AS/NZS 4360:1999

Australian/New Zealand Standard™

Risk management

Standards Australia

STANDARDS NEW ZEALAND
Paerewa Aotearoa

Risk Management

AS/NZS 4360:1999

STANDARDS AUSTRALIA

STANDARDS
NEW ZEALAND
Paerewa Aotearoa

This Joint Australian/New Zealand Standard was prepared by Joint Technical Committee OB/7 – Risk Management. It was approved on behalf of the Council of Standards Australia on 2 April 1999 and on behalf of the Council of Standards New Zealand on 22 March 1999. It was published on 12 April 1999.

The following interests are represented on the Committee OB/7:

Australian Computer Society
Australian Customs Service
Australian Institute of Risk Management
Department of Administrative Services, Australia
Department of Defence, Australia
Environmental Risk Management Authority, New Zealand
Institution of Engineers, Australia
Institution of Professional Engineers, New Zealand
Insurance Council of Australia
Insurance Institute of New Zealand
Ministry of Agriculture and Forestries, New Zealand
Ministry of Commerce, New Zealand
Ministry of Emergency Management and Civil Defence, New Zealand
Local Government New Zealand
N.S.W. Department of Urban Affairs and Planning
N.S.W. Treasury Managed Fund
National Insurance Brokers Association of Australia
Securities Institute of Australia
The Association of Risk and Insurance Managers of Australasia
University of New South Wales

This Standard was issued in draft form for comment as DR 98549.

First published as AS/NZS 4360:1995.
Revised AS/NZS 4360:1999.

Review of Australian Standards

To keep abreast of progress in industry, Australian Standards are subject to periodic review and are kept up-to-date by the issue of amendments or new editions as necessary. It is important therefore that Standards users ensure that they are in possession of the latest edition, and any amendments thereto.

Full details of all Australian Standards and related publications will be found in the Standards Australia Catalogue of Publications; this information is supplemented each month by the magazine *The Australian Standard*, which subscribing members receive, and which gives details of new publications, new editions and amendments, and of withdrawn Standards.

Suggestions for improvements to Australian Standards, addressed to the head office of Standards Australia, are welcomed. Notification of any inaccuracy or ambiguity found in an Australian Standard should be made without delay in order that the matter may be investigated and appropriate action taken.

ISBN 0 7337 2647 X

Published by Standards Association of Australia, PO Box 1055, Strathfield NSW 2135

Preface

This Joint Standard was prepared by the Joint Standards Australia/ Standards New Zealand Committee OB/7 on Risk Management as a revision of AS/NZS 4360:1995 *Risk management*. Accordingly it retains the objective of providing a generic framework for establishing the context, identification, analysis, evaluation, treatment, monitoring and communication of risk. It should be read in conjunction with other applicable or relevant Standards.

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.

Risk management is an iterative process consisting of well-defined steps which, taken in sequence, support better decision-making by contributing a greater insight into risks and their impacts. The risk management process can be applied to any situation where an undesired or unexpected outcome could be significant or where opportunities are identified. Decision makers need to know about possible outcomes and take steps to control their impact.

Risk management is recognized as an integral part of good management practice. To be most effective, risk management should become part of an organization's culture. It should be integrated into the organization's philosophy, practices and business plans rather than be viewed or practiced as a separate program. When this is achieved, risk management becomes the business of everyone in the organization.

If for any reason it is not possible to integrate risk management across an entire organization, it may still be possible to apply it successfully to individual departments, processes or projects.

The terminology used in this Standard has been chosen to be acceptable across as wide a range of risks and risk management disciplines as possible. Words which have slightly different meanings in different branches of risk management have been avoided and replaced by words which might be less commonly used in current practice but which could be defined to have a precisely common meaning. An example is the term risk treatment which is defined to cover more than is usually meant by the term 'risk control'.

AS/NZS 3931 *Risk analysis of technological systems—Application guide*, (which is identical with IEC 60300-3-9:1995, Dependability Management, Part 3: Application guide, Section 9: Risk analysis of

technological systems) defines the risk management process as starting at risk analysis without the first two steps of establishing the context and identifying risks. This definition of the risk management process was not followed in this Standard because it was not sufficiently generic to risk management, as practiced across all disciplines, and did not allow sufficient weight to be given to the initial steps necessary to establish management of all risks.

The term 'informative' has been used in this Standard to define the application of the appendix to which it applies. An 'informative' appendix is only for information and guidance.

Contents

This page has been left blank

1 Scope, application and definitions

1.1 Scope

This Standard provides a generic guide for the establishment and implementation of the risk management process involving establishing the context and the identification, analysis, evaluation, treatment, communication and ongoing monitoring of risks.

1.2 Application

Risk management is recognized as an integral part of good management practice. It is an iterative process consisting of steps, which, when undertaken in sequence, enable continual improvement in decision-making.

Risk management is the term applied to a logical and systematic method of establishing the context, identifying, analyzing, 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 opportunities. Risk management is as much about identifying opportunities as avoiding or mitigating losses.

This Standard may 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 differing studies are carried out at different stages of a project.

NOTE: This Standard may be applied to a very wide range of activities or operations of any public, private or community enterprise, or group. Examples are given in Appendix A.

1.3 Definitions

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

1.3.1 Consequence
the outcome of an event expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event.

1.3.2 Cost
of activities, both direct and indirect, involving any negative impact, including money, time, labour, disruption, goodwill, political and intangible losses.

1.3.3 Event
an incident or situation, which occurs in a particular place during a particular interval of time.

1.3.4 Event tree analysis
a technique which describes the possible range and sequence of the outcomes which may arise from an initiating event.

1.3.5 Failure mode and effects analysis (FMEA)
a procedure by which potential failure modes in a technical system are analysed. An FMEA can be extended to perform what is called failure modes, effects and criticality analysis (FMECA). In a FMECA, each failure mode identified is ranked according to the combined influence of its likelihood of occurrence and the severity of its consequences.

1.3.6 Fault tree analysis
a systems engineering method for representing the logical combinations of various system states and possible causes which can contribute to a specified event (called the top event).

1.3.7 Frequency
a measure of the rate of occurrence of an event expressed as the number of occurrences of an event in a given time. See also Likelihood and Probability.

1.3.8 Hazard
a source of potential harm or a situation with a potential to cause loss.

1.3.9 Likelihood
used as a qualitative description of probability or frequency.

1.3.10 Loss
any negative consequence, financial or otherwise.

1.3.11 Monitor
to check, supervise, observe critically, or record the progress of an activity, action or system on a regular basis in order to identify change.

1.3.12 Organization

a company, firm, enterprise or association, or other legal entity or part thereof, whether incorporated or not, public or private, that has its own function(s) and administration.

