LICENCE

for

AS/NZS 4360 SET Risk Management Set

Licensee: Carmen Green Zevallos

Date: 06 Jun 2007

Conditions of use: **Click here for full conditions of Licence**

WEB LINKS

- Check if this document is current
- Find similar documents
- StandardsWatch *(info and login)*
- Visit our website

HB 436:2004

RISK MANAGEMENT GUIDELINES

Companion to AS/NZS 4360:2004

STANDARDS AUSTRALIA

STANDARDS NEW ZEALAND
Paerewa Aotearoa

Handbook

Risk Management Guidelines Companion to AS/NZS 4360:2004

Originated as HB 142—1999 and HB 143:1999.
Jointly revised and redesignated as HB 436:2004.
Reissued incorporating Amendment No. 1 (December 2005).

Jointly published by Standards Australia International Ltd, GPO Box 5420, Sydney, NSW 2001 and Standards New Zealand, Private Bag 2439, Wellington 6020

ISBN 0 7337 5960 2

Preface

This Handbook provides generic guidance for establishing and implementing effective risk management processes in any organization. It demonstrates how to establish the proper context, and then how to identify, analyse, evaluate, treat, communicate and monitor risks.

This Standard incorporates Amendment No. 1 (*December 2005). The changes required by the Amendment are indicated in the text by a marginal bar and amendment number against the clause, note, table, figure or part thereof affected.*

This Handbook is based on the Joint Australian/New Zealand Standard, AS/NZS 4360:2004, *Risk management* (the Standard). Each Section contains an extract from the Standard, followed by practical advice and relevant examples.

This basic guide provides a generic framework for managing risk. It may be applied in a very wide range of organizations including:

- public sector entities at national, regional and local levels;
- commercial enterprises, including companies, joint ventures, firms and franchises;
- partnerships and sole practices;
- non-government organizations; and
- voluntary organizations such as charities, social groupings and sporting clubs.

It provides a reference for directors, elected officials, chief executive officers, senior executives, line managers and staff when developing processes, systems and techniques for managing risk that are appropriate to the context of their organization or their roles.

The contents are intended to provide only a broad overview of risk management. Organizations are expected to interpret this guide in the context of their own environments and to develop their own specific risk management approaches. Ultimately it is up to the risk makers and the risk takers to develop and manage their own risk management programmes.

Attributions

Standards Australia International acknowledges, with thanks, the contribution of the following organizations in the development of this Handbook:

Australian Computer Society

Australian Customs Service

Australia New Zealand Institute of Insurance and Finance

CSIRO (Commonwealth Scientific and Industrial Research Organisation)

Department of Defence (Australia)

Department of Finance and Administration

Emergency Management Australia

Environmental Risk Management Authority (New Zealand)

Institute of Chartered Accountants (Australia)

Institution of Engineers Australia

Institution of Professional Engineers New Zealand

Local Government New Zealand

Massey University (New Zealand)

Minerals Council of Australia

Ministry of Agriculture and Forestry (New Zealand)

Ministry of Economic Development (New Zealand)

NSW Treasury Managed Fund

New Zealand Society for Risk Management

Risk Management Institution of Australasia

Safety Institute of Australia

Securities Institute of Australia

University of New South Wales

Victorian WorkCover Authority

Water Services Association of Australia

Contents

Introduction

Risk management is a key business process within both the private and public sector around the world. Sound and effective implementation of risk management is part of best business practice at a corporate and strategic level as well as a means of improving operational activities.

This Handbook states in Clause 4.2 that risk is the chance of something happening that will have an impact on objectives. In English, usage of the word 'risk' usually has negative connotations, and risks are regarded as something to be minimized or avoided. In our more general definition, it is recognized that activities involving risk can have positive as well as negative outcomes. The processes described here can be used to identify and exploit opportunities for enhancing organizational outcomes as well as reducing negative consequences.

Risk management, as described here, is a holistic management process applicable in all kinds of organizations at all levels and to individuals. Readers should be aware that this usage of the term differs from a more restricted usage in some sectors. For example, in some areas the terms 'risk management' or 'risk control' are used to describe ways of dealing with identified risks, for which we use the term 'risk treatment'.

Some other terms used in this document also have different usages. For example the terms 'risk analysis', 'risk assessment' and 'risk evaluation' are variously used in risk management literature. They often have overlapping and sometimes interchangeable definitions, and they sometimes include the risk identification step. We have selected terminology that forms the basis of international standards.

Other handbooks have been developed that address applications of AS/NZS 4360 in specific areas (see Section 12).

In some areas there is a division of responsibility between those who carry out the analytical process of identifying and analysing risk and those who make the decisions about risk evaluation and the selection of actions to deal with identified risks. This is beneficial where it is important that risk analysis be seen to be independent, and possibly undertaken by technical specialists, with decision aspects of risk evaluation and selection of risk treatment options being the responsibility of senior decision makers. This guide does not deal with such divisions of responsibility, but they are compatible with the processes described here.

1 Scope and general

AS/NZS 4360:2004

1.1 Scope and application

This Standard provides a generic guide for managing risk. This Standard may be applied to a very wide range of activities, decisions or operations of any public, private or community enterprise, group or individual. While the Standard has very broad applicability, risk management processes are commonly applied by organizations or groups and so, for convenience, the term 'organization' has been used throughout this Standard.

This Standard specifies the elements of the risk management process, but it is not the purpose of this Standard to enforce uniformity of risk management systems. It is generic and independent of any specific industry or economic sector. The design and implementation of the risk management system will be influenced by the varying needs of an organization, its particular objectives, its products and services, and the processes and specific practices employed.

This Standard should be applied at all stages in the life of an activity, function, project, product or asset. The maximum benefit is usually obtained by applying the risk management process from the beginning. Often a number of discrete studies are carried out at different times, and from strategic and operational perspectives.

The process described here applies to the management of both potential gains and potential losses.

1.2 Objective

The objective of this Standard is to provide guidance to enable public, private or community enterprises, groups and individuals to achieve—

- a more confident and rigorous basis for decision-making and planning;
- better identification of opportunities and threats;
- gaining value from uncertainty and variability;
- pro-active rather than re-active management;
- more effective allocation and use of resources;
- improved incident management and reduction in loss and the cost of risk, including commercial insurance premiums;
- improved stakeholder confidence and trust;
- improved compliance with relevant legislation; and
- better corporate governance.

1.3 Definitions

For the purpose of this Standard, the definitions below apply.

1.3.1 Consequence

outcome or impact of an **event** (1.3.4)

NOTE 1: There can be more than one consequence from one event.

NOTE 2: Consequences can range from positive to negative.

NOTE 3: Consequences can be expressed qualitatively or quantitatively.

NOTE 4: Consequences are considered in relation to the achievement of objectives.

1.3.2 Control

an existing process, policy, device, practice or other action that acts to minimize negative risk or enhance positive opportunities

NOTE: The word 'control' may also be applied to a process designed to provide reasonable assurance regarding the achievement of objectives.

1.3.3 Control assessment

systematic review of processes to ensure that **controls** (1.3.2) are still effective and appropriate

NOTE: Periodic line management review of controls is often called 'control self assessment'.

1.3.4 Event

occurrence of a particular set of circumstances

NOTE 1: The event can be certain or uncertain.

NOTE 2: The event can be a single occurrence or a series of occurrences.

(ISO/IEC Guide 73, in part)

1.3.5 Frequency

A measure of the number of occurrences per unit of time.

1.3.6 Hazard

a source of potential harm

(ISO/IEC Guide 51, in part)

1.3.7 Likelihood

used as a general description of probability or frequency

NOTE: Can be expressed qualitatively or quantitatively.

1.3.8 Loss

any negative **consequence** (1.3.1) or adverse effect, financial or otherwise

1.3.9 Monitor

to check, supervise, observe critically or measure the progress of an activity, action or system on a regular basis in order to identify change from the performance level required or expected

1.3.10 Organization

group of people and facilities with an arrangement of responsibilities, authorities and relationships

EXAMPLE: Includes company, corporation, firm, enterprise, institution, charity, sole trader, association, or parts or combination thereof.

NOTE 1: The arrangement is generally orderly.

NOTE 2: An organization can be public or private.

NOTE 3: This definition is valid for the purposes of quality management system standards. The term 'organization' is defined differently in ISO/IEC Guide 2.

(AS/NZS ISO 9000)

1.3.11 Probability

a measure of the chance of occurrence expressed as a number between 0 and 1

NOTE 1: ISO/IEC Guide 73 defines probability as the 'extent to which an event (1.3.4) is likely to occur'

NOTE 2: ISO 3534-1:1993, definition 1.1, gives the mathematical definition of probability as 'a real number in the scale 0 to 1 attached to a random event'. It goes on to note that probability 'can be related to a long-run relative frequency of occurrence or to a degree of belief that an event will occur. For a high degree of belief, the probability is near 1.'

NOTE 3: 'Frequency' or 'likelihood' rather than 'probability' may be used in describing **risk** (1.3.13).

1.3.12 Residual risk

risk (1.3.13) remaining after implementation of **risk treatment** (1.3.26)

NOTE: See ISO/IEC Guide 51 for safety related applications.

1.3.13 Risk

the chance of something happening that will have an impact on objectives

NOTE 1: A risk is often specified in terms of an event or circumstance and the consequences that may flow from it.

NOTE 2: Risk is measured in terms of a combination of the consequences of an event (1.3.4) and their likelihood (1.3.7).

NOTE 3: Risk may have a positive or negative impact.

NOTE 4: See ISO/IEC Guide 51, for issues related to safety.

1.3.14 Risk analysis

systematic process to understand the nature of and to deduce the level of risk

NOTE 1: Provides the basis for risk evaluation and decisions about risk treatment.

NOTE 2: See ISO/IEC Guide 51 for risk analysis in the context of safety.

1.3.15 Risk assessment

the overall process of **risk identification** (1.3.19), **risk analysis** (1.3.14) and **risk evaluation** (1.3.18), refer to Figure 3.1

1.3.16 Risk avoidance

a decision not to become involved in, or to withdraw from, a **risk** (1.3.13) situation

1.3.17 Risk criteria

terms of reference by which the significance of **risk** (1.3.13) is assessed

NOTE: Risk criteria can include associated cost and benefits, legal and statutory requirements, socioeconomic and environmental aspects, the concerns of **stakeholders** (1.3.27), priorities and other inputs to the assessment.

1.3.18 Risk evaluation

process of comparing the level of **risk** (1.3.13) against **risk criteria** (1.3.17)

NOTE 1: Risk evaluation assists in decisions about risk treatment.

NOTE 2: See ISO/IEC Guide 51 for risk evaluation in the context of safety.

1.3.19 Risk identification

the process of determining what, where, when, why and how something could happen

1.3.20 Risk management

the culture, processes and structures that are directed towards realizing potential opportunities whilst managing adverse effects

1.3.21 Risk management process

the systematic application of management policies, procedures and practices to the tasks of communicating, establishing the context, identifying, analysing, evaluating, treating, monitoring and reviewing **risk** (1.3.13)

1.3.22 Risk management framework

set of elements of an **organization's** (1.3.10) management system concerned with managing **risk** (1.3.13)

NOTE 1: Management system elements can include strategic planning, decision making, and other strategies, processes and practices for dealing with risk.

NOTE 2: The culture of an organization is reflected in its risk management system.

1.3.23 Risk reduction

actions taken to lessen the **likelihood** (1.3.7), negative **consequences** (1.3.1), or both, associated with a **risk** (1.3.13)

1.3.24 Risk retention

acceptance of the burden of loss, or benefit of gain, from a particular **risk** (1.3.13)

NOTE 1: Risk retention includes the acceptance of risks that have not been identified.

NOTE 2: The level of risk retained may depend on **risk criteria** (1.3.17).

(ISO/IEC Guide 73, in part)

1.3.25 Risk sharing

sharing with another party the burden of loss, or benefit of gain from a particular **risk** (1.3.13)

NOTE 1: Legal or statutory requirements can limit, prohibit or mandate the sharing of some risks.

NOTE 2: Risk sharing can be carried out through insurance or other agreements.

NOTE 3: Risk sharing can create new risks or modify an existing risk.

1.3.26 Risk treatment

process of selection and implementation of measures to modify **risk** (1.3.13)

NOTE 1: The term 'risk treatment' is sometimes used for the measures themselves.

NOTE 2: Risk treatment measures can include avoiding, modifying, sharing or retaining risk.

(ISO/IEC Guide 73, in part)

1.3.27 Stakeholders

those people and **organizations** (1.3.10) who may affect, be affected by, or perceive themselves to be affected by a decision, activity or risk.

NOTE: The term 'stakeholder' may also include 'interested parties' as defined in AS/NZS ISO 14050 and AS/NZS ISO 14004.

(Based on ISO/IEC Guide 73)

1.4 Terminology and translation

The English-language version of this Standard uses the word 'likelihood' to refer to the chance of something happening, whether defined, measured or estimated objectively or subjectively, or in terms of general descriptors (such as rare, unlikely, likely, almost certain), frequencies or (mathematical) probabilities.

ISO/IEC Guide 73 uses the word 'probability', in this general sense, to avoid translation problems of 'likelihood' in some non-English languages that have no direct equivalent. Because 'probability' is often interpreted more formally in English as a mathematical term, 'likelihood' is used throughout this Standard, with the intent that it should have the same broad interpretation as 'probability' as defined in ISO/IEC Guide 73.

1.5 Referenced documents

The following documents are referenced to in this Standard:

ISO/IEC Guide 51	*Safety aspects—Guidelines for their inclusion in standards*
ISO/IEC Guide 73	*Risk management—Vocabulary—Guidelines for use in standards*
ISO 3534-1	*Statistics; Vocabulary and symbols; Part 1: Probability and general statistical terms*

	AS/NZS ISO 9000	*Quality management systems—Fundamentals and vocabulary*
	AS/NZS ISO 14004	*Environmental management systems—General guidelines on principals, systems and supporting techniques*
	AS ISO 14050	*Environmental management—Vocabulary*
	AS ISO 15489	*Records management*
	HB 18.2	*Standardization and related activities—General vocabulary*
	HB 436	*Risk Management Guidelines—Companion to AS/NZS 4360:2004*

Commentary

1.1 Background to risk management

Risk is inherent in everything we do, whether it be riding a bicycle, managing a project, dealing with clients, determining work priorities, purchasing new systems and equipment, taking decisions about the future or deciding not to take any action at all.

We manage risks continuously, sometimes consciously and sometimes without realizing it. The need to manage risk systematically applies to all organizations and individuals and to all functions and activities within an organization. This need should be recognized as of fundamental importance by all managers and staff.

The alternative to risk management is risky management, or making reckless decisions, or decisions that are not based on a careful consideration of the facts. Risky management is unlikely to ensure desired outcomes.

(a) *Managing risks involves both threats and opportunities*

Risk management is about identifying potential variations from what we plan or desire and managing these to maximize opportunity, minimize loss and improve decisions and outcomes. Managing risk means identifying and taking opportunities to improve performance as well as taking action to avoid or reduce the chances of something going wrong.

(b) *Managing risk requires rigorous thinking*

Managing risk is a logical and systematic process that can be used when making decisions to improve the effectiveness and efficiency of performance. It is a means to an end, not an end in itself. It should be integrated into everyday work.

(c) *Managing risk requires forward thinking*

Managing risk involves identifying and being prepared for what might happen rather than always managing retrospectively.

Formal risk management encourages an organization to manage proactively rather than reactively.

(d) *Managing risk requires accountability in decision making*

The top manager is responsible for managing risks in an organization and for defining the responsibility and authority of those who must act on a day-to-day basis.

Managing risk involves making decisions that accord with those statutory requirements and acting in ways that are consistent with corporate objectives.

It is important to maintain the balance between responsibility for a risk and the ability to control that risk.

(e) *Managing risk requires communication*

Risk management takes place in a social context and in many circumstances an organization will need to interact with internal and external stakeholders to ensure that all relevant risks are addressed. In order to ensure that risk management actions are properly implemented and adhered to, it is important to ensure that effective communication occurs within an organization.

(f) *Managing risk requires balanced thinking*

A balance needs to be struck between the cost of avoiding threats or enhancing opportunities and the benefits to be gained.

1.2 Benefits of risk management

Management of risk is an integral part of good business practice and quality management. Learning how to manage risk effectively enables managers to improve outcomes by identifying and analysing the wider range of issues and providing a systematic way to make informed decisions.

A structured risk management approach also enhances and encourages the identification of greater opportunities for continuous improvement through innovation.

The underlying principles of managing risk are generic in nature and largely independent of any individual type of organizational structure.

Risk management techniques provide people, at all levels, with a systematic approach to managing the risks that are integral parts of their responsibilities.

Some of the specific benefits of risk management include:

(a) *Fewer surprises*

Control of adverse events is enhanced by identifying and taking actions to minimize their probability and reduce their effects. Even when such events cannot be prevented the organization can achieve a degree of resilience through planning and preparedness.

(b) *Exploitation of opportunities*

Opportunity seeking behaviour is enhanced if people have confidence in their understanding of risks and have the capabilities needed to manage them.

(c) *Improved planning, performance and effectiveness*

Access to strategic information about the organization, its operations and its environment allows for more sound and effective planning. This in turn enhances the organization's ability to capitalize on opportunities, mitigate negative outcomes and to achieve better performance.

(d) *Economy and efficiency*

Benefits in economy and efficiency can be achieved in the targeting of resources, protection of assets and avoidance of costly mistakes.

(e) *Improved stakeholder relationships*

Risk management encourages an organization to identify its internal and external stakeholders and to develop a two-way dialog between the stakeholders and the organization. This communication channel provides the organization with informed insight into how the stakeholders will respond to new policies, products or decisions, and allows stakeholders to understand why particular actions have been taken.

(f) *Improved information for decision making*

Risk management provides more accurate information and analysis in support of strategic decision-making, such as major investments, mergers and acquisitions.

(g) *Enhanced reputation*

Investors, lenders, insurers, suppliers and customers are increasingly drawn to organizations that are known to have a sound process for managing risk.

(h) *Director protection*

Sound risk management facilitates enhanced disclosure to directors and company officers through raising awareness of potential risks, and in demonstrating a proper level of due diligence.

(i) *Accountability, assurance and governance*

Benefits can be obtained by demonstrating and documenting the management approach adopted, and by focusing each level of the organization on conformance with requirements and enhanced organizational performance.

(j) *Personal wellbeing*

Effective risk management of personal risk generally improves health and wellbeing of self and others.

1.3 Applications of risk management

The risk management process can be applied to decisions in all organizations, and at all levels in an organization (that is, at the organization, department, team and individual level). The risk management process can also be applied to an activity or function.

Risk can be considered, formally or informally, for any decision. Typically, the risk management process should be applied when planning and making decisions about significant issues. For example, when considering changes in policy, introducing new strategies and procedures, managing projects, expending large amounts of money, managing internal organizational differences or managing potentially sensitive issues.

Risk management has a range of applications including:

(a) strategic, operational and business planning;

(b) asset management and resource planning;

(c) business interruption and continuity;

(d) change: organizational, technological and political;

(e) design and product liability;

(f) directors' and officers' liability;

(g) public policy development;

(h) environmental issues;

(i) ethics, fraud, security and probity issues;

(j) resource allocation;

(k) public risk and general liability;

(l) feasibility studies;

(m) compliance;

(n) health and safety;

(o) operations and maintenance systems;

(p) project management; and

(q) purchasing and contract management.

The range of applications for risk management is unlimited, and less formal processes may be appropriate for less important decisions.

1.4 Corporate governance

Corporate governance can be defined as 'the system by which organizations are directed and controlled. Corporate governance is concerned with improving the performance of companies for the benefit of shareholders, stakeholders and economic growth. It focuses on the conduct of, and relationship between, the board of directors, managers and the company shareholders. Corporate governance generally refers to the processes by which organizations are directed, controlled and held to account.' *

* AS 8000—2003, *Corporate governance—Good governance principles.*

Risk management contributes to good corporate governance by providing reasonable assurance to boards and senior managers that the organizational objectives will be achieved within a tolerable degree of residual risk.

Sound risk management not only contributes to good governance, it also provides some protection for directors and office holders in the event of adverse outcomes. Provided risks have been managed in accordance with the process set out in the Standard, protection occurs on two levels. Firstly, adverse outcomes may not be as severe as they might otherwise have been. Secondly, those accountable can, in their defence, demonstrate that they have exercised a proper level of diligence.

In its focus on positive outcomes risk management provides a major contribution to those aspects of corporate governance directed to enhancing organizational performance.

Risk management provides a structure to facilitate communication and consultation between external stakeholders, governing bodies, management, and personnel at all levels on defining and achieving organizational goals.

