine, and litigation and legal costs up to $999k	Event or disruption that will require senior management time over several weeks

(*continued*)

Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

TABLE C2 (*continued*)

Consequence Level	Financial impact	People effects (employees, volunteers and clients)	Reputation	Service outputs	Legal and Compliance	Management impact
2	$10k–$299k	Significant medical treatment, lost injury time <2 weeks	Local media coverage, and complaint to management	Sizable improvement in services OR Some service disruption in one area	Breach of regulations Minor fine or legal costs Minor litigation	Event or disruption that can be managed with careful attention. Will require some senior management time over many days or a few weeks
1	<$10k	First aid or minor medical treatment	No media coverage and complaint to employee	Minimal enhancement or disruption	Minor legal issues, or breach of regulations	Will require some management attention over several days

COPYRIGHT

Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

COPYRIGHT

TABLE C3

EXAMPLE CONSEQUENCE SCALES FOR HYPOTHETICAL ORGANIZATION (MINERIGHT LIMITED)
(Illustrative example only: Derive actual scales and metrics from Paragraphs C2.2 and C2.3)

Consequence level	Financial (EBITDA)	Growth (NPV)	People	Environment and community	Reputation	Legal
6	>$100m	>$500m	More than one fatality from one event or significant irreversible effects on 10s of people	Regional and long term impact on an area of significant environmental value Destruction of an important population of plants and animals with recognized conservation value Complete remediation impossible Complete loss of trust by affected community threatening the continued viability of the business	Prominent International media coverage Long term impact on share price Leads to changes at Executive or Board level	Public inquiry taking up considerable resources and Executive management time Major litigation or prosecution with damages/fines of >$50m plus significant costs Custodial sentence for a manager Suspension of shares by the ASX
5	>$10m, <$100m	>$50m – <$500m	Single fatality or severe irreversible disability to one or more persons	Destruction of an important population of plants or animals or of an area of significant environmental value Complete remediation not practical or possible Long-term community unrest and outrage significantly impacting business performance	National media coverage over several days Shareholders and Board exercise control Potential for class action Major customers cancel key contracts	Major litigation or prosecution with damages or fines of <$50m plus significant costs Imposition of a fine by ASIC Major breach of regulation leading to cancellation of operating license

(*continued*)

Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

TABLE C3 (*continued*)

Consequence level	Financial (EBITDA)	Growth (NPV)	People	Environment and community	Reputation	Legal
4	>$1m, <$10m	>$5m, <$50m	Extensive injuries/illnesses or irreversible disability or impairment to one or more persons	Extensive and medium-term impact to an area, plants or animals of recognized environmental value Remediation possible but might be difficult or expensive Community protest requiring intervention and substantial management attention	State media coverage over several days Publicly disclosed involvement by regulator(s)	Litigation or prosecution costing <$5m or involving substantial management time (manager level and above) Publishing of a warning by the FSMA Breach of regulation leading to suspension of operating license
3	>$100k, <$1m	>$500k, <$5m	Medium-term reversible disability to one or more persons, such as significant medical treatment, disabling or lost time injury	Localized and medium term impact to areas, plants or animals of significant environmental value Remediation may be difficult or expensive Persistent community complaints	State media coverage. Interest by regulator(s) and NGOs.	Major breach of regulation with punitive fine Involvement of senior management
2	>$10k, <$100k	>$50k, <$500k	Recordable injuries or illnesses with up to one week of job restrictions or lost time	Localized and short term impact to an area, plants or animals of environmental value Minor remediation is required Complaints from interested parties	Local media coverage interest by local NGOs One or two community complaints	Breach of regulation with investigation or report to authority with possible prosecution and fine
1	<$10k	<$50k	Minor injury or illness, first aid or medical treatment without job restrictions	Localized and short term environmental or community impact requiring no or very minor remediation	Kept on site—no media or community interest	Minor legal issues, non-compliances and breaches of regulation

COPYRIGHT

Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

C2.4 Step 3: Decide how likelihood will be expressed

The scale or scales for likelihood measures relate to the likelihood of experiencing the consequences across a relevant timeframe (e.g. the lifetime of a person, the expected life of an asset, the duration of a project or government decisions affecting many generations). The range of likelihoods should be capable of expressing and distinguishing consequences that are almost inevitable and highly likely, and also those that are expected to occur infrequently or are improbable.

The scales for likelihood in qualitative risk analysis may be derived from known (or estimated) probabilities or frequencies, durations (return periods), or other informed judgements. As noted in Clause 5.3.5(3) of this Handbook, these expressions need to be selected with care and take into account the nature of the decisions being made (of which the risk analysis forms part) and the frame of reference, including the time frame.

If expressions such as ‘likely’ or ‘improbable’ are used in the scale, they need to be defined as specifically as possible (see Table C4 by way of example) because, as demonstrated by research, such descriptors are subjected to personal or even cultural interpretation.

When using judgement to develop likelihood scales (and, subsequently, assigning likelihoods to such scales), care is needed to avoid a natural bias assuming that high consequences are more likely to occur than available evidence suggests, or to be unduly influenced by the recent occurrence of a high consequence low likelihood event (e.g. a major damaging earthquake, even though the recurrence interval might be several thousand years).

As with consequences, the number of levels in the likelihood scale should depend on how many are required for a useful level of resolution. Less than five levels might not offer sufficient resolution, while more than seven might prove too cumbersome.

