

RISK MANAGEMENT FOR NOT-FOR-PROFIT ORGANISATIONS



TABLE OF CONTENTS

| | |
|---|----------|
| 1 INTRODUCTION | 3 |
| 1.1 Who is this document for? | 3 |
| 1.2 What is the risk? | 3 |
| 1.3 What is risk management? | 3 |
| 1.4 Why do you need to manage risk? | 3 |
| 1.5 How to use this document | 4 |
| 1.6 How has this document been developed? | 5 |

2 GLOSSARY 5

PART A

BACKGROUND: DEVELOPING A RISK MANAGEMENT FRAMEWORK

| | |
|--|----------|
| 3 TYPES OF RISK | 6 |
| 3.1 Compliance risks | 6 |
| 3.2 Organisational risks | 6 |
| 3.3 Opportunity risks | 6 |
| 4 ATTITUDE TO RISK | 6 |
| 5 BUILDING BLOCKS OF THE RISK MANAGEMENT SYSTEM | 7 |
| 5.1 Principles | 7 |
| 5.2 Framework | 7 |
| 5.3 Develop a risk register | 9 |

PART B

RISK MANAGEMENT STEPS

| | |
|--|-----------|
| 6 OVERVIEW OF THE RISK MANAGEMENT PROCESS | 10 |
| 7 ESTABLISHING THE CONTEXT (STEP 1) | 10 |
| 7.1 Confirm organisational objectives | 10 |
| 7.2 Identify stakeholders | 11 |
| 7.3 Define risk assessment criteria | 11 |
| 8 RISK ASSESSMENT (Step 2) | 11 |
| 8.1 Risk identification (Step 2.1) | 12 |
| 8.2 Risk analysis (Step 2.2) | 13 |
| 8.3 Risk evaluation (Step 2.3) | 15 |
| 9 RISK TREATMENT (STEP 3) | 16 |
| 10 COMMUNICATION AND CONSULTATION (ONGOING PROCESS) | 17 |
| 10.1 Communication | 17 |
| 10.2 Consultation | 17 |
| 11 MONITOR AND REVIEW (ONGOING PROCESS) | 18 |
| 11.1 Establish formal review and reporting mechanisms | 18 |

PART C

EXAMPLES, TOOLS & TEMPLATES

APPENDIX 1

| | |
|---------------------------------------|-----------|
| EXAMPLE RISK MANAGEMENT POLICY | 19 |
| Overview | 19 |
| Policy | 19 |
| Risk Tolerance | 19 |
| Accountability | 19 |
| Risk management oversight | 20 |
| Reporting, Monitoring and Review | 20 |
| Communication and Consultation | 20 |

APPENDIX 2

| | |
|--|-----------|
| RISK REGISTER TEMPLATE AND EXAMPLES | 21 |
| Risk Register | 21 |

APPENDIX 3

| | |
|---|-----------|
| CHECKLIST FOR DEVELOPING THE RISK REGISTER | 25 |
|---|-----------|

APPENDIX 4

| | |
|------------------------------------|-----------|
| EXAMPLES OF RISK CATEGORIES | 26 |
|------------------------------------|-----------|

APPENDIX 5

| | |
|--------------------------------------|-----------|
| EXAMPLES OF RISK DESCRIPTIONS | 26 |
|--------------------------------------|-----------|

APPENDIX 6

| | |
|---------------------------------|-----------|
| RISK IDENTIFICATION FORM | 27 |
|---------------------------------|-----------|

APPENDIX 7

| | |
|--|-----------|
| EXAMPLE RISK CONSEQUENCE CRITERIA | 28 |
|--|-----------|

APPENDIX 8

| | |
|---|-----------|
| EXAMPLE RISK LIKELIHOOD CRITERIA | 29 |
|---|-----------|

APPENDIX 9

| | |
|--|-----------|
| EXAMPLE ESCALATION AND RETENTION GUIDELINES | 29 |
|--|-----------|

APPENDIX 10

| | |
|---|-----------|
| RISK TREATMENT PLAN TEMPLATE AND EXAMPLE | 30 |
|---|-----------|

The material provided in this resource has been prepared to provide general information only. It is not intended to be relied upon as, or be a substitute for, legal or other professional advice. While all care has been taken in the preparation of this material, no responsibility is accepted by the Department of Education and Communities, for any errors, omissions or inaccuracies. No responsibility can be accepted by the Department of Education and Communities for any known or unknown consequences that may result from reliance on any information provided in this publication.

1 INTRODUCTION

1.1 WHO IS THIS DOCUMENT FOR?

This document is for all those in not-for-profit organisations who are responsible for risk management – executive directors, managers, senior staff, and any other relevant officers. It provides a step-by-step approach to help you identify, assess, monitor and manage risk in your organisation.

1.2 WHAT IS RISK?

It is common to think of risk as what might go wrong in an organisation. But a more precise definition is the effect of uncertainty on an organisation's objectives. In this regard, risk includes both (a) potential threats to achieving those objectives (negative risk), and (b) potential opportunities for achieving those objectives (positive risk).

Threats and opportunities come and go, or evolve, as an organisation's internal dynamics change, as its relationships with stakeholders change, and as the external environment in which it operates changes. Keeping abreast of the risks that may affect your organisation must therefore be an ongoing activity.

1.3 WHAT IS RISK MANAGEMENT?

Risk management aims firstly to anticipate risks. Then, in the case of negative risks, it aims to prevent them from eventuating or to minimize their impact if they do. In the case of positive risks, it aims to capitalise on opportunities that present themselves. This document is mainly concerned with managing negative risks.

Because responding to risk is intended to help the organisation achieve its objectives, risk management must be integral to strategic planning, decision-making, and resource allocation.

A risk management system encompasses many elements: a risk management policy, a risk management framework, and various risk management tools and processes – all of which are explained in this document.

Finally, risk is present at all levels of activity. There are risks that may affect the organisation as a whole. There are risks that may affect only financial

activities, or only service delivery activities, as well as risks that may affect both. There are risks specific to each and every project. What this means is that everyone in an organisation bears some responsibility for managing risk.

1.4 WHY DO YOU NEED TO MANAGE RISK?

Risk management is good business practice and can assist with meeting a range of compliance, statutory, organisational and governance requirements.

1.4.1 COMPLIANCE AND STATUTORY REQUIREMENTS

Not-for-profit compliance and statutory requirements will vary depending on whether the organisation is registered as a company under the Corporations Act 2001, as an incorporated association, or an unincorporated association or cooperative and whether or not the organisation is registered as a charity with the recently established Australian Charities and Not-for-profits Commission.

As such, it is important that executive directors, senior managers, or other relevant officers of not-for-profits are aware of the specific circumstances of their organisation in order to meet related statutory requirements. Further advice is available at:

- Australian Securities and Investment Commission www.asic.gov.au
- NSW Fair Trading www.fairtrading.nsw.gov.au
- Australian Charities and Not-for-profits Commission www.acnc.gov.au

1.4.2 ORGANISATIONAL AND GOVERNANCE REQUIREMENTS

Risk management is important for good governance, as well as legal compliance.

By effectively managing the risks it faces, your organisation can guard against poor decision-making, complacency and inadvertent exposure to any potentially debilitating consequences of its actions, as well as meet its objectives in delivering services to clients.

In addition, the principles of good governance dictate that those responsible for the management of an organisation have an obligation to protect

the interests of its stakeholders. Many stakeholders expect not-for-profits to manage risks in accordance with good governance principles and practices.

For all these reasons, risk management policies, processes and activities need to be aligned with the other policies, processes and activities in an organisation in order to support the Board, or Management Committee or equivalent (here after referred to as 'the Board'). Alignment of risk management policies to other organisational policies and processes also supports the practice of good governance.

1.4.3 BENEFITS OF RISK MANAGEMENT

As well as contributing to legal compliance and good governance, effective risk management can contribute to strategic and business planning and the general running (operational activities) of an organisation. It creates confidence that your organisation can deliver the desired outcomes, manage threats to an acceptable degree, and make informed decisions about opportunities.