This page has been left blank intentionally

2 Risk management process overview

AS/NZS 4360:2004

2.1 General

This Section gives a brief overview of the risk management process. Each step of the risk management process is discussed in greater detail in Section 3.

Management of risk is an integral part of good management. It is an iterative process of continuous improvement that is best embedded into existing practices or business processes.

2.2 Main elements

The main elements of the risk management process, as shown in Figure 2.1, are the following:

(a) *Communicate and consult*

Communicate and consult with internal and external stakeholders as appropriate at each stage of the risk management process and concerning the process as a whole.

(b) *Establish the context*

Establish the external, internal and risk management context in which the rest of the process will take place. Criteria against which risk will be evaluated should be established and the structure of the analysis defined.

(c) *Identify risks*

Identify where, when, why and how events could prevent, degrade, delay or enhance the achievement of the objectives.

(d) *Analyse risks*

Identify and evaluate existing controls. Determine consequences and likelihood and hence the level of risk. This analysis should consider the range of potential consequences and how these could occur.

(e) *Evaluate risks*

Compare estimated levels of risk against the pre-established criteria and consider the balance between potential benefits and adverse outcomes. This enables decisions to be made about the extent and nature of treatments required and about priorities.

(f) *Treat risks*

Develop and implement specific cost-effective strategies and action plans for increasing potential benefits and reducing potential costs.

(g) *Monitor and review*

It is necessary to monitor the effectiveness of all steps of the risk management process. This is important for continuous improvement.

Risks and the effectiveness of treatment measures need to be monitored to ensure changing circumstances do not alter priorities.

Risk management can be applied at many levels in an organization. It can be applied at a strategic level and at tactical and operational levels. It may be applied to specific projects, to assist with specific decisions or to manage specific recognized risk areas.

For each stage of the process records should be kept to enable decisions to be understood as part of a process of continual improvement.

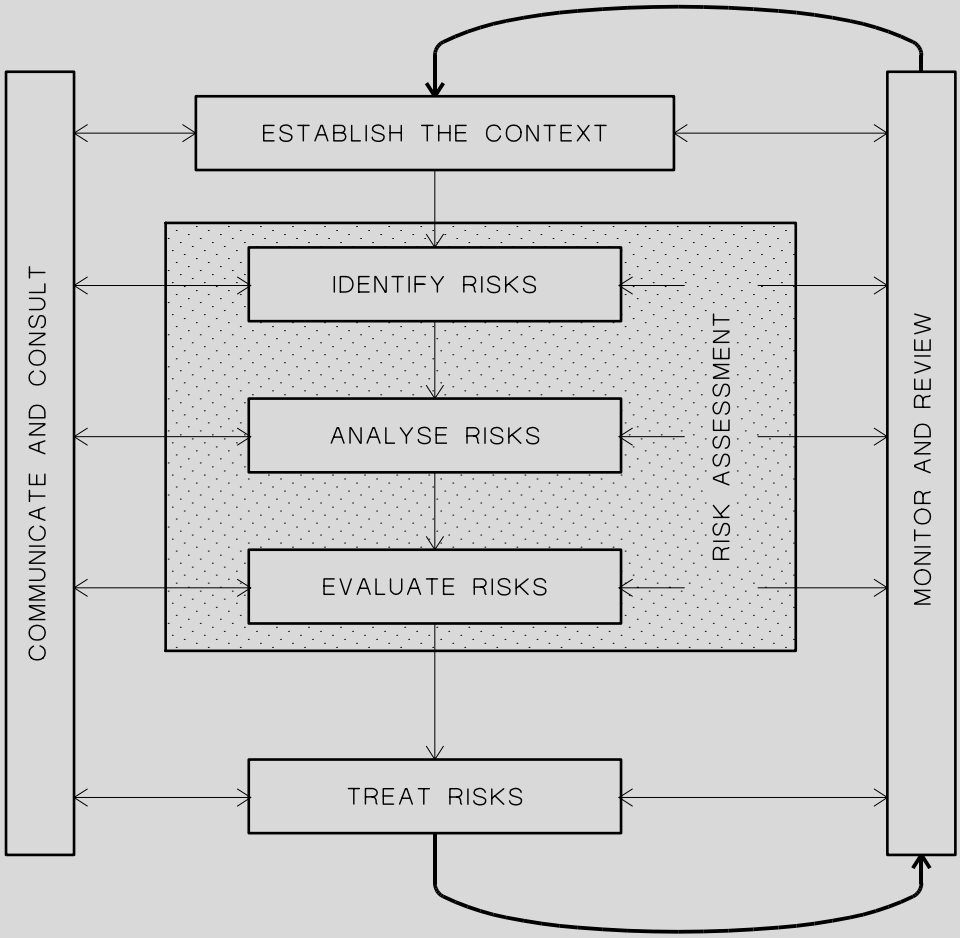


FIGURE 2.1 RISK MANAGEMENT PROCESS – OVERVIEW

Commentary

The above extract provides a general overview of the risk management process, and has been included in this Handbook for the purpose of completion.

Detailed guidance on the application of each of the steps in the risk management process can be found in Figure 3.1 and the Sections to follow.

AS/NZS 4360:2004

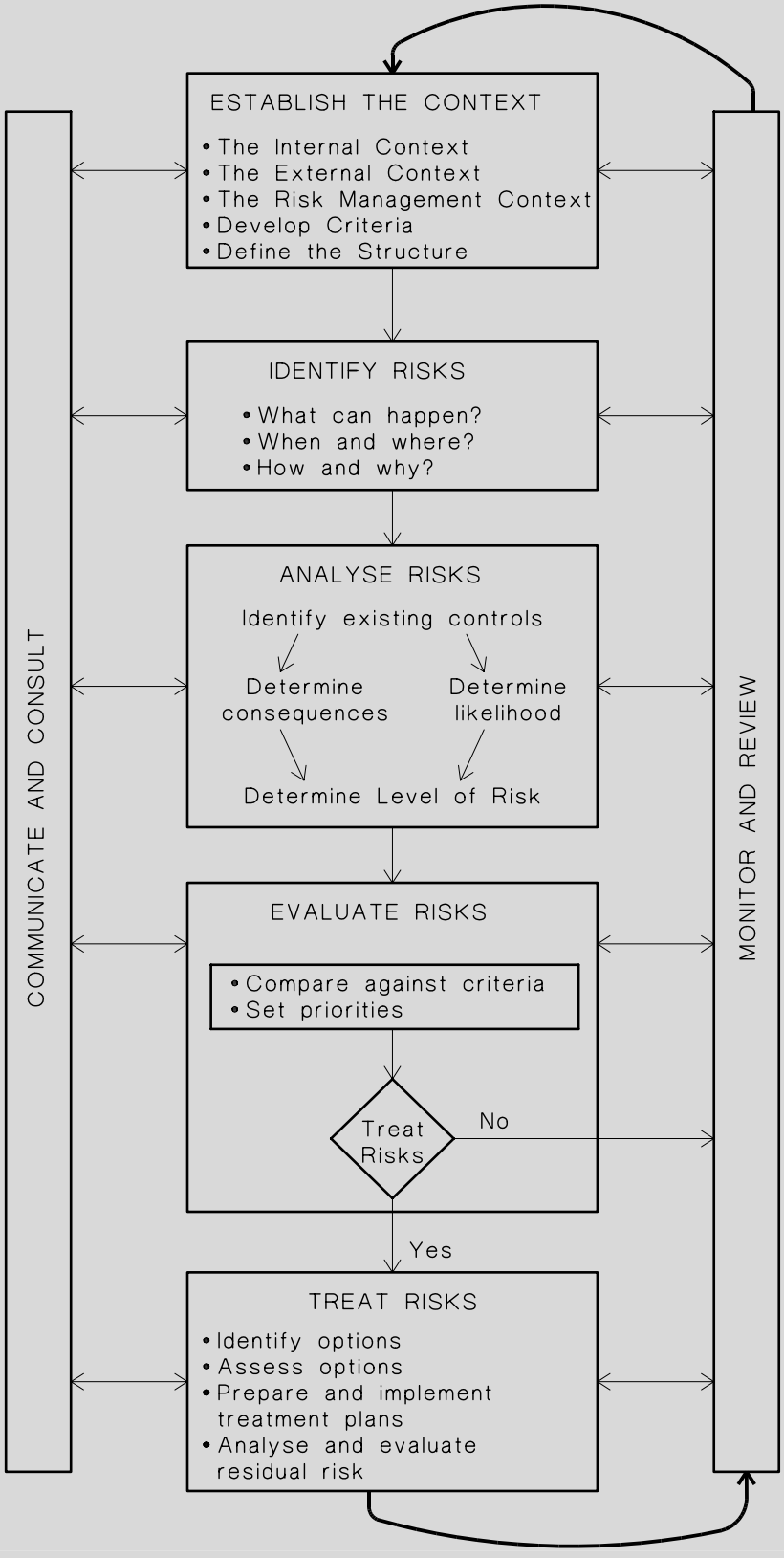


FIGURE 3.1 RISK MANAGEMENT PROCESS – IN DETAIL

This page has been left blank intentionally

3 Communication and consultation

AS/NZS 4360:2004

3.1 Communicate and consult

Communication and consultation are important considerations at each step of the risk management process. They should involve a dialogue with stakeholders with efforts focused on consultation rather than a one way flow of information from the decision maker to other stakeholders.

It is important to develop a communication plan for both internal and external stakeholders at the earliest stage of the process. This plan should address issues relating to both the risk itself and the process to manage it.

Effective internal and external communication is important to ensure that those responsible for implementing risk management, and those with a vested interest, understand the basis on which decisions are made and why particular actions are required.

Stakeholders are likely to make judgments about risk based on their perceptions. These can vary due to differences in values, needs, assumptions, concepts and concerns as they relate to the risks or the issues under discussion. Since the views of stakeholders can have a significant impact on the decisions made, it is important that their perceptions of risk be identified and recorded and integrated into the decision making process.

A consultative team approach is useful to help define the context appropriately, to help ensure risks are identified effectively, for bringing different areas of expertise together in analysing risks, for ensuring different views are appropriately considered in evaluating risks and for appropriate change management during risk treatment. Involvement also allows the 'ownership' of risk by managers and the engagement of stakeholders. It allows them to appreciate the benefits of particular controls and the need to endorse and support a treatment plan.

Records of communication and consultation will depend on factors such as the scale and the sensitivity of the activity.

Commentary

3.1 General

Risk management is not just a technical task but, rather, actions and decisions that take place in a social context. Communication and consultation are integral to the risk management process and should always be considered explicitly. Risk management will be enhanced by parties understanding each other's perspectives and, where appropriate, being actively involved in decision-making.

Appropriate communication and consultation seeks to:

- improve people's understanding of risks and the risk management process;
- ensure that the varied views of stakeholders are considered; and
- ensure that all participants are aware of their roles and responsibilities.

3.2 What is communication and consultation?

The concept of 'risk communication' is generally defined as an interactive process of exchange of information and opinion, involving multiple messages about the nature of risk and risk management*. This applies inside organizations, departments or business units or outside to external stakeholders. Risk communication will not solve all problems or resolve all conflict. Inappropriate communication about risk can lead to a breakdown in trust and/or poor risk management.

Consultation can be described as a process of informed communication between organization and its stakeholders on an issue prior to making a decision or determining a direction on a particular issue. Consultation has the following characteristics:

- It is a process not an outcome.
- It impacts on a decision through influence rather than power.
- It is about inputs to decision making not necessarily joint decision making.

* Adapted from the National Research Council, 1989. *Improving risk communication*. National Academy Press. Washington D.C.

Communication and consultation may be conducted at different levels according to the requirements of the situation. At its simplest:

(a) one-way communication describes the provision of information such as annual reports, newsletters, meeting minutes etc.; and

(b) two-way communication involves the sharing of perspectives, beliefs, positions etc. between interested parties, and between an organization and its stakeholders.

3.3 Why communication and consultation are important

3.3.1 General

Communication and consultation are intrinsic to the process of risk management and should be considered at each step. An important aspect of 'establishing the context' is to identify stakeholders and seek and consider their needs. A communications plan can then be developed. This plan should specify the purpose or goal for the communication, who is to be consulted and by whom, when it will take place, how the process will occur, and how it will be evaluated.

Within an organization, good communication is essential in developing a 'culture' where the positive and negative dimensions of risk are recognized and valued. Communication about risk helps an organization to establish its attitude towards risk.

Involving others, or at least looking at things from another point of view, is an essential and crucial ingredient of an effective approach to risk management. Engagement with stakeholders makes risk management explicit and more soundly based, and adds value to an organization. It is particularly important where stakeholders may—

- impact on the effectiveness of the proposed risk treatments;
- be affected in risk incidents;
- add value in the assessment of risk;
- incur additional costs; or
- be constrained by future risk controls.

In some situations an organization may consider it not to be appropriate to communicate with stakeholders, for commercial or security reasons. In these circumstances the communication plan should document a conscious decision not to involve stakeholders but could still take their perspective into account through other means, for example, intelligence or business information.

3.3.2 Making risk management explicit and relevant

We all consider risk implicitly in our decision making and thinking. However, by discussing each step with other interested parties it becomes a conscious and formal discipline. It provides a mechanism to help ensure that the lessons of the past are taken into account.

Engaging with others can help embed risk management as a regular part of the business, so that it becomes part of business as usual. Risk management is then directly linked with other organizational functions including market research, business intelligence and environmental scanning, policy consultation, regulatory compliance, client feedback, strategic planning or audit and evaluation.

3.3.3 Adding value to the organization

Sharing information and perspectives on risk within an organization helps to create organizational coherence. It identifies critical areas for joint achievement and joint strategies to help achieve goals. It pinpoints how success will be monitored. For example, it creates opportunities for dialogue between field operatives, line staff and senior management. Consultation on risk may be used as the mechanism by which these members take part in governance both from performance and conformance aspects.

Communication with external stakeholders can provide assurance and confidence on critical areas of interest. This external engagement also adds value by creating potential for partnering with other groups and for win-win outcomes. For example, other external stakeholders may have common risks that are more effectively managed by joint action. Consultation may add to the organization's technical understanding of the risk.

3.3.4 Integrating multiple perspectives

Members of the organization and other stakeholders are likely to make judgements about a risk based on their perception of that risk. Perceptions of risk can vary due to differences in values, experiences, beliefs, assumptions, needs and concerns. Since stakeholders can have a significant impact on risk management activities, it is important that their perceptions of risk be identified and recorded and the underlying reasons for them understood and addressed.

Perceptions may also vary amongst technical experts, project team members, decision-makers and other stakeholders. It is therefore essential to effectively communicate the level of risk if informed and valid decisions are to be made and implemented. Similarly it is important to communicate assumptions and any uncertainties associated with the risks.

People tend to make decisions about acceptability of risk, based on a range of factors including:

(a) the degree of personal control that can be exercised over the activity;

(b) the potential for an event to result in catastrophic consequences;

(c) the nature of the potential consequences;

(d) the distribution of the risks and benefits amongst those potentially affected;

(e) the degree to which exposure to the risk is voluntary; and

(f) the degree of familiarity with or understanding of the activity.

People are less accepting of risks over which they believe they have little or no control (for example, the siting of hazardous facilities), where the consequences are dreaded (e.g. cancer causing) or otherwise considered horrific, or the activity is unfamiliar.

Successfully communicating the nature of uncertainty is extremely difficult. To make decisions stakeholders need to know not only the predicted levels of risk but also the certainty with which this is believed to be true.

Where an organization has a direct community of interest, for example residents living near a hazardous site, then stakeholder understanding of a risk can be enhanced by involving the community in aspects of risk management through activities such as community consultation.

3.3.5 Developing trust

Communication between an organization and its external stakeholders allows an organization to develop an association with its community of interest, and to establish relationships based on trust. This is particularly important in the management of low likelihood and high consequence risks such as natural hazards. Community involvement brings a greater diversity of perspectives and views about objectives. Where uncertainties are high, people's beliefs and values are very important. Risk communication may be a significant component in implementing the risk treatments.

Trust within the organization is also important for similar reasons.

3.3.6 Enhancing risk assessment

Stakeholder experience and expertise will often improve understanding of the risk. Taking account of diversity of perceptions broadens the risk assessment and avoids 'groupthink'. For example, senior management may be taking the organization in different directions with new risks or may have a different view of risk consequences than management at other levels. Workers may see risks that others overlook and

may have a better appreciation of the likelihood of risk events occurring than 'head office'.

Organizations should seek to validate risk judgements by, over time, taking a comprehensive account of the various stakeholder input.

3.3.7 Effective risk treatment

Stakeholder experience and expertise are crucial in developing treatments that will be effective and acceptable. Obtaining ownership of decisions relating to risk treatment helps to ensure that recommended treatments will be accepted.

At the stage of implementing the treatments a greater emphasis on more directive forms of communication may be appropriate. For example, communicating what action various stakeholders need to take.

3.4 Developing a process for communication and consultation

3.4.1 Stakeholder identification

Stakeholders are those who may affect, be affected by, or perceive themselves to be affected by the organization or the risk management process. In other words, stakeholders are those people or groups who have a legitimate interest in the organization.

There will be differences of opinion on who should be included as stakeholders but generally, in determining stakeholders, it is important to be as inclusive as possible. Some examples of stakeholders are given in Clause 4.3.

It is important to identify stakeholders and to realize that the organization does not pick the stakeholders they choose themselves. If a group is missed initially, it is likely they will emerge later and benefits of early consultation will be missed.

3.4.2 The communication and consultation plan

The extent of the consultation and communication will depend on the situation. For example, risk management in the course of on-the-spot operational decision making necessarily entails a less formal communication process than strategic risk management at the level of an organization overall. Also at the outset of a risk management exercise an organization might decide to concentrate initial attention on internal stakeholders and to engage with external stakeholders progressively in subsequent cycles as part of the iterative and dynamic approach to risk management.

The essential elements of a communication and consultation plan (whether a formal document or a checklist) include:

(a) The **objectives** of the communication.

(b) The **participants** who need to be included, for example:

(i) Stakeholder groups and individuals.

(ii) Specialists/experts.

(iii) Communication team.

(c) The **perspectives** of the participants that need to be taken into consideration.

(d) The communication **methods** to be used.

(e) The **evaluation** process to be used.

The method of communication and consultation may need to be varied throughout the risk management cycle.

A communication and consultation plan in the organization will be influenced by what is trying to be achieved in relation to risk management. For example, you need to decide whether your communication is about:

(i) Building awareness and understanding about a particular issue.

(ii) Learning from stakeholders.

(iii) Influencing the target audience.

(iv) Obtaining a better understanding of the context, the risk criteria, the risk, or the effect of risk treatments.

(v) Achieving an attitudinal or behavioural shift in relation to a particular matter.

(vi) Any combination of the above.

This page has been left blank intentionally

4 Establish the context

AS/NZS 4360:2004

3.2.1 General

Establishing the context defines the basic parameters within which risks must be managed and sets the scope for the rest of the risk management process. The context includes the organization's external and internal environment and the purpose of the risk management activity. This also includes consideration of the interface between the external and internal environments.

This is important to ensure that the objectives defined for the risk management process take into account the organizational and external environment.

3.2.2 Establish the external context

This step defines the external environment in which the organization operates.

It also defines the relationship between the organization and its external environment. This may, for example, include:

- the business, social, regulatory, cultural, competitive, financial and political environment;
- the organization's strengths, weaknesses, opportunities and threats;
- external stakeholders; and
- key business drivers.

It is particularly important to take into account the perceptions and values of external stakeholders and establish policies for communication with these parties.

Establishing the external context is important to ensure that stakeholders and their objectives are considered when developing risk management criteria and that externally generated threats and opportunities are properly taken into account.

3.2.3 Establish the internal context

Before a risk management activity, at any level, is commenced, it is necessary to understand the organization. Key areas include:

- culture;
- internal stakeholders;
- structure;

- capabilities in terms of resources such as people, systems, processes, capital; and
- goals and objectives and the strategies that are in place to achieve them.

Establishing the internal context is important because:

- risk management takes place in the context of the goals and objectives of the organization;
- the major risk for most organizations is that they fail to achieve their strategic, business or project objectives, or are perceived to have failed by stakeholders;
- the organizational policy and goals and interests help define the organization's risk policy; and
- specific objectives and criteria of a project or activity must be considered in the light of objectives of the organization as a whole.

3.2.4 Establish the risk management context

The goals, objectives, strategies, scope and parameters of the activity, or part of the organization to which the risk management process is being applied, should be established. The process should be undertaken with full consideration of the need to balance costs, benefits and opportunities. The resources required and the records to be kept should also be specified.

Setting the scope and boundaries of an application of risk management involves—

- defining the organization, process, project or activity and establishing its goals and objectives;
- specifying the nature of the decisions that have to be made;
- defining the extent of the project activity or function in terms of time and location;
- identifying any scoping or framing studies needed and their scope, objectives and the resources required; and
- defining the depth and breadth of the risk management activities to be carried out, including specific inclusions and exclusions.

