AS/NZS 4360:2004

Australian/New Zealand Standard®

RISK MANAGEMENT

STANDARDS AUSTRALIA

STANDARDS NEW ZEALAND
Paerewa Aotearoa

Risk management

AS/NZS 4360:2004

STANDARDS AUSTRALIA

STANDARDS NEW ZEALAND

This Joint Australian/New Zealand Standard was prepared by Joint Technical Committee OB-007, Risk Management. It was approved on behalf of the Council of Standards Australia on 21 July 2004 and on behalf of the Council of Standards New Zealand on 20 August 2004.
This Standard was published on 31 August 2004.

The following are represented on Committee OB-007:

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

This Standard was issued in draft form for comment as DR 03360.

Originated as AS/NZS 4360:1995.
Second edition 1999.
Third edition 2004

Keeping Standards up-to-date

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 Standards may also be withdrawn.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

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

Alternatively, both organizations publish an annual printed Catalogue with full details of all current Standards. For more frequent listings or notification of revisions, amendments and withdrawals, Standards Australia and Standards New Zealand offer a number of update options. For information about these services, users should contact their respective national Standards organization.

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

ISBN 0 7337 5904 1

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

Preface

This Standard was prepared by the Joint Standards Australia/ Standards New Zealand Committee OB-007, Risk Management as a revision of AS/NZS 4360:1999, *Risk management*. It provides a generic framework for establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risk.

This revised Standard incorporates the insights gained through the application of the 1999 edition, and current thinking on risk management.

Some of the changes from the 1999 edition include—

- greater emphasis on the importance of embedding risk management practices in the organization's culture and processes;
- greater emphasis on the management of potential gains as well as potential losses; and
- moving and expanding indicative examples into a new handbook.

HB 436, *Risk Management Guidelines—Companion to AS/NZS 4360:2004* contains specific guidance on the implementation of the Standard. The two documents are intended to be used together.

In addition, Standards Australia and Standards New Zealand have published a range of handbooks on the way the risk management process can be applied in a variety of sectors and a range of subject areas.

Contents

Foreword

Risk management involves managing to achieve an appropriate balance between realizing opportunities for gains while minimizing losses. It is an integral part of good management practice and an essential element of good corporate governance. It is an iterative process consisting of steps that, when undertaken in sequence, enable continuous improvement in decision-making and facilitate continuous improvement in performance.

Risk management involves establishing an appropriate infrastructure and culture and applying a logical and systematic method of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risks associated with any activity, function or process in a way that will enable organizations to minimize losses and maximize gains.

To be most effective, risk management should become part of an organization's culture. It should be embedded into the organization's philosophy, practices and business processes rather than be viewed or practiced as a separate activity. When this is achieved, everyone in the organization becomes involved in the management of risk.

Although the concept of risk is often interpreted in terms of hazards or negative impacts, this Standard is concerned with risk as exposure to the consequences of uncertainty, or potential deviations from what is planned or expected. The process described here applies to the management of both potential gains and potential losses.

Organizations that manage risk effectively and efficiently are more likely to achieve their objectives and do so at lower overall cost.

This page has been left blank intentionally

1 Scope and general

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*

2 Risk management process overview

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.