Some benefits of effective risk management are that it:

1. improves the quality of decision-making (appropriate, fast, accurate, and effective)
2. enables effective execution of decisions (improved confidence, known quantity)
3. when embedded within an organisation's day-to-day operations, is part of 'business as usual' rather than an additional task or burden
4. when integrated with business strategy, ensures that strategic decisions are informed and based on up-to-date information and sound judgment
5. improves planning processes by enabling the key focus to remain on core activities, and helps ensure continuity of service delivery
6. reduces the likelihood of potentially costly 'surprises'
7. prepares for challenging events and improves overall resilience
8. prioritises budgeted resources
9. optimises performance through efficiencies in service delivery, major change and quality assurance initiatives
10. contributes to the development of a positive organisational culture of improved governance, as well as helps establish clear purpose, roles and accountabilities for all staff
11. improves stakeholder relationships and stakeholders' confidence in the organisation through enhanced accountability and reporting processes.

1.5 HOW TO USE THIS DOCUMENT

On the next page is a useful **glossary** of risk management terms commonly used throughout this document.

Part A of the document explains preparatory things you need to consider before getting down to the business of identifying, assessing and managing specific risks. These include: understanding the different types of risk and organisational attitudes to risk; understanding the building blocks of a risk management system (principles, framework, process); and developing a Risk Register (a document in which to record risks and how you're managing them).

Part B is the 'nuts and bolts' of this document and walks you step-by-step through the risk management process – i.e. identifying, assessing and managing specific risks.

Part C is a series of appendices containing examples of key tables and tools discussed in the document, as well as some blank templates of tools (e.g. the Risk Register) that you may wish to use as a model or starting point for your own purposes.

Because every organisation is unique in size, function, operation and charter, you should not simply 'cut and paste' from this document into your own risk management system. What you find here you will need to customise to your organisation's particular needs. Use this resource in whatever ways will best serve your organisation's interests, rather than adhere to it rigidly.

Note: Throughout this document we discuss the risk management system as it would apply to an organisation as a whole. But it can also be applied to, say, a specific project. The principles and steps are the same, just on a different scale.

1.6 HOW HAS THIS DOCUMENT BEEN DEVELOPED?

This document has been developed in accordance with two documents:

- AS/NZS ISO 31000:2009 Risk management – Principles and guidelines (ISO 31000). This is the international benchmark for risk management, and is otherwise known as the ‘Standard’. Importantly, the Standard is intended for guidance, not compliance. A copy of the Standard is available from the International Standards Organisation at www.iso.org
- Enterprise Risk Management in the Department of Education and Communities – Guidelines, May 2012. A copy of this document is available from the Department of Education and Communities at <https://www.det.nsw.edu.au/policiesinter/atoz/search.do?level>.

2 GLOSSARY

Here are some specialist terms, and specialist uses of common terms, you will encounter in this document.

| | |
|--|---|
| Acceptable level of risk, or ‘valid’ risk. | The acceptable level of risk reflects the decision by the organisation’s management to accept the risk (likelihood and consequences of a risk). In some cases it may be more appropriate for a not-for-profit to consider a risk ‘valid’. This is also known as the organisation’s risk appetite. |
| Communication and consultation | Continual and iterative processes that an organisation conducts to provide, share or obtain information, and to engage in dialogue with stakeholders regarding the management of risk. |
| Consequence | The outcome of an event affecting objectives. |
| Control | A measure that modifies (usually, reduces) risk. |
| Likelihood | The chance of something happening. |
| Residual risk level | The risk remaining after risk treatment. |
| Risk | The effect of uncertainty on objectives. |
| Risk appetite | The amount and type of risk that an organisation is willing to retain. |
| Risk assessment | The overall process of risk identification, risk analysis and risk evaluation. |

| | |
|---------------------------|--|
| Risk level | The risk rating calculated using likelihood and consequence criteria after considering the existing control environment. |
| Risk management | Coordinated activities undertaken by an organisation to control or reduce risk. |
| Risk Management Framework | This broadly articulates how risk management is integrated into and aligned with your organisation’s policies, procedures, practices and values. |
| Risk Management Policy | An organisation’s formal statement of its overall intentions and direction regarding risk management. |
| Risk Management Process | The systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk. |
| Risk matrix | A tool for ranking and displaying risks by identifying ranges for consequence and likelihood. |
| Risk owner | A person or entity with the accountability and authority to manage a risk. |
| Risk Register | A record of risks identified and how they’re managed. |
| Risk retention | Acceptance of the potential benefit, or burden, of a particular risk. |
| Risk tolerance | An organisation’s or stakeholder’s readiness to bear the risk after treatment in order to achieve its objectives. |
| Risk treatment | The process of selecting and implementing measures or ‘treatment options’ to modify risks or their potential consequences. |
| Stakeholder | A person or organisation that may affect, be affected by, or perceive themselves to be affected by, a decision or activity. |

PART A

BACKGROUND: DEVELOPING A RISK MANAGEMENT FRAMEWORK

3 TYPES OF RISK

3.1 COMPLIANCE RISKS

Compliance risks are those where the organisation fails to meet its corporate and legal obligations. These include reporting, accounting, licensing, workplace relations, and work health and safety activities.

Tolerance for compliance risks assessed as 'high' or 'extreme' is generally low. While organisations must comply with such obligations, with risk management controls in place the same risks may receive an assessment of 'medium' or 'low' and therefore may be considered valid.

3.2 ORGANISATIONAL RISKS

Organisational risks are those where the organisation fails to achieve objectives such as level of service delivery, standard of service delivery, or meeting stakeholder expectations. Consequences arising from such risks eventuating may include loss of reputation or high staff turnover.

3.3 OPPORTUNITY RISKS

Some risks arise from the pursuit of opportunities – 'positive risks' – that may enhance the organisation in some way or allow it to more easily achieve its objectives. Such risks can be listed in an Opportunities Register (separate from the Risk Register described in 5.3). For these risks, consideration should be given to the potential gains for the organisation as well as to the resources required to pursue the opportunities.

4 ATTITUDE TO RISK

Every organisation has an attitude to risk – whether this is defined explicitly or whether it's implicit in its culture and values – which is a combination of risk tolerance and risk appetite.

Risk tolerance is the amount of risk an organisation is prepared to bear. Generally, an organisation has low tolerance for high level risks due to their potentially serious consequences. High level risks may include such things as compliance, legal and statutory risks.

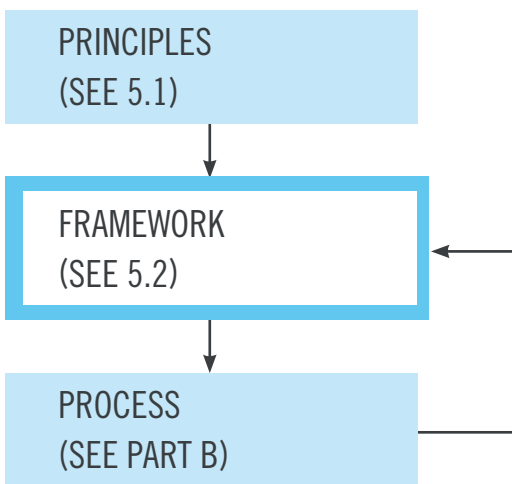
Risk appetite is the level of risk an organisation is prepared to retain or pursue. In general, an organisation is more likely to have an appetite for low level risks than for high level risks. There may be exceptions – i.e. a high level risk, where the potential benefits of which may warrant 'taking the risk' – but these are for each organisation to consider carefully.

Here's an example of risk appetite. Consider a risk such as 'failure to adequately resource a new service program, resulting in potential impact on objectives and reputation'. It may be that the 'new service program' is a desirable outcome for the organisation but requires additional resources. If the organisation cannot resource it adequately, the program may not be delivered and the organisation's objectives may not be achieved. The outcome would be undesirable but not severe, so attempting to deliver the program may be 'worth the risk'. The organisation would be said to have an appetite for this risk.