Specific issues that may also be discussed include the following:

- The roles and responsibilities of various parts of the organization participating in the risk management process.
- Relationships between the project or activity and other projects or parts of the organization.

3.2.5 Develop risk criteria

Decide the criteria against which risk is to be evaluated. Decisions concerning whether risk treatment is required may be based on operational, technical, financial, legal, social, environmental, humanitarian or other criteria. The criteria should reflect the context defined above. These often depend on an organization's internal policies, goals and objectives and the interests of stakeholders.

Criteria may be affected by the perceptions of stakeholders and by legal or regulatory requirements. It is important that appropriate criteria be determined at the outset.

Although the broad criteria for making decisions are initially developed as part of establishing the risk management context, they may be further developed and refined subsequently as particular risks are identified and risk analysis techniques are chosen. The risk criteria must correspond to the type of risks and the way in which risk levels are expressed.

3.2.6 Define the structure for the rest of the process

This involves subdividing the activity, process, project or change into a set of elements or steps in order to provide a logical framework that helps ensure significant risks are not overlooked. The structure chosen depends on the nature of the risks and the scope of the project, process or activity.

Commentary

4.1 Context

Establishing the context is concerned with understanding the background of the organization and its risks, scoping the risk management activities being undertaken and developing a structure for the risk management tasks to follow. This step is needed:

- to clarify the organizational objectives;
- to identify the environment in which objectives are pursued;
- to specify the main scope and objectives for risk management, boundary conditions and the outcomes required;
- to identify a set of criteria against which the risks will be measured; and
- to define a set of key elements for structuring the risk identification and assessment process.

This step aims to provide a comprehensive appreciation of all the factors that may have an influence on the ability of an organization to achieve its intended outcomes. The output from this step is a concise statement of the organizational objectives and specific criteria for success, the objectives and scope for risk management, and a set of key elements for structuring the risk identification activity in the next stage. It is particularly important that the scope is clearly defined so that the rest of the process stays within the required boundaries.

4.2 Objectives and environment

Risk is the chance of something happening that will have an impact on objectives. Therefore, to ensure that all significant risks are captured, it is necessary to know the objectives of the organization function or activity that is being examined. Objectives lie at the heart of the context definition. Organizational success criteria are the basis for measuring the achievement of objectives, and so are used to identify and measure the impacts or consequences of risks that might jeopardize those objectives.

The first step in establishing the context identifies the organizational objectives and the external and internal environment in which the objectives are pursued. The second step identifies the scope of the risk management activity and the main questions and issues of concern to the organization, and the relationship with the organization's strategy and business objectives.

Key documents may be consulted here, such as the strategic plan, business plans and budgets, annual reports, economic analyses, and any other relevant documentation about the organization and its purpose. External documents such as relevant legislation should also be consulted. Strategic analysis documents, such as SWOT analyses, may be valuable, as they assist in focussing on relevant aspects of the external and internal environment, as illustrated in Figure 4.1, adapted from Rowe, Mason, Dickel and Snyder (1989).

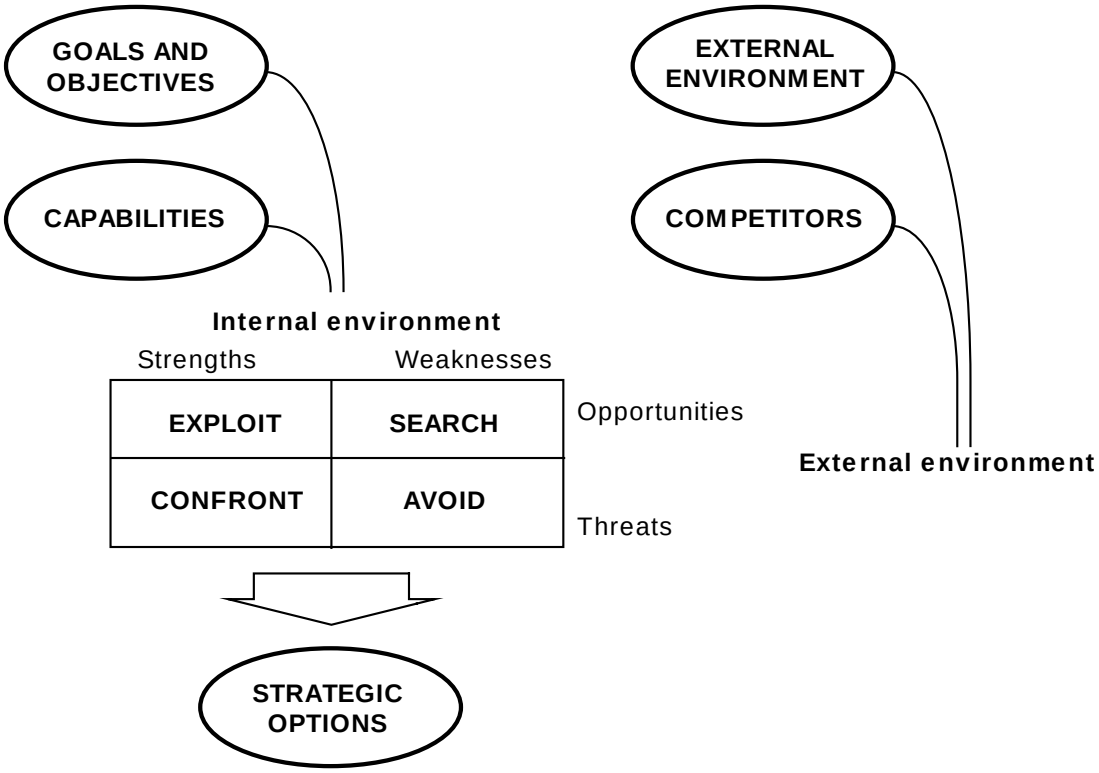


FIGURE 4.1 SWOT ANALYSIS STRUCTURE

4.3 Stakeholder identification and analysis

Stakeholder analysis is important in risk management for most activities. It is usually undertaken at an early stage of planning. For example, external and internal stakeholders who may have to be considered include:

- In a corporate business, the Board and controlling shareholders.
- In a Government agency, the Portfolio Minister, other Ministers and local members whose electorates may be affected by activities or associated employment or other opportunities.
- Senior executives and the managers of business units who may be affected by the organizational activities.

- Staff, their families, unions and other representative organizations.
- Customer business unit or agency, where an entity is acting on behalf of an end-user.
- The user community, including the management, staff and clients of the organization.
- Legislators and regulators.
- People who may be affected by the organization or its activities.
- The environment and the community, as general proxy stakeholders.
- Special interest groups, such as environmental lobby groups.
- Contractors and suppliers.
- Emergency services organizations.
- Financial institutions and other providers of private sector funding.
- The media.

Stakeholder analysis provides decision-makers with a documented profile of stakeholders so as to better understand their needs and concerns. Such analysis plays an important part in demonstrating the integrity of the process and in ensuring the objectives of the risk assessment encompass all legitimate stakeholders' objectives and expectations.

Stakeholders should be appropriately engaged at each point and cycle of the risk management process through a process of communication and consultation (refer to Section 3). Involving stakeholders builds acceptance and can generate constructive solutions. Failure to identify and include the stakeholders may lead to failure in the acceptance of the proposal and its strategy by management, customers, staff, regulators and the community.

The main aims and objectives of relevant stakeholders should be considered explicitly. This may take a very simple form, or more sophisticated analyses may be appropriate where major social and community risks are anticipated.

4.4 Criteria

Important criteria which should be considered are—

- the kinds of consequences that will be considered;
- how likelihood will be defined; and
- how it is determined whether the risk level is such that further treatment activities are required.

The criteria against which the level of risk is assessed will play a part in defining the methods to be used to analyse risk. It is therefore important that appropriate criteria be considered at the outset of the process.

It is not essential that all facets of the criteria be defined at this point. It is, however, appropriate for the major issues to be acknowledged.

Criteria may be affected by the perceptions of stakeholders and by legal or regulatory requirements.

The requirements of the organization and of relevant stakeholders can be used to establish a set of critical performance measures. These critical performance measures will provide specific criteria against which to assess the risk in the later stage of risk assessment.

4.5 Consequence criteria

The requirements of the organization and the key stakeholders are used to derive a set of criteria for the analysis. These will be used to determine the specific scales against which the consequences of risks will be assessed in the following stages of the risk analysis.

The range of criteria may be wide. Table 4.1 shows an example from a medium-scale project where community acceptance was important. This list of criteria was a valuable guide for the project manager through the initial planning and design stages of the project.

TABLE 4.1
Criteria for a medium-scale project (case example)

Criterion	Notes
Availability	The availability of existing facilities must be maximized by reducing the disruption to current business operations as far as possible
Community relations	The highest standards of community consultation and liaison must be maintained
Economics	The project must be clearly justifiable in economic terms, measured by profitability and rate of return
Environment	The solutions to the technical issues must be environmentally sound; an alternative solution should be available
Funding	Avoid expenditure outside allocated budgets; maximize the use of special purpose grant funds
Industrial relations	Optimize industrial relations by negotiation with staff representatives and use of appropriate enterprise agreements
Probity	Good corporate governance and transparent decision making are regulatory requirements
Quality	The client requires equipment that is properly engineered and reliable
Safety	Project delivery processes must ensure the highest standards of safety; contract conditions must contain appropriate clauses
Staff development	The project delivery method and outcomes should enhance the core skills of the organization and the abilities of the staff involved
Timing	The project must be completed by the specified date to meet user obligations

The criteria and the associated objectives for a business that depends on physical assets are shown in Table 4.2.

4.6 Key elements

Risk identification will generally be unproductive if an attempt is made to consider the organization or activity as a whole. It is much more effective to disaggregate the activity into sections or key elements.

Key elements are a set of topics to be considered one by one during risk identification. Each topic is somewhat narrower than the activity as a whole, allowing those performing the identification to focus their thoughts and go into more depth than they would if they tried to deal with everything at once. A well-designed set of key elements will stimulate creative thought, and ensure that all important issues are put before those responsible for identifying risks. When a brainstorming meeting is used to identify risks, the key elements form the agenda and the basis of the timetable for that meeting.

TABLE 4.2
Criteria related objectives for a business (case example)

Criteria	Objectives
Production loss or restriction	Maximize the value of assets Increase sustainable production Meet annual production targets and costs
Facility integrity	Minimize disruption to operations Maintain asset or system condition and performance
Project performance	Cost effective strategy Operating entities are involved Timely implementation and operation of project facilities Time, cost and performance related to budget
Financial impacts	Supply costs reduced by 10% Capital costs optimized Operating costs improved No losses, no increased or additional costs
Employees	Low turnover, grow skills and experience Health, safety and environmental performance Minimize health, safety and environmental (HSE) risks during construction
Health & safety	Health and safety performance Minimize health and safety risks during construction No injuries, fatalities or long term health problems
Environment & community	Environment and community performance Minimize environmental and community risks during construction No releases to the environment or public outrage
Image & reputation	Exceptional high performance Shareholder and public support and trust

The key element structure depends on the objectives and the key issues of concern to the organization and the other stakeholders. Table 4.3 indicates some of the ways of structuring the elements for different purposes.

Structuring key elements requires judgement from the person responsible. There will be a trade-off between the effectiveness of the risk analysis process and the integration of its outcomes with other aspects of business analysis and planning. In most circumstances, it is recommended that the structure that is most effective for the risk analysis be chosen. Using an inappropriate structure can lead to significant items being omitted inadvertently, with potentially serious consequences, as well as making the process very inefficient.

TABLE 4.3
Elements for structuring the risk assessment

Purpose, objectives, relevant issues	Basis for selecting the elements
Business planning and strategic direction	Business activities
Budget constraints; external financing	Budget items, cost items
Operating issues; fitness for purpose; value for money	Functions of the supplied product or service
Technical and environmental issues; reliability; allocation of technical and management effort	Physical components
Environmental aspects; effect of the environment on the outcomes (e.g. access, weather)	Physical locations, activities
Timing and schedule; industrial relations aspects; implementation risks	Business or project activities
General project risks, undertaken early in the planning stage; stop/go decisions; commercial structuring; overall procurement approach strategy	Project phases
Environmental and community issues; approval processes; financing aspects	Stakeholders

4.7 Documentation of this step

For a major analysis, this step should be documented to demonstrate that the full range of environmental and contextual factors has been considered.

For a low level activity, a brief record of the analysis would be appropriate.

Documentation should identify—

(a) the scope of the risk management activities being undertaken and their intended outcomes;

(b) organizational objectives and success measures;

(c) important factors within the internal and external environment;

(d) relevant stakeholders;

(e) major risk evaluation criteria;

(f) documents consulted in establishing the context; and

(g) key elements by which the rest of the process will be structured.

5 Risk identification

AS/NZS 4360:2004

3.3.1 General

This step seeks to identify the risks to be managed. Comprehensive identification using a well-structured systematic process is critical, because a risk not identified at this stage may be excluded from further analysis. Identification should include risks whether or not they are under the control of the organization.

3.3.2 What can happen, where and when?

The aim is to generate a comprehensive list of sources of risks and events that might have an impact on the achievement of each of the objectives identified in the context. These events might prevent, degrade, delay or enhance the achievement of those objectives. These are then considered in more detail to identify what can happen.

3.3.3 Why and how it can happen?

Having identified what might happen, it is necessary to consider possible causes and scenarios. There are many ways an event can occur. It is important that no significant causes are omitted.

3.3.4 Tools and techniques

Approaches used to identify risks include checklists, judgements based on experience and records, flow charts, brainstorming, systems analysis, scenario analysis and systems engineering techniques. These tools and techniques are discussed in more detail in HB 436.

The approach used will depend on the nature of the activities under review, types of risk, the organizational context and the purpose of the risk management study.

Commentary

5.1 Aim

The aim of risk identification is to develop a comprehensive list of sources of risks and events that might have an impact on the achievement of each of the objectives (or key elements) identified in the context.

The list should be comprehensive as unidentified risks can pose a major threat to the organization or result in significant opportunities being missed.

5.2 Components of a risk

A risk is associated with:

(a) A **source** of risk or hazard – the thing which has the intrinsic potential to harm or assist e.g. a dangerous chemical, competitors, government.

(b) An **event or incident** – something that occurs such that the source of risk has the impact concerned e.g. a leak, competitor expands into or leaves your market area, new or revised regulations, or some measure or observation reaching a particular trigger level.

(c) A **consequence**, outcome or impact on a range of stakeholders and assets e.g. environmental damage, loss or increase of market/profits, regulations increase or decrease competitiveness.

(d) A **cause** (what and why) (usually a string of direct and underlying causes) for the presence of the hazard or the event occurring e.g. design, human intervention, funding, prediction or failure to predict competitor activity, failure to or expansion of market presence.

(e) **Controls** and their level of effectiveness e.g. detection systems, clean up systems, policies, security, training, market research and surveillance of market.

(f) **When** could the risk occur and **where** could it occur.

These components of risk should not be confused and need to be separately identified. Ideally, a risk should be identified in the following terms:

> (Something happens) leading to (outcomes expressed in terms of impact on objectives).

For example:

- A thunderstorm damages goods leading to cost of rework.
- We identify a market niche leading to increased sales.
- A spill of oil in the creek damages our reputation with the local community.

5.3 Identification process

To develop a comprehensive list of risks a systematic process should be used that starts with the statement of context. To demonstrate that risks have been identified effectively it is useful to step through the process, project or activity in a structured way using the key elements defined while establishing the context. This can help provide confidence that the process of identification is complete and major issues have not been missed.

The process then asks the following questions about each of the key elements:

(a) What is the source of each risk?

(b) What might happen that could:

  (i) increase or decrease the effective achievement of objectives;

  (ii) make the achievement of the objectives more or less efficient (financial, people, time);

  (iii) cause stakeholders to take action that may influence the achievement of objectives.

  (iv) produce additional benefits?

(c) What would the effect on objectives be?

(d) When, where, why, how are these risks (both positive and negative) likely to occur?

(e) Who might be involved or impacted?

(f) What controls presently exist to treat this risk (maximize positive risks or minimize negative risks)?

(g) What could cause the control not to have the desired affect on the risk?

After reviewing each element, the following general questions should be considered:

- What is the reliability of the information?
- How confident are we that the list of risks is comprehensive?
- Is there a need for additional research into specific risks?
- Are the objectives and scope covered adequately?
- Have the right people been involved in the risk identification process?

5.4 Information for identifying risks

Good quality information is important in identifying risks. The starting point for risk identification may be historical information about this or similar organizations and then discussions with a wide range of stakeholders about historical, current and evolving issues, some examples include:

- Local or overseas experience.
- Expert judgment.
- Structured interviews.
- Focus group discussions.
- Strategic and business plans including SWOT analysis and environmental scanning.
- Insurance claims reports.
- Post event reports.
- Personal experience or past organizational experience.
- Results and reports from audits, inspections and site visits.
- Surveys and questionnaires.
- Checklists.
- Historical records, incident databases and analysis of failures and previous risk registers if they exist.

It is essential that people involved in identifying risks are knowledgeable about the detailed aspects of the risk study being undertaken. Identifying risks can also require imaginative thinking and appropriate experience. Teams allow for the pooling of experience. Team involvement also helps build commitment and ownership into the risk management process and helps ensure that risks to different stakeholders are considered where appropriate.

5.5 Approaches to identifying risks

The approach used for risk identification depends on the risk management context. In selecting an approach to risk identification, the following considerations apply:

- Team-based brainstorming for example, where facilitated workshops is a preferred approach as it builds commitment, considers different perspectives and incorporates differing experiences.
- Structured techniques such as flow charting, system design review, systems analysis, Hazard and Operability (HAZOP) studies and operational modelling should be used where the potential consequences are catastrophic and the use of such intensive techniques are cost effective.
- For less clearly defined situations, such as the identification of strategic risks, processes with a more general structure such as ‘what-if’ and scenario analysis could be used.
- Where resources available for risk identification and analysis are constrained, the structure and approach may have to be adapted to achieve efficient outcomes within budget limitations. For example, where less time is available, a smaller number of key elements may be considered at a higher level, or a checklist may be used.

- In many circumstances, multi-level risk identification is useful and efficient. In a first or preliminary scoping stage, risks may be identified at high level and initial priorities assigned, with a detailed level identification and analysis applied to a subset of high priority areas.

5.6 Documentation of this step

Documentation of this step should include—

(a) the approach or method used;

(b) the scope covered by the identification;

(c) the participants in the risk identification and the information sources consulted; and

(d) a risk register (see Section 10).

This page has been left blank intentionally

6 Risk analysis

AS/NZS 4360:2004

3.4.1 General

Risk analysis is about developing an understanding of the risk. It provides an input to decisions on whether risks need to be treated and the most appropriate and cost-effective risk treatment strategies. Risk analysis involves consideration of the sources of risk, their positive and negative consequences and the likelihood that those consequences may occur. Factors that affect consequences and likelihood may be identified. Risk is analysed by combining consequences and their likelihood. In most circumstances existing controls are taken into account.

A preliminary analysis can be carried out so that similar risks are combined or low-impact risks are excluded from detailed study. Excluded risks should, where possible, be listed to demonstrate the completeness of the risk analysis.

3.4.2 Evaluate existing controls

Identify the existing processes, devices or practices that act to minimize negative risks or enhance positive risks and assess their strengths and weaknesses. Controls may arise as outcomes of previous risk treatment activities.

3.4.3 Consequences and likelihood

The magnitude of the consequences of an event, should it occur, and the likelihood of the event and its associated consequences, are assessed in the context of the effectiveness of the existing strategies and controls. An event may have multiple consequences and affect different objectives. Consequences and likelihood are combined to produce a level of risk. Consequences and likelihood may be estimated using statistical analysis and calculations. Where no reliable or relevant past data is available, subjective estimates may be made which reflect an individual's or group's degree of belief that a particular event or outcome will occur.

The most pertinent information sources and techniques should be used when analysing consequences and likelihood. Sources of information may include the following:

- Past records.
- Practice and relevant experience.
- Relevant published literature.

- Market research.
- The results of public consultation.
- Experiments and prototypes.
- Economic, engineering or other models.
- Specialist and expert judgements.

Techniques include:

- structured interviews with experts in the area of interest;
- use of multi-disciplinary groups of experts;
- individual evaluations using questionnaires; and
- use of models and simulations.

Where appropriate, the confidence placed on estimates of levels of risk should be included.

Assumptions made in the analysis should be clearly stated.