Although it is common practice when developing a matrix for combining consequences and their likelihoods to have the same number of levels of likelihood as consequence, there is no requirement or rational reason for this to always be the case. The decision regarding the number of intervals on each scale should be based on all of the above considerations.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

TABLE C4

EXAMPLE OF A LIKELIHOOD SCALE RELATING DESCRIPTORS, FREQUENCY AND PROBABILITY

(Illustrative example only: Derive actual scales and metrics from Paragraph C2.4)

Descriptor	Description	Indicative return period*	Indicative probability (over the time frame or activity of interest)
Almost certain	The consequence expected to occur on an annual basis	Every year or more frequently	>0.9
Likely	The event has occurred several times or more in your career	Every three years	>0.3, <0.9
Possible	The event might occur once in your career	Every ten years	>0.1, <0.3
Unlikely	The event does occur somewhere from time to time	Every thirty years	>0.03, <0.1
Very unlikely	Heard of something like that occurring elsewhere	Every 100 years	>0.01, <0.03
Extremely unlikely	Have never heard of this happening	Every 1000 years	>0.001, <0.01
Incredibly rare	Theoretically possible but not expected to occur	Every 10 000 years	<0.001

* Return period is an estimate of the likelihood of an outcome occurring. It is also known as recurrence interval.

C2.5 Step 4: Use a table or matrix to derive the level of risk

The simplest way to combine consequences and likelihoods pairs in qualitative risk analysis is to use a table to indicate the level of risk that the organization decides should correspond to each combination. An illustrative example of such a table is shown in Table C5. Such tables are created by asking members of the organization or stakeholders how they might perceive the level of risk from particular combinations of consequences and likelihoods. This process is aided if the descriptors for the various levels are defined by tangible measures.

Such a table is of the utmost importance to the organization as it will determine how all risks are evaluated. For this reasons, the table should be validated and agreed by the governing body.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

TABLE C5

ILLUSTRATIVE EXAMPLE OF USE OF A TABLE FOR LEVEL OF RISK USING QUALITATIVE MEASURES

Level of consequences	Level of likelihood	Level of risk
Severe	Very likely	Very high
Severe	Occasional	High
Severe	Infrequent	High
Moderate	Very likely	High
Moderate	Occasional	Medium
Moderate	Infrequent	Medium
Minor	Very likely	Medium
Minor	Occasional	Low
Minor	Infrequent	Low

Instead of a table, organizations can use a simple graph with an overlying grid (called a matrix) to combine levels of consequences and likelihoods. This has the advantage of a more visual illustration of the relationships between consequence and likelihood chosen by the organization. An example is shown in Table C6. But this is only illustrative and this example should not be used unless an organization has decided that it accurately reflects its risk attitude.

TABLE C6

ILLUSTRATIVE EXAMPLE MATRIX WITH 'SKEW'

Likelihood	**V**	Medium	High	High	Very high	Very high
	IV	Low	High	High	Very high	Very high
	III	Low	Medium	Medium	High	Very high
	II	Low	Low	Medium	High	Very high
	I	Low	Low	Medium	Medium	High
		1	**2**	**3**	**4**	**5**
		Consequences				

It can be seen that in the matrix in Table C6 there is a skew so that risks with the highest levels of consequence, even if the likelihood is very low, are rated high or very high. This might be appropriate for an organization with a risk attitude that is strongly averse to high consequence events. By contrast, Table C7 would be appropriate for an organization with no such aversion.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

TABLE C7

ILLUSTRATIVE EXAMPLE MATRIX WITHOUT 'SKEW'

Likelihood	**V**	Medium	High	Very high	Very high	Very high
	IV	Medium	High	High	Very high	Very high
	III	Low	Medium	Medium	High	Very high
	II	Low	Low	Medium	Medium	High
	I	Low	Low	Low	Medium	High
		1	**2**	**3**	**4**	**5**
		Consequence				

All such matrices should be accompanied by a legend that explicitly describes the steps on the scales.

If there are multiple consequence and likelihood pairs for a particular risk (which is the common case), there is the option of combining several pairs, or adopting a rule set for selection of one or more representative pairs. For example, the distribution of the pairs can be represented by the mode of the distribution of consequence (i.e. the consequence that is most likely to result from the event), or by a pair with high consequence and a pair with high likelihood, or by using a three point estimate approach to derive a single point by considering all three of the previous pairs.

Whichever method is used to combine consequences and likelihoods, it is important that it is validated and agreed by the organization's governing body. One way of assisting the governing body to do this is to use the proposed risk criteria to analyse some of the organization's risks, and then for the governing body to examine the results in terms of whether they align with their perceptions and expectations.

C2.6 Step 5: Decide how the level of risk will be expressed

Simple labels such as high, medium and low can be used to express the level of risk or a numerical scale could be used. To avoid confusion, it is preferable that the terms (or numbers) used to describe the level of risk are different from those used to describe levels of consequences or likelihood. For example, a 1, 2, 3… scale could be used for one, whereas as I, II, III or A, B, C scale could be used for another—this also helps remind those using these scales not to attempt invalid arithmetical manipulations (refer to Table 4). Because consequences may be beneficial or detrimental, pejorative terms such as 'extreme' or 'undesirable' should be avoided.

The training and communication aspects of the risk organization's risk management framework should ensure there is consistency in use and appreciation of the risk criteria across the organization.

Once the organization decides how many levels of risk it wishes to discriminate, colour coding each of the squares of the matrix to correspond with the level of risk assigned to that combination of consequence and likelihood is useful. However, this depends on the users of the diagram understanding the meaning, on that particular matrix, of each of the selected colours, and therefore the relative levels of risk represented by each colour.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

There is little point having many levels of risk (and labels for these) if the organization cannot meaningfully resolve and respond to that level of resolution. On the other hand, too few graduations means that within one level (or colour), there can be quite a wide range of values making it more difficult to realistically portray the risk, especially if there is significant uncertainty in the analysis. In practice, this normally will mean that four or five levels of risk are sufficient (as noted, the number of graduations of consequences and likelihood need not be symmetrical).