5 BUILDING BLOCKS OF THE RISK MANAGEMENT SYSTEM

The diagram below illustrates the main building blocks of risk management – Principles, Framework, and Process – and how they fit together. These building blocks are sometimes called the risk management architecture.

DIAGRAM 1: BUILDING BLOCKS OF RISK MANAGEMENT¹



Note that there is a circular, iterative relationship between Process and Framework. The Framework will inform how you undertake the Process. The results of undertaking the Process will feed back into, and may modify, the Framework. This will become clearer as you read through the document.

5.1 PRINCIPLES

The Standard contains 11 Principles which provide useful guidance for integrating risk management into your organisation. These Principles are that risk management:

1. creates and protects value
2. is an integral part of all organisational processes
3. is part of decision-making
4. explicitly addresses uncertainty
5. is systematic, structured and timely

6. is based on the best available information
7. is tailored to the organisation's requirements
8. takes human and cultural factors into account
9. is transparent and inclusive
10. is dynamic, iterative and responsive to change
11. facilitates continual improvement of the organisation.

The most important Principle is the first. It means risk management should demonstrably contribute to the achievement of your organisation's objectives and to the improvement of performance in all areas of activity. In contrast, if risk management is done purely for compliance reasons (as often occurs in organisations), then value is 'created' and/or 'protected' for legal obligations but not for decision-making, resource allocation, and so on.

5.2 FRAMEWORK

The Risk Management Framework (the Framework) articulates how risk management is integrated into the framework and aligned with your organisation's governance, strategy and planning; management, work plans and activities; internal and external reporting processes and communication mechanisms; policies, procedures, values and culture.

It clarifies the accountabilities, reporting and escalation processes, as well as the communication and consultation mechanisms for internal and external stakeholders.

It is advisable to have some documentation of the Framework. Larger organisations may have an extensive Framework document. Smaller organisations may have a briefer document simply stating the understanding of the organisation's broad approach to risk management. Either way, the steps detailed below should be taken into consideration.

¹ AS/NZS ISO 31000:2009 Risk management – Principles and guidelines

5.2.1 DEVELOPING A RISK MANAGEMENT FRAMEWORK

The steps for developing a Risk Management Framework are as follows:

- consider the Risk Management Principles
- understand your organisation and its context
- develop a Risk Management Policy
- establish accountabilities
- integrate risk management into your organisation's processes, culture and values
- allocate sufficient time and resources
- establish internal and external communication and reporting mechanisms.

You will notice some overlap between these steps and the steps involved in the Risk Management Process (see Part B). As mentioned earlier, that's because there is a circular, iterative relationship between Process and Framework: each informs the other.

5.2.2 CONSIDER THE RISK MANAGEMENT PRINCIPLES

First, consider how some or all of the 11 Principles might inform the design, implementation and periodic review of your Framework.

If you are working within an existing Framework, you can use the Principles as a benchmark against which to measure your risk management system and identify areas for improvement.

5.2.3 UNDERSTAND YOUR ORGANISATION AND ITS CONTEXT

In establishing the Framework, you need to take into account the social, cultural, financial, legal and regulatory environment in which your organisation operates. You will need to consider your organisation's mission or purpose, its management style, its size, and the simplicity or complexity of its processes and practices.

5.2.4 DEVELOP A RISK MANAGEMENT POLICY

Your organisation's Risk Management Policy will be a high-level statement of its intentions and directions as to how risk will be managed.

The Policy should be established by the Board and operationalised by the Executive Director or equivalent. It should be communicated to employees and volunteers, as appropriate, to ensure that all risk management processes and practices are carried out in accordance with it.

The Policy should generally be reviewed every year by the Board's Risk Management Committee or relevant officer to ensure it meets the organisation's evolving needs and circumstances.

An example of a Risk Management Policy document is given in Appendix 1. This is for guidance only; you will need to tailor it to suit your organisation.

5.2.4.1 RISK TOLERANCE AND APPETITE

The Policy should include statements as to your organisation's risk tolerance and risk appetite (see 4.0). These are policy positions that help the organisation decide what actions to take, if any, for risks assessed at different levels, i.e. extreme, high, medium or low (see 8.2.)

5.2.5 ESTABLISH ACCOUNTABILITIES


To make risk management work, there needs to be accountability for integrating risk management into the organisation and for managing specific risks.

Typically, the Board delegates overall responsibility for risk management to the Executive Director, or a position of similar seniority. The tasks of managing the Framework and undertaking the Risk Management Process (identifying, assessing and treating risks) are generally carried out by a senior manager – Coordinator, Finance Officer or Senior Administration Officer – who generally has a good understanding of all the organisational processes. In some organisations, the title of the role may be 'Risk Management Coordinator' or 'Risk Manager'. Only in very large organisations is there a dedicated 'Chief Risk Officer' role.

To achieve accountability for specific risks, it is useful to assign risks to nominated risk owners who are then accountable for managing them (see also 8.2.6). Risk owners are usually senior managers or officers who have the requisite authority to allocate resources to develop risk treatment actions and plans to manage risks to acceptable or tolerable levels (see also 9).

5.2.6 INTEGRATE RISK MANAGEMENT INTO YOUR ORGANISATION'S PROCESS, CULTURE AND VALUES

Aligning how risk management is carried out with how your organisation is managed and operated secures a greater level of engagement from



management and staff when it comes to specific risk management activities. For example, you should try to align risk management processes with existing organisational processes such as the business planning cycle and the management meeting cycle. You might also consider how you can best leverage your organisation's governance and culture to facilitate the integration and adoption of risk management.

5.2.7 ALLOCATE SUFFICIENT TIME AND RESOURCES

All risk management activities require time and resources – limited commodities in all organisations. As part of your Framework, therefore, you need to determine what time and resources you can allocate to risk management activities in order to achieve the organisation's objectives and meet stakeholder requirements.

Initial activities such as developing the Risk Management Policy, Framework and Risk Register will take some time and effort. Ongoing activities such as risk assessments and risk reviews should be less demanding and so should form a normal part of each manager's role within the organisation.

You might also build into your Framework a timeframe for implementing various risk management activities and goals.

5.2.8 ESTABLISH INTERNAL AND EXTERNAL COMMUNICATION AND REPORTING MECHANISMS

Risk management activities need to be communicated and/or reported to relevant internal and external stakeholders. Much of this can be done through your organisation's existing communication and reporting mechanisms, so you should factor these into the Framework. You may find that additional mechanisms are required to keep all relevant officers, employees, volunteers and other stakeholders informed of risk management activities. If so, you will need to identify and develop such mechanisms as part of the Framework.

5.3 DEVELOP A RISK REGISTER

The Risk Management Process (see Part B) will generate a lot of important information. To document this information systematically and coherently, we recommend you develop a dedicated Risk Register.

A template for a Risk Register is shown in Appendix 2. You don't need to understand the purpose of all the columns yet. Just begin with the blank template; and as you work through each step in Part B of this document, you will be able to fill in another column or two. (An example of a completed Risk Register is also shown in Appendix 2.)

Remember that both the blank template and the completed example are guides only.

5.3.1 HOW TO CREATE A SIMPLE RISK REGISTER

You can create a simple Risk Register manually using Word (as shown in Appendix 2) or using Excel.

There are of course customised risk management tools and specialised risk management software available, if you wish to invest in them. However, in most cases a simple record of the risk information will suffice.

A checklist of questions to ask yourselves when creating a Risk Register is shown in Appendix 3.