3.4.4 Types of analysis

Risk analysis may be undertaken to varying degrees of detail depending upon the risk, the purpose of the analysis, and the information, data and resources available. Analysis may be qualitative, semi-quantitative or quantitative or a combination of these, depending on the circumstances. The order of complexity and costs of these analyses, in ascending order, is qualitative, semi-quantitative and quantitative. In practice, qualitative analysis is often used first to obtain a general indication of the level of risk and to reveal the major risk issues. Later it may be necessary to undertake more specific or quantitative analysis on the major risk issues.

The form of analysis should be consistent with the risk evaluation criteria developed as part of establishing the context (see Clause 3.2).

In detail, the types of analysis are:

(a) *Qualitative analysis*

Qualitative analysis uses words to describe the magnitude of potential consequences and the likelihood that those consequences will occur. These scales can be adapted or adjusted to suit the circumstances, and different descriptions may be used for different risks.

Qualitative analysis may be used:

- as an initial screening activity to identify risks which require more detailed analysis;
- where this kind of analysis is appropriate for decisions; or
- where the numerical data or resources are inadequate for a quantitative analysis.

Qualitative analysis should be informed by factual information and data where available.

(b) *Semi-quantitative analysis*

In semi-quantitative analysis, qualitative scales such as those described above are given values. The objective is to produce a more expanded ranking scale than is usually achieved in qualitative analysis, not to suggest realistic values for risk such as is attempted in quantitative analysis. However, since the value allocated to each description may not bear an accurate relationship to the actual magnitude of consequences or likelihood, the numbers should only be combined using a formula that recognizes the limitations of the kinds of scales used.

Care must be taken with the use of semi-quantitative analysis because the numbers chosen may not properly reflect relativities and this can lead to inconsistent, anomalous or inappropriate outcomes. Semi-quantitative analysis may not differentiate properly between risks, particularly when either consequences or likelihood are extreme.

(c) *Quantitative analysis*

Quantitative analysis uses numerical values (rather than the descriptive scales used in qualitative and semi-quantitative analysis) for both consequences and likelihood using data from a variety of sources (such as those referred to in Clause 3.4.3). The quality of the analysis depends on the accuracy and completeness of the numerical values and the validity of the models used.

Consequences may be determined by modelling the outcomes of an event or set of events, or by extrapolation from experimental studies or past data. Consequences may be expressed in terms of monetary, technical or human impact criteria, or any of the other criteria referred to in Clause 3.2.5. In some cases, more than one numerical value is required to specify consequences for different times, places, groups or situations.

The way in which consequences and likelihood are expressed and the ways in which they are combined to provide a level of risk will vary according to the type of risk and the purpose for which the risk assessment output is to be used.

The uncertainty and variability of both consequences and likelihood should be considered in the analysis and communicated effectively.

3.4.5 Sensitivity analysis

Since some of the estimates made in risk analysis are imprecise, a sensitivity analysis should be carried out to test the effect of uncertainty in assumptions and data. Sensitivity analysis is also a way of testing the appropriateness and effectiveness of potential controls and risk treatment options as described in Clause 3.6.2.

Commentary

6.1 Overview

6.1.1 General

Risk analysis aims to establish an understanding of the level of risk and its nature. Aside from the absolute level of risk, analysis will help to set treatment priorities and options (Section 8). The level of risk is determined by combining consequence and likelihood. Suitable scales and methods for combining them should be consistent with the criteria defined when establishing the context. For more technical analysis, the nature of the data and required output will dictate the required analysis methods.

The process of analysis will often commence with a simple qualitative approach that gives a general understanding. Where greater detail or understanding is required, more focused and robust investigation may be needed as well. It is inappropriate to assume that quantitative is superior to qualitative analysis. It is more appropriate to ensure the best approach to fit the situation at hand.

The analysis can be conducted at various points, such as at the outset of a new project, as part of ongoing management, or as a study of what may occur after risks have been treated. Usually the analysis looks at the current level of risk with existing controls.

6.1.2 Basis of the analysis

The choice of analysis method will be influenced by the context, objectives and available resources. For example, at a strategic level, broad categories of risk may be identified and analysed to provide an organizational risk profile that shows important issues for which management systems and risk treatments need to be established. At a project or team level, managers need to identify and prioritize the specific risks that threaten the objectives they are tasked to achieve.

Some risks may need to be examined in more detail. Reasons for detailed analysis, which may be quantitative or qualitative, are—

(a) to obtain more information about consequences or likelihood so decisions about priorities are based on information and data rather than guesswork;

(b) to better understand the risk and its causes so that treatment plans can be directed at true rather than superficial causes of problems;

(c) where decision criteria require more in-depth analysis (often this is where decision criteria are expressed quantitatively);

(d) to help people choose between options where each has different costs and benefits and potential opportunities and threats;

(e) to provide a better understanding of risk to individuals who must operate with the risks; or

(f) to provide an understanding of residual risk after treatment strategies have been applied.

6.1.3 Qualitative analysis

Qualitative analysis is any method of analysis which uses description rather than numerical means to define a level of risk. It may involve providing descriptive information about the nature of consequences (particularly where there are many different consequences to different stakeholders or some consequences are intangible).

This information may be brought together and summarized as single word descriptions of consequence and likelihood to use in a risk ranking table. However, the underlying information on which the ranking is based may need to be recorded to assist decision makers and support the conclusions drawn.

Qualitative analysis may be used—

(a) where quantitative precision is not needed;

(b) to perform an initial screening of risks prior to further, more detailed analysis;

(c) where the level of risk does not justify the time and resources needed to do a numerical analysis; or

(d) where the numerical data are not available or inadequate for a more quantitative analysis.

Even when qualitative analysis is used, best possible use should be made of available information, including quantitative.

6.1.4 Semi-quantitative and quantitative analysis

If using a semi-quantitative approach, it is important not to interpret the results to a finer level of precision than is actually contained in the initial descriptive rankings. Numbers should not be used to give an appearance of a level of precision which does not exist.

The level of risk can be calculated using a quantitative method in situations where the consequences and likelihood of occurrence can be quantified. For example, fraud risk assessments may be quantitative where the likelihood can be expressed numerically and the potential impacts are measured in terms of monetary loss.

In many instances relatively straightforward methods are used effectively, although more refined techniques are sometimes necessary. However, even sophisticated quantitative techniques may have their weaknesses and these need to be kept in mind. In particular, the assumptions that underlie the quantitative techniques should be clearly stated and understood.

6.1.5 Measurement and scales

Whatever type of analysis is used, some form of measurement of consequence and likelihood is necessary. The choice of the type of scale used to carry out this measurement is largely dependent upon the nature and range of the consequence and the level of knowledge and variability of the likelihood. It is essential that having chosen suitable types of scales, the limitations and freedoms offered by each type be fully understood. The type of analysis possible is linked directly to the limitations. Measurement scales can be characterized as:

(a) Nominal.

(b) Ordinal.

(c) Interval.

(d) Ratio.

The nature and limitations of each of these scales is described in Table 6.1.

TABLE 6.1
Types of measurement scales

Type of scale	Description	Limitations/Freedoms	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.	Heat, colour, texture
Ordinal	Comparative scales. Can be judged as more or less than. . . .	Not measures of absolute magnitude, only relative. Summation is arbitrary in absence of zero points	Rankings such as High, Medium, Low or 1, 2, 3, 4, 5 where numerical value does not relate to value or quantity	Cold, warm, hot
Interval	Quantitative intervals between units of measurement are constant (10 exceeds 9 as 2 exceeds 1)	Can integrate, 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°] not defined)
Ratio	Quantitative. Similar to Interval Scale but with set or non-arbitrary set point.	Measures magnitude not 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 (e.g. a scale such as ‘no loss’, $1 loss’, ‘$2 loss’, etc	10°C, 100°C (set point = 0°C = freezing point)

6.1.6 Analysis principles

Analysis tools enable risk to be expressed from the combination of its two components, namely, consequence and likelihood. The relationship between these two will depend on many factors that in turn reflect the true nature of the risk and the way it is perceived. This is a function of the context. Particularly, where human values apply, the relationship between the components may well be non-linear and even discontinuous. The more complex the problem, the less certain or definable may be this relationship. For example, a series of minor environmental mishaps may reach a threshold where consequences become of public concern.

From the definition, risk is a function of both likelihood and a measure of consequence. In its simplest form risk can be shown as:

Risk = A function of (Consequence and Likelihood)

Whether using qualitative or quantitative analysis, the nature of the function and underlying logic needs to be understood. Any mathematical operation subsequently applied must conform to that logic, and in particular any use of units must be valid. Indeed, inspection of the units offers a useful check of the underlying logic.

If it is taken that the level of risk is proportional to each of its two components (consequence or likelihood) the risk function is essentially a product. This can be shown mathematically as:

$$\text{Risk} = \text{Consequence} \times \text{Likelihood} \qquad (R = C \times L)$$

This simple relationship does not take account of the complicating factors such as non linear relationships between utility and the value of consequences. As a result, for quantitative analysis, a fuller relationship is likely to need to include a weighting factor for one of the two components (to achieve a required relative scale between them) and may also require an exponential operator ('raise to power' operators, x and y) for one or both components. For example:

$$\text{Risk} = (C \times \text{weighting factor})^{x} \times (L)^{y}$$

Each of the above descriptions of risk are quite likely to only hold true within a given range. For example, where the frequency is high or an event almost certain, then the risk becomes equal to the consequence alone. Likewise, high consequence outcomes may be so unacceptable that the frequency of occurrence is not a relevant factor.

6.1.7 Graphical representation

In its simplest qualitative form, the relationship between risk and its components can be considered and illustrated by means of a simple matrix. For example, it is important to note that the relationship that defines the level of risk may be dominated by either consequence or likelihood or the two components may carry similar or equal weight (see Figure 6.1).

The number of steps or divisions along each axis will be determined by the level of detail, the nature of the measures as well as the context, scope, resources and use to which the output will be used.

A particular strength of the qualitative approach is that no attempt need be made to understand the true consequence/probability/risk relationship. However, any matrix is invalid unless each possible combination is explored to ensure the tool accurately reflects the organizational perception of risk.

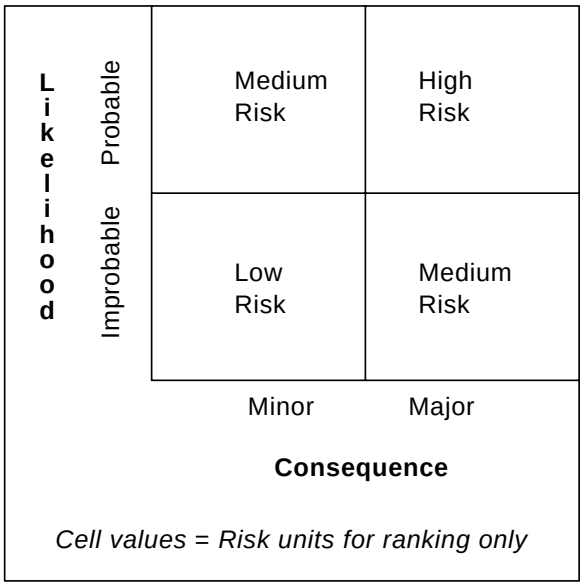


FIGURE 6.1 QUALITATIVE REPRESENTATION

A similar approach can be used to illustrate a semi-quantitative analysis tool (see Figure 6.2).

Frequency				
0.1	10	30	100	300
0.01	1	3	10	30
0.001	0.1	0.3	1	3
0.0001	0.01	0.03	0.1	0.3
(Events /yr)	V.low (100	Low 300	Medium 1000	High 3000)

Consequence ($ x 1000)

Cell values = Risk units for ranking only

FIGURE 6.2 SEMI-QUANTITATIVE REPRESENTATION

As with the qualitative analysis the scales for each component need not be linear.

In the case of semi-quantitative analysis some form of mathematical manipulation may be used. It is therefore important that the limitations of the chosen scale types be considered to ensure the manipulation is valid (see Table 6.1). It should be noted however, that although ordinal scales are commonly used, the manipulation that can be carried out are very limited. The use of ratio scales on the other hand allow most mathematical operations to be performed provided suitable units or conversions are applied (see Figure 6.3).

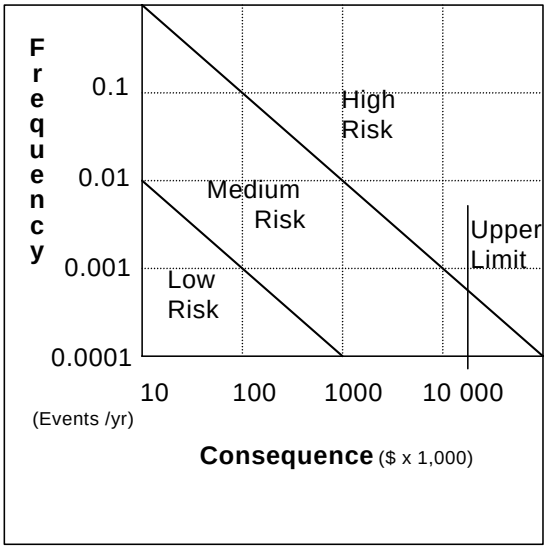
A1

Note that if the risk relationship is taken to be the product of the two components (consequence and likelihood), a constant risk line will not appear straight on the plot unless logarithmic scales are used. Where a simple mathematic expression is used to represent them, a diagram is not needed.

The simplest form of quantitative analysis is similar in concept to semi-quantitative but with usually more rigorous use and manipulation of the values that represent the two components of risk. The use of any scale other than a form of 'ratio' is usually not valid.

However, even where the values are relatively easy to define, there may still need to be some allowance (usually in the form of a weighting or other factor or mathematical function) to account for the human value or utility of a given consequence or perception of likelihood.

When carrying out a quantitative analysis, the measurement units should always be stated.



A1

FIGURE 6.3 SEMI-QUANTITATIVE REPRESENTATION

6.2 Consequence and likelihood tables

6.2.1 General

Consequence and likelihood tables are used to provide definitions for rating scales so there is a common understanding of their meaning. Tables should be consistent with the specific objectives and context of the risk management activity.

Note that the descriptors in these examples have been chosen so as not to use the same words in consequence, likelihood and risk scales to avoid duplication within any matrix or subsequent report.

6.2.2 Consequences

Table 6.2 shows a simple qualitative consequence table that might be used by an organization with criteria related to health and safety, the environment and financial success. It also considers the political and financial impacts of risks, such as might be encountered in a public sector programme analysis. Table 6.3 shows a very simple descriptive table.

Where differing types of consequence are shown together in a table or where the same descriptor is used for the level, then an equivalence between each consequence will be inferred. If this is not true then separate tables and descriptors need to be used. Where equivalence is intended, then great care needs to be taken to ensure this is defendable and, where appropriate, agreed with stakeholders.

TABLE 6.2
Consequences scale – Example 1

Severity level	Consequences Types					
	Profit reduction	**Health and safety**	**Natural environment**	**Social/cultural heritage**	**Community/ govt/ reputation/ media**	**Legal**
V	US$10M–US$100M	Multiple fatalities, or significant irreversible effects to >50 persons	Very serious, long-term environmental impairment of ecosystem functions			Significant prosecution and fines Very serious litigation including class actions
IV	US$1M–US$10M	Single fatality and/or severe irreversible disability (>30%) to one or more persons		On-going serious social issues. Significant damage to structures/items of cultural significance	Serious public or media outcry (international coverage)	Major breach of regulation Major litigation
III	US$100 000–US$1M	Moderate irreversible disability or impairment (<30%) to one or more persons	Serious medium term environmental effects		Significant adverse national media/public/NGO attention	Serious breach of regulation with investigation or report to authority with prosecution and/or moderate find possible
II	US$10 000–US$100 000	Objective but reversible disability requiring hospitalization	Moderate, short-term effects but not affecting ecosystem functions	On-going social issues. Permanent damage to items of cultural significance	Attention from media and/or heightened concern by local community. Criticism by NGOs	Minor legal issues, non-compliances and breaches or regulation
I	<US$10 000	No medical treatment required	Minor effects on biological of physical environment	Minor medium-term social impacts on local population. Mostly repairable	Minor, adverse local public or medical attention or complaints	

A1

TABLE 6.3
Simple consequence scale – Example 2

Descriptive	Definition
Severe	Most objectives cannot be achieved
Major	Some important objectives cannot be achieved
Moderate	Some objectives affected
Minor	Minor effects that are easily remedied
Negligible	Negligible impact upon objectives

6.2.3 Likelihood

Scales need to be constructed to meet the circumstances of the study in hand. Tables 6.4 and 6.5 are examples of likelihood scales. The first uses order of magnitude scales to span a range of likelihoods from approximately yearly to one in 10 000 years. The second example shows a scale that is more suited to a defined period of time where the absolute likelihood of an event may be related to given activities – a project for example where the chance of achieving a certain outcome may need to be considered. Again, the scale must match the need.

TABLE 6.4
Example likelihood scale – Example 1

Level	Descriptor	Description	Indicative Frequency (expected to occur)
A	Almost certain	The event will occur on an annual basis	Once a year or more frequently
B	Likely	The event has occurred several times or more in your career	Once every three years
C	Possible	The event might occur once in your career	Once every ten years
D	Unlikely	The event does occur somewhere from time to time	Once every thirty years
E	Rare	Heard of something like the occurring elsewhere	Once every 100 years
F	Very rare	Have never heard of this happening	One in 1000 years
G	Almost incredible	Theoretically possible but not expected to occur	One in 10 000 years

TABLE 6.5
Example likelihood scale (probability) – Example 2

Descriptor	Description	Alternative Descriptor
Probable	Can be expected to occur during the project	Good odds
Possible	Not expected to occur during the project	Low to even odds
Improbable	Conceivable but highly unlikely to occur during the project	Poor odds

The number of occurrences in a time period will depend on the population, area or number of assets etc. being considered. Interpretation of indicative frequency scales such as in Table 6.4 must reflect the scope defined in the context and be consistent across a study.

The likelihood of gain or loss can be considered to be a function of both the exposure to the source of risk and the probability that the outcome will occur. These two factors can be assessed separately. For example, in Occupational Health and Safety, one might consider the exposure to a chemical hazard and the probability that harm will occur following exposure.

Systems engineering techniques such as fault tree analysis can be used to analyse probabilities in more detail.

6.3 Level of risk

The way that the level of risk is described will depend upon the type of analysis undertaken. A qualitative approach can only describe risk in qualitative ways – and this is usually done with descriptive terms. An example of this is given in Table 6.6. Quantitative analysis may on the other hand produce a single figure, datum or value or a mass of detailed data. Where this is the case, great care needs to be taken to ensure the units of risk are expressed and understood. Particular care must be taken with quantitative analysis when examining consequences that are intangible or difficult to quantify such as environmental or safety effects or reputation.

Assumptions and their impact as well as the level of certainty also need to be given.

Table 6.6 also illustrates the process and descriptors that may be used to combine a level of consequences with a level of likelihood to determine a level of risk. The number of categories of risk defined in a table like this should reflect the needs of the study.

TABLE 6.6
Example matrix for determining the level of risk

Likelihood Label	Consequences Label				
	I	II	III	IV	V
A	Medium	High	High	Very high	Very high
B	Medium	Medium	High	High	Very high
C	Low	Medium	High	High	High
D	Low	Low	Medium	Medium	High
E	Low	Low	Medium	Medium	High

NOTE: The relationship between consequence and likelihood will differ for each application: the level of risk assigned to each cell needs to reflect this.

The categories may be linked to the level of management attention that is recommended or the time scale of the response required. For example:

(a) Very high or high risk: senior executive management attention needed, action plans and management responsibility specified.

(b) Medium risk: manage by specific monitoring or response procedures, with management responsibility specified.

(c) Low risk: manage by routine procedures, unlikely to need specific application of resources.

Another simple example is shown in Table 6.7.