C2.7 Step 6: Establish the rules for evaluating risk

The organization should develop a rule set to enable consistent decision making when evaluating risk. The components of the rule set are described in Clause 5.3.5(6) of this Handbook. The rule set provides the basis for making decisions about whether to treat risk, the priority for doing so, the urgency for completion of risk treatment plans, and the willingness of the organization to continue to tolerate particular levels of risk (pending completion). The rule set may include cautions about ensuring that, where relevant, risk is considered in the aggregate. The rule set will also have relevance to both the selection and implementation of risk treatments, which are described in Clauses 5.5.2 and 5.5.3 of the Standard respectively.

The evaluation rule set should also reflect and incorporate the organization's system of delegated authorities* to accept risk that is normally established as part of the risk management framework.

ALARP

A common form of risk acceptance criteria that can form part of the risk evaluation rule set is 'as low as reasonably practicable' or 'ALARP'. Essentially, this works on the assumption that there are some levels of risk that are not acceptable under any circumstances (e.g. those where the level of risk is very high), and there are also some levels of risk that do not warrant further consideration (e.g. those where the level of risk is low).

Risks where the level of risk is between these levels should be treated, unless and until the effort and cost required is grossly disproportionate to the benefit derived from the reduction in risk (e.g. determined by using cost benefit analysis).

This latter consideration is particularly relevant to regulators who sometimes respond to the advancement of knowledge by adding additional controls without also repealing requirements for controls that were based on superseded technologies or methods. This overlooks that a strong driver for the adoption of the ALARP approach is to facilitate efficient risk management.

If particular types of risk are subject to regulation or there is an associated potential for litigation, risk criteria will need to be consistent with the legislation or relevant common law.

As a general rule, if risk treatment is warranted, the preferred outcome will be to modify the risk as soon as possible in order to obtain the benefits from doing so and avoid the disbenefits of continuing exposure to unwanted risk. However, even with the best intentions, it is seldom possible or practicable to implement and complete all risk treatment plans immediately (see the box below for examples of such considerations).

* The role of formal delegations of authority to accept risk can be found in the opening paragraphs of Clause 5.3.5 of this Handbook.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

Practical considerations affecting implementation of risk treatment plans

Common factors that can prevent immediate implementation include the following:

- A need for consultation with stakeholders likely to be affected by the treatment.
- The time required to plan the detail of the treatment and then to obtain budgetary approval.
- Reliance on the same workforce to implement several treatments.

In some cases where the treatment would result in significant disruption (e.g. if the work involved required continuously operating equipment to be shut down followed by a lengthy restart process), it may be warranted to schedule the work to coincide with the next planned shutdown, depending on the urgency for completion of the treatment.

If all treatments can't be implemented immediately, it makes sense to give priority to those where the level of risk is highest and where treatment will bring about the greatest benefits to the organization. In many cases, where it is not practically possible to fully implement a treatment that has high priority, every effort should be made to devise an interim mix of actions to gain appreciable, if not full, modification of risk (e.g. posting temporary guards and floodlighting throughout the construction period for a new security fence).

The rules for evaluating risk should therefore include consistent rules relating to the continued exposure to risks, pending completion of treatments.

Table C8 gives an example of an evaluation rule set that incorporates many of the above considerations. Along with other aspects of the risk criteria, it should be signed off by the governing body, understood by managers, and used to report against in relation to progress with outstanding risk treatments.

TABLE C8

ILLUSTRATIVE EXAMPLE OF RISK EVALUATION RULE SET

Level of risk	Acceptability	Urgency for implementation of treatment	Authority for continued toleration of risk at this level
Very high	Not permitted unless approved by the Board. Reduce the level of risk to high or below.	Immediate—stop until treated. For complex treatments, implement short-term controls with permanent treatments completed within 1 month.	Board
High	Only acceptable if it is not practicable or efficient to reduce the level of risk. Otherwise reduce the level of risk to medium or below.	As soon as possible, but complete within 3 months.	Chief Executive Officer
Medium	Acceptable for a limited period of time to allow treatment to be in keeping with the business or project plan priorities.	Treat as soon as practicable but within 1 year.	General Managers
Low	Plan to treat in keeping with all other priorities.	Ongoing control as part of general or routine management activities	Managers

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

C3 USE OF MATHEMATICAL DISTRIBUTIONS TO EXPRESS LEVEL OF RISK

It is not always appropriate or helpful to express the level of risk as a point value. Reasons for this include the following:

- The range of consequences is uncertain because there is insufficient historical data or other reliable methods of prediction (e.g. the effect of a new virus, either health or software related).
- The consequences of events range considerably according to the circumstances (e.g. the effect of bushfires).
- The magnitude of a given event can vary according to a power law (e.g. the amount of energy released by an earthquake).
- The magnitude of the consequences can vary according to a power law (e.g. the consequences of an earthquake of a given size at any one location).
- There is a non-linear relationship between consequences and probability.
- There is a bi-modal relationship between consequences and probability (e.g. the effect of prolonged high temperatures on a general population, which reflects the greater susceptibility of the young and old).

This Paragraph (C3) outlines considerations to be taken into account when analysing risk using quantitative methods, where it is required to demonstrate the level of risk as a distribution of consequences and their respective likelihoods.

There are many methods for assessing likelihood (of events or of consequences). Some of these methods are described in HB 89:2013, *Risk management—Guidelines on risk assessment techniques*. They include Monte Carlo simulation and Bayesian networks. There are also probability boxes, loop analysis, cognitive maps, fuzzy sets, interval analysis and info-gaps.*

Similarly, there are many techniques that can be used to assess the extent of consequences. They include utility analysis, swing weights, values trees, consequence chains and willingness to pay.