5.3.2 USING OUR ADVANCED RISK REGISTER TOOL

If you have a reasonable knowledge of Excel and would prefer to use a more advanced tool that automates certain processes (risk assessment, rating and scoring), you may prefer to use the Risk Register Tool developed by the Office of Communities. The tool is available from the link below:

[Office of Communities Risk Register Tool Template](#)

This tool is an Excel spreadsheet that contains:

- instructions on how to use the Risk Register
- places where you can enter risks, categories of risk, and risk management controls
- a facility to link risks to categories of risk, and risk management controls to risks
- risk assessment criteria – which you can customise
- a risk treatment plan template – which you can link to the risks
- a risk profile – this is created automatically.

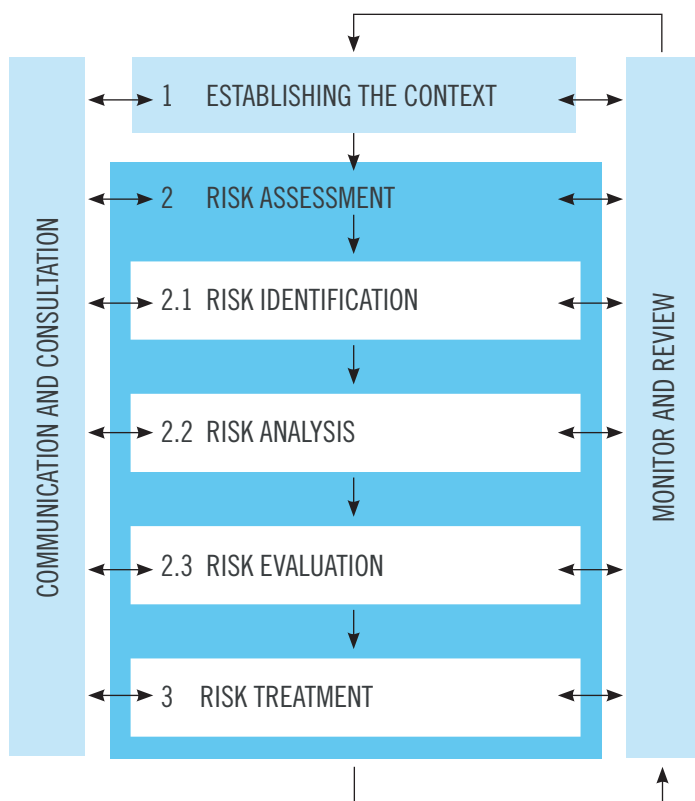
PART B

RISK MANAGEMENT STEPS

6 OVERVIEW OF THE RISK MANAGEMENT PROCESS

Broadly, the Risk Management Process is the whole set of activities you carry out to identify, assess, manage and monitor any risks to which your organisation may be exposed. The diagram below outlines the main steps.

DIAGRAM 2: RISK MANAGEMENT PROCESS²



² AS/NZS ISO 31000:2009 Risk management - Principles and guidelines

Each of the numbered steps is discussed in turn in the following pages. As you work through these steps, you will generate information that can be entered into your Risk Register (see 5.3 and Appendices 2 and 3).

Note that 'Communication and consultation' and 'Monitor and review' are not numbered. They are not steps in the sequence, but ongoing processes conducted as part of every step. They are discussed at the end of Part B.

7 ESTABLISHING THE CONTEXT (STEP 1)

The purpose of this step is to determine the scope for all risk management activities. This includes both the internal and external environments in which risks may occur: strategic, operational, financial, competitive, stakeholder, social, cultural and legal.

In this step you will need to:

- Confirm organisational objectives
- Identify stakeholders
- Define risk assessment criteria

7.1 CONFIRM ORGANISATIONAL OBJECTIVES

Because risk is 'the effect of uncertainty on organisational objectives', you cannot begin to assess risk until you know exactly what your organisation's objectives are. The first step is to confirm these objectives. They will have been established as part of your business planning or organisational planning processes.

Examples of organisational objectives

- Achieve “A” service outcomes by the end of the year.
- Increase funding from state government to “B” by year end.
- Increase funding from benefactors to “C” by year end.
- Manage staff turnover rates to “D” per annum.
- Reduce client complaints (or adverse outcomes) by “E” by end of year.

Importantly, objectives may change from year to year as the organisation evolves. They may also change in response to developments and opportunities in the external operating environment.

7.2 IDENTIFY STAKEHOLDERS

Part of the context for risk is stakeholders – those with whom your organisation consults, communicates and interacts. Developing a list of stakeholders generally assists in determining what risk information is communicated to whom, and who should be consulted on which risk issues. This process will also help inform your initial and ongoing consultation and communication processes (see 10).

Typical stakeholders in not-for-profit organisations

- Board members
- Staff
- Volunteers
- Clients
- Student placements
- Suppliers
- Funders
- Partners
- Government agencies
- Community members and representatives
- Associations

7.3 DEFINE RISK ASSESSMENT CRITERIA

You need to define criteria against which the significance of a risk can be evaluated. These criteria should reflect your organisation’s objectives, values and resources, and should be consistent with your Risk Management Policy (5.2.4). Some criteria will necessarily be imposed by, or derived from, legal and regulatory requirements and any other requirements your organisation subscribes to.

Factors to consider when defining risk assessment criteria include the following:

- the nature and types of causes and consequences that can occur and how they will be measured
- how ‘likelihood’ will be defined
- the timeframe(s) of the likelihood and/or consequence(s)
- how the level of risk is to be determined
- the views of stakeholders
- the level at which risk becomes acceptable or tolerable
- whether combinations of multiple risks should be taken into account and, if so, how and which combinations should be considered.

Once you’ve defined and documented your organisation’s risk assessment criteria, don’t forget to review them on a regular basis. They may need to be amended or refined as the organisation evolves and/or as the external environment changes.

8 RISK ASSESSMENT (STEP 2)

Having established the context, you can now begin the process of assessing the potential risks to your organisation. There are 3 stages:

- Risk identification
- Risk analysis
- Risk evaluation

These are discussed on the following page in turn.

8.1 RISK IDENTIFICATION (STEP 2.1)

The purpose of this step is to identify all of the risks your organisation may be exposed to, as well as their sources and causes, their potential consequences and areas of impact, and any risk management controls already in place.

As you work through this step, gathering information, enter it into your Risk Register. By the end, you should have a comprehensive list of risks and controls.

It is important that all potential risks are identified in this step. Any risk overlooked here will not be captured in the subsequent analysis and evaluation stages.

There are three tasks:

- Identify categories of risk
- Identify risks
- Identify existing risk management controls

8.1.1 IDENTIFY CATEGORIES OF RISK

Before you attempt to identify specific risks, it helps to identify the categories (or broad areas) in which risks may occur. These categories will guide the more detailed work of identifying specific risks.

You may want to start by focusing on broad areas of internal risk (i.e. risk to the organisation's operational processes) before moving on to areas of external risk (i.e. risk in the environment your organisation operates in).

Examples of *internal* risk categories

- Financial management of the organisation
- Management of human resources
- Regulatory and statutory requirements
- Information management activities and IT systems

Examples of *external* risk categories

- Economic and political change
- Social change
- Changes in the funding and reporting environment
- Legal and compliance changes

You can then list all the identified categories in the Risk Category column in your Risk Register. Examples of risk categories are given in Appendix 4.

8.1.2 IDENTIFY RISKS

Having established the categories of risk, you can now 'zoom in' to identify specific risks within each category. You'll end up with something like the list shown in Appendix 5, which you can enter in the Risk Name/Description column in your Risk Register.

8.1.2.1 HOW TO IDENTIFY RISKS

There are various ways your organisation may wish to approach this. For example:

- by conducting one-on-one interviews with the relevant managers or officers across the organisation
- by running workshops with the relevant managers or officers, facilitated by the Risk Management Coordinator (or relevant officer).

Interviews

If the interview technique is preferred, consider using a Risk Identification Form to record the information elicited (see Appendix 6 for an example). Make sure the interviewees include the people responsible for organisational processes and outcomes in each of the identified risk categories and send forms beforehand to allow interviewees to consider all risks.