TABLE 6.7
Example—Simple risk level matrix

	Consequences		
Likelihood	**Major**	**Moderate**	**Minor**
Likely	Red	Red	Amber
Possible	Red	Amber	Green
Unlikely	Amber	Green	Green

Risk Treatment Key

Red	Immediate action
Amber	Heightened action
Green	Business as usual

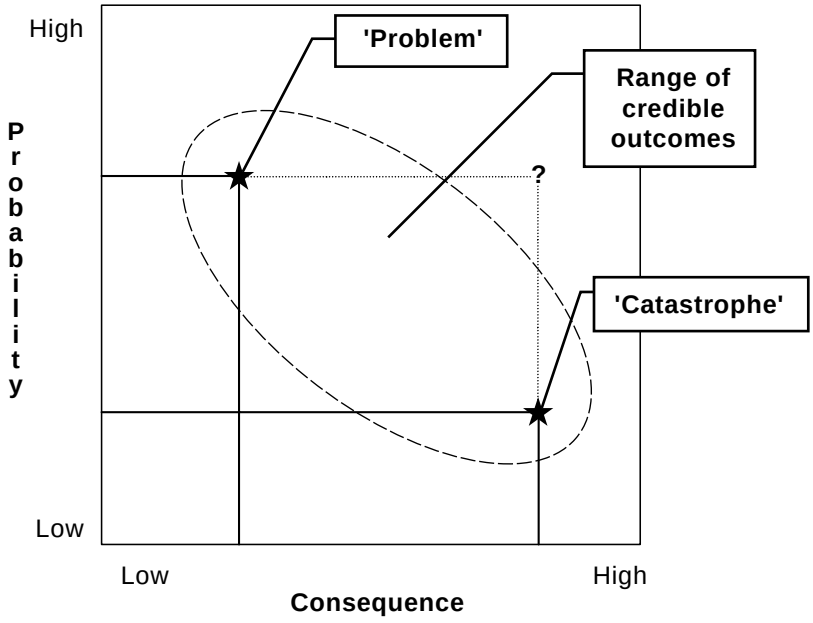


FIGURE 6.4 RISKS WITH A RANGE OF OUTCOMES

Many risk events may arise in a variety of ways, with a range of outcomes and associated likelihoods. For example, if a processing error were to occur in a business, it might be a minor problem, or it might cause a very large loss. Usually, the minor problems are much more frequent than the catastrophes, and the potential risks fall in a pattern such as that shown in Figure 6.4. When selecting a risk for assessment, there are now several choices: select a typical problem, with low consequence but high probability; or a representative catastrophe, with a high consequence but a low probability, or some intermediate outcome.

In many cases it is appropriate to focus on events with potentially catastrophic outcomes, as these are the ones that pose the largest threats and are often of greatest concern to managers.

In some cases it may be important to identify and analyse both 'problems' and 'catastrophes' as separate risks. For example, a frequent but low-impact (or chronic) problem may have large cumulative or long-term effects that are at least as important as those of a rare but high-consequence (or acute) event. In addition, the treatment actions for dealing with these two distinct kinds of risks are often quite different, so it is sensible to distinguish between them and to record them both.

It is important to be consistent when analysing risks that might occur in different ways like this. For example, selecting a consequence rating corresponding to a rare catastrophe and a probability rating corresponding to a frequent problem would identify a risk outside the feasible range in Figure 6.4, not a valid outcome for further analysis. For example if a consequence rating corresponding to a rare catastrophe is selected the likelihood rating must correspond to the likelihood of that catastrophic outcome. If a likelihood more appropriate to a frequent problem is selected, the selected risk would lie outside the feasible range as shown by the question mark in Figure 6.4, not a valid outcome.

6.4 Uncertainty

Risk is characterized by 'uncertainty'. The following possibilities, although not meant to be definitive, serve to illustrate the point:

(a) Risks for which we know or can assume the range of outcomes and their likelihood, but for where the specific value is not known within the range.

(b) Risks where we either don't know all the possible outcomes or the likelihood of each outcome or both (but we may know the main parameters).

(c) Risks where we 'don't know what we don't know'.

(d) Risks where causal chains or networks are uncertain (indeterminacy).

(e) Risks where there is variability in the nature and extent of exposure or in susceptibility. Sometimes probability or frequency distributions can be used to analyse variability. Or one may look at different special cases including best feasible case and worst feasible case scenarios.

There are various logical and mathematical ways to deal with uncertainty and variability. A generally high level of knowledge and skill is required to explore and communicate uncertainty. The availability of simple-to-use software tools can give the appearance of robust analysis of uncertainty even where the underlying logic is flawed. Great care should therefore be taken, both by those undertaking the analyses as well as those using the information.

Clearly, in many cases further information may reduce uncertainty. However, it is important to strike a balance between the effort required to obtain further information, and the value of that information to the decision process. Consultation and communication may help to determine which aspects of uncertainty require greatest effort. In some circumstances it will not be possible to obtain further information, or ignorance may mean that uncertainty cannot be resolved.

It is important to record and explain uncertainty and its effect on the analysis as the decision maker needs to know both the estimated level of risk and the degree of certainty with which it is known.

6.5 Analysing opportunities

Many risk analyses are directed to the negative consequences of risks, and the consequence scales reflect the losses or undesired outcomes that might arise. However, the risk management approach can be used to identify and prioritize opportunities (or 'positive' risks) with little change to the process.

When considering opportunities, the likelihood should be relevant to the nature of the beneficial outcomes being envisaged.

A1

An example is shown in Table 6.8, corresponding to the negative outcomes in Table 6.3; as with Table 6.3, the measures used should reflect the needs and nature of the organization and activity under study.

TABLE 6.8
Example of detailed description for positive consequence

Level	Descriptor	Description
1	Insignificant	Small benefit, low financial gain
2	Minor	Minor improvement to image, some financial gain
3	Moderate	Some enhancement to reputation, high financial gain
4	Major	Enhanced reputation, major financial gain
5	Outstanding	Significantly enhanced reputation, huge financial gain

A qualitative opportunity analysis matrix like that in Figure 6.5 can be used with a probability ranking table to combine the likelihood and consequence ratings to determine the level of opportunity. All that need change is the legend, with the focus of action being on capturing and exploiting the opportunity rather than avoiding or mitigating the problems:

(a) Very high opportunity; detailed planning required at senior levels to prepare for and capture the opportunity.

(b) High opportunity; senior executive management attention needed and management responsibility specified.

(c) Medium opportunity; manage by specific monitoring or response procedures.

(d) Low opportunity; manage by routine procedures, unlikely to need specific application of resources.

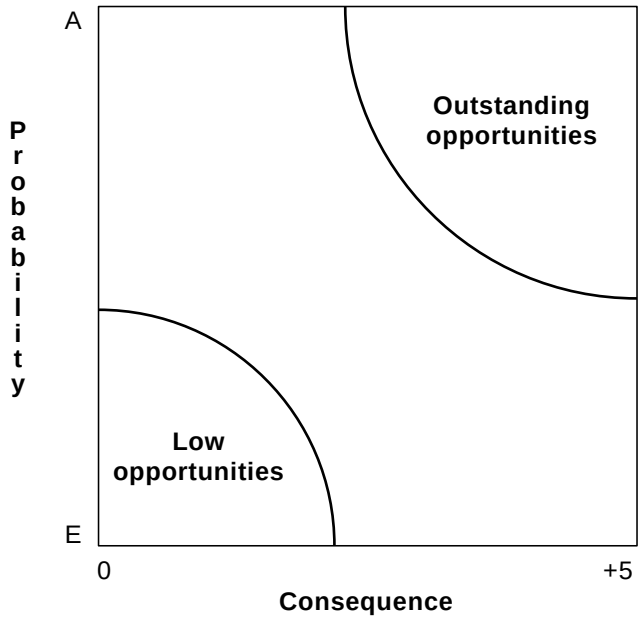


FIGURE 6.5 OPPORTUNITIES

6.6 Methods of analysis

Qualitative methods for generating information for risk analysis include—

(a) evaluation using multi-disciplinary groups;

(b) specialist and expert judgment; and

(c) structured interviews and questionnaires.

Quantitative methods of risk analysis include—

- consequence analysis;
- statistical analysis of historical data;
- fault tree and event tree analysis;
- influence diagrams;
- life cycle cost analysis;
- network analysis;
- simulation and computer modelling;
- statistical and numerical analysis;
- test marketing and market research; and
- probability analysis.

6.7 Key questions in analysing risk

Key questions in analysing risk include:

(a) What current systems may prevent, detect or lower the consequences or likelihoods of undesirable risks or events?

(b) What current systems may enhance or increase the consequences or likelihoods of opportunities or beneficial events?

(c) What are the consequences or range of consequences of the risks if they do occur?

(d) What is the likelihood or range of likelihoods of the risks happening?

(e) What factors might increase or decrease the likelihoods or the consequences?

(f) What additional factors may need to be considered and modelled?

(g) Are there limits of likelihood and consequence beyond which the analysis does not hold true?

(h) What are the limitations of the analysis and assumptions made?

(i) How confident are you in your judgement or research specifically in relation to high consequence and low likelihood risks?

(j) What drives variability, volatility or uncertainty?

(k) Is the logic behind the analysis methods sound?

(l) For quantitative analysis, what if any statistical methods may be used to understand the effect of uncertainty and variability?

Where there is a high level of uncertainty remaining following the analysis, it may be appropriate to flag this and review the work at some future date and in light of experience.

6.8 Documentation of the analysis

Documentation of this step should include—

(a) key assumptions and limitations;

(b) sources of information used;

(c) explanation of the analysis method, and the definitions of the terms used to specify the likelihood and consequences of each risk;

(d) existing controls and their effectiveness;

(e) description and severity of consequences;

(f) the likelihood of these specific occurrences;

(g) resulting level of risk; and

(h) effect of uncertainty.

Detailed documentation may not be required for very low risks, however a record should be kept of the rationale for initial screening of very low risks.

Documentation of risk analysis is often included in the risk register, see Section 10.

This page has been left blank intentionally

7 Risk evaluation

AS/NZS 4360:2004

3.5 Evaluate risks

The purpose of risk evaluation is to make decisions, based on the outcomes of risk analysis, about which risks need treatment and treatment priorities.

Risk evaluation involves comparing the level of risk found during the analysis process with risk criteria established when the context was considered.

The objectives of the organization and the extent of opportunity that could result should be considered. Where a choice is to be made between options, higher potential losses may be associated with higher potential gains and the appropriate choice will depend on an organization's context.

Decisions should take account of the wider context of the risk and include consideration of the tolerability of the risks borne by parties other than the organization that benefits from it.

In some circumstances, the risk evaluation may lead to a decision to undertake further analysis.

Commentary

7.1 Overview

Risk evaluation uses the understanding of risk obtained by risk analysis to make decisions about future actions.

Decisions may include:

- Whether a risk needs treatment.
- Whether an activity should be undertaken.
- Priorities for treatment.

The nature of the decisions that need to be made and the criteria which will be used to make those decisions were decided when establishing the context but need to be revisited in more detail at this stage now more is know about the particular risks identified.

7.2 Types of evaluation criteria

Criteria used to make decisions must be consistent with the defined external, internal and risk management context and take account of the objectives, of the organization, the objectives of the risk exercise and stakeholder views etc.

Decisions may be based on the level of risk but may also be based on thresholds specified in terms of—

(a) specified consequences;

(b) the likelihood of specified events or outcomes;

(c) the cumulative effect of multiple events; and

(d) the range of uncertainty for the risk levels at some specified level of confidence.

Criteria may be expressed quantitatively or qualitatively.

7.3 Evaluation from qualitative analysis

No organization has limitless resources to take advantage of opportunities or to deal with adverse risk. It is therefore necessary to define priorities. Qualitative analysis is often used to set priorities or treatment based on the level of risk. Priorities may also be set on the basis of consequences alone or other criteria as defined in Clause 7.2.

The different levels of risk in a qualitative risk matrix are sometimes used to define different actions required as in Clause 6.3 and hence act implicitly as risk criteria. However since judgments of consequence and likelihood and the divisions between qualitative levels of risk on the matrix are defined to suit particular circumstances, matrices of this kind have limitations as decision tools.

7.4 Tolerable risk

The concept of tolerable risk derives from Sir Frank Layfield who in 1987 noted that 'although acceptable risk is often used in balancing risks and benefits it does not adequately convey the reluctance with which possibly substantial risks and benefits may be tolerated'. Thus individuals are prepared to 'tolerate' some risks under certain circumstances in return for specified benefits.

The simplest risk criteria divides risks that need treatment from those which do not. This gives attractively simple results but does not reflect uncertainties either in estimating risks and in defining the boundary between those that require treatment and those that do not.

A common approach is to divide risks into three bands:

(a) An upper band where adverse risks are intolerable whatever benefits the activity may bring, and risk reduction measures are essential whatever their cost.

(b) A middle band (or 'grey' area) where costs and benefits, are taken into account and opportunities balanced against potential adverse consequences.

(c) A lower band where positive or negative risks are negligible, or so small that no risk treatment measures are needed.

For risks with significant potential health, safety or environmental consequences, this is expressed as the 'As Low As Reasonably Practicable' or ALARP concept illustrated in Figure 7.1 but the concept is also applicable for other risks.

The width of the cone indicates the size of risk and the cone is divided into bands as discussed above.

When risk is close to the intolerable level the expectation is that risk will be reduced unless the cost of reducing the risk is grossly disproportionate to the benefits gained. Where risks are close to the negligible level then action may only be taken to reduce risk where benefits exceed the costs of reduction.

The concept of practicability in ALARP contains within it the ideas of practicality (*Can something be done?*) as well as the costs and benefits of action or inaction (*Is it worth doing something in the circumstances?*). These two aspects need to be balanced carefully if the risks the organization is treating are related to an expressed or implied duty of care.

Lord Justice Asquith in 1949 provided a definition of 'reasonably practicable'.

> '"Reasonably practicable" is a narrower term than "physically possible" and it seems to me to imply that a computation must be made by the owner, in which the quantum of risk is placed on one scale and the sacrifice involved in the measures necessary for averting the risk (whether in money, time or trouble) is placed in the other;

and that if it be shown that there is a gross disproportion between them — the risk being insignificant in relation to the sacrifice — the defendants discharge the onus on them.

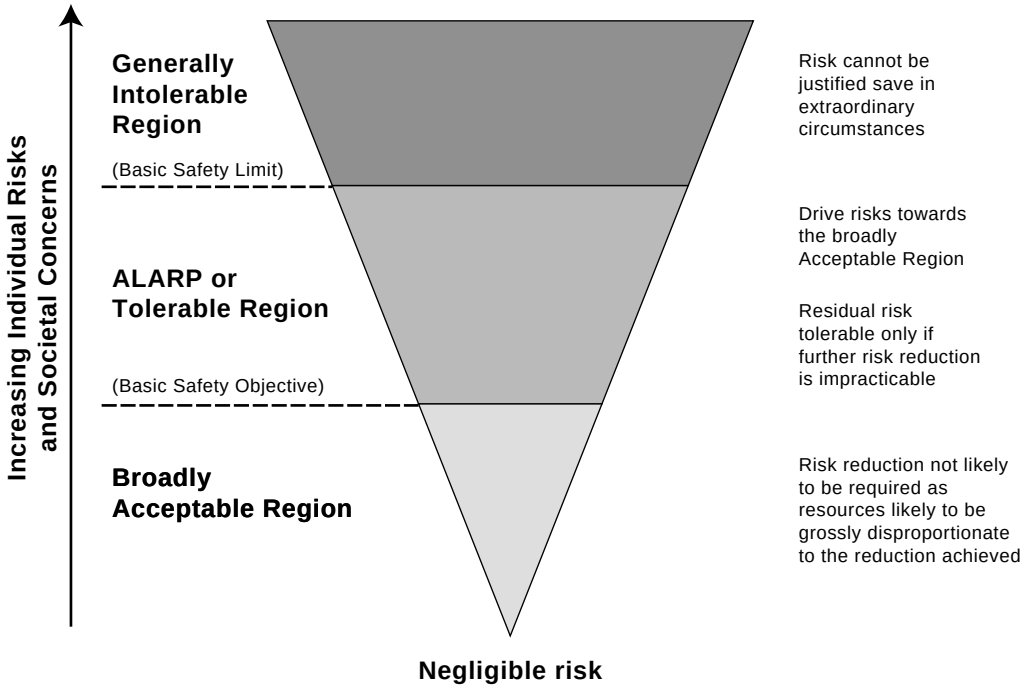


FIGURE 7.1 THE ALARP PRINCIPLE

7.5 Judgement implicit in criteria

Value judgements are implicit in many criteria. These depend on an individual's familiarity with the risk, their trust in the effectiveness of exiting risk controls, and their perceptions of the risks and benefits of the activity.

The same risk may seem negligible to one person and very high to another. The criteria should therefore try to represent an objective view, taking account of the needs of all those affected, and also the people actually subjected to the risk.

Communication and consultation may address these points (see Section 3).

7.6 Evaluation criteria and historical events

The criteria for deciding whether a risk needs to be treated are often set with reference to events from similar activities in the past or by background risks experienced in daily life. However data can be distorted by:

(a) Large incidents, one-off catastrophes or windfalls that dominate the dataset.

(b) A declining level of risk due to increased controls as lessons have been learned from incidents and standards of control have improved. This means that criteria based on old historical risks may not be strict enough to control the modern situation.

(c) Changes in the activities or circumstance covered now as compared with the past situation. For example, the overall risk from a sample of activities may be different in the past.

Setting evaluation criteria from historical risk estimates introduces the problems that:

- A risk may need to be treated in one set of circumstances, but not in another.
- A risk may have been 'accepted' in the past but may not be 'acceptable' now using current methods of analysis and taking into account society's current level of tolerance.
- Background risks are different in different situations (e.g. different countries), raising the question of whether evaluation criteria should be tailored to the situation and not globally applied.

As a result of problems like these, political or economic judgements may be used in addition to available risk data.

This page has been left blank intentionally

8 Risk treatment

AS/NZS 4360:2004

3.6.1 General

Risk treatment involves identifying the range of options for treating risks, assessing these options and the preparation and implementation of treatment plans.

3.6.2 Identifying options for the treatment of risks with positive outcomes

Treatment options for risks having positive outcomes (opportunities) which are not necessarily mutually exclusive or appropriate in all circumstances, include:

- Actively seeking an opportunity by deciding to start or continue with an activity likely to create or maintain it (where this is practicable).

  Inappropriate pursuit of opportunities without consideration of potential negative outcomes may compromise other opportunities as well as resulting in unnecessary loss.

- Changing the likelihood of the opportunity, to enhance the likelihood of beneficial outcomes.

- Changing the consequences, to increase the extent of the gains.

- Sharing the opportunity.

  This involves another party or parties bearing or sharing some part of the positive outcomes of the risk, usually by providing additional capabilities or resources that increase the likelihood of the opportunity arising or the extent of the gains if it does. Mechanisms include the use of contracts and organizational structures such as partnerships, joint ventures, royalty and farm-in arrangements. Sharing the positive outcomes usually involves sharing some of the costs involved in acquiring them.

  Sharing arrangements often introduce new risks, in that the other party or parties may not deliver the desired capabilities or resources effectively.

- Retaining the residual opportunity.

  After opportunities have been changed or shared, there may be residual opportunities that are retained without any specific immediate action being required.

3.6.3 Identifying options for treating risks with negative outcomes

Treatment options for risks having negative outcomes are similar in concept to those for treating risks with positive outcomes, although the interpretation and implications are clearly different. Options include:

- Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk (where this is practicable).

  Risk avoidance can occur inappropriately if individuals or organizations are unnecessarily risk-averse. Inappropriate risk avoidance may increase the significance of other risks or may lead to the loss of opportunities for gain.

- Changing the likelihood of the risk, to reduce the likelihood of the negative outcomes.

- Changing the consequences, to reduce the extent of the losses. This includes pre-event measures such as reduction in inventory or protective devices and post-event responses such as continuity plans.

- Sharing the risk.

  This involves another party or parties bearing or sharing some part of the risk, preferably by mutual consent. Mechanisms include the use of contracts, insurance arrangements and organizational structures such as partnerships and joint ventures to spread responsibility and liability. Generally there is some financial cost or benefit associated with sharing part of the risk with another organization, such as the premium paid for insurance.

  Where risks are shared in whole or in part, the organization transferring the risk has acquired a new risk, in that the organization to which the risk has been transferred may not manage the risk effectively.

- Retaining the risk.

  After risks have been changed or shared, there will be residual risks that are retained. Risks can also be retained by default, e.g. when there is a failure to identify or appropriately share or otherwise treat risks.

3.6.4 Assessing risk treatment options

Selecting the most appropriate option involves balancing the costs of implementing each option against the benefits derived from it. In general, the cost of managing risks needs to be commensurate with the benefits obtained. When making such cost versus benefit judgements the context should be taken into account. It is important to consider all direct and indirect costs and benefits whether tangible or intangible, and measured in financial or other terms.

A number of options may be considered and applied either individually or in combination. Sensitivity analysis (see Clause 3.4.5) is one way of testing the effectiveness of different options for treating risk. The organization may benefit through the adoption of a combination of options. An example is the effective use of contracts and specific risk treatments supported by appropriate insurance and other risk financing.

Decisions should take account of the need to consider carefully rare but severe risks that may warrant risk treatment actions that are not justifiable on strictly economic grounds. Legal and social responsibility requirements may override simple financial cost benefit analysis.

Risk treatment options should consider the values and perceptions of stakeholders and the most appropriate ways to communicate with them.

If the budget for risk treatment is constrained the treatment plan should clearly identify the priority order in which individual risk treatments should be implemented. It is important to compare the full cost of not taking action against the budgetary saving.

Risk treatment may itself introduce new risks that need to be identified, assessed, treated and monitored.

If, after treatment, there is a residual risk, a decision should be taken about whether to retain this risk or repeat the risk treatment process.