The likelihood of experiencing any particular consequence must take into account two likelihoods—the likelihood of occurrence of event(s) of the type revealed during the risk identification, step and the likelihood that this will trigger the particular type and level (or value) of consequence also identified during this step.

This recognizes that the event might or might not happen, or will do so with greater or less certainty (which will be influenced by a range of relevant factors and predecessor circumstances), and that variability in those and other factors (such as the reliability of controls) means that the extent of the consequences can also be uncertain, and therefore a range of effects is possible.

The combination of the estimates of the above two likelihoods and the extent of consequence can be mathematical or judgemental.

If mathematical, each point on the consequence range is given a likelihood estimate of its occurrence, and then the expected value is used to represent the best linear unbiased estimate of the consequence.

If judgemental, then there are estimates of the low point of the consequence range, the likely mid-point, and the upper point of the range. Then various formulae are used to determine the point estimate for the consequence.

---

* Further guidance is available from Hayes, K (2011) Uncertainty and uncertainty analysis methods, *Report EP102467*. Canberra, Australia: CSIRO.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

Combining likelihood and consequence can be used to determine the expected value of the consequence. Expected value of the consequence is familiar to financial analysts or statisticians as the mean value. A mean is the point estimate of a set of outcomes multiplied by the probability of each outcome, if the probability distribution of the consequence scale is normal (or Gaussian). This determination requires a complete set of combinations of likelihood for each consequence value.

In many situations, decisions about whether to treat risk and the selection of risk treatments need to take into account not only the expected value, but also the variations that might occur.

As noted, point estimates of likelihood or the extent of impact can be over precise (and even inaccurate). Risk analysts often use three point estimates (low, likely and high) to represent the uncertainty in their judgement of these parameters. After that, a formula is used to combine these estimates into a single figure that is used in subsequent calculations.

Traditionally, the composite formula has been (low + 4 × likely + high)/6. The formula has been derived from the properties of a normal or Gaussian distribution. There is a better basis for point estimates that does not have the same need for a purely normal distribution. The preferred basis is the Pearson–Tukey approximation:

$$[0.63 \times \text{Median} + 0.185 \times (0.05\% + 0.95\%)].$$

Regarding likelihood or consequence as a fixed estimate rather than a band of estimates does not matter much, as long as the distribution of possible values is symmetrical around a point on the scale. Any formula will result in the point estimate being the same as the central estimate (mean or median).

The main assumption that underlies the use of this combination of consequence and likelihood is that the probability distribution of the consequence scale is normal. It is possible that the consequence scale, at least, follows a probability distribution that is not normal. An example of such a distribution is the power law function found for the severity of earthquakes.

In these cases, the use of expected value does not apply. The mean is no longer representative of the central point of the distribution and the standard deviation is not suitable as the representation of the spread of the distribution. The combinations of likelihood and consequence can be most misleading.

If a power law applies to the probability distribution then it can be difficult, if not impossible, to derive the expected value or variance as point estimates. For some distributions, depending upon the exponent in the power law equation, the mean or variance can be infinite. In other cases it might be finite but unobservable, with samples unable to converge to a population result. In these cases, a log normal distribution might be a more useful, if somewhat inaccurate, approximation.

As well, if the range of likelihood is within a single scale point used in the qualitative approach, then its spread has no effect upon estimating risk exposure. Awareness of the assumptions underlying the estimates is therefore necessary in the consideration of the results, however it is preferable to use a technique for determining the level of risk that avoids making these assumptions.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

APPENDIX D

INTEGRATION GUIDELINES

D1 INTRODUCTION

For an organization to always understand its risks, and to decide whether and how to treat those risks, its risk management framework needs to provide the capacity and capability to routinely apply the risk management process to its decisions. Achieving this understanding requires the components of the framework to be quickly integrated into the organization's normal systems of governance and management.

Paragraph D2 provides guidance as to how to integrate the components of the risk management framework into the organization's systems of governance and management.

Paragraph D3 explains how to routinely integrate the risk management process into all forms of decision making, irrespective of level or purpose.

Such integration promotes two forms of efficiency. Firstly, it favours amending existing organizational practices wherever possible rather than creating entirely new components solely for the purpose of managing risk (with the potential for confusion, conflict and repetition). This is particularly valuable for an organization making the transition to align with the Standard as it also facilitates faster progress. Secondly, it avoids the organization finding itself in the situation of making decisions, only to discover later—after risk assessment—that the decisions need to be changed or corrected, with additional meetings, often resulting in additional cost and frustration, and slower progress.

D2 INTEGRATION OF COMPONENTS OF THE RISK MANAGEMENT FRAMEWORK

D2.1 General

The components of the risk management framework provide the intent and capacity that enables the organization to apply the risk management process to decisions.

The general forms of many components of a risk management framework are not unique to risk management activities. The following are examples:

- Many organizations already direct their activities through the use of documented policies and processes (in some organizations these may include standardized management subsystems such as ISO 9001).
- It is common to use written job descriptions and delegations to document accountabilities and responsibilities.
- Individual performance is often evaluated using formalized measures such as key performance indicators (KPIs).
- Many organizations already have systems to collect and manage information, and to provide staff training.
- Internal and external auditors are deployed to monitor and review the organization's activities in order to provide assurance.

The above components (and many others like them) can be modified, or have subcomponents or other features added to support or facilitate application of the risk management process. Taking one example from the above list, the requirement in the Standard to allocate accountabilities could be simply achieved by amending existing position descriptions and delegations.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

Other components (such as risk information and training systems to provide necessary risk management competencies) will often be most conveniently hosted by existing functions in the organization, even though they are specific to risk management. In practice very few, if any, components of the risk management framework can or should operate on a standalone basis.