Workshops

If the workshop approach is preferred, use the identified risk categories as a framework for discussion. Working through your list of risk categories in order will help discipline the discussion and ensure nothing is overlooked.

Choose an approach (or approaches) to identifying risks that best suits your organisation. Interviews and workshops are not the only possibilities.

Using the 'cause-effect' technique

There are also numerous techniques to help identify risks. A common one is the cause-effect technique. This involves two related questions:

- What could go wrong in this part of the organisation? (potential effect)
- Why might it happen? (potential cause)

Bear in mind that a 'cause' may comprise several contributing factors. Identifying the various contributing factors may provide further insights into other risks and their flow-on effects.

8.1.2.2 HOW TO DESCRIBE RISKS ('RISK STATEMENTS')

A risk, by definition, is a potential for something to happen; a possibility not an actuality. Any event, action or situation that is occurring, is therefore not a risk but a known condition. Consequently the language you use to describe risks should express this element of potentiality or uncertainty. Risk statements should use words like may, might, could. A risk statement that says something will occur, is not describing a risk at all.

Examples of *acceptable, or valid, risk statements*

- 'Failure to effectively manage the organisation's financial resources, which *may* lead to financial loss'
- 'Inadequate compliance systems in place, *possibly* resulting in fines and penalties from the regulator'
- 'Inability to adequately resource programs, with *potential* impact on reputation'

8.1.3 IDENTIFY EXISTING RISK MANAGEMENT CONTROLS

Often an organisation will already have in place operational controls or measures that help manage risk. It is important to identify them. This is because you will generally take such controls into account when you come to evaluate risks (see 8.3). For example, a potential work, health and safety hazard will present a lower level of risk if an organisation has WHS policies and procedures in place.

Record any existing risk management controls you identify in the Controls column of your Risk Register.

Examples of operational and management controls

- Policies
- Procedures
- Work manuals
- Internal audit
- Human resource management system
- Recruitment policies
- Reporting
- IT network use agreement
- WHS management system
- Meetings
- Escalation process
- Budgeting
- Strategic planning process.

This is a guide only. You will need to develop a list of risk management controls specific to your organisation.

8.2 RISK ANALYSIS (STEP 2.2)

Having identified the potential risks to your organisation, for each risk you now need to determine the likelihood of its occurring, the consequences should it occur, and any other attributes of the risk that may be informative for analytical purposes.

The stages are:

- Define risk consequence and likelihood criteria
- Assess risks against the consequence and likelihood criteria
- Develop a risk matrix
- Determine risk levels and scores using the risk matrix
- Develop a risk profile
- Assign risk ownership

8.2.1 DEFINE RISK CONSEQUENCE AND LIKELIHOOD CRITERIA

To be in a position to evaluate the level of threat or opportunity a risk presents, you will need to know (a) how serious the consequences of the risk would be, and (b) how likely it is that the risk will happen.

First, then, you need to define criteria for this: risk consequence criteria and risk likelihood criteria.

You may wish to workshop this process. However you approach it, the consequence and likelihood criteria will need to reflect:

- the organisation's size, culture, values, objectives and activities
- the organisation's overarching risk assessment criteria (see 7.3)
- any risk management controls already in place (see 8.1.3).

8.2.1.1 RISK CONSEQUENCE CRITERIA

These criteria define the types and levels of impact a risk may have on your organisation. They answer the question 'How would the organisation be affected if risk x eventuates?'

Types of potential impacts include financial, reputation, work health and safety, legal, etc. (see table in Appendix 7).

Levels of impact may range from insignificant to critical (see table in Appendix 7). For small organisations, three levels of impact may suffice – high, medium, and low.

Note that a single risk may have multiple consequences and affect multiple organisational objectives.

8.2.1.2 RISK LIKELIHOOD CRITERIA

These criteria define levels of likelihood around a risk event occurring. They answer the question 'How likely is it that the organisation will be exposed to risk x?'

Typically, organisations adopt five levels of likelihood, and for each level they provide descriptors and an estimate of probability (see table in Appendix 8).

8.2.2 ASSESS RISKS AGAINST THE CONSEQUENCE AND LIKELIHOOD CRITERIA

Having established the criteria, you can now assess the risks identified earlier (see 8.1.2) against these criteria. In doing so, take into account the following points:

- The context of the risk. If a risk has a financial impact, assess it against the financial criteria

in the risk consequence table. If it has a work health and safety impact, assess it against the work health and safety criteria and so on. Bear in mind that some risks may have impacts across multiple criteria.

- Any risk management controls already in place.

As you assess each risk, enter your assessment in the Consequence and Likelihood columns in the Risk Register.

8.2.3 DEVELOP A RISK MATRIX

The next step is to rate each risk by determining its level and score. You do this using a risk matrix (Diagram 3).

The risk matrix lets you rate a risk based on its consequences and likelihood (assessed in the previous step). The matrix is constructed using the five levels of likelihood and the five levels of consequence, and contains the following four levels of risk:

| | |
|---------|--|
| EXTREME | |
| HIGH | |
| MEDIUM | |
| LOW | |

³ IEC/ISO 31010:2009 Risk management – Risk assessment techniques

DIAGRAM 3: EXAMPLE RISK MATRIX

| | | | | | | |
|------------|---------------------|--------------------|------------|---------------|------------|---------------|
| LIKELIHOOD | ALMOST CERTAIN 5 | Yellow | Yellow | Orange | Red | Dark Red |
| | LIKELY 4 | Green | Yellow | Orange | Red | Dark Red |
| | POSSIBLE 3 | Green | Yellow | Orange | Red | Dark Red |
| | UNLIKELY 2 | Green | Green | Yellow | Orange | Red |
| | RARE | Green | Green | Green | Yellow | Orange |
| | | INSIGNIFICANT 1 | MINOR 2 | MODERATE 3 | MAJOR 4 | CRITICAL 5 |
| | | CONSEQUENCE | | | | |

This is a guide only. You will need to develop a risk matrix to suit your organisation. As noted above, small organisations may need only three levels of consequence: high, medium, low.

8.2.4 DETERMINE RISK LEVELS AND SCORES USING THE RISK MATRIX

Using the risk matrix, you can now assign each risk a level and score. You do this by plotting the risk's 'consequence' against its 'likelihood'.

For example: if a risk is 'moderate' (consequence) and 'unlikely' (likelihood), its risk level will be 'medium'.

In addition, it will have a score of 6:

- 3 (for consequence) x 2 (for likelihood) = 6

Remember that an otherwise significant risk may have a 'low' risk level and score because effective controls are in place to manage it.

8.2.5 DEVELOP A RISK PROFILE

You can develop a risk profile for your organisation by plotting all the risks into the risk matrix.

This requires some time, so you may choose not to do it. However, developing a risk profile and then comparing it against a risk review carried out after risk treatment plans have been developed (see 9) can be a useful method for demonstrating the effectiveness of risk management activities. This information can then be communicated to stakeholders such as the Board.

8.2.6 ASSIGN RISK OWNERSHIP

As each risk is assessed, assign the risk to an owner who will be responsible for managing it. Risk owners are usually senior managers or staff who have authority to manage risks and to allocate resources for risk treatment actions (see 9).

Assigning ownership to risks is an important element in integrating risk management into the organisation. Risk ownership improves accountability for managing risks within acceptable, or valid, levels of tolerance (see 4.0) and for escalating any risks deemed unacceptable (see 8.3.3).

8.3 RISK EVALUATION (STEP 2.3)

The purpose of this step is to list risks in order of priority for action. The list will show which risks need treatment and which don't; and of those requiring treatment, which are the most urgent. There are three stages:

- Develop escalation and retention guidelines
- Evaluate risks
- Escalate risks

8.3.1 DEVELOP ESCALATION AND RETENTION GUIDELINES

Begin by developing some guidelines for the actions to be taken for each risk level. This step is about prioritising risks to be addressed. Actions may range from risk retention (i.e. monitoring the situation) to escalation. (see the table in Appendix 9 for an example).