3.6.5 Preparing and implementing treatment plans

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

- proposed actions;
- resource requirements;
- responsibilities;
- timing;
- performance measures; and
- reporting and monitoring requirements.

Treatment plans should be integrated with the management and budgetary processes of the organization.

Commentary

8.1 Introduction

Risk evaluation provides a list of risks requiring treatment, often with associated ratings or priorities. Risk treatment involves identifying a range of options for treating these risks, evaluating those options, preparing treatment plans and implementing them.

Before appropriate treatment actions can be determined, the analysis of each risk may need to be revisited and extended to draw out the information needed to identify and explore different treatment options. The design of risk treatment measures should be based on a comprehensive understanding of the risks concerned; this understanding comes from an appropriate level of risk analysis. It is particularly important to identify the causes of the risks so that these are treated and not just the symptoms.

It will usually not be cost-effective or even desirable to implement all possible risk treatments. It is, however, necessary to choose, prioritise and implement the most appropriate combination of risk treatments. Treatment options, or more usually combinations of options, are selected by considering factors such as costs and benefits, effectiveness and other criteria of relevance to the organization. Factors such as legal, social, political and economic considerations may need to be taken into account.

Treatment of individual risks will seldom occur in isolation and should be part of an overall treatment strategy. Having a clear understanding of a complete treatment strategy is important to ensure that critical dependencies and linkages are not compromised. For this reason development of an overall treatment strategy should be a top-down process, driven jointly by the need to achieve business objectives while controlling uncertainty to the extent that is desirable.

It is wise to be flexible and consult broadly about risk treatment with stakeholders and perhaps the wider community as well as peers and specialists. Many treatments need to be acceptable to stakeholders or those who are involved in implementation if they are to be effective and sustainable.

Figure 8.1 outlines the risk treatment process and the iterative nature of the development of treatment action plans.

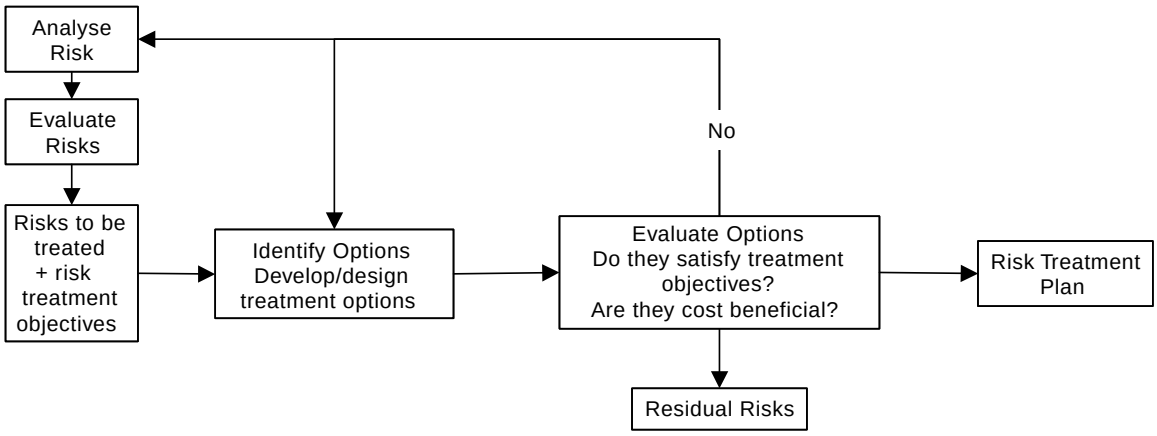


FIGURE 8.1 TREATING RISKS

8.2 Identify options

8.2.1 General

The starting point for identifying options is often a review of existing guides for treating that particular type of risk. For example, in many safety, environmental and construction areas there are requirements laid down in legislation and standards. However, these will need to be reviewed for completeness and suitability.

For many risks, such guides don't exist and treatment options will need to be developed from first principles in order to be effective.

One treatment option available is to avoid the risk entirely by eliminating it altogether by deciding not to proceed with or discontinuing an activity. This will remove possibilities of harm but will also often eliminate the opportunity. More usually risk treatment involves changing either the likelihood or the consequences of the risk or both.

Figure 8.2 illustrates how treatments can be directed to all or some of the elements that give rise to consequences (i.e. before the event or post-event).

8.2.2 Understanding cause

Risk treatment design should be based on a comprehensive understanding of how risks arise. This includes understanding not only the immediate causes of an event but also the underlying factors that influence whether the proposed treatment will be effective. These factors are sometimes called 'root causes' and stem from underlying needs, beliefs or circumstances.

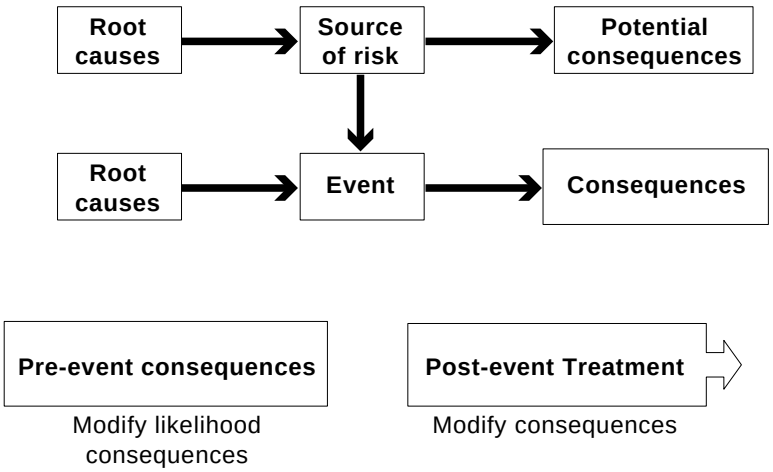


FIGURE 8.2 GENERAL SCHEME FOR CAUSING AND TREATING RISK

Root causes can include facets of an organizational culture such as ingrained processes and practices or paradigms that need to change to successfully treat a risk from occurring (and reoccurring). Sources of risk that flow on from the attitudes within organizational culture, cannot be treated successfully unless changes are made to these facets.

To influence the root causes, treatment measures should seek to establish appropriate beliefs and culture so that motivation is clear and positive in terms of the achievement of organizational objectives and is consistent with the organization's policy. Examples are policy statements, the actions of executives (in setting good examples) or key performance indicators (KPIs) that act to support and promote the correct beliefs and motivation.

Sources of risk may be treated by removal, reduction or enhancement, depending on whether the outcome is positive or negative. For example, creating a new market for your products may enhance positive outcomes associated with profit and growth in market share, or reducing the stores of hazardous chemicals may reduce negative outcomes associated with leaks or spills.

Events may be external and outside the control of the organization, such as currency changes or natural disasters. For these risks, the available option will be reduce the vulnerability of the organization to the event (e.g. improving earthquake design to resist shaking of particular magnitude).

Events may be internally generated in which case they may be able to be prevented or encouraged as required. Treatment to change the likelihood of an event occurring can include, for example, design and planning of activities and processes, compliance monitoring training and supervision.

In some situations it may be possible to reduce negative consequences by protecting those things that are exposed, for example by designing buildings to withstand fires or preparing communities for natural disaster. Detection mechanisms to give early warning are an important part of protection.

It is also possible to make things more open to opportunity, for example by designing future expansion capacity into new plant and equipment. Analysis in this case involves gaining an understanding the potential for opportunity and the factors that enhance the likelihood of achieving it.

Consequences may also be modified by planning post-event actions such as contingency plans (designed for opportunities as well as loss) and business continuity plans in the event of a major loss. An organization can also reduce negative consequences after an event by manipulating the way in which financial losses are allocated. This may be done through contracts, or through insurance and other financial instruments. These two kinds of treatment options are described further below.

8.2.3 Contingency planning

One way of treating consequences is to undertake planning and preparedness for contingencies so that an organization can act quickly to take advantage of unexpected gains or stem losses and prevent or limit disruption. This requires plans to be well founded in good risk management principles, tested and up-to-date.

When an event occurs, the organization's management may need to respond quickly to mitigate the impact of the event on the achievement of business objectives such as revenue stream, product quality, corporate reputation or customer satisfaction.

In most circumstances, these impacts may be managed as part of normal management processes. However, when the scale of the event overwhelms management's normal capacity to cope, a systematic approach to critical incident management is needed. Figure 8.3 shows how the various types of plan fit into the general chronology and phases of a critical incident.

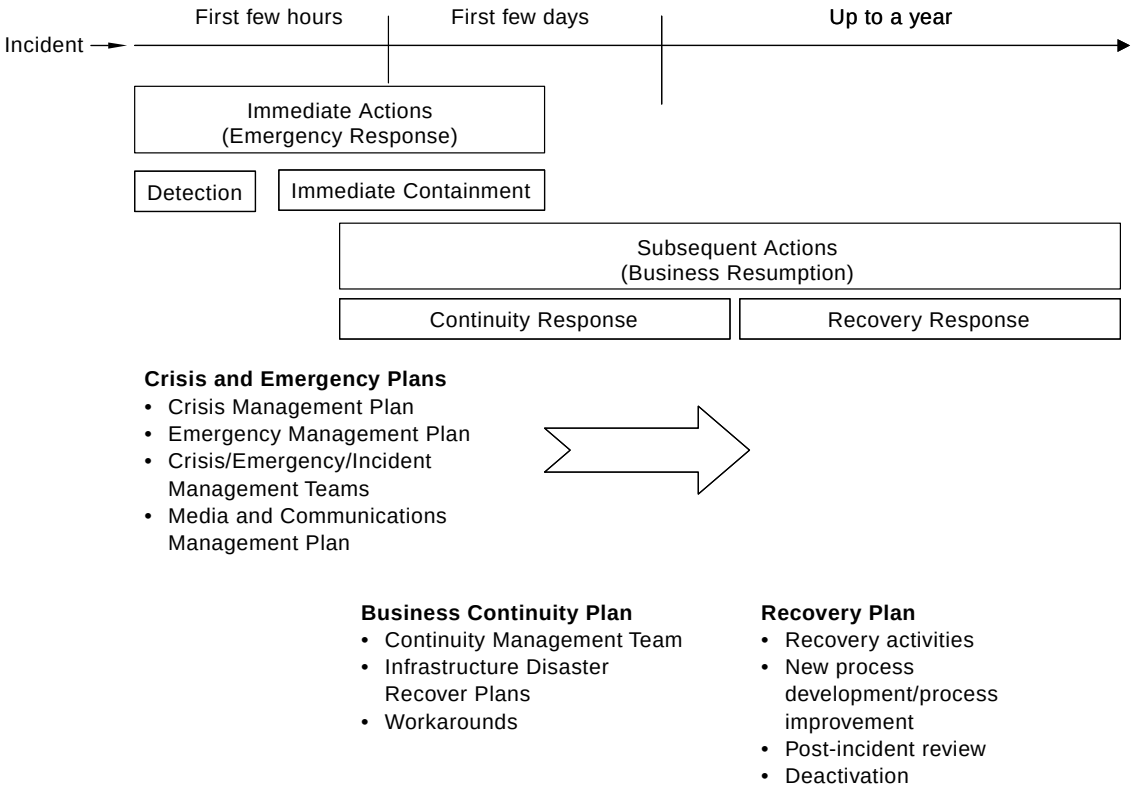


FIGURE 8.3 CRITICAL INCIDENT MANAGEMENT

At the core of critical incident management is Business Continuity Management (BCM), which provides an organization with a disciplined capability to continue to operate sustainability in the face of potential significant business disruption. Appropriately implemented, BCM can provide a robust framework for addressing disruption risk exposures in a cost effective and timely manner. It provides a key component for the organization to sustain good corporate governance, maintain its customer base and market share, retain the confidence of its stakeholders, and manage its reputation in the face of an increasingly turbulent economic, industrial and security environment. As a minimum response, effective BCM will prevent an emerging crisis from becoming more persistent or widespread.

Full advice on the practical development and implementation of business continuity management can be found in Australian/New Zealand Standards Handbook, HB 221.

8.2.4 Sharing Risk

Risk sharing involves another organization bearing or sharing some or all of the risk, usually via a contract. The most common forms of risk sharing are subcontracting, outsourcing and insurance.

8.2.5 Contracting

Contracts are agreements between parties for the conduct of specific actions or functions, in return for a fee. Contracts of all sizes and for all purposes are intended to transfer or share risks, allocating them to an individual or an organization to be managed for the duration of the arrangement. Contracting can be a very complex process at times, but the principles remain the same – allocate risk to the party best placed to manage it, through specific wording in the contract document. Inappropriate transferring of risk can lead to a change in the nature of a risk, or the emergence of new risks.

When contracts are being contemplated, as well as the direct costs and benefits of the contractual arrangement, uncertainties in those costs and benefits should be considered as well as new risks which may arise.

Often legislation will determine whether or how risks may be shared.

For further information on the risks associated with outsourcing see Australia/New Zealand Handbook, HB 240.

8.2.6 Insurance

Few organizations have adequate internal financial resources to be able to cover the cost of major losses. Insurance is a means of arranging funding for particular types of losses in return for paying a premium. For example, insurance cover may be available for damage to property and consequential costs (such as loss of revenue or increased operating costs), or liability for the financial consequences of another party due to failure to discharge a legal obligation.

Not all major risks are insurable. For example, it is generally not possible to insure an organization's reputation, but there are some types of organization for whom loss of trust by their stakeholders could be fatal. While changes in currency exchange rates can be insured by hedging, it is unlikely that the effect of a global economic downturn can be insured against.

Insurance works on the premise of the premiums of the many being sufficient to pay for the losses of the few, as well as providing a return on the insurer's capital investment and operating costs, across the portfolio of insured risks. In setting the premium for a particular risk, insurers have regard to likelihood and consequence and take account of existing controls. In some cases, insurers may insist on additional treatments to reduce the risk, or they may agree to charge less if additional controls are implemented or if the insured party agrees to share the risk, for example by paying the first part of any loss to an agreed amount or excess (deductible).

It is usually a good investment to provide quality information about the risk being offered to the insurer, as this helps reduce uncertainties and make it more likely that the insurer will be prepared to offer cover and or do so on more attractive terms.

Decisions about insurance are best taken in the context of other risk treatment activities to ensure sound decisions are made about the extent of insurance required and to optimize the connection between availability of cover, risk, excess and price.

Some things to bear in mind when buying insurance are:

- An insurance policy provides no more cover than the legal effect of the policy wording. Most policies will have clauses excluding or limiting what is covered. If those exclusions create a large financial exposure, some other form of control will be needed.
- An insurance policy is only as good as the insurer's financial ability to pay. The major financial rating agencies provide information about the financial security of insurers but ultimately this is only a guide. There have been major insurance company failures despite positive rating information.
- There is an explicit obligation of disclosure by both parties to an insurance contract. An organization must not mislead its insurer. To do so can void the cover. This obligation includes reporting losses to the insurer quickly.
- Should a loss occur, an insured organization is expected to act as if it is uninsured and to do what is reasonable to minimize the scale of loss, for example by re-securing a property after a break-in, and not to admit liability before the insurer has been able to examine the issue.

These and other technicalities relating to insurance suggest that organizations should seek the advice of a professional before taking and implementing decisions about the type and extent of cover bought.

8.3 Evaluate treatment options

8.3.1 General

In general, a combination of treatment options will be selected from the range of options identified. The options selected need to be compatible with overall objectives of the organization and with the risk evaluation criteria.

8.3.2 Designing risk treatment

The careful design of the combination of treatment options is important to ensure 'fit for purpose', ongoing effectiveness and maintainability of the measures. Too much treatment is as undesirable as too little if resources and management attention are diverted from more business-critical activities.

For some type of risks there are guides to designing treatment measures. For example, in the field of occupational health and safety, the key elements of a good permit to work system are well known and can be looked up in the safety literature. The same is true, to some extent, for some financial and accounting activities.

A 5-step process is suggested below for general risk treatment design. While this is primarily aimed at the development of new measures, it is also a very useful basis for the assurance and assessment of existing treatment measures as part of, for example, control self-assessment.

Step 1: Review causes and controls

This step involves revisiting the risk analysis as discussed above, ensuring that risk is fully understood. A gap analysis can be carried out to look at and assess how well the risks and the factors which influence them are addressed by existing treatments.

This gap analysis then leads to the specification of the treatment objectives for any additional treatment measures as part of a complete control plan.

Step 2: Treatment objectives

The broad intent of risk treatment is to change the risk to a level where the benefit exceeds the total cost of the treatment (where costs and benefits have both monetary and more intangible components). Cost Benefit Analysis (CBA) can also be used, in part, to distinguish between different treatment options. This is considered further in Clause 8.4.

The intent of a risk treatment plan can be created in terms of treatment objectives. These can state:

(a) The risks that are to be treated.

(b) The causes, sources or events that the treatment should target.

(c) What the treatment measures should do, when (where) and how.

(d) The required performance level of treatment in terms of efficacy, reliability and availability.

Two examples of statements of treatment objective are:

> 'The treatment plan should act to reduce human error associated with the transaction processing by encouraging accurate data input, reducing the opportunity for errors by reconciliation and checking, and automatically detecting

and warning of errors if they do occur. The measures need to be effective at year-end reconciliation and they should act to ensure that no errors are made that create material balance differences.'

'The treatment plan should act to prevent the exposure of employees to the dust exceeding exposure limit of 1 mg/m^3. The measures should act to motivate the correct operation of the machine at all times during normal operations and also during maintenance. If the level of dust exceeds the exposure limit at any time, the operation should be stopped.'

Step 3: Detailed design of treatment measures

The detailed design of treatments should consider their practicality and maintainability.

Many of the risks that the organization and its stakeholders face can, in theory, be changed to any extent required. In other cases, there is little that can practically be done, other than to take action to 'adapt to the risk' (examples here are some commodity price risks and tax legislation changes). In some cases the organization can only wait, 'reserve position' and monitor the situation until the source of risk changes. In this case treatment is directed at mitigation, through early detection, assessment and action. Contingency plans may be worthwhile in some circumstances.

The key to practical control design is to involve in the process those who will be involved in the activity concerned and who will be affected by the measures.

Wherever possible, measures should be designed to be 'embedded' in normal business processes, activities and systems. They should not impede the logical and natural flow of processes and should be easy to understand and appreciate.

Step 4: Design review

Even the simplest of treatments should be subject to some degree of design review. This should include checking, as a minimum that—

(a) the treatment objectives will be satisfied;

(b) the design is fit for purpose—in other words, that it is realistically capable of achieving levels of effectiveness, reliability and availability consistent with the importance of the associated activity to the organization;

(c) it takes into account realistic and reasonably anticipated operational conditions;

(d) it is easily capable of being checked and monitored, or is self-checking;

(e) the treatments will last and endure and can be maintained easily; and

(f) the proposed risk treatments do not introduce new risks, or if they do the new risks are at a lower level of concern than the old.

For the most critical situations, where treatment failure could lead to major losses or have a significant effect on the organization's objectives, then more rigorous design review is required.

Step 5: Communication and implementation

No treatment can be expected to work effectively unless those who will be involved in the activity concerned and those who would be affected by the treatment measures understand what the plan is, and what it is designed to achieve. The development of a communications plan should be an integral part of the treatment design process.

Control self-assessment and other participative assurance processes also provide a very effective means of communication through involvement.

8.4 Selecting options for treatment

8.4.1 General

When selecting options the following issues should be considered:

- Some benefits arising from the treatment may be more important than others.
- At times non-quantifiable benefits and costs may be regarded as more important that quantifiable ones. In this case, decisions should not be based solely on quantitative analysis.
- Direct and indirect benefits and costs associated with risk treatments may occur over different time periods and this should be taken into account in any quantitative and qualitative analysis.
- Estimates of direct and indirect benefits and costs may be subject to different levels of uncertainty and may follow different probability distribution curves.
- Social expectation as well as legal duty may mandate particular risk treatment actions.
- There is often a particular aversion to events that reflect 'human dread'.
- There is an analogous form of 'corporate dread' for events that conflict with organizational values and that may damage its reputation and image.

Specific issues that might be considered in making decisions about options are listed in Table 8.1.

TABLE 8.1
Decision making issues

Acceptability	Is the option likely to be accepted by relevant stakeholders?
Administrative efficiency	Is this option easy to implement or will it be neglected because of difficulty of administration or lack of expertise?
Compatibility	How compatible is the treatment with others that may be adopted?
Continuity of effects	Will the effects be continuous or only short term? Will the effects of this option be sustainable? At what cost?
Cost effectiveness	Is it cost-effective, could the same results be achieved at lower cost by other means?
Economic and social effects	What will be the economic and social impacts of this option?
Effects on the environment	What will be the environmental impacts of this option?
Equity	Are risks and benefits distributed fairly e.g. do those responsible for creating the risk pay for its reduction?
Individual freedom	Does the option deny any basic rights?
Jurisdictional authority	Does this level of organization or government have the authority to apply this option? If not, can higher levels be encouraged to do so?
Leverage	Will the treatment options lead to additional benefits in other areas?
Objectives	Are organizational objectives advanced by this option?
Regulatory	Does the treatment (or lack of treatment) breach any regulatory requirements?
Political acceptability	Is it likely to be endorsed by the relevant government authority? Will it be acceptable to communities?
Risk creation	Will this treatment introduce new risks?
Timing	Will the beneficial effects be realized quickly?