1.3.13 Probability

the likelihood of a specific event or outcome, measured by the ratio of specific events or outcomes to the total number of possible events or outcomes. Probability is expressed as a number between 0 and 1, with 0 indicating an impossible event or outcome and 1 indicating an event or outcome is certain.

1.3.14 Residual risk

the remaining level of risk after risk treatment measures have been taken.

1.3.15 Risk

the chance of something happening that will have an impact upon objectives. It is measured in terms of consequences and likelihood.

1.3.16 Risk acceptance

an informed decision to accept the consequences and the likelihood of a particular risk.

1.3.17 Risk analysis

a systematic use of available information to determine how often specified events may occur and the magnitude of their consequences.

1.3.18 Risk assessment

the overall process of risk analysis and risk evaluation, refer to Figure 3.1.

1.3.19 Risk avoidance

an informed decision not to become involved in a risk situation.

1.3.20 Risk control

that part of risk management which involves the implementation of policies, standards, procedures and physical changes to eliminate or minimize adverse risks.

1.3.21 Risk engineering

the application of engineering principles and methods to risk management.

1.3.22 Risk evaluation

the process used to determine risk management priorities by comparing the level of risk against predetermined standards, target risk levels or other criteria.

1.3.23 Risk financing

the methods applied to fund risk treatment and the financial consequences of risk.

NOTE: In some industries risk financing only relates to funding the financial consequences of risk.

1.3.24 Risk identification
the process of determining what can happen, why and how.

1.3.25 Risk management
the culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects.

1.3.26 Risk management process
the systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risk.

1.3.27 Risk reduction
a selective application of appropriate techniques and management principles to reduce either likelihood of an occurrence or its consequences, or both.

1.3.28 Risk retention
intentionally or unintentionally retaining the responsibility for loss, or financial burden of loss within the organization.

1.3.29 Risk transfer
shifting the responsibility or burden for loss to another party through legislation, contract, insurance or other means. Risk transfer can also refer to shifting a physical risk or part thereof elsewhere.

1.3.30 Risk treatment
selection and implementation of appropriate options for dealing with risk.

1.3.31 Sensitivity analysis
examines how the results of a calculation or model vary as individual assumptions are changed.

1.3.32 Stakeholders
those people and organizations who may affect, be affected by, or perceive themselves to be affected by, a decision or activity.

NOTE: The term stakeholder may also include interested parties as defined in ISO 14050:1998 and AS/NZS ISO 14004:1996.

2 Risk management requirements

2.1 Purpose

The purpose of this Section is to describe a formal process for establishing a systematic risk management program.

The development of an organizational risk management policy and support mechanism is needed to provide a framework for carrying out a more detailed risk management program at the project or sub-organizational level.

2.2 Risk management policy

The organization's executive shall define and document its policy for risk management, including objectives for, and its commitment to, risk management. The risk management policy shall be relevant to the organization's strategic context and its goals, objectives and the nature of its business. Management will ensure that this policy is understood, implemented and maintained at all levels of the organization.

2.3 Planning and resourcing

2.3.1 Management commitment

The organization should ensure that:

a) a risk management system is established, implemented and maintained in accordance with this Standard; and

b) the performance of the risk management system is reported to the organization's management for review and as a basis for improvement.

2.3.2 Responsibility and authority

The responsibility, authority and the interrelationship of personnel who perform and verify work affecting risk management shall be defined and documented, particularly for people who need the organizational freedom and authority to do one or more of the following:

a) initiate action to prevent or reduce the adverse effects of risk;

b) control further treatment of risks until the level of risk becomes acceptable;

c) identify and record any problems relating to the management of risk;

d) initiate, recommend or provide solutions through designated channels;

e) verify the implementation of solutions; and

f) communicate and consult internally and externally as appropriate.

2.3.3 Resources

The organization shall identify resource requirements and provide adequate resources, including the assignment of trained personnel for management, performance of work, and verification activities including internal review.

2.4 Implementation program

A number of steps are required to implement an effective risk management system within an organization. Examples are provided in Appendix B. Depending on the organization's overall risk management philosophy, culture and structure, it should be possible to combine or omit certain steps. However, all steps should receive consideration.

2.5 Management review

The organization's executive shall ensure a review of the risk management system is carried out at specified intervals, sufficient to ensure its continuing suitability and effectiveness in satisfying the requirements of this Standard, and the organization's stated risk management policy and objectives (see Clause 2.2). Records of such reviews shall be maintained.

3 Risk management overview

3.1 General

Management of risk is an integral part of the management process. Risk management is a multifaceted process, appropriate aspects of which are often best carried out by a multi-disciplinary team. It is an iterative process of continual improvement.

3.2 Main elements

The main elements of the risk management process, as shown in Figure 3.1, are the following:

a) Establish the context

Establish the strategic, organizational 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.

b) Identify risks

Identify what, why and how things can arise as the basis for further analysis.

c) Analyse risks

Determine the existing controls and analyse risks in terms of consequence and likelihood in the context of those controls. The analysis should consider the range of potential consequences and how likely those consequences are to occur. Consequence and likelihood may be combined to produce an estimated level of risk.

d) Evaluate risks

Compare estimated levels of risk against the pre-established criteria. This enables risks to be ranked so as to identify management priorities. If the levels of risk established are low, then risks may fall into an acceptable category and treatment may not be required.

e) Treat risks

Accept and monitor low-priority risks. For other risks, develop and implement a specific management plan which includes consideration of funding.

f) Monitor and review

Monitor and review the performance of the risk management system and changes which might affect it.

g) 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.

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

Risk management is an iterative process that can contribute to organizational improvement. With each cycle, risk criteria can be strengthened to achieve progressively better levels of risk management.

For each stage of the process adequate records should be kept, sufficient to satisfy independent audit.