8.3.2 EVALUATE RISKS

To evaluate a risk, compare its risk level and score (see 8.2.4) against the organisation's risk tolerance and appetite (see 4.0).

8.3.3 ESCALATE RISKS

Compare each evaluated risk to your escalation and retention guidelines. Escalate accordingly.

9 RISK TREATMENT (STEP 3)

The purpose of this step is to identify and implement the most appropriate means to mitigate risks deemed to be at an unacceptable level. These risk treatments, in effect, will become new risk management controls or will augment existing controls.

There are four stages:

- Identify risk treatment options
- Select the most suitable risk treatment option(s)
- Develop risk treatment plans
- Implement and review risk treatments

9.1 IDENTIFY RISK TREATMENT OPTIONS

The options for risk treatment may include:

- avoiding the risk by not starting or carrying on the activity that gives rise to it, or by changing how the activity is undertaken
- removing the source or cause of the risk
- reducing the likelihood of the risk's occurring
- limiting or minimising the consequences of the risk should it occur
- sharing the risk with another party or parties (i.e. insurance, contracts, partnering)
- retaining the risk by informed decision and approval of the Board or senior management.

These are just some options. They are not necessarily mutually exclusive. They may not be appropriate in all circumstances.

9.2 SELECT THE MOST SUITABLE RISK TREATMENT OPTION(S)

To choose the most suitable risk treatment option (or options), you need to weigh the costs of implementing a treatment against the benefits it is likely to deliver. Issues to consider include:

- the financial and other resources required to implement the treatment
- the feasibility (including timing) of implementing the treatment
- how effective the treatment is likely to be in reducing or removing the risk
- the potential impact of the treatment on

stakeholders' values, perceptions and interests – some treatments may be more acceptable to stakeholders than others

- whether the treatment will compromise or be in conflict with any legal, regulatory or other obligations your organisation has
- possible unintended consequences of the treatment – risk treatments themselves may affect other existing risks, or may introduce new risks (known as secondary risks)
- the failure or ineffectiveness of a risk treatment is itself a risk.

Organisations often benefit from adopting a combination of treatment options.

9.3 DEVELOP RISK TREATMENT PLANS

Risk treatment plans are where you document how the selected treatment option(s) will be implemented. These plans should then be integrated into your organisation's processes and activities and discussed with appropriate stakeholders.

The kind of information to include in a risk treatment plan is shown in Appendix 10 (which includes both a blank template and a completed example). At a minimum, the following information is required:

- the name of the treatment plan
- the risk(s) the plan is intended to mitigate
- the plan's objectives
- the proposed actions
- the name(s) of the person(s) accountable for the plan's development and execution
- the risk owner
- resource requirements including time, costs and other inputs
- performance measures and monitoring of progress made (weekly, monthly or quarterly)
- timing and scheduling.

You may wish to include additional information such as:

- the priority of the plan (vis-à-vis any other risk treatment plans)

- secondary risks that may arise from the treatment (see 9.4) – the link with secondary risks should be maintained
- (if the plan includes more than one treatment option) the order in which risk treatment options should be implemented.

9.4 IMPLEMENT AND REVIEW RISK TREATMENTS

The implementation of a risk treatment may have varying degrees of success. It may lessen the risk, remove the risk entirely, or have no effect at all. It may also lead to secondary risks. It's therefore important to monitor and review treatments.

In summary, implementing and reviewing risk treatments is a cyclical process of:

- implementing the risk treatment
- assessing its effectiveness
- deciding whether any remaining risk (known as residual risk) is at a tolerable level
- (if it is not tolerable) implementing a new risk treatment
- assessing the effectiveness of that treatment.

After implementing a risk treatment, you should also re-assess and re-rate the risk, but now with the treatment in place. The treatment, in other words, has become a new risk management control.

10 COMMUNICATION AND CONSULTATION (ONGOING PROCESS)

In all steps of the Risk Management Process you should ensure that the appropriate stakeholders (external and internal) are consulted and/or informed about what's going on. You should therefore develop plans and mechanisms for doing this at an early stage.

10.1 COMMUNICATION

Effective communication (e.g. reports) will ensure that those responsible for implementing the Process, as well as other relevant stakeholders,

understand the basis on which decisions are made and the reasons why particular actions are required. It will also support and encourage accountability for ownership of risks.

10.1.1 WHO SHOULD BE INFORMED?

A useful guide as to who should be informed, and what aspects of risk and risk management they should be informed about, is the list of stakeholders identified in Step 1 Establishing the context (see 7.2).

Internal stakeholders

The Board needs to be fully informed of the outcomes of risk assessments and risk reviews. In particular, they must be informed of risks at levels beyond the acceptable or tolerable. Staff and managers need to be informed of the outcomes of risk assessments and risk reviews so they can manage risks appropriately and in accordance with risk management policy.

External stakeholders

There may be certain risk information you are required to communicate to external stakeholders due to statutory and governance obligations. Besides that, you should think carefully about what you choose to communicate. For example, it is unlikely that you would inform potential suppliers about individual risks or your Risk Register. However, you may decide to inform them that you have a Risk Management Policy and Framework to manage risks, because this information may assist in negotiating favourable terms or conditions for the procurement of goods and services.

10.2 CONSULTATION

A consultative approach will yield more successful outcomes by helping to engage managers and staff in the Risk Management Process and to integrate risk management into the organisation. For example, it will:

- help establish the context appropriately
- ensure the interests of stakeholders are understood and considered
- help ensure that risk categories and risks are

adequately identified

- bring together different areas of expertise for analysing risks
- ensure that different views are considered when defining risk criteria and evaluating risks
- secure endorsement and support for treatment plans
- enhance appropriate change management during the Risk Management Process
- develop an appropriate external and internal communication and consultation plan.

10.2.1 WHO SHOULD BE CONSULTED?

A useful guide as to who should be consulted, and on what areas of risk management they should be consulted, is the list of stakeholders identified in Step 1 Establishing the context (see 7.2).

Senior managers or officers are usually involved in identifying, assessing and managing risks, so they should be consulted. In particular, ensure that those responsible for the organisational processes and outcomes in each risk category (see 8.1.1) are consulted. Consultation can be done through one-on-one interviews, group workshops or other methods (see 8.1.2.1).

11.1 ESTABLISH FORMAL REVIEW AND REPORTING MECHANISMS

As well as conducting ongoing monitoring activities, we recommend you set up formal review and reporting mechanisms. These mechanisms are a requirement of good governance, provide the management team with regular and up-to-date information on risks, risk treatment plans and any issues arising, and assure the Board that risks are being managed in line with the Risk Management Policy and Framework.

Formal review and reporting mechanisms would look something like this:

- On an annual basis (typically), review your organisation's Risk Management Policy and Framework, risk assessment criteria, and the Risk Management Process and its integration and alignment with other organisational processes.
- On a monthly or quarterly basis (or whatever the Board meeting cycle is), report to the Board with an update on the Risk Register and risk treatment plans (particularly for 'extreme' and 'high' risks).
- On a monthly basis (or whatever the management/senior staff meeting cycle is), review risks and risk treatment plans.

11 MONITOR AND REVIEW (ONGOING PROCESS)

Risk management must be responsive to change – both within the organisation and in the external environment. Therefore, the activities of monitoring and reviewing must be ongoing, and are integral to every step in the Risk Management Process.

By monitoring risks, controls and risk treatment plans, you can ensure that risks are being managed in accordance with your organisation's Risk Management Policy and Framework. You can also determine the effectiveness (impacts, benefits and costs) of your risk management strategies. Monitoring is therefore part of the continual improvement process and will enhance organisational value.

PART C

EXAMPLES, TOOLS & TEMPLATES

APPENDIX 1

EXAMPLE RISK MANAGEMENT POLICY

OVERVIEW

(Name of not-for-profit organisation) recognises that the organisation is exposed to certain risks due to the nature of its activities and the environment in which it operates. The key to (Name of not-for-profit)'s success is the effective management of risk to ensure its organisational objectives are achieved.