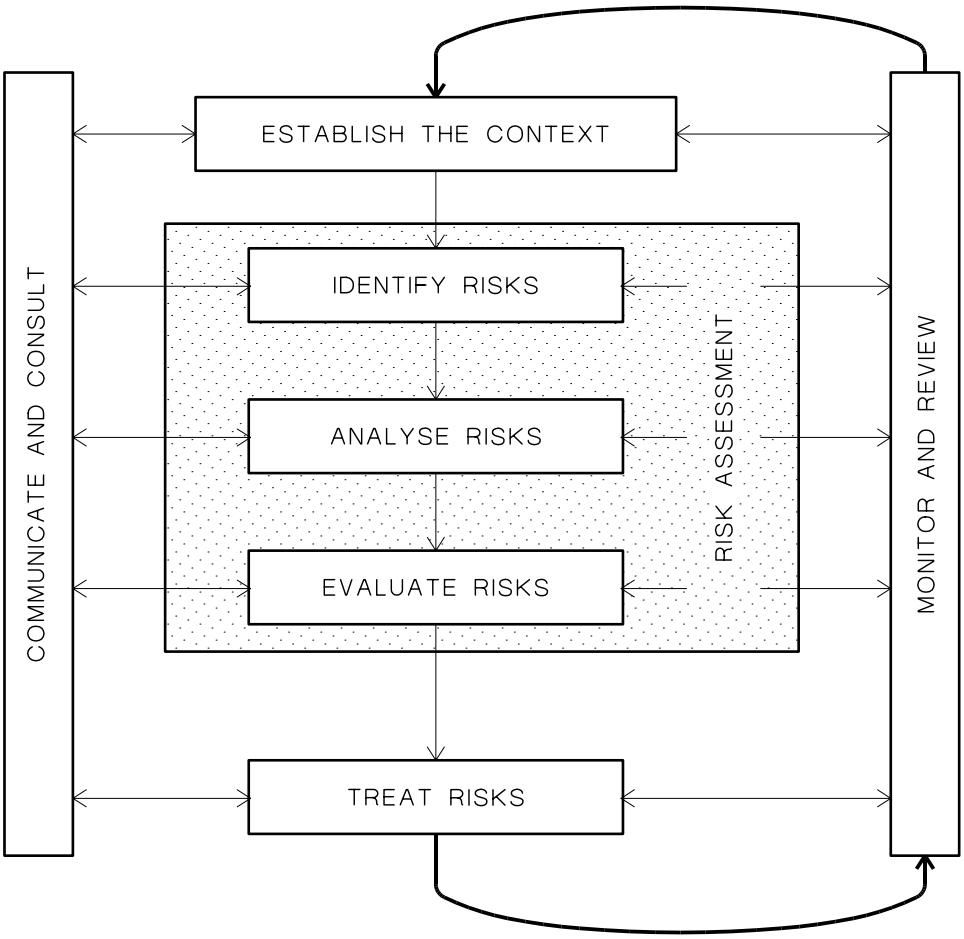

FIGURE 2.1 RISK MANAGEMENT PROCESS – OVERVIEW

This page has been left blank intentionally

3 Risk management process

The details of the risk management process are shown in Figure 3.1.

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.

3.2 Establish the context

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.

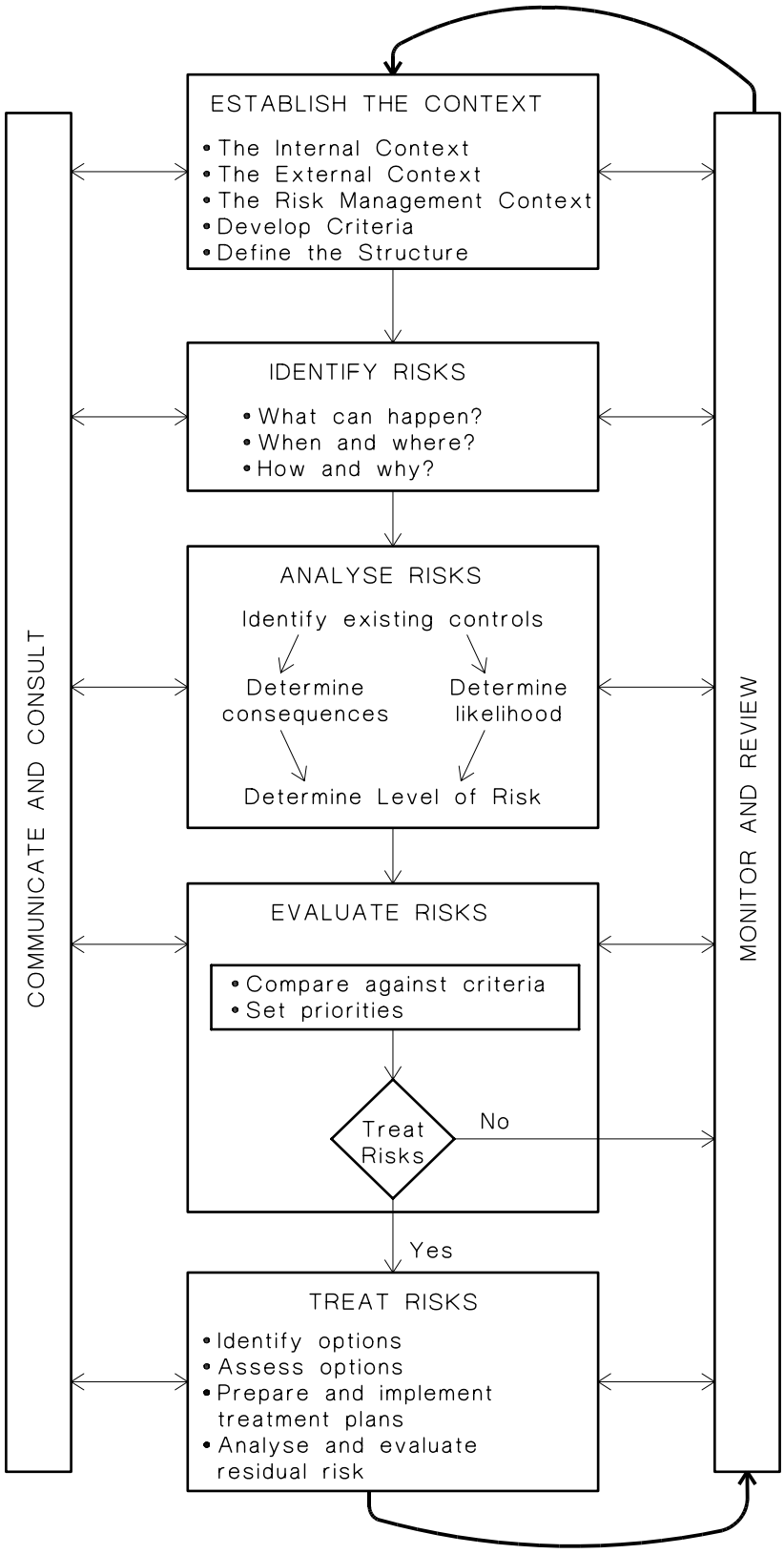

FIGURE 3.1 RISK MANAGEMENT PROCESS – IN DETAIL

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.

3.3 Identify risks

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.

3.4 Analyse risks

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.

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.

3.6 Treat risks

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.

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.

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)

This page has been left blank intentionally

4 Establishing effective risk management

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.

NOTES

NOTES

ISBN 0-7337-5904-1