Such integration makes it more likely that risk management activities are performed consistently and effectively as a part of the organization's normal planning and operations.

Therefore, aligning the organization's risk management framework with the Standard will mainly involve adjustment and adaption of numerous current practices within the organization's overall systems of management, rather than creating an entirely new set of institutional arrangements.

Incorporating any required changes into existing practice is best achieved using conventional change management practices (refer to Paragraph D.2.2). Depending upon the extent of change, this may also have the consequential effect of changing aspects of the organization's culture. For example, by creating a general enthusiasm for the usefulness of the risk management process as a means of making better decisions.

Because the external environment and internal conditions are likely to change, monitoring and review practices to detect and respond to such changes should also be an integral part of the risk management framework. This also facilitates continuous improvement wherever this is possible.

D2.2 Method

D2.2.1 *Transitioning*

Transitioning the risk management framework to align with the Standard is best achieved using conventional change management practices, as explained in greater detail in Appendix A of this Handbook. This transitioning is generally as follows:

- Identify the required framework components in detail and the required performance of each (this will require consideration of the results of the analysis of decision making practices that are described in Paragraph D3).
- Identify which components are already part of the organization's systems of management and where in those systems that they exist.
- Evaluate existing risk management framework components against what is required.
- Identify any new components, and decide where and how these can be best integrated into existing organizational systems.
- Develop a plan to make necessary changes, including any related or consequential changes (e.g. changing what risk management information is to be reported monthly may require a change to reporting templates and related training).
- Decide how the component will be monitored and reviewed on an ongoing basis, and integrate such assurance arrangements into the plan.
- Assess the risks associated with the plan.
- Implement the plan.
- Monitor and review on an ongoing basis, and improve where possible.

D2.2.2 *Accommodating other, existing formal management subsystems and legislation that apply different meanings to the terms defined in the Standard*

Although the Standard uses the expression 'risk', the Standard is actually providing principles and guidelines for managing the effect of uncertainty on objectives. The central focus is therefore the organization's objectives and the uncertainties involved in pursuing those objectives.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

Other documents or legislation may also use the expression ‘risk’, but have a different focus, for example, on particular risk sources (such as hazards) or the possible magnitude of particular types of consequences. Such differences are neither right nor wrong.

Differences in meaning of words can also reflect the fact that the other documents may have predated the Standard and the related ISO risk management vocabulary document ISO Guide 73. However, the risk management process in the Standard can only be relied upon to achieve the outcomes described in Annex A of the Standard if it is properly applied to all decisions (see also Section 6 of this Handbook).

Paragraph D3 provides techniques for identifying decision points, and therefore where and when the risk management process should be applied. These methods are applicable for organizations that have adopted standardized management subsystems, as well as those that have not.

Therefore, for organizations that have adopted published standardized management subsystems, the most important tasks for integrating the components of the risk management will be to—

- ensure those involved understand the central focus of the Standard on the organization’s objectives and on uncertainty, and therefore become accustomed to making decisions based on the likelihood of experiencing particular consequences rather than, for example, just the scale of the consequences;
- recognize and understand any differences in meaning between words used in the Standard and in the particular management subsystem, so as to avoid misapplication of the Standard;
- wherever practical, accurately substitute the relevant terminology from the Standard and meanings by amending the wording of internal documents required by standards for particular management subsystems (although such management subsystems may not be described in their title as being concerned with risk management, most are e.g. although ISO 9001 is widely known as a standard about quality management, its whole purpose is in fact to manage quality related risk);
- identify decision making points in the management subsystem, and ensure that at those points risk is assessed and as necessary treated by applying the risk management process; and
- acquire the necessary skills.

D3 INTEGRATING THE RISK MANAGEMENT PROCESS INTO DECISION MAKING

D3.1 General

This Section provides advice about how the risk management process (which is the method for revealing and understanding risk, and modifying where necessary) can be integrated into an organization’s decision making processes, irrespective of the level at which those decisions are made or the apparent significance of the decision. This requires people to be aware of making decisions at the time decisions are made.

The importance of applying the risk management process to decisions is because risk is generated or modified when decisions are taken and acted on. However, decision making occurs constantly throughout every organization, and ranges in significance from strategic decisions affecting the future direction of the organization to operational decisions through which daily tasks are completed.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

The relative importance of a decision (e.g. strategic versus operational) is not necessarily indicative of the resultant level of risk. Decisions that may seem minor can have strategically calamitous (or beneficial) consequences. That is why Principle (c) of Clause 3 of the Standard states 'Risk management is part of decision making'.

The words 'part of' in Principle (c) emphasize that risk should be assessed (and, if necessary modified) at the time the decision is being made, that is as an integral part of the decision-making process. If risks are consciously considered only after the decision has been made and implementation is already underway, additional action to treat the risk may be necessary. Such retrospective treatment may involve additional cost, and either change the net benefit of the activity or even cause it to be abandoned. Integrating the risk management process into decision making is clearly more efficient.

This is not so difficult when major decisions are being taken (e.g. approving a large capital investment), but there is often less awareness of apparently insignificant decisions of the type made each day.

Decision making often involves a sequence of decisions, sometimes with different people holding ultimate accountability at each decision point. Unless each decision in the sequence is fit for purpose, and therefore subject to risk assessment and as necessary risk treatment, there may be compounding error and cumulative risk. The decisions that take place during a typical project lifecycle are illustrated in Figure 9. The risk management process should be applied when making each of the decisions depicted.