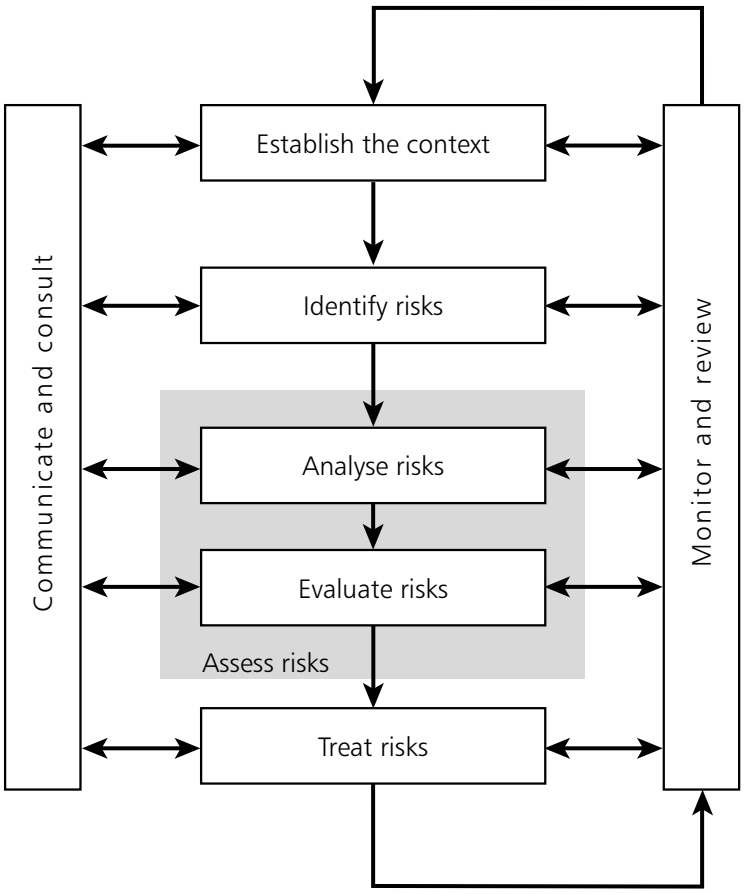

Figure 3.1 Risk management overview

4 Risk management process

4.1 Establish the context

4.1.1 General

The details of the risk management process are shown in Figure 4.1. The process occurs within the framework of an organization's strategic, organizational and risk management context. This needs to be established to define the basic parameters within which risks must be managed and to provide guidance for decisions within more detailed risk management studies. This sets the scope for the rest of the risk management process.

4.1.2 Establish the strategic context

Define the relationship between the organization and its environment, identifying the organization's strengths, weaknesses, opportunities and threats. The context includes the financial, operational, competitive, political (public perceptions/image), social, client, cultural and legal aspects of the organization's functions.

Identify the internal and external stakeholders, and consider their objectives, take into account their perceptions, and establish communication policies with these parties.

NOTE: Appendix C sets out a list of potential stakeholders.

This step is focused on the environment in which the organization operates. The organization should seek to determine the crucial elements which might support or impair its ability to manage the risks it faces.

Strategic analysis may be undertaken. It should be endorsed at the executive level, set the basic parameters and provide guidance for the more detailed risk management processes. There should be a close relationship between an organization's mission or strategic objectives and its management of all the risks to which it is exposed.

4.1.3 Establish the organizational context

Before a risk management study is commenced, it is necessary to understand the organization and its capabilities, as well as its goals and objectives and the strategies that are in place to achieve them.

This is important for the following reasons:

a) Risk management takes place in the context of the wider goals, objectives and strategies of the organization;

b) Failure to achieve the objectives of the organization or the specific activity, or project being considered is one set of risks which shall be managed;

c) The organizational policy and goals help define the criteria by which it is decided whether a risk is acceptable or not, and form the basis of options for treatment.

4.1.4 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 the risk management process involves:

a) Defining the project or activity and establishing its goals and objectives;

b) Defining the extent of the project in time and location;

c) Identifying any studies needed and their scope, objectives and the resources required. Generic sources of risk and areas of impact may provide a guide for this.

NOTE: For examples of generic sources of risk and their areas of impact, refer to Appendix D.

d) Defining the extent and comprehensiveness of the risk management activities to be carried out.

Specific issues which may also be discussed include the following:

i) The roles and responsibilities of various parts of the organization participating in managing risk;

ii) Relationships between the project and other projects or parts of the organization.

4.1.5 Develop risk evaluation criteria

Decide the criteria against which risk is to be evaluated. Decisions concerning risk acceptability and risk treatment may be based on operational, technical, financial, legal, social, humanitarian or other criteria. These often depend on an organization's internal policy, goals, objectives and the interests of stakeholders.

Criteria may be affected by internal and external perceptions and legal requirements. It is important that appropriate criteria be determined at the outset.

Although risk criteria 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, i.e. the risk criteria must correspond to the type of risks and the way in which risk levels are expressed.