8.4.2 Trade off between costs and benefits

Treatment options may have an incremental benefit depending on how much is spent on the implementation. An organization may consider a trade off between the benefit and the cost of implementation. This trade off is demonstrated in Figure 8.4.

Any one of several decision points may be chosen. These include:

- a satisfactory (but not optimum) solution;
- the most cost-effective solutions;
- the accepted practice (industrial norm, good business practice)
- the best achievable result (given current technology); and
- the absolute minimum.

Which criterion is considered to be the most acceptable, depends on the circumstances and the established risk context within which the decision has to be made. Given the right scenario, a valid argument could be made for choosing any of the above decision points.

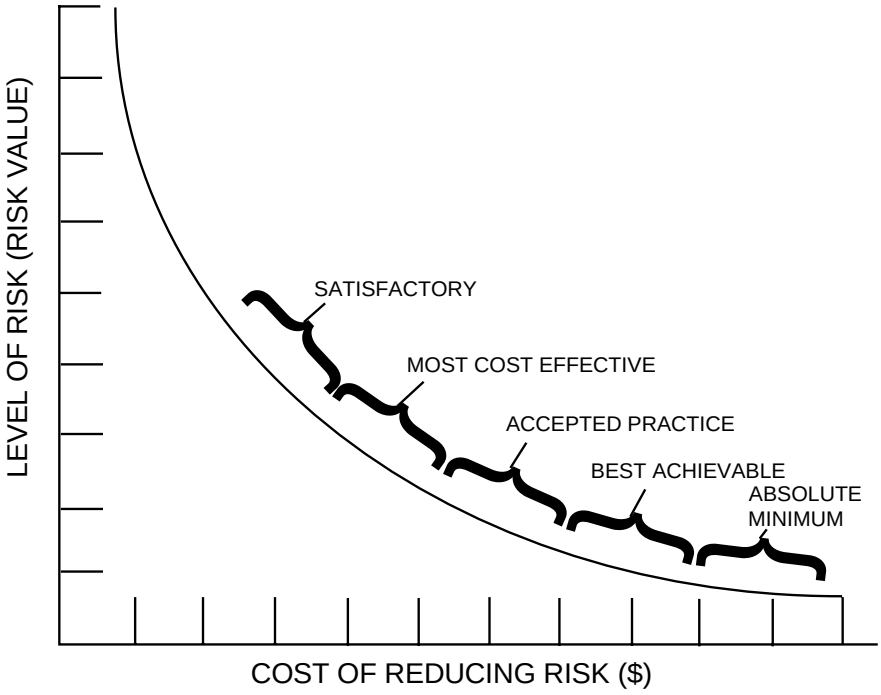


FIGURE 8.4 TRADE OFF BETWEEN LEVEL OF RISK AND COST OF REDUCING RISK

8.4.3 Cost benefit analysis

Evaluating and selecting treatment options requires decisions be made about feasibility and the range of benefits and costs that are involved. Formal cost benefit analysis (CBA) provides an objective means of comparing the costs and benefits of the risk without treatment and the comparable costs and benefits of the treated risk. There should be a consistent approach to comparing costs and benefits of different options. This can be conducted in a purely quantitative manner but in most cases, it is also important to take into account less tangible costs and benefits such as some of the issues summarized in Table 8.1.

This is particularly so where the ALARP principle is applied (see Clause 7.4) or where legislation requires some form of reasonably practicable treatment.

CBA should involve consideration of all the benefits to be experienced; where appropriate, both direct benefits and indirect benefits need to be included in the analysis. It should also involve both direct and indirect costs. Costs and benefits may be quantitative or qualitative.

When there is uncertainty about either the costs to be incurred or the benefits to be gained, the values used may be weighted to take the likelihood of occurrence into account.

Benefits can rise:

(a) Directly from the reduction in risk that leads to either the prevention or minimization of loss or a reduction in the likelihood that loss or harm occurs either to the organization or its stakeholders.

(b) Increased opportunities.

(c) Indirectly such as from greater management confidence, savings such as insurance premium reductions, or improvements in intangibles like reputation or credit rating.

Benefits are also associated with treatments that act to create or enable opportunities for the organization that have ascribable value.

Costs may involve:

(i) The direct costs such as the cash costs associated with treatment options and their implementation.

(ii) Increased risk of negative outcomes or reduced opportunities.

(iii) Indirect costs such as loss of productivity, management time, distraction from core business activity, loss of utility or diversion of capital from value-adding projects.

Costs and benefits may extend beyond the organization. In some circumstances it may be important that external and internal costs and benefits are taken into account in the CBA.

When comparing treatment options, the *status quo* should also be taken into account, so the option of doing nothing, tolerating and retaining the risk is evaluated too. Remember, however, that the *status quo* will not be static and will need to be reviewed over time.

8.4.4 Qualitative analysis of costs and benefits

Cost benefit analysis (CBA) involves comparing estimates of costs and benefits. This requires that, where possible, both measures be expressed in similar and comparable units; normally in monetary terms such as dollars. However, often it will not be possible to quantify all costs and all benefits and sometimes the greatest benefits are not quantifiable at all. This is particularly the case with ancillary and indirect costs and benefits. For example, preventing the damage to reputation caused by a major incident may not be easily quantifiable and yet may be of greater actual benefit to an organization than just the pure avoidance of physical damage, compensation costs and loss of revenue.

Where a CBA involves both easily quantifiable or 'hard' costs and benefits and not so easily quantifiable, 'soft' costs and benefits, both hard and soft elements should be presented to the decision maker. The process that should be followed is to:

(a) List all types of costs and benefits.

(b) Group all costs and benefits into hard and soft categories.

(c) Calculate a quantitative measure for hard costs and benefits (such as those described below).

(d) Evaluate the soft costs and benefits using some equivalence scale such as those shown for risk rating in Table 6.2.

(e) Present the results of both the 'hard' and 'soft' cost benefit analyses together.

If there is notable aversion or preference towards some costs or benefits, then this should be made clear in the presentation of the results to the decision maker.

8.4.5 Quantitative CBA

In its simplest form, quantitative CBA will involve adding together the dollar amounts for direct and indirect costs and for direct; and indirect benefits and then comparing the total amounts as a ratio of total benefits over total costs. If this ratio is greater than a predetermined level, then the control is worthwhile. This level may simply be 1 (i.e. total benefits exceed total costs), or it may be a number different from 1. In many cases there will be a requirement for the benefits to clearly exceed the costs, so the threshold number will be greater than one. However, for some occupational health and safety legislation, there is a requirement that safety improvements should be implemented unless the cost is grossly disproportionate to the incremental benefit.

This simple form of CBA is only suitable where—

- there is reasonably confidence that the full value of the benefit will be gained and that the costs will be as predicted;
- most of the costs will be incurred within a year or so;
- there is early payback (most benefits occur within the first year or so and in the same time frame as costs are incurred);
- costs and benefits are distributed evenly; and
- intangibles can be incorporated into quantitative CBA by allocating dollar values using techniques such as willingness to pay.

If most of the costs or the benefits are unlikely to be experienced within the first year or so then it may be necessary to discount the benefits and costs to allow the assessment to be made 'in today's money'. This is particularly true where the direct costs may be incurred now, but the benefits and indirect costs may be experienced for some time going forward.

This discounting provides a means to take into account the opportunity cost of capital and involves the application of a discount rate to the annual value of the cost or benefit.

Net Present Value (NPV) is the most often used measure for Discounted CBA. Discounted CBA and NPV calculation is appropriate where—

- there is significant uncertainty that the full value of the benefit will be gained or that the cost will be as predicted; and
- most of the costs and benefits will not be incurred within the first year or so.

(*Handbook of cost benefit analysis* (1991)).

8.5 Preparing treatment plans

Once treatment options for individual risks have been selected, they should be assembled into action plans: risk treatment plans or strategies. Treatment actions for different risks need to be combined and compared so as to identify and resolve conflicts and eliminate redundancy.

Treatment plans should:

- Identify responsibilities, schedules, the expected outcome of treatments, budgets, performance measures and the review process to be set in place.
- Include mechanisms for assessing and monitoring treatment effectiveness against treatment objectives, individual responsibilities and organizational objectives, and processes for monitoring treatment plan progress against critical implementation milestones. This information should all arise from the treatment design process.
- Document how, practically, the chosen options will be implemented.

The successful implementation of the risk treatment plan requires an effective management system that specifies the methods chosen, assigns responsibilities and individual accountabilities for actions, and monitors them against specified criteria. Communication is a very important part of treatment plan implementation.

8.6 Residual risk

Residual risk is the risk that remains after treatment options have been identified and treatment plans have been implemented.

It is important that stakeholders and decision makers are aware of the nature and extent of the residual risk. The residual risk should therefore be documented and subjected to monitor and review.

9 Monitoring and review

AS/NZS 4360:2004

3.7 Monitor and review

Ongoing review is essential to ensure that the management plan remains relevant. Factors that may affect the likelihood and consequences of an outcome may change, as may the factors that affect the suitability or cost of the treatment options. It is therefore necessary to repeat the risk management cycle regularly.

Actual progress against risk treatment plans provide an important performance measure and should be incorporated into the organization's performance management, measurement and reporting system.

Monitoring and review also involves learning lessons from the risk management process, by reviewing events, the treatment plans and their outcomes.

Commentary

9.1 Purpose

Monitoring provides routine surveillance of actual performance for comparison with expected or required performance. Review involves periodic investigation of the current situation, usually with a specific focus.

Monitoring and review is an essential and integral part of managing risk, and is one of the most important steps of the risk management process organizationally. It is necessary to monitor risks, the effectiveness and appropriateness of the strategies and management systems set up to implement risk treatments and the risk management plan and system as a whole.

Assurance and monitoring processes should be continuous and dynamic. It is not sufficient to rely only on occasional, third party reviews and audits.

9.2 Changes in context and risks

Risk management processes should be embedded in organizational processes so risk management is dynamic and changes as the organization changes

Periodic reviews of risks and treatment strategies are particularly useful when they are associated with business and strategic plan development and change management.

When organizational changes are planned or external changes are detected there may be changes in:

- Organizational context (for example, objectives, the internal or external environment or risk criteria).
- Risks and levels of risk.
- The effectiveness of risk treatments.

Change may be sudden (acute) or gradual and persistent (chronic). Both can have high consequences so the risks should be identified and assessed and new treatment plans devised. The treatment may involve either an alteration to the change proposed or even its abandonment. Changes should not be implemented or imposed without regard to the risks involved.

9.3 Risk management assurance and monitoring

9.3.1 General

Systems to monitor and review risks and the risk management process require careful selection, targeting and planning as they absorb scarce resources. Priority should be given to monitoring:

(a) High risks.

(b) Credible failure of treatment strategies, especially where this would result in high, or frequent, consequences.

(c) Risk-related activities that feature high incidence of change.

(d) Risk tolerance criteria especially where this results in high levels of residual risk.

(e) Technological advances that may offer more effective or lower cost alternatives to current risk treatment.

In general terms, monitoring and review practices will be one of three types:

- Continuous (or at least frequent) monitoring through routinely measuring or checking particular parameters (for example pollution levels, or cash flows).
- Line management reviews of risks and their treatments (sometimes called 'control self assessments') which are often selective in scope but typically routine and regular and which should be selected on risk-weighted criteria.
- Auditing, using both internal and external audit staff. As far as possible these audits should test systems rather than conditions. They will be more selective in scope and lower frequency than the above measures. Absence of outstanding reported audit deficiencies does not, therefore equate to current assurance but does bring a measure of independent perspective.

Figure 9.1 illustrates these as a hierarchy with the regime at the top, if properly designed, providing the most powerful level of assurance. However, the monitoring and review program should include all three elements.

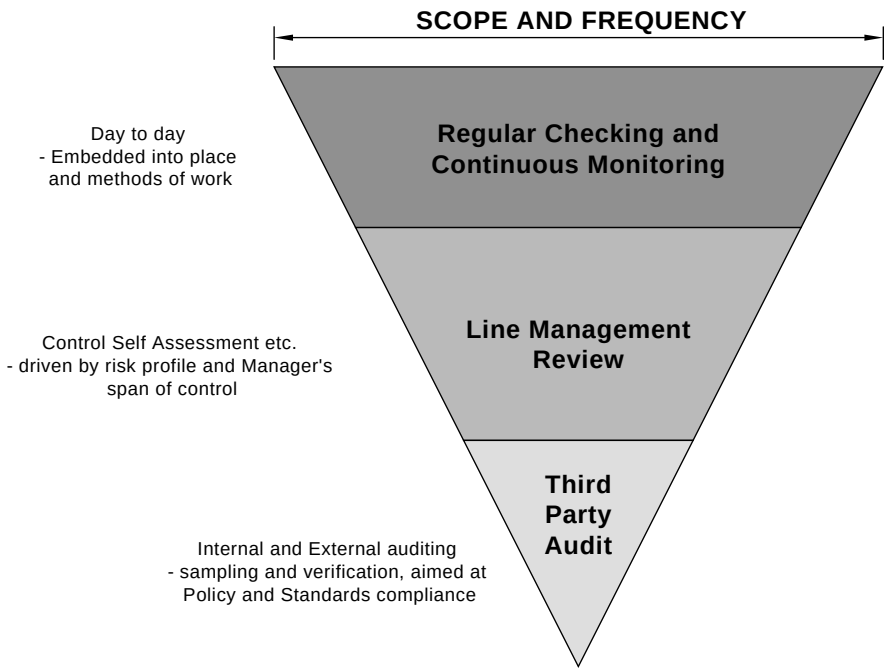


FIGURE 9.1 HIERARCHY OF ASSURANCE ACTIVITIES

9.3.2 Continuous monitoring

When risk treatments are established, an appropriate monitoring regime should be established to provide ongoing assurance that they are effective.

The risk register will normally contain a record of existing controls and treatments so should be consulted when establishing a monitoring regime. Priorities should take account of issues in Clause 9.2.

To help ensure that new risks are not created without appropriate assessment and treatment, the monitoring regime should also ensure that the risk register remains current.

It is useful to document the results of monitoring but it may be sufficient to simply document that the monitoring activity has occurred and has not produced any out-of-tolerance results.

9.3.3 Line management review

Periodically line management should review processes systems and activities to ensure that new risks have not arisen and treatment strategies are still effective and appropriate.

Consideration should be given to the options of sample review across a range of issues that are subject to continuous monitoring, or to undertaking short intensive reviews of a few specific areas.

Problems detected should be considered in the light of whether these are indicative of general weakness in the risk management systems. If so, a more comprehensive review may be initiated.

Through a mix of techniques, line managers should ensure that over time, all areas of their responsibility are considered.

9.3.4 Third party audit

Whether from internal or external sources, third party audits bring a measure of independence and perspective. They need not have prior notice or consent although generally they should be an anticipated and planned as a transparent part of the risk management assurance system.

Audits may focus on compliance with standards (internal or external), procedures or legislative requirements. Often they are risk based, concentrating on the effectiveness and appropriateness of treatment measures.

Audits are inevitably selective in scope so priorities for audit will take account of priorities listed in Clause 9.2.

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.

Findings of audits will usually indicate systemic weakness. Response to audits should be focused on remedying the system and not just the symptoms.

9.4 Risk management performance measurement

Performance indicators (PIs) are quantitative measures of the level of performance of a given item or activity. They need to be measurable and appropriate to individual business units and hold individuals accountable while forming the basis for continuing improvement.

Organizations should use their normal organizational planning processes to generate performance measures for the risk management system and processes

The performance indicators should reflect the range of key organizational objectives defined when the context was established at the start of the process.

Performance indicators may monitor outcomes (for example, specific losses or gains) or processes (for example, consistent performance of risk treatment procedures).

Normally a blend of indicators is used but outcome performance indicators usually significantly lag the changes that give rise to them so in a dynamic environment process indicators are likely to be more useful.

Performance indicators should reflect the relative importance of risk management actions, with the greatest effort and focus applied to:

- The highest risks.
- The most critical treatments or other processes.
- Those treatments or processes with the greatest potential for improvements in efficiency.

In choosing performance indicators, it is important to check that:

- They are reasonably able to be measured.
- They are efficient in terms of demands on time, effort and resource.
- The measuring process/surveillance encourages or facilitates desirable behaviours and does not motivate undesirable behaviours (such as fabrication of data).
- Those involved understand the process and expected benefits and have the opportunity to input to the procedure.
- The results are captured and reported in a form that will facilitate learning and improvement.

Some examples of useful risk management performance indicators are:

- Decline in total cost of risk.
- Progress towards a specific organizational objective.
- The extent to which recommendations for risk treatment are implemented.

To ensure that risk management performance indicators reflect the range of key organizational drivers, some organizations incorporate performance indicators in the balanced scorecards of staff and managers so that, for example, financial, stakeholder, internal efficiency and learning and growth objectives are considered. The Kaplan and Norton (2000) methodology is one way of applying the balanced scorecard approach.

Watch points concerning performance indicators:

- Effective measurement of performance requires resources. These should be identified and allocated as part of the development of the performance indicators.
- Some risk management activities may be difficult to measure. This does not make them less important but it may be necessary to use surrogate indicators. For example, resources devoted to risk management activities, may be a surrogate measure of commitment to risk management.
- Any variance between performance indicators measurement data and instinctive ‘feel’ is important and should be investigated (e.g. if despite numerous risk assessments indicating low residual risk, management remain worried).
- While sudden deterioration in indicators will usually attract attention, progressive deterioration can be equally problematic and trends in performance indicators should be monitored and analysed.

9.5 Post-event analysis

Incidents, accidents and successes provide a useful occasion to monitor and review risks and treatments and to gain insight on how the risk management process can be improved. The intention should be to adopt a systematic process to review causes of successes, failures and near misses to learn useful lessons for the organization. Ideally a systematic analysis process would be used.

When successes and failures are analysed, the questions to we answered are:

- Did we previously identify and analyse the risks involved?
- Did we identify the actual causes in risk identification?
- Did we rate and assess risks and controls correctly?
- Did the controls operate as intended?
- Were the treatment plans effective? If not, where could improvements be made?
- Were our monitoring and review processes effective?
- How could our risk management process in general be improved?
- Who needs to know about these learnings and how should be disseminate these learnings to ensure that learning was most effective?
- What do we need to do to ensure that failure events are not repeated but that successes are?

This page has been left blank intentionally

10 Recording the risk management process

AS/NZS 4360:2004

3.8 Record the risk management process

Each stage of the risk management process should be recorded appropriately. Assumptions, methods, data sources, analyses, results and reasons for decisions should all be recorded.

The records of such processes are an important aspect of good corporate governance.

Decisions concerning the making and capture of records should take into account—

- the legal and business needs for records;
- the cost of creating and maintaining records; and
- the benefits of re-using information.

(Refer AS ISO 15489)

Commentary

10.1 Overview

Documenting each step of the risk management process is important:

(a) to demonstrate to stakeholders that the process has been conducted properly;

(b) to provide evidence of a systematic approach to risk identification and analysis;

(c) to enable decisions or processes to be reviewed;

(d) to provide a record of risks and to develop the organization's knowledge database;

(e) to provide decision makers with a risk management plan for approval and subsequent implementation;

(f) to provide an accountability mechanism and tool;

(g) to facilitate continuing monitoring and review;

(h) to provide an audit trail; and

(i) to share and communicate information.

In some circumstances, an appropriate level and standard of documentation may be needed to satisfy an independent audit.

Whatever the reasons for documenting the process, risk management need not impose another layer of paperwork if a sensible approach is taken. Subject to legislative requirements, decisions and processes involving risk management should be documented to the extent appropriate to the circumstances.

Decisions concerning the extent of documentation may involve costs and benefits and should take into account the reasons for documenting the process. Thus, a process that is of low consequence may be documented only by a diary note or a brief record on file. On the other hand a redesign of a major client service delivery operation might require a detailed explanation of the process for audit and review. There is a range between these extremes, and prudent practical judgement is needed to decide the level of documentation in particular circumstances.

At each stage of the process, documentation should include—

(i) the objectives of the stage;

(ii) the information sources on which the outcomes were based;

(iii) all major assumptions made in the process;

(iv) who was involved; and

(v) the decisions that were agreed.