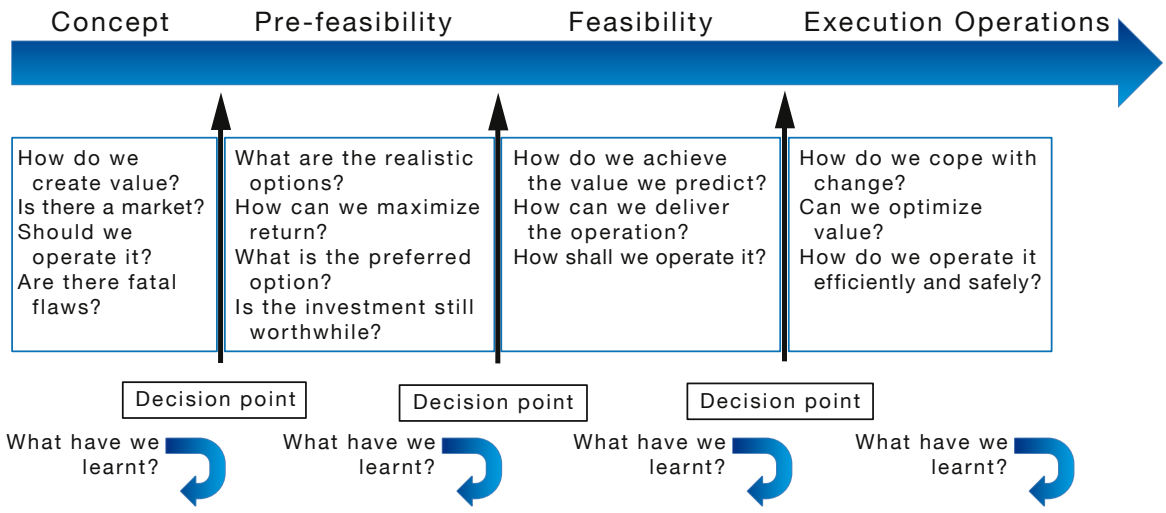

FIGURE 9 SEQUENTIAL DECISION MAKING WITHIN PROJECT PHASES REQUIRING THE APPLICATION OF THE RISK MANAGEMENT PROCESS (Aligned with IEC 62198)

D3.2 Methods

D3.2.1 *Recognizing decision making*

The following three methods help recognize when and where decisions are being made and increase awareness of decisions having being made:

(a) **Formal decision making:** Identify all forms of formalized decision making practices that already exist within the organization (including those that occur as part of 'plan, do, check, act' management practices).

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

Example

In large organizations particularly there are likely to be numerous specified procedures that require formal approvals for a wide range of decisions. These may include procedures for approval of the annual strategic plan, capital expenditure, employment of new staff, modification of process controls, staff travel, etc.

(b) **Flow charting:** Use flow charting or some other technique to map the main decision making practices, including sequences, used both in projects and in other aspects routine activities throughout the organization. This should extend to governance, as well as management decision making at all levels and in all parts of the organization.

If there are activities that are being managed through application of a formalized management system (e.g. managing quality through use of ISO 9001) then the decision points in such systems should form part of this analysis. Similarly, if the organization has any form of delegated decision making authority (e.g. authority to incur expenditure) such delegations should be included in the analysis.

The end result should be a coherent and documented picture of where decisions are made, who makes those decisions, and the existing processes applicable to such decisions such as is shown in the example below D3.2.1(c).

(c) **Awareness training:** Specific training can be used to create awareness of less formal decision making (i.e. the type of decision that is often perceived as 'just a normal part of my job') and to encourage integration of the risk management process into such decision making.

Example

Even the simple technique of asking each manager and supervisor to list all the decisions that they had taken the previous day (irrespective of apparent importance) can considerably improve awareness of decisions having been made. This initial awareness technique can be reinforced informally on an ongoing basis by managers routinely asking their subordinates to discuss the decisions they took in the past period (e.g. past shift, past day or past week).

D3.2.2 *Timing*

Ensure that the risks associated with decisions are understood at the time the decision is being made so that any necessary treatment is incorporated in the final decision. In practice, this generally means that the decision making process will occur in two stages—the development of a draft or a tentative decision, and the finalization of that decision based on assessment of the risks associated with the draft.

The amount of effort required will usually depend on the risk management competencies of those involved and the complexity of the decision. For example, the risk assessment of a major infrastructure project could take several weeks, whereas the risk assessment of a small maintenance task might take only a minute. Competencies will reflect training but typically increase rapidly with the practical experience of application of the risk management process.

D3.2.3 *Amending decision making processes*

Integration of the risk management process into the type of formalized decision making processes referred to above is achieved by—

- making changes to the decision making process and documenting those changes, for example in the organization's project management manual;
- training those involved; and
- adjusting the assurance arrangements to monitor and review actual performance.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

Adjustments may also be needed to any formal statements of responsibility such as in job descriptions or delegations.

In projects, decisions would typically occur at (at least) each of the following stages:

- Business case.
- Feasibility.
- Technical design.
- Detailed budgeting and planning (specification).
- Implementation (e.g. construction).
- Handover.

Formal risk assessment at each of these stages will also help decide between options (including the option to terminate the project). This increases the likelihood of project success and realization of objectives and improves efficiency and, often, reputation. The reverse is also true (see box).

Example

The roll out of a very innovative type of new airliner was initially delayed by several years due to unforeseen design, supply chain and construction problems. Soon after entering service, it was grounded for several months after undetected technical design problems resulted in inflight emergencies. It is apparent that adequate risk assessment had not been integrated into the decisions made at some points during the development of the airliner.

D3.2.4 *Ad hoc decision making*

Simple standardized forms of the risk management process can be developed for risk assessment of small frequently performed and often ad hoc operational decisions. These should still be consistent with each of the steps of the risk management process, otherwise there can be no certainty that they will reflect the organization's objectives or that the risks will be within the organization's criteria.