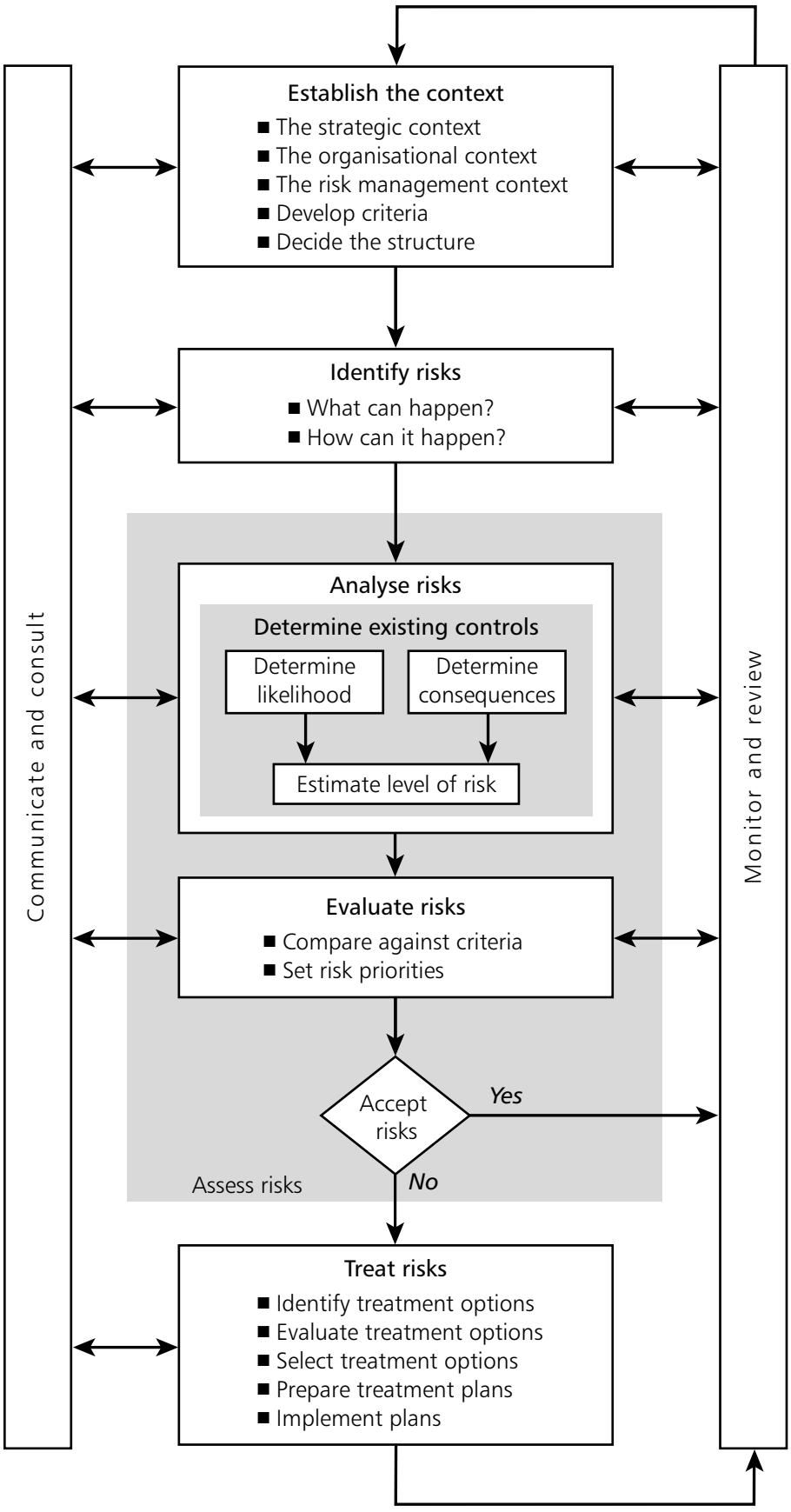

Figure 4.1 Risk management process

4.1.6 Define the structure

This involves separating the activity or project into a set of elements. These elements provide a logical framework for identification and analysis which helps ensure significant risks are not overlooked. The structure chosen depends on the nature of the risks and the scope of the project or activity.

4.2 Risk identification

4.2.1 General

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

4.2.2 What can happen

The aim is to generate a comprehensive list of events which might affect each element of the structure referred to in Clause 4.1.6. These are then considered in more detail to identify what can happen.

NOTE: Appendix D provides information on generic sources of risk and their areas of impact.

4.2.3 How and why it can happen

Having identified a list of events, it is necessary to consider possible causes and scenarios. There are many ways an event can be initiated. It is important that no significant causes are omitted.

4.2.4 Tools and techniques

Approaches used to identify risks include checklists, judgments based on experience and records, flow charts, brainstorming, systems analysis, scenario analysis and systems engineering techniques.

The approach used will depend on the nature of the activities under review and the types of risk.

4.3 Risk analysis

4.3.1 General

The objectives of analysis are to separate the minor acceptable risks from the major risks, and to provide data to assist in the evaluation and treatment of risks. Risk analysis involves consideration of the sources of risk, their consequences and the likelihood that those consequences may occur. Factors which affect consequences and likelihood may be identified. Risk is analysed by combining estimates of consequences and likelihood in the context of existing control measures.

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

4.3.2 Determine existing controls

Identify the existing management, technical systems and procedures to control risk and assess their strengths and weaknesses. Tools used in 4.2.4 may be appropriate, as well as approaches such as inspections and control self-assessment techniques ('CSA').

4.3.3 Consequences and likelihood

The magnitude of consequences of an event, should it occur, and the likelihood of the event and its associated consequences, are assessed in the context of the existing controls. Consequences and likelihood are combined to produce a level of risk. Consequences and likelihood may be determined using statistical analysis and calculations. Alternatively where no past data are 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.

To avoid subjective biases the best available information sources and techniques should be used when analysing consequences and likelihood. Sources of information may include the following:

a) Past records;

b) Relevant experience;

c) Industry practice and experience;

d) Relevant published literature;

e) Test marketing and market research;

f) Experiments and prototypes;

g) Economic, engineering or other models;

h) Specialist and expert judgements.

Techniques include:

i) structured interviews with experts in the area of interest;

ii) use of multi-disciplinary groups of experts;

iii) individual evaluations using questionnaires;

iv) use of computer and other modeling; and

v) use of fault trees and event trees.

Wherever possible, the confidence placed on estimates of levels of risk should be included.

4.3.4 Types of analysis

Risk analysis may be undertaken to various degrees of refinement depending upon the risk information and data 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. Later it may be necessary to undertake more specific quantitative analysis. In detail, the types of analyses are as follows:

a) Qualitative analysis

Qualitative analysis uses word form or descriptive scales 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.

NOTE: Tables E1 and E2 in Appendix E show examples of simple qualitative or descriptive scales for likelihood and consequences. Table E3 is an example of a matrix in which risks are assigned to priority classes by combining their likelihood and consequence. These tables need to be tailored to meet the needs of an individual organization or the particular subject of the risk assessment.

Qualitative analysis is used:

i) as an initial screening activity to identify risks which require more detailed analysis;

ii) where the level of risk does not justify the time and effort required for a fuller analysis; or

iii) where the numerical data are inadequate for a quantitative analysis.

b) Semi-quantitative analysis

In semi-quantitative analysis, qualitative scales such as those described above are given values. The number allocated to each description does not have to bear an accurate relationship to the actual magnitude of consequences or likelihood. The numbers can be combined by any one of a range of formulae provided that the system used for prioritization matches the system chosen for assigning numbers and combining them. The objective is to produce a more detailed prioritization than is usually achieved in qualitative analysis, not to suggest any realistic values for risk such as is attempted in quantitative analysis.

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

Sometimes it is appropriate to consider likelihood to be composed of two elements, usually referred to as frequency of exposure and probability.

Frequency of exposure is the extent to which a source of risk exists, and probability is the chance that when that source of risk exists, consequences will follow. Caution must be exercised in situations where the relationship between the two elements is not completely independent, i.e. where there is a strong relationship between frequency of exposure and probability.

This approach may be applied in semi-quantitative and quantitative analysis.

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 sub-paragraphs (a) to (h) of Clause 4.3.3). The quality of the analysis depends on the accuracy and completeness of the numerical values used.

Consequences may be estimated by modeling 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 criteria, or any of the other criteria referred to in Clause 4.1.5. In some cases, more than one numerical value is required to specify consequences for different times, places, groups or situations.

Likelihood is usually expressed as either a probability, a frequency, or a combination of exposure and probability.

The way in which likelihood and consequences 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 context in which the level of risk is to be used.

NOTE: Some examples of quantitative risk expressions are given in Appendix F.

4.3.5 Sensitivity analysis

Since some of the estimates made in quantitative analysis are imprecise, a sensitivity analysis should be carried out to test the effect of changes in assumptions and data.

4.4 Risk evaluation

Risk evaluation involves comparing the level of risk found during the analysis process with previously established risk criteria.