10.2 Compliance and due diligence statement

In some circumstances a compliance and due diligence statement may be required, so that managers formally acknowledge their responsibility to comply with risk management policies and procedures.

Often documentation of the risk management process is required to show compliance with a regulatory process (e.g. major hazard 'safety cases') or to show due diligence.

10.3 Risk register

For each risk identified, a risk register records—

(a) a description of the risk, its causes and its impacts;

(b) an outline of the existing controls;

(c) an assessment of the consequences of the risk should it occur and the likelihood of the consequence occurring, given the controls;

(d) a risk rating; and

(e) an overall priority for the risk.

Refer to the sample proforma in Tables 10.1 and 10.2 as a guide.

10.4 Risk treatment schedule and action plan

A risk treatment schedule and action plan documents the new management actions and controls to be adopted. It usually lists the following information:

(a) The actions to be taken and the risks they address.

(b) Who has responsibility for implementing the plan.

(c) What resources are to be utilized.

(d) The budget allocation.

(e) The timetable for implementation.

(f) Details of the mechanism and frequency of review of with the status of the treatment plan.

Table 10.3 provides a sample proforma for a risk treatment schedule. Table 10.4 shows a possible structure for a simple risk treatment plan. Plans for high risk areas may need to be more specific and detailed.

10.5 Monitoring and audit documents

Monitoring and audit records should document:

(a) Details of the mechanism and frequency of review of risks and the risk management process as a whole.

(b) The outcomes of audits and other monitoring procedures.

(c) Details of how previous review recommendations have been followed up and implemented.

10.6 Incident data base

Much can be learned from incidents which also provide an indication of the success of risk management efforts. It is useful to develop a database of incidents with both details of the incident and surrounding issues which may later allow detection of patterns or analysis of causal sequences which can provide input to the design or evaluation of risk control measures. As well as being able to be interrogated by those responsible for risk-related decisions, it is useful if the database can also automatically identify data sets of interest and communicate these automatically to relevant persons with risk management responsibilities (e.g. occurrence frequency for particular types of incident that exceed threshold criteria).

10.7 Risk Management Plan

The Risk Management Plan provides a high-level view of risk management within the organization and how it is embedded in the organization's activities. It is neither appropriate nor practical to include in it a mass of detail about particular functional areas of the organization nor specific business activities, particularly if they may change through time.

The Risk Management Plan may contain:

(a) A statement of the organization's risk management policy.

(b) A description of the external and internal context, arrangements for corporate governance and supervision, and the environment in which the organization operates.

(c) Details of the scope and objectives of the risk management activities in the organization, including organizational criteria for assessing whether risks are tolerable.

(d) Risk management responsibilities and functions in the organization.

(e) The list of risks identified and an analysis of them, usually in the form of a risk register included as an appendix.

(f) Summaries of the risk treatment plans for major risks, incorporated as an Appendix or by reference to a treatment schedule like Table 10.3 or some other status document.

TABLE 10.1
Risk register example

Function/Activity:		Compiled by:		Date:	
Date of risk review:		Reviewed by:		Date:	

Reference	The risk	What can happen? (event)	How can it happen?	What can happen? (consequ-ences)	Identify existing controls	Effectiveness and implementation of existing controls	Analysis			Risk priority	Treat risk Y/N	Further action
							Likelihood	Consequences	Level of risk			

NOTE:Indicative example only.

TABLE 10.2
Risk register

Function/Activity:		Compiled by:		Date:	
Date of risk review:		Reviewed by:		Date:	

Reference	The risk: what can happen and how it can happen	The consequences of an event happening		Adequacy of existing controls	Consequence rating	Likelihood rating	Level of risk	Risk priority
		Consequence	Likelihood					

NOTE:Indicative example only.

TABLE 10.3
Risk treatment schedule plan example

Function/Activity:		Compiled by:		Date:	
Date of risk review:		Reviewed by:		Date:	

Risk (in priority order from the risk register)	Possible treatment options	Preferred options	Result of cost-benefit analysis A: accept B: reject	Person responsible for implementation of option	Timetable for implementation	How will this risk and the treatment be monitored?

NOTE: Indicative example only.

TABLE 10.4
Risk treatment plan example

Function/Activity:			
Risk:		Ref:	
Summary: Recommended response and impact			
Action plan 1. Proposed actions			
2. Resource requirement			
3. Responsibility			
4. Timing			
5. Reporting and monitoring required			
Compiled By:	Date:	Reviewed by:	Date:

NOTE: This table is indicative only.

11 Establishing effective risk management

AS/NZS 4360:2004

4.1 Purpose

The purpose of this Section is to describe how to develop, establish and sustain systematic risk management in an organization.

An organization should develop a risk management policy, plan and support arrangements. This will enable risk management to be implemented effectively throughout the organization. The plan should address strategies for embedding risk management in the organization's systems, processes and practices.

While the detailed approach described here is designed for larger organizations, all the aspects are relevant to some degree to smaller entities. The same principles apply in the public, not-for-profit and private sectors.

4.2 Evaluate existing practices and needs

In many organizations existing management practices and processes include elements of risk management. Some organizations may have adopted risk management processes for particular categories of risk.

Before starting to develop a risk management plan, the organization should critically review and assess those elements of the risk management process that are already in place. This review should reflect the risk management needs of the organization and its context.

The review should deliver a structured appreciation of:

- the maturity, characteristics and effectiveness of existing business and risk management culture and systems;
- the degree of integration and consistency of risk management across the organization and across different types of risks;
- the processes and systems that should be modified or extended;
- constraints that might limit the introduction of systematic risk management;
- legislative or compliance requirements; and
- resource constraints.

4.3 Risk management planning

4.3.1 Develop risk management plans

The risk management plan should define how risk management is to be conducted throughout the organization. Risk treatment plans may be separate or included in the risk management plan.

The aim of the risk management plan should be to embed risk management in all the organization's important practices and business processes so that it is relevant, effective, efficient and sustained. In particular, risk management should be embedded into the policy development, business and strategic planning and change management processes. It is also likely to be embedded in other plans and processes such as those for asset management, audit, business continuity, environmental management, fraud control, human resources, investment and project management.

The risk management plan may include specific sections for particular functions, areas, projects, activities or processes. In practice, these sections may be separate plans; these should be consistent with the organization's risk management policy.

4.3.2 Ensure the support of senior management

An awareness of and commitment to risk management at senior management levels is important. This may be achieved by:

- obtaining the active, ongoing support of the organization's directors and senior executives for risk management and for the development and implementation of the risk management policy and plan;
- appointing a senior manager or similar 'champion' (or team) to lead and sponsor initiatives; and
- obtaining the commitment and support of all senior managers for the execution of the risk management plan.

4.3.3 Develop and communicate the risk management policy

The organization's board or executive should define and document its policy for managing risk, including the objectives for and its commitment to risk management. The policy may include:

- the objectives and rationale for managing risk;
- the links between the policy and the organization's strategic plans;
- the extent and types of risk the organization will take and the ways it will balance threats and opportunities;
- the processes to be used to manage risk;
- accountabilities for managing particular risks;
- details of the support and expertise available to assist those accountable for managing risks;

- a statement on how risk management performance will be measured and reported;
- a commitment to the periodic review of the risk management system; and
- a statement of commitment to the policy by directors and the organization's executive.

Publishing and communicating a policy statement of this type demonstrates the commitment of the organization's executive to risk management. Communication may include:

- establishing a team, including senior managers, responsible for communicating about managing risk and about the organization's policy; and
- raising awareness about managing risks and the risk management process throughout the organization.

4.3.4 Establish accountability and authority

The directors and senior executives are ultimately responsible for managing risk in the organization. All personnel are responsible for managing risks in their areas of control. This may be facilitated by:

- specifying those accountable for the management of particular risks or categories of risk, for implementing treatment strategies and for the maintenance of risk controls;
- establishing performance measurement and reporting processes; and
- ensuring appropriate levels of recognition, reward, approval and sanction.

4.3.5 Customize the risk management process

The risk management process should be customized for the organization, its policies, procedures and culture taking into account the review process described in Clause 4.2.

4.3.6 Ensure adequate resources

The organization should identify resource requirements for risk management. This should include consideration of:

- people and skills;
- documented processes and procedures;
- information systems and databases; and
- money and other resources for specific risk treatment activities.

The risk management plan should specify how the risk management skills of managers and staff will be developed and maintained.

Risk management information systems may possess the capability to:

- record details of risks, controls and priorities and show any changes in them;
- record risk treatments and associated resource requirements;

- record details of incidents and loss events and the lessons learned;
- track accountability for risks, controls and treatments;
- track progress and record the completion of risk treatment actions;
- allow progress against the risk management plan to be measured; and
- trigger monitoring and assurance activity.

Commentary

11.1 Policy

Management of risk should be integrated into the management philosophy of an organization. It is necessary for the Board or senior executives to take ownership for setting the risk management policy. The policy is a brief, high level document; approving a risk management approach as well as creating linkages with other corporate strategies. It should be incorporated as part of an organization's management policies.

Examples of information that may be included in an organization's policy statement include—

(a) the objectives and rationale for managing risk;

(b) the links between the policy and the organization's strategic and corporate plans;

(c) the extent or range of risks that need to be managed;

(d) guidance on what may be regarded as acceptable risk;

(e) who is responsible for managing risks;

(f) the support and expertise available to assist those responsible for managing risks;

(g) the level of documentation required; and

(h) the requirements for monitoring and reviewing organizational performance in regard to the policy.

11.2 Management commitment

Implementing effective risk management programmes at all levels is difficult. Its success will largely depend on the support and sponsorship of the top manager and senior executive team.

Managing risk effectively needs to become part of every organization's philosophy, goals and accepted practices. It should be integral to organizations' business plans and training programmes.

As with any introduction of a new business initiative at an organizational level, effective change management will be needed in the coordination of plans and activities across the organization. Involvement of staff from operational areas in the process is vital for achieving coordination and laying the foundation for effective risk management.

It is possible for the prevailing organizational culture to act as a disincentive to managing risk. Senior managers should approach the implementation of risk management as an opportunity for beneficial cultural change. This culture change should influence managers and supervisors to encourage appropriate risk

management behaviour in their staff and for all staff to accept the challenge of managing their risks.

Effective leadership can shape culture by encouraging the application of risk management through organizational recognition and reward systems.

11.3 Responsibility and authority

There should be clear and designated accountability for—

(a) integration of risk management with organizational processes and ensuring there is an appropriate culture;

(b) managing and administering the risk management process within the organizational framework; and

(c) managing specific identified threats and opportunities and undertaking treatment actions.

Treatments may be managed by persons external to your organization.

11.4 Resources and infrastructure

The risk management plan defines the level of resources and associated infrastructure for the effective management of risks. Provision of these resources will be included as part of the Board and or senior management approval.

Resources and infrastructure are required for the following:

(a) providing support and expertise to those responsible for managing risks, including where necessary external suppliers;

(b) acquiring the knowledge and skills needed to manage risk;

(c) incorporating risk management training into internal staff development programmes;

(d) integrating risk management principles to existing procedures and practices;

(e) communication and dialogue throughout the organization about managing risk and about the organization's philosophy;

(f) ensuring that systems for staff rewards, recognition and sanctions include risk management;

(g) ensuring that internal review and evaluation programmes such as internal audit take account of the organization's philosophy towards managing risk when evaluating performance;

(h) incorporating risk management issues into business planning; and

(i) co-ordinating the interface between risk management and quality assurance.

11.5 Culture change

The process required to establish effective risk management as a part of day-to-day business at an organizational level and subsequently at operational, project or team levels is likely to require a change of culture for many organizations.

Activities that will support a cultural change include:

(a) Securing the support of senior management.

(b) Developing a risk management philosophy and an awareness of risk at all senior management levels. This could be facilitated by training, education and briefing of executive management and by examining how risks have been managed in the past.

(c) Success stories should be developed and 'sold'.

(d) An endorsed person (or team) at a senior level may be appointed to sponsor or 'champion' the initiative.

(e) Managers need to encourage and support staff to manage risks. Failure to manage risks may result in lost opportunities or pose threats to staff and the objectives of the organization.

11.6 Monitor and review risk management effectiveness

Senior management should ensure that risk management aligns well with the organization's critical performance measures.

This may lead to a number of questions relevant to the risk management approach:

(a) Are the organization's objectives valid and measurable?

(b) Is the risk management approach consistent with the organization's objectives and context?

(c) Are risk management reports being taken note of and used in the organization's decision making processes?

These questions and many others are part of the iterative process of management, with management approaches being continually developed to meet business strategies and programs of work.

Managing risk provides opportunities for managers and staff at every level to continuously improve performance. It contributes to improved performance by—

(i) providing a structured approach to decision-making;

(ii) encouraging analysis of a broader range of options than might otherwise be possible;

(iii) promoting the identification of new opportunities;

(iv) providing an enhanced focus on outcomes;

(v) reviewing the 'tried and true ways' of doing things and identifying ways to simplify processes; and

(vi) supporting more effective, efficient and appropriate use of resources.

Improvements must be able to be measured so that they become tangible and can be communicated to all interested parties

11.7 The challenge for leaders—Integration

Risk management will be more efficient and effective if it is integrated with other management activities.

Further efficiencies will be gained by integrating risk management activities for different types of risk that are closely related or different types of risk management activity that concern the same risk. For example:

(a) The risks of harm to people, property and the environment all involve personal behaviour and the physical environment, there are therefore substantial overlaps in the controls needed to manage these risks.

(b) Business continuity plans and business interruption insurance both help manage the risk of business disruption. Integration of these activities is likely to reduce cost.

Traditionally, some types of risk management activities have taken place without having been recognized as 'risk management', with the consequence in some cases, that the rigour of the risk management process is not applied to that activity. For example:

(i) Business Continuity Management may not be integrated with the AS/NZS 4360:2004 framework.

(ii) The experience gained in managing the risk of inadequate quality (i.e. quality assurance) has not been fully utilized to assist in improving management of other risks.

Different skills may be required for these activities, but a whole of risk approach is still desirable. It is important that there is cross representation and communication if different departments or individuals are involved.

11.8 The challenge for managers—Leadership

The challenge for managers is to support and encourage prudent risk management by—

(a) playing an active part, and not simply mandating production of reports;

(b) empowering subordinates and staff to manage risks effectively;

(c) acknowledging, rewarding and publicizing good risk management;

(d) having processes that promote learning from errors, rather than punishing;

(e) encouraging discussion and analysis of unexpected results, both positive and negative; and

(f) not over-responding to problems by introducing restrictive or blanket controls.

11.9 The challenge for all—Continuous improvement

AS/NZS 4360:2004 describes a process that will naturally lead to continuous improvement in an organization's risk management. It follows that the more consistently that the process is applied, and the greater maturity of risk management practice, the greater the benefits described in Clause 1.2.

11.10 Key messages and questions for managers

Managers must consistently signal that—

(a) risk management is everyone's business;

(b) risk management is part of business as usual, not an add on or additional burden; and

(c) the process for managing risk is logical and systematic and should become a natural practice.

Key messages include:

(i) There are risks to be managed in all activities.

(ii) Everyone is responsible and accountable for managing the risks in their activities.

(iii) People should be encouraged and supported by their leaders to manage risks.

(iv) AS/NZS 4360:2004 provides a framework or systematic approach for making decisions about how best to manage risks.

(v) Legislative requirements and the political, social and economic environment need to be considered when managing risks.

(vi) Action taken to manage risks should be integrated with (not be separate from) existing planning and operational processes at all levels.

(vii) Effective risk management relies on quality information.

Key questions managers should ask include:

(1) Are the risk management programme objectives aligned with organizational performance objectives and values?

(2) Are the risk management programme outcomes measurable in these terms?

(3) Can you determine if the risk management programme has generated value for the organization?

(4) Would you make a decision to expand or contract the risk management programme based on this information?

(5) Does the risk management programme reflect the realities of the environment in which you operate?

(6) Can you report information concisely and clearly for evaluation by senior management and Board (where appropriate)?

12 References

12.1 Standards and Handbooks

AS 8000, *Corporate governance—Good governance principles*, Standard Australia.

AS 8001, *Corporate governance—Fraud and corruption control*, Standards Australia.

AS 8002, *Corporate governance—Organizational codes of conduct*, Standards Australia.

AS 8003, *Corporate governance—Corporate social responsibility*, Standards Australia.

AS 8004, *Corporate governance—Whistleblower protection programs for entities*, Standards Australia.

AS/NZS 3931, *Risk analysis of technological systems—Application guide,* Standards Australia/Standards New Zealand.

AS/NZS 4360, *Risk management*, Standards Australia/Standards New Zealand.

HB 141, *Risk financing guidelines*, Standards Australia.

A1

HB 203, *Environmental risk management—Principles and process*, Standards Australia/Standards New Zealand.

HB 221, *Business continuity management*, Standards Australia/Standards New Zealand.

HB 228, *Guidelines for managing risk in the healthcare sector*, Standards Australia/Standards New Zealand.

HB 231, *Information security risk management guidelines*, Standards Australia/Standards New Zealand.

HB 240, *Guidelines for managing risk in outsourcing utilizing the AS/NZS 4360 process,* Standards Australia/Standards New Zealand.

HB 254*, Guide to control assurance and risk management*. Standards Australia.

HB 400, *Introduction to Corporate Governance*, Standards Australia.

HB 401, *Applications of Corporate Governance*. Standards Australia.

HB 402, *Business planning*. Standards Australia.

HB 403, *Best Practice Board Reporting*, Standards Australia.

HB 405, *Disclosure and Transparency Frameworks*. Standards Australia.

CAN/CSA-Q 850-1997, *Risk Management: Guideline for Decision-Makers*, Canadian Standards Association, ISSN 0317-5669.

JIS Q 2001, *Guidelines for development and implementation of risk management system*, Japanese Standards Association July 2001.

99/402 000DC, *Draft Guide to the Management of Business Related Project Risks*, British Standards Institute.

12.2 Further reading

BERNSTEIN, P.L. *Against the Gods: The Remarkable Story of Risk'.* ISBN 0 471 12104 5.

CHAPMAN, C.B. and Ward, S.C. (1997) *Project Risk Management: Processes, Techniques and Insight*s, John Wiley & Sons, Chichester. ISBN 0 471 95804 2.

COOPER, D.F. GREY, S.J., RAYMOND G.A. and WALKER P.R. (2004) *Project Risk Management Guidelines: Managing Risk in Large Projects and Complex Procurements*. John Wiley & Sons Chichester.

Emergency Risk Management—Applications Guide, Emergency Management Australia, 2000.

Environmental Protection Agency (1998) 'Guidelines for Ecological Risk Assessment', Risk Assessment Forum, US EPA, Washington, DC, EPA/630/R-95/002F.
(See www.epa.gov/ncea/ecorsk.htm.).

Financial Reporting of Risk - Proposals for a Statement of Business Risk. Institute of Chartered Accountants in England & Wales 1998.

GREY, S. (1995) *Practical Risk Assessment for Project Management*, John Wiley & Sons, Chichester.
ISBN 0 471 93979 X.

Department of Finance (1991), *Handbook of cost benefit analysis,* Australian Government Publishing Service.

KAPLAN and NORTON (2000) *Having trouble with strategy? Then map it,* Harvard Business Review, Vol. 78, No. 5, September-October 2000.

Learning about Risk: Choices, Connections and Competencies (July 1998) Canadian Institute of Chartered Accountants

New South Wales Government (1993) *Risk Management Guidelines*, Public Works Department, Policy Division, Sydney, NSW. ISBN 0 7310 2704 3.

New South Wales Government (1999) *Multi-Level Risk Assessment*, Department of Urban Affairs and Planning, Sydney, NSW: Revised Edition. ISBN 0 7347 0062 8.

A1

Reducing Risk, Protecting People, HSE's decision making process The Health and Safety Executive (HSE) 2001.
ISBN 0 7176 2151 0.

ROWE, A.J., MASON, R.O., DICKEL, K.E., and SNYDER, N.H., (1989) *Strategic Management: A Methodological Approach*, Third Edition, Addison-Wesley, Reading, MA.

The Royal Society of London (1992) *Risk: Analysis, perception and management*. The Royal Society, London.

TWEEDDALE, H.M. (2003) *Managing Risk and Reliability of Process Plants*. Gulf Professional Publishing Amsterdam. ISBN 0756677341.

VOSE, D. (2000) *Risk Analysis: A Quantitative Guide*, John Wiley & Sons, Chichester. ISBN 0 471 99765 X.

AMENDMENT CONTROL SHEET

HB 436:2004

Amendment No. 1 (2005)

CORRECTION

SUMMARY: This Amendment applies to the Clauses 6.1.7, 6.3, 6.5, 12.1, 12.2 and Table 6.3.

Published on 20 December 2005.

NOTES

NOTES

NOTES

ISBN 0-7337-5960-2