Such standardized methods are especially suitable where people are working without direct supervision and having to rely on their own judgement. A key component of these methods is to create heightened awareness of assumptions as inputs to decisions. By definition, assumptions are a source of uncertainty.

These standardized processes can be specific to the type of decision making involved, to particular groups of people, to particular tasks or to typical work environments. Such simple systems sometimes have a name such as 'take five' (meaning, take five minutes to understand the task and the risks and if necessary, adjust the risks), and can often be codified on a pocket sized instruction card carried by all those involved in that type of decision.

D3.2.5 *Implications for the risk management framework*

Implementation of the foregoing methods for integrating the risk management process into all decision making may require adjustments to some of the components of the risk management framework, such as the following examples:

- Amendment of the organization's risk management policy.
- Arrangements to carry out the initial investigation and mapping of decision making practice.
- Amendments to procedure manuals including those associated with formalized management systems.
- Development of standardized methods for ad hoc decisions.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

- Training of managers and staff (and, if necessary, those on the governance oversight body).
- Specific training of those whose work is carried out in accordance with a specific management system.
- Adjustment of the organization's system of assurance in order to monitor application of the risk management process to all forms of decision making and review the quality of the risk assessments.

Effective internal communication and consultation with those who will be affected by such changes will help both the design of the change and subsequent uptake. Simple communication techniques can also be used to increase awareness of daily operational decision making (see box).

Example

Eyes of awareness

One insurance company encouraged awareness of decisions relevant to fire safety by introducing small signs with a symbol consisting of two stylized eyes. The stickers were placed in their client's premises on such things as fire doors which were meant to be closed or pressure gauges that were meant to be checked. The stickers were supported by staff training that linked the symbol to the slogan 'the eyes of awareness'. The objective was to create awareness that in deciding whether to leave the door open or closed (for example), an important decision was being made.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

APPENDIX E

DEALING WITH PARTICULAR CHALLENGES TO EFFECTIVE COMMUNICATION AND CONSULTATION

E1 Introduction

This Appendix lists some frequently encountered challenges to communication and consultation and provides a range of practical solutions.

E2 Language differences

- Select people with clear diction and well-modulated voices to speak on behalf of the organization.
- Make greater use of visual information such as graphs and charts.
- Provide a written version of what is to be said, or provide subsequent notes, minutes or transcripts.
- Provide a written, oral or signing translation, particularly of essential points.
- Offer access to a translation service.
- Repeat back questions to ensure the intent is understood, and confirm that answers have been understood and sufficiently addressed the question.

E3 Technical complexity

- Attempt to establish the level of technical knowledge in a non-patronizing way (e.g. at a public consultation about a new cell-phone tower, 'would anyone be assisted if I was to explain how electromagnetic waves can affect people'), and adjust the language and structure of the discussion accordingly.
- Use plain language to explain technically complex issues without recourse to jargon, and use people who are skilled in doing so.
- Use illustrations, every day comparisons and other examples (but ensure the examples are appropriate).
- If one participant asks a complex but valid question or uses jargon, translate or paraphrase the question into language able to be comprehended by the other participants (checking as necessary with the questioner that the original meaning has not been lost).
- Provide opportunities for further explanation at another time.

E4 Uncertainty

- Uncertainty can take many forms (see Clause 2.2 of this Handbook). Therefore, explain the nature of the particular uncertainties and the reason for the uncertainty while providing as much certainty as possible. For example, if the exact magnitude of some future event is unknown but it is known that it will occur within a particular range, both facts should explained rather than simply saying that it is uncertain as to when it will happen.
- Avoid implying certainty to appease anxieties if there is still residual uncertainty. For example, if asked if money invested in a company with a 'AAA' rating is safe, the answer should explain that there are no cast-iron guarantees and that there is still risk that investors could lose money.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

E5 Timing

- Legitimate issues of urgency might require decision making to occur within a compressed timeframe. If so, explain the reasons for that, and demonstrate that the best possible effort is being made to allow effective communication and consultation in the time available, even if this must be compressed. This might involve a change of technique (e.g. using web surveys rather than interviews) or scheduling meetings at more convenient times.
- Meetings might need to be completed within a finite duration while still covering the subject matter. Plan the time accordingly, explain the constraints from the outset, and stick closely to the plan. If it appears that people have not been able to have their say, provide an additional communication option such as an email address (and deadline) for submissions.
- Communication and consultation planning should consider the timeliness of certain activities, having regard to the timing of the other elements of the risk management process. This should consider the time needed by people to assimilate information.

E6 Large meetings

- Meetings are demanding of participant's time and are dependent for their effectiveness on all participants being and feeling able to contribute. In some cases it might be possible to achieve the purpose of a meeting using alternative media such as blogs or other social media, as these allow everyone to express their views or challenge those of others in their own time.
- Clear ground rules should be set for meetings with ample emphasis on rights and opportunities for the audience, rather than simply constraints and prohibitions.
- Well-attended meetings present logistical and other management challenges, particularly if contentious viewpoints are involved. Participants should be able to observe from the organizational arrangements (e.g. available seating, audibility, sightlines, roving microphones, readability of exhibits, provision of toilets, etc.) that their reasonable needs have been considered, and that their presence is appreciated and welcomed.
- Try to become aware of any intentions by individuals to sabotage meetings and be prepared.
- Use amplification to ensure audibility.
- Use an experienced facilitator adept at conveying even-handedness.
- Have the facilitator brief or train any experts who have to speak but are not accustomed to speaking to this type of audience.
- Clearly explain, agree and strictly follow an agenda.
- Ensure that participants not adept at speaking are treated with respect and assisted if necessary to express their views (e.g. confirming their question but, if necessary, in a more succinct way).
- Adopt some method that allows people to see that their views have been heard and taken into account (e.g. using a whiteboard to note bullet points).
- Confirm that questioners accept that their question has been answered (even if they are not in agreement with the answer).
- Where it is necessary to give undertakings to make further inquiries before providing answers, explain how and when the answers will be provided.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

E7 Conflicts of interest

- Be aware of actual, potential and perceived conflicts of interest.
- The general rule for a conflicted individual or organization is to declare the conflict and explain how it is being managed (e.g. the conflicted party—while making their knowledge available—won't participate in the resulting decision, or some other party will deal with questions falling within the scope of the conflict).
- In some cases it might be helpful to provide copies of a signed conflict of interest declaration and an agreed management plan, and to make these freely available.