Risk analysis and the criteria against which risks are compared in risk evaluation should be considered on the same basis. Thus qualitative evaluation involves comparison of a qualitative level of risk against qualitative criteria, and quantitative evaluation involves comparison of

numerical level of risk against criteria which may be expressed as a specific number, such as fatality, frequency or monetary value.

The output of a risk evaluation is a prioritized list of risks for further action.

The objectives of the organization and the extent of opportunity which could result from taking the risk should be considered.

Decisions shall 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 which benefits from it.

If the resulting risks fall into the low or acceptable risk categories they may be accepted with minimal further treatment. Low and accepted risks should be monitored and periodically reviewed to ensure they remain acceptable.

If risks do not fall into the low or acceptable risk category, they should be treated using one or more of the options considered in Clause 4.5.

4.5 Risk treatment

Risk treatment involves identifying the range of options for treating risk, assessing those options, preparing risk treatment plans and implementing them.

4.5.1 Identifying options for risk treatment

Figure 4.2 illustrates the risk treatment process. Options, which are not necessarily mutually exclusive or appropriate in all circumstances, include the following:

a) Avoid the risk by deciding not to proceed with the activity likely to generate risk (where this is practicable).

   Risk avoidance can occur inappropriately because of an attitude of risk aversion, which is a tendency of many people (often influenced by an organization's internal system). Inappropriate risk avoidance may increase the significance of other risks.

   Risk aversion results in:

   i) decisions to avoid or ignore risks regardless of the information available and costs incurred in treating those risks.

   ii) failure to treat risk;

   iii) leaving critical choices and/or decisions up to other parties;

   iv) deferring decisions which the organization cannot avoid; or

   v) selecting an option because it represents a potential lower risk regardless of benefits.

b) Reduce the likelihood of the occurrence

   NOTE: Examples are shown in Appendix G.

c) Reduce the consequences

   NOTE: Examples are shown in Appendix G.

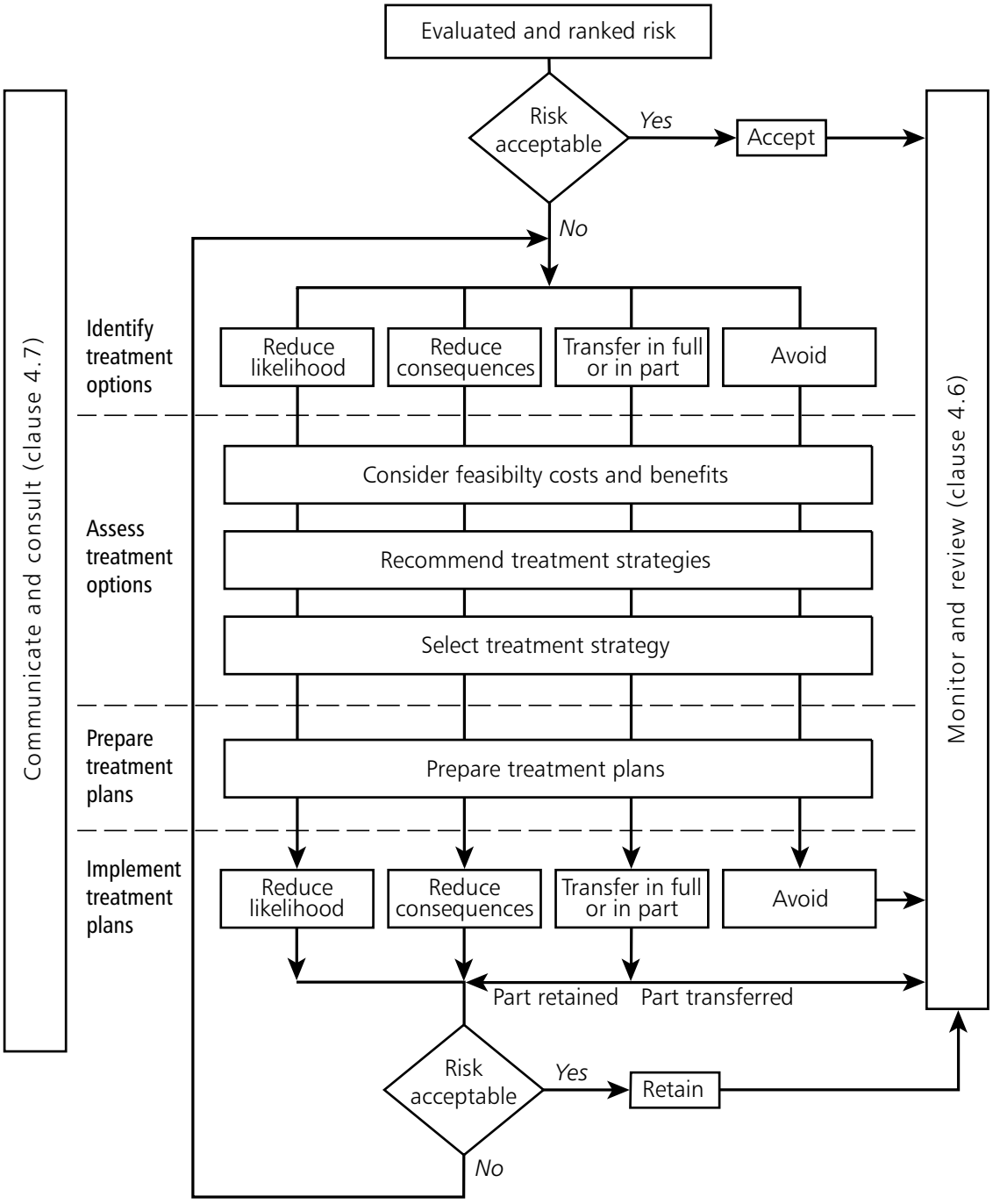

Figure 4.2 Risk treatment process

d) Transfer the risk

This involves another party bearing or sharing some part of the risk. Mechanisms include the use of contracts, insurance arrangements and organizational structures such as partnership and joint ventures.

The transfer of a risk to other parties, or physical transfer to other places, will reduce the risk for the original organization, but may not diminish the overall level of risk to society.

Where risks are transferred 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.

e) Retain the risk

After risks have been reduced or transferred, there may be residual risks which are retained. Plans should be put in place to manage the consequences of these risks if they should occur, including identifying a means of financing the risk. Risks can also be retained by default, i.e. when there is a failure to identify and/or appropriately transfer or otherwise treat risks.

Reduction of consequence and likelihood may be referred to as risk control. Risk control involves determining the relative benefit of new controls in the light of the effectiveness of existing controls. Controls may involve effectiveness policies, procedures or physical changes.