Risks arise due to the organisation's operational undertakings and from external sources. Risks occur in numerous ways and have the potential to impact financial performance, reputation, health and safety, community and the overall performance of the organisation.

POLICY

In order to fully understand such risks, (Name of not-for-profit) has established a Risk Management Policy which provides the framework for how risk will be managed within the organisation. The Risk Management Policy is based on the Australian Standard, AS/NZS ISO 31000:2009 Risk management – Principles and guidelines, and forms part of the governance framework of the organisation. It also integrates with the strategic planning process. The Policy addresses both strategic and operational risks.

We will use our skills and expertise to identify risks across the organisation. (Name of not-for-profit) will also identify operational controls in place which manage risk.

We will assess the size or degree of risk by taking into consideration the potential impact to our operations. Risks will be ranked in a common and consistent manner and a Risk Register will be maintained containing material risks to the organisation.

Risk treatment actions and plans will be developed for risks which are unacceptable to the organisation. Risks, and the effectiveness of the risk management system will be monitored on a regular basis and we will communicate and consult with relevant stakeholders on our approach to managing risk.

RISK TOLERANCE

Our tolerance for adverse risks will be used to determine which risks are treated through the development of risk treatment actions to manage risks to an acceptable level. During this process we will consider additional control measures to manage the risks to acceptable levels.

INTEGRATION WITH GOVERNANCE AND STRATEGIC PLANNING

The Risk Management Policy forms part of the governance framework and integrates with the strategic planning process. The Policy addresses both strategic and operational risks and the requirement of the organisation to operate in its regulatory environment.

ACCOUNTABILITY

Ownership of risks and risk treatment actions will be assigned to relevant roles within the organisation. (Name of not-for-profit) has incorporated risk management accountability in executive, management and supervisory roles which are required to report on risks and risk treatment actions.



RISK MANAGEMENT OVERSIGHT

(Name of not-for-profit)'s Audit and Risk Committee (or Board if the organisation does not have an Audit and Risk Committee) will oversee the Risk Management Policy and the organisation's exposure to risk. Oversight of the effectiveness of our risk management processes and activities will provide assurance to the Board and stakeholders and will support our commitment to continuous organisational improvement.

REPORTING, MONITORING AND REVIEW

(Name of not-for-profit) will monitor risks and treatment actions on an ongoing basis. Performance of the risk management system and outstanding risk treatment actions will be reported to the Audit and Risk Committee (or Board if the organisation does not have an Audit and Risk Committee) on a regular basis. Formal reviews of both the risk management system and the Risk Register will take place on an annual basis and the Board will assess the effectiveness of the Risk Management Policy annually.

COMMUNICATION AND CONSULTATION

(Name of not-for-profit) will communicate and consult with its stakeholders (internal and external) on its approach to risk management.

(Name)

Chief Executive Officer / Chair / Managing Director

(Date established)

(Date for review)

APPENDIX 2 – RISK REGISTER TEMPLATE AND EXAMPLES

RISK REGISTER

| RISK NO. | RISK CATEGORY | RISK NAME/DESCRIPTION | CONTROLS | CONSEQUENCE | LIKELIHOOD | RISK RATING LEVEL | RISK SCORE | RISK OWNER |
|----------|---------------|-----------------------|----------|-------------|------------|-------------------|------------|------------|
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

RISK REGISTER (CONTINUED)

| TREATMENT NO. | RISK(S) TREATED | TREATMENT PLAN (REFER DETAILED PLANS) | RESIDUAL CONSEQUENCE | RESIDUAL LIKELIHOOD | RESIDUAL RISK RATING/ LEVEL | RESIDUAL RISK SCORE | ADDITIONAL ACTION |
|---------------|-----------------|---------------------------------------|----------------------|---------------------|-----------------------------|---------------------|-------------------|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |



EXAMPLES

RISK REGISTER

| RISK NO. | RISK CATEGORY | RISK NAME/DESCRIPTION | CONTROLS | CONSEQUENCE | LIKELIHOOD | RISK RATING LEVEL | RISK SCORE | RISK OWNER |
|----------|-----------------------|---|--|-------------|------------|-------------------|------------|-------------------------|
| 5 | Legal/ Commercial | Failure to adequately report to the regulator resulting in potential fines and penalties | Governance framework Reporting Policies and procedures | Major | Possible | High | 12 | Chief Executive Officer |
| 2 | Financial/ funding | Inability to raise adequate funding resulting in the potential impact on program delivery | Funding process Grants Financial control | Moderate | Possible | High | 9 | Chief Financial Officer |
| 10 | Human resources | Inability to adequately implement (human) resource programs with possible program delays and impact on reputation | HR process Retention policy Remuneration policy | Moderate | Unlikely | Medium | 6 | Human Resources Manager |
| 4 | Health & Safety | Failure of staff to follow procedures resulting in potential injury and health & safety incident | Health & Safety policy Health & Safety Procedures Training Internal Health & Safety Reviews | Moderate | Unlikely | Medium | 6 | Health & Safety Officer |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

NOTE: THE RISKS ARE ASSESSED WITH THE EXISTING CONTROLS IN PLACE TO MANAGE THE RISKS.

RISK REGISTER (CONTINUED)

| TREATMENT NO. | RISK(S) TREATED | TREATMENT PLAN (REFER DETAILED PLANS) | RESIDUAL CONSEQUENCE | RESIDUAL LIKELIHOOD | RESIDUAL RISK RATING/ LEVEL | RESIDUAL RISK SCORE | ADDITIONAL ACTION |
|---------------|-----------------|---|----------------------|---------------------|-----------------------------|---------------------|---|
| 1 | 5 | Review and strengthen the reporting system and include in the audit process | Major | Unlikely | Medium | 8 | |
| 2 | 2 | Develop stronger communication structures with state government agencies and enhance existing relationships | Moderate | Unlikely | Medium | 6 | Report monthly on relationship outcomes |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

NOTE: THE RISKS ARE RE-ASSESSED AFTER THE RISK TREATMENT PLANS HAVE BEEN DEVELOPED AND IMPLEMENTED.

APPENDIX 3

CHECKLIST FOR DEVELOPING THE RISK REGISTER

The following checklist has been prepared to assist in the development of your Risk Register. It contains key questions to be asked, and shows how various components of the Risk Register link together.

| Communication and consultation (10) | STEP | KEY CONCERNS | Monitor and review (11) |
|---|----------------------------------|--|---|
| <p>– ongoing process</p> <ul style="list-style-type: none"> • Has consideration been given to maintaining communication throughout the entire Risk Management Process? • Have stakeholders been identified? • Have decisions been made to communicate what and to whom? • Has a reporting and communication process been established? <p>Linkages: Risk Management Framework</p> | 1 Establishing the context (7.0) | <ul style="list-style-type: none"> • Have the organisation's objectives been taken into account? • Have stakeholders been identified? • Have the risk criteria been defined? • Have the risk assessment criteria been defined? | <p>– ongoing process</p> <ul style="list-style-type: none"> • Have the established procedures been followed? • Is there a requirement to escalate or de-escalate risks to the next level? <p>Linkages: Risk Management Framework</p> |
| | 2 Risk assessment (8.0) | <ul style="list-style-type: none"> • What can go wrong, when and how? • What is the potential cost to time, money and performance? • How likely is it to happen? • What are the impacts of each risk? • What is the source of the risk? • What can be done to reduce/control the risk? | |
| | 2.2 Risk analysis (8.2) | <ul style="list-style-type: none"> • Are there any existing controls? • Have the consequences of the risk been considered? • Has the likelihood criteria been applied? • Has a risk matrix been developed? | |
| | 2.3 Risk evaluation (8.3) | <ul style="list-style-type: none"> • Have the risks been compared against the set criteria? • Have escalation and retention guidelines been developed? • Has a decision been made to treat the risks? • If yes, go to Step 3. • If no, continue to monitor and review the risks. | |
| | 3 Risk treatment (9) | <ul style="list-style-type: none"> • Have all treatment options been identified? • Have all options been assessed? • Have treatment plans been prepared and are they ready for implementation? • Have residual risks been analysed and evaluated? • Consider communication and consultation requirements. | |

APPENDIX 4 EXAMPLES OF RISK CATEGORIES

| RISK CATEGORY |
|-----------------------------------|
| Compliance/ statutory |
| Legal/ commercial |
| Political/ economic |
| Financial/ funding |
| Management |
| Operational |
| Service delivery |
| Work Health and Safety |
| Human resources |
| Stakeholders (clients/ suppliers) |
| IT/ information management |
| Security |
| Reputational |

This is a guide only. You will need to develop risk categories specific to your organisation. You can also choose whether to arrange your categories alphabetically, in order of importance, or in some other way.