Tips

- Seek and understand the views and concerns of stakeholders, and involve them from the outset.
- Release information as it becomes available.
- Differentiate between fact and opinion.
- Recognize genuine misunderstanding and help stakeholders obtain a correct appreciation of facts.
- Avoid secrecy, be frank.
- Check facts.
- Be familiar with relevant local knowledge and history.
- When dealing with stakeholders, recognize there are no dumb questions.
- Adjust the language to suit the audience and purpose.
- Avoid jargon and complex forms of expression.
- Give people time to assimilate complex issues.
- Acknowledge any uncertainties and limits of available information.
- Only make promises that can be kept.

E8 Anger

- Anger is best dealt with by the preparatory measures already described, but should it occur, is usually best countered with patience, calmness, a quiet voice, respect, giving a fair hearing by clearly paying attention to the concerns of those who are angry, and with even-handedness. This applies to all forms of communication.
- At meetings, remind those seeking to monopolize the discussion that they are encroaching on the reasonable aspirations of others to be heard.

E9 Meeting dynamics

- Be aware of any reticence of participants to contribute because of the dominant position, perceived or actual, of one person present (e.g. due to their seniority, or their technical or verbal expertise).
- Techniques to counter this might include holding multiple meetings, positioning the dominant people to the side or out of the line of sight of the facilitator, and positively eliciting inputs from reticent or shy participants.

E10 Precedents

- Be mindful of creating precedents through hasty on-the-spot decision making or definitive statements. Anyone is entitled to have sufficient time to give consideration to questions before answering if these are complex or cover new ground (take questions on notice).
- If precedents are set, including stating a position, notes should be made for future reference.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

E11 Design of questionnaire/survey

- Surveys and questionnaires need careful design and unambiguous wording that avoids bias or assumptions.
- Questions should be even-handed (non-directive), and wherever possible open rather than closed (yes or no), although where options are clear, multiple-choice type questions might be appropriate.
- Avoid mixing two ideas in the same question.
- For some questions it can be useful to provide a scale for responses (e.g. using 1 for ‘completely agree’, down to 7 for ‘completely disagree’).
- It can be helpful and will generally build trust to provide an opportunity for additional comment.
- Use a test group to trial the questionnaire or survey before it is issued.

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

APPENDIX F
TERMS AND DEFINITIONS

This Appendix contains the terms and definitions in Clause 2 of AS/NZS ISO 31000:2009, as copied from Clauses 1, 2 and 3 of ISO Guide 73:2009.

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]

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

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 3.5.1.4]

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** (2.4)

[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** for the **risk management policy**

[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;

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

- 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, treatment or other aspects 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 a particular 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]

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

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 3.5.1.1]

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 3.5.1.2]

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]

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

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** 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]

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

2.24

risk evaluation

process of comparing the results of **risk analysis** (2.21) with **risk criteria** (2.22) to determine whether the risk 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;
- retaining the risk by informed choice;
- 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]

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

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]

COPYRIGHT
Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

NOTES

Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

Standards Australia

Standards Australia is an independent company, limited by guarantee, which prepares and publishes most of the voluntary technical and commercial standards used in Australia. These standards are developed through an open process of consultation and consensus, in which all interested parties are invited to participate. Through a Memorandum of Understanding with the Commonwealth government, Standards Australia is recognized as Australia's peak national standards body.

Standards New Zealand

The first national Standards organization was created in New Zealand in 1932. The Standards Council of New Zealand is the national authority responsible for the production of Standards. Standards New Zealand is the trading arm of the Standards Council established under the Standards Act 1988.

Australian/New Zealand Standards

Under a Memorandum of Understanding between Standards Australia and Standards New Zealand, Australian/New Zealand Standards are prepared by committees of experts from industry, governments, consumers and other sectors. The requirements or recommendations contained in published Standards are a consensus of the views of representative interests and also take account of comments received from other sources. They reflect the latest scientific and industry experience. Australian/New Zealand Standards are kept under continuous review after publication and are updated regularly to take account of changing technology.

International Involvement

Standards Australia and Standards New Zealand are responsible for ensuring that the Australian and New Zealand viewpoints are considered in the formulation of international Standards and that the latest international experience is incorporated in national and Joint Standards. This role is vital in assisting local industry to compete in international markets. Both organizations are the national members of ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission).

Visit our web sites

www.standards.org.au www.standards.co.nz

Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086

ISBN 978 - 1 - 74342 - 633 - 3

Standards Development
Standards Australia
GPO Box 476
Sydney NSW 2001
Phone: 02 9237 6000
Fax: 02 9237 6010
Email: mail@standards.org.au
Internet: www.standards.org.au

Sales and Distribution
SAI Global
Phone: 13 12 42
Fax: 1300 65 49 49
Email: sales@saiglobal.com

Sheridan College - reproduced with permission from Standards Australia under copyright licence 1801-c086