4.5.2 Assessing risk treatment options

Options should be assessed on the basis of the extent of risk reduction, and the extent of any additional benefits or opportunities created, taking into account the criteria developed in Clause 4.1.5. A number of options may be considered and applied either individually or in combination.

Selection of the most appropriate option involves balancing the cost 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.

Where large reductions in risk may be obtained with relatively low expenditure, such options should be implemented. Further options for improvement may be uneconomic and judgment needs to be exercised as to whether they are justifiable. This is illustrated in Figure 4.3.

Decisions should take account of the need to carefully consider rare but severe risks, which may warrant risk reduction measures that are not justifiable on strictly economic grounds.

In general the adverse impact of risks should be made as low as reasonably practicable, irrespective of any absolute criteria.

If the level of risk is high, but considerable opportunities could result from taking the risk, such as the use of a new technology, then acceptance of the risk needs to be based on an assessment of the costs of risk treatment, and the costs of rectifying the potential consequences versus the opportunities afforded by taking the risk.

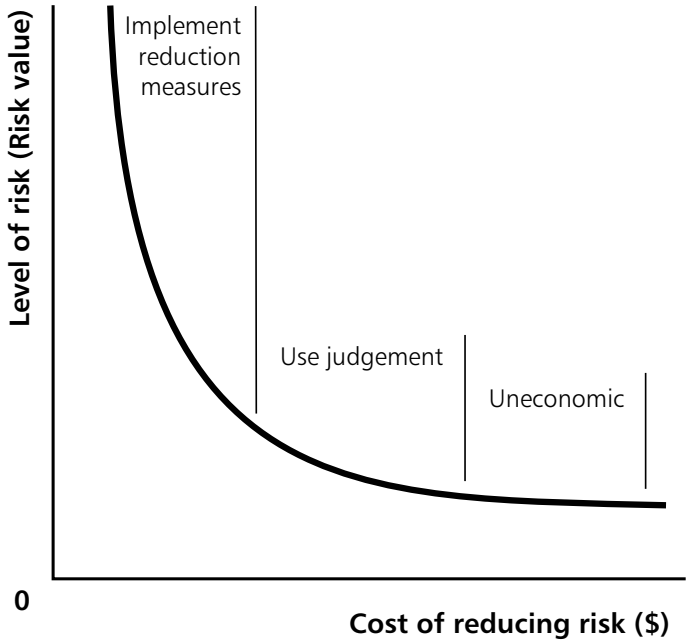

Figure 4.3 Cost of risk reduction measures

In many cases, it is unlikely that any one risk treatment option will be a complete solution for a particular problem. Often the organization will benefit substantially by a combination of options such as reducing the likelihood of risks, reducing their consequences, and transferring or retaining any residual risks. An example is the effective use of contracts and risk financing supported by a risk reduction program.

Where the cumulative cost of implementing all risk treatments exceeds the available budget, the plan should clearly identify the priority order in which individual risk treatments should be implemented. Priority ordering can be established using various techniques, including risk ranking and cost-benefit analysis. Risk treatments which cannot be implemented within the limit of the available budget must either await the availability of further financial resources or, if for whatever reason any or all of the remaining treatments are considered important, a case must be made to secure additional finances.

Risk treatment options should consider how risk is perceived by affected parties and the most appropriate ways to communicate to those parties.

4.5.3 Preparing treatment plans

Plans should document how the chosen options shall be implemented.

The treatment plan should identify responsibilities, schedules, the expected outcome of treatments, budgeting, performance measures and the review process to be set in place.

NOTE: Refer to Part H5, Appendix H, for details.

The plan should also include a mechanism for assessing the implementation of the options against performance criteria, individual responsibilities and other objectives, and to monitor critical implementation milestones.

4.5.4 Implementing treatment plans

Ideally, responsibility for treatment of risk should be borne by those best able to control the risk. Responsibilities should be agreed between the parties at the earliest possible time.

The successful implementation of the risk treatment plan requires an effective management system which specifies the methods chosen, assigns responsibilities and individual accountabilities for actions, and monitors them against specified criteria.

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

4.6 Monitoring and review

It is necessary to monitor risks, the effectiveness of the risk treatment plan, strategies and the management system which is set up to control implementation. Risks and the effectiveness of control measures need to be monitored to ensure changing circumstances do not alter risk priorities. Few risks remain static.

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

4.7 Communication and consultation

Communication and consultation are an important consideration at each step of the risk management process. 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.

Communication and consultation involve a two way dialogue between stakeholders with efforts focused on consultation rather than a one way flow of information from the decision maker to other stakeholders.

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.

Perceptions of risk can vary due to difference in assumptions and concepts and the needs, issues and concerns of stakeholders as they relate to the risk or the issues under discussion. Stakeholders are likely to make judgments of the acceptability of a risk based on their perception of risk. Since stakeholders can have a significant impact on the decisions made, it is important that their perceptions of risk, as well as their perceptions of benefits, be identified and documented and the underlying reasons for them understood and addressed.

5 Documentation

5.1 General

Each stage of the risk management process should be documented. Documentation should include assumptions, methods, data sources and results.

5.2 Reasons for documentation

The reasons for documentation are as follows:

a) to demonstrate the process is conducted properly;

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

c) to provide a record of risks and to develop the organisation's knowledge database;

d) to provide the relevant decision makers with a risk management plan for approval and subsequent implementation;

e) to provide an accountability mechanism and tool;

f) to facilitate continuing monitoring and review;

g) to provide an audit trail; and

h) to share and communicate information.

Decisions concerning the extent of documentation may involve costs and benefits and should take into account the above factors.

Guidance: To assist and give some guidance about appropriate documentation, examples are provided in Appendix H. These examples are indicative rather than comprehensive.

This page has been left blank

APPENDIX

A Applications of risk management

(Informative)

A1 Organizations

This Standard may be applied to a very wide range of organizations including:

a) public:

- national, regional, local;

b) commercial:

- companies, joint ventures, firms, franchises, sole practices; and

c) voluntary:

- charities, social, sporting.

A2 Applications

The Standard has a range of applications including, but not confined to:

i) asset management and resource planning;

ii) business interruption;

iii) change: organizational, technological and political;

iv) construction activity;

v) contingency, disaster and emergency planning;

vi) design and product liability;

vii) directors' and officers' liability;

viii) employment procedures, training, discrimination and harassment;

ix) environmental issues;

x) ethics and probity issues;

xi) feasibility studies;

xii) fire detection/fire prevention;

xiii) foreign exchange operations;

xiv) fraud prevention, detection and management;

xv) human, animal and plant health;

xvi) information systems/computer networks;

xvii) investments;

xviii) legislative compliance;

xix) occupational health and safety;

xx) operations and maintenance systems;

xxi) project management;

xxii) public risk and general liability;

xxiii) purchasing contract management;

xxiv) professional advice;

xxv) reputation and image issues;

xxvi) security;

xxvii) transport including air, sea, road, rail; and

xxviii) treasury and finance.

APPENDIX

B Steps in developing and implementing a risk management program

(Informative)

Step 1: Support of senior management

Develop an organizational risk management philosophy and awareness of 'risk' at senior management levels. This could be facilitated by training, education and briefing of executive management.

- The active ongoing support of the organization's Chief Executive Officer is necessary.
- A senior executive manager or similar 'champion' (or team) needs to sponsor the initiative.
- All senior executives shall give full support.

Step 2: Develop the organizational policy

Develop and document a corporate policy and framework for managing risks, to be endorsed by the organization's executive and implemented throughout the organization. The policy may include information such as:

- the objectives of the policy and rationale for managing risk;
- the links between the policy and the organization's strategic/corporate plan;
- the extent, or range of issues to which the policy applies;
- guidance on what may be regarded as acceptable risk;
- who is responsible for managing risks;

- the support/expertise available to assist those responsible for managing risks;
- the level of documentation required; and
- the plan for reviewing organizational performance in regard to the policy.

Step 3: Communicate the policy

Develop, establish and implement an infrastructure or arrangements to ensure that managing risk becomes an integral part of the planning, management processes and the general culture of the organization. This may include:

- establishing a team containing senior management personnel to be responsible for internal communications about the policy;
- raising awareness about managing risks;
- communication/dialogue throughout the organization about managing risk and the organization's policy;
- acquiring risk management skills, e.g. consultants, and developing the skills of staff through education and training;
- ensuring appropriate levels of recognition, rewards and sanctions; and
- establishing performance management processes.

Step 4: Manage risks at organizational level

Develop and establish a program for managing risks at the organizational level through the application of the risk management system outlined in Section 2. The process for managing risks should be integrated with the strategic planning and management processes for the organization. This will involve documenting:

- the organization and risk management context;
- the risks identified for the organization;
- the analysis and evaluation of these risks;
- the treatment strategies;
- the mechanisms to review the program; and
- the strategies for awareness raising, skills acquisition, training and education.

Step 5: Manage risks at the program, project and team level

Develop and establish a program to manage the risks for each sub-organizational area, program, project, or team activity through the application of the risk management process outlined in Section 4. The process for managing risks should be integrated with other planning and management activities. The process followed, the decisions taken, and the actions planned, should be documented.

Step 6: Monitor and review

Develop and apply mechanisms to ensure ongoing review of the risks. This will ensure that the implementation and the risk management policy remain relevant, as circumstances are changing all the time and review of previous decisions is vital. Risks are not static. The effectiveness of the risk management process should also be monitored and reviewed.

APPENDIX

C Stakeholders

(Informative)

Stakeholders are those individuals who are, or perceive themselves to be, affected by a decision or activity. They can include:

- individuals inside the organization, such as employees, management, senior management, and volunteers;
- decision-makers;
- business or commercial counterparties;
- employee groups;
- union groups;
- financial institutions;
- insurance organizations;
- regulators and other government organizations that have authority over activities;
- politicians (at all levels of government) who may have an electoral or portfolio interest;
- non-government organizations such as environmental groups and public interest groups;
- customers;
- suppliers, service providers and contractors to the activity;
- the media, who are potential stakeholders as well as conduits of information to other stakeholders;
- individuals or groups who are interested in issues related to the proposal;
- local communities; and
- society as a whole.

Over time, the mix of stakeholders may change. New stakeholders may join and wish to be included in any considerations, while others may drop out, through no longer being involved in the process. Consequently, the stakeholder analysis process should be continuous and, as such, should be an integral part of the risk management process.

The level of stakeholder concern may change in response to new information, either because the stakeholder's needs and concerns have been addressed, or because new information has given rise to new needs, issues or concerns. Note also that different stakeholders may have different opinions and different levels of knowledge regarding a particular issue.

APPENDIX

D Generic sources of risk and their areas of impact

(Informative)

D1 General

Identifying sources of risk and areas of impact provides a framework for risk identification and analysis. Because of the potentially large number of sources and impacts, developing a generic list focuses risk identification activities and contributes to its more effective management.

Generic sources of risk and areas of impact are selected according to their relevance to the activity being studied (see Clauses 4.1.4 and 4.2.2). Components of each generic category may form the basis for a thorough study of risks.

D2 Sources of risk

Each generic source has numerous components, any of which can give rise to a risk. Some components will be under the control of the organization conducting the study, while others will be outside its control. Both types need to be considered when identifying risks. Generic sources of risk include:

a) Commercial and legal relationships

   Between the organization and other organizations, e.g. suppliers, subcontractors, lessees.

b) Economic circumstances

   Of the organization, country, internationally, as well as factors contributing to those circumstances e.g. exchange rates.

c) Human behaviour

   Of both those involved and those not involved in the organization.

d) Natural events

e) Political circumstances

   Including legislative changes and factors which may influence other sources of risk.

f) Technology and technical issues

   Both internal and external to the organization.

g) Management activities and controls

h) Individual activities

D3 Areas of impact

Risk analysis may concentrate on impacts in one area only or on several possible areas of impact.

Areas of impact include the following:

a) Asset and resource base

   Of the organization, including personnel.

b) Revenue and entitlements

c) Costs

   Of activities, both direct and indirect.

d) People

e) Community

f) Performance

g) Timing and schedule of activities

h) The environment

i) Intangibles

   Such as reputation, goodwill, quality of life.

j) Organizational behaviour

D4 Risk identification

One method of summarizing the way in which risk arises in an organization is by using a risk identification template of the kind shown in Table D1. The entries may be made either with ticks to show where the risks occur, or with more detailed descriptive notes.

D5 Other classifications of risk

Different disciplines often categorize sources of risk in other ways, using such terms as hazards or risk exposures. These classifications may be subsets of the sources of risk listed in D2 above. Examples are as follows:

a) Diseases

e.g. affecting humans, animals and plants.

b) Economic

e.g. currency fluctuations, interest rates, sharemarket.

c) Environmental

e.g. noise, contamination, pollution.

d) Financial

e.g. contractual risks, misappropriation of funds, fraud, fines.

e) Human

e.g. riots, strikes, sabotage, error.

f) Natural hazards

e.g. climatic conditions, earthquakes, bushfires, vermin, volcanic activity.

g) Occupational health and safety

e.g. inadequate safety measures, poor safety management.

h) Product liability

e.g. design error, substandard quality control, inadequate testing.

i) Professional liability

e.g. wrong advice, negligence, design error.

j) Property damage

e.g. fire, water damage, earthquakes, contamination, human error.

k) Public liability

e.g. public access, egress and safety.

l) Security

e.g. cash arrangements, vandalism, theft, misappropriation of information, illegal entry.

m) Technological

e.g. innovation, obsolescence, explosions and dependability.

Table D1 Example of risk identification template

Sources of Risk	Area of impact Select as applicable from Paragraph D3*					
	*	*	*	*	*	*
Commercial and legal relationships						
Economic						
Human behaviour						
Natural events						
Political circumstances						
Technology/technical issues						
Management activities and controls						
Individual activities						

NOTE: Sources of risk and areas of impact should be adapted to suit the individual organization or activity.

APPENDIX

E Examples of risk definition and classification

(Informative)

Table E1 Qualitative measures of consequence or impact

Level	Descriptor	Example detail description
1	Insignificant	No injuries, low financial loss
2	Minor	First aid treatment, on-site release immediately contained, medium financial loss
3	Moderate	Medical treatment required, on-site release contained with outside assistance, high financial loss
4	Major	Extensive injuries, loss of production capability, off-site release with no detrimental effects, major financial loss
5	Catastrophic	Death, toxic release off-site with detrimental effect, huge financial loss

NOTE: Measures used should reflect the needs and nature of the organization and activity under study.

Table E2 Qualitative measures of likelihood

Level	Descriptor	Description
A	Almost certain	Is expected to occur in most circumstances
B	Likely	Will probably occur in most circumstances
C	Possible	Might occur at some time
D	Unlikely	Could occur at some time
E	Rare	May occur only in exceptional circumstances

NOTE: These tables need to be tailored to meet the needs of an individual organization.

Table E3 Qualitative risk analysis matrix—level of risk

	Consequences				
	Insignificant	Minor	Moderate	Major	Catastrophic
Likelihood	1	2	3	4	5
A (almost certain)	H	H	E	E	E
B (likely)	M	H	H	E	E
C (moderate)	L	M	H	E	E
D (unlikely)	L	L	M	H	E
E (rare)	L	L	M	H	H

NOTE: The number of categories should reflect the needs of the study.

Legend

E: extreme risk; immediate action required

H: high risk; senior management attention needed

M: moderate risk; management responsibility must be specified

L: low risk; manage by routine procedures

APPENDIX

F Examples of quantitative risk expressions

(Informative)

F1 Risk of financial loss or gain

The financial loss (or gain) multiplied by the annual frequency of loss (or gain) gives the expected value in dollars per annum.

F2 Fatality risk

The fatality risk from an activity may be calculated as:

$$\frac{\text{Number of deaths per annum from activity}}{\text{Exposed population}}$$

F3 Natural or man-made disasters

Consequences can be modeled using computerized simulations and likelihood estimated from historical data, fault trees or other systems engineering techniques.

F4 Health risks

Health risks are commonly expressed in the following different ways:

a) The number of new ill-health cases per annum in an exposed population compared with the total of that population, i.e. five new cases in an exposed population of 100 000 is a risk of 5×10^{-5} per exposed person, per year.

b) The ratio of the probability of death before a certain age, with and without exposure.

c) The number of fatalities by age 70 that are expected to result from an exposure, divided by the number of people exposed.

Health risks can be derived from epidemiological data (population surveys of fatalities or illness) or from experimental data based on animal studies.

NOTE: Rather than calculate average value of a risk, the distribution of possible values can be calculated by replacing average values of the variables on which the outcome depends by appropriate distributions of values.

APPENDIX

G Identifying options for risk treatment

(Informative)

G1 Actions to reduce or control likelihood

These can include:

i) audit and compliance programs;

ii) contract conditions;

iii) formal reviews of requirements, specifications, design, engineering and operations;

iv) inspection and process controls;

v) investment and portfolio management;

vi) project management

vii) preventative maintenance;

viii) quality assurance, management and standards;

ix) research and development, technological development;

x) structured training and other programs;

xi) supervision;

xii) testing;

xiii) organizational arrangements; and

xiv) technical controls.

G2 Procedures to reduce or control consequences

These can include:

i) contingency planning;

ii) contractual arrangements;

iii) contract conditions;

iv) design features;

v) disaster recovery plans;

vi) engineering and structural barriers;

vii) fraud control planning;

viii) minimizing exposure to sources of risk;

ix) portfolio planning;

x) pricing policy and controls;

xi) separation or relocation of an activity and resources;

xii) public relations; and

xiii) ex gratia payments.

APPENDIX

H Risk management documentation

(Informative)

H1 General

To manage risk properly, appropriate documentation is required. This may need to be sufficient to satisfy independent audit. Decisions concerning the extent of documentation may involve costs and benefits and should take into account the factors listed in Clause 5.2. The risk management policy statement should define the documentation needed.

At each stage of the process, documentation should include:

a) objectives;

b) information sources;

c) assumptions; and

d) decisions.

This Appendix H includes an example of a risk register, and a treatment schedule and action plan. Plans for high risk areas may need to be more specific and detailed.

H2 Policy

Examples of information which may be included in an organization's policy statement are given in Appendix B.

H3 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.

H4 Risk register*

For each risk identified, a risk register records:

a) source;

b) nature;

c) existing controls;

d) consequences and likelihood;

e) initial risk rating; and

f) vulnerability to external/internal factors.

Refer to the sample proforma below as a guide.

H5 Risk treatment schedule and action plan*

A risk treatment and action plan documents the management controls to be adopted and lists the following information:

a) Who has responsibility for implementation of the plan;

b) What resources are to be utilized;

c) Budget allocation;

d) Timetable for implementation;

e) Details of the mechanism and frequency of review of compliance with the treatment plan.

H6 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 review recommendations are followed up and implemented.

* These examples are indicative only

Risk register

Date of risk review.....

Compiled by ..... Date .....

Function/activity..... Reviewed by ..... Date .....

Ref	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
		Consequences	Likelihood					

Risk treatment schedule and plan

Date of risk review .....

Compiled by ..... Date .....

Function/activity..... Reviewed by ..... Date .....

The risk in priority order from Risk register	Possible treatment options	Preferred options	Risk rating after treatment	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 options be monitored

NOTE: This form may be enlarged on A3 sized paper in order to facilitate the handwriting of the information or else it can be set up on an electronic spreadsheet.

Risk action plan

Item	Ref
Risk	
Summary – Recommended response and impact	
Action plan 1 Proposed actions 2 Resource requirements 3 Responsibilities 4 Timing 5 Reporting and monitoring required	
Compiler ..... Date ..... Reviewer ..... Date	

ISBN 0 7337 2647 X