APPENDIX 5 EXAMPLES OF RISK DESCRIPTIONS

| RISK CATEGORY | RISK NAME/DESCRIPTION |
|------------------------------------|---|
| Compliance / statutory | Inadequate compliance systems in place which may result in fines and penalties from the regulator |
| Legal / commercial | Breach of contract resulting in potential fines or litigation |
| Political / economic | Changes in the political landscape resulting in possible loss of funding |
| Financial / funding | Failure to effectively manage the financial resources of the organisation which may result in financial loss |
| Management | Poor management systems resulting in duplication and potential loss of productivity |
| Operational | Disruption to day-to-day activities due to systems or process failure resulting in potential loss of productivity |
| Service delivery | Reduced quality of service delivery resulting in potential loss of reputation |
| Work Health and Safety | Failure of staff to follow procedures resulting in potential injury and health and safety incident |
| Human resources | Inability to adequately resource programs with possible program delays and loss of reputation |
| Stakeholders (clients / suppliers) | Financial failure of key supplier resulting in potential impact to delivery of services |
| IT / information management | Loss of digital records through inadequate IT systems resulting in potential loss of reputation and / or loss of productivity |
| Security | Breach of security due to failure to follow procedures resulting in potential theft/or loss of assets |
| Reputational | Adverse media attention and/or heightened concern of local community |

You don't need to 'fill' each category with risks. Some categories might be empty. Also, the number of risks in a category is likely to change over time.

APPENDIX 6

RISK IDENTIFICATION FORM

| | | | |
|------|--|-----------|--|
| Date | | Reference | |
|------|--|-----------|--|

| | | | |
|---------------|--|--------------------|--|
| Risk Category | | Person Responsible | |
|---------------|--|--------------------|--|

| Risk Name or Description | | | |
|--------------------------|--|--|--|
| | | | |
| | | | |
| | | | |

| Contributing Factors (Causes) | Outcomes (Consequences) |
|-------------------------------|-------------------------|
| | |
| | |
| | |
| | |
| | |

| Controls | |
|----------|--|
| | |
| | |
| | |
| | |
| | |
| | |
| | |

APPENDIX 7

EXAMPLE RISK CONSEQUENCE CRITERIA

| RISK NO. | RISK CATEGORY | RISK NAME/ DESCRIPTION | CONTROLS | CONSEQUENCE | LIKELIHOOD |
|-------------------|---|--|--|--|---|
| SEVERITY LEVEL | Financial | Management Effort | Work Health & Safety | Reputation/ community | Legal/ Compliance |
| CRITICAL (5) | Loss, error or omission >15% of annual budget or projected revenue | An event so severe in nature it could lead to a significant restructure of the organisation or its major parts or a change in the management structure | Fatality and/or severe irreversible disability (>30%) to one or more persons or permanent disabling injury or disabling illness to one or more persons | Ongoing serious public or media outcry (state or national coverage) | Significant prosecution and fines, very serious litigation |
| MAJOR (4) | Loss, error or omission 10% - 15% of annual budget or projected revenue | An event, which with proper management can be endured, may involve some changes in management, additional resources required | Series of significant but reversible disabilities requiring hospitalisation | Serious public or media outcry (local coverage) | Major breach of regulation, prosecution or major litigation |
| MODERATE (3) | Loss, error or omission 5% - 10% of annual budget or projected revenue | An event that can be managed under normal circumstances, additional resources required, potential reallocation of resources | Significant but reversible disability requiring hospital visit | Heightened and/or significant adverse media attention | Breach of regulation with investigation or report to authority with prosecution and/or moderate fine possible |
| MINOR (2) | Loss, error or omission 1% - 5% of annual budget or projected revenue | An event, where the consequences can be absorbed but management effort is required to minimise the impact, potential reallocation of resources | First aid treatment required | Adverse media attention and/or heightened concern of local community | Minor legal issues, non-compliances and breaches or regulations |
| INSIGNIFICANT (1) | Loss, error or omission up to 1% of annual budget or projected revenue | An event, where the impact can be absorbed through business as usual activity | Minor incident not requiring first aid | Minor local adverse public attention or complaints | Minor compliance issue |

This is a guide only, drawing on common examples. You will need to define risk consequence criteria specific to your organisation.

APPENDIX 8

EXAMPLE RISK LIKELIHOOD CRITERIA

| LIKELIHOOD | | |
|--------------------|---|--------------|
| LIKELIHOOD LEVEL | DESCRIPTION | PROBABILITY |
| Almost Certain (5) | Is expected to occur in most circumstances – frequently during the year | > 95% - 100% |
| Likely (4) | Will probably occur – once during the year | 70% - 95% |
| Possible (3) | Might occur at some time – once every 3 years | 30% - 70% |
| Unlikely (2) | Could occur at some time – once every 5 years | 5% - 30% |
| Rare (1) | May occur only in exceptional circumstances. This event is known to have occurred elsewhere – once every 5+ years | <5% |

This is a guide only. You will need to define risk likelihood criteria specific to your organisation.

APPENDIX 9

EXAMPLE ESCALATION AND RETENTION GUIDELINES

| RISK LEVEL | RISK TREATMENT GUIDELINES | ESCALATION AND RETENTION GUIDELINES |
|------------|--|---|
| EXTREME | Immediate action required to actively manage risk and limit exposure | Escalate to the Board, risks generally not accepted or retained |
| HIGH | Cost/benefit analysis required to assess extent to which risk should be treated - monitor to ensure risk does not adversely change over time | Escalate to Head of Agency, risks generally not accepted or retained |
| MEDIUM | Constant/regular monitoring required to ensure risk exposure is managed effectively, disruptions minimised and outcomes monitored | Escalate to relevant senior officer or senior management level, specify risk management actions, risks may generally be retained and managed at operational level |
| LOW | Effectively manage through routine procedures and appropriate internal controls | Monitor and manage at the relevant officer, or operational level, risks generally retained |

This is a guide only. You will need to develop guidelines to suit the structure of your organisation and the relevant levels of responsibility as identified by your own organisation.

APPENDIX 10

RISK TREATMENT PLAN TEMPLATE AND EXAMPLE

RISK TREATMENT PLAN

| | | | |
|-----------------------|--|----------------|--|
| RISK #: | | PLAN REF #: | |
| RISK NAME: | | DATE LOGGED: | |
| COMPILED BY: | | REVIEW DATE: | |
| TREATMENT PLAN OWNER: | | TARGET DATE: | |
| REVIEWER: | | PRIORITY H/M/L | |

| | |
|------------------------|--|
| TREATMENT PLAN: | |
|------------------------|--|

| | |
|--|--|
| Treatment Plan Objective(s): | |
| 1 Proposed actions: | |
| 2 Resources required: | |
| 3 Responsibilities: | |
| 4 Timing for implementation: | |
| 5 Monitoring requirements (i.e. weekly/monthly): | |

EXAMPLE RISK TREATMENT PLAN

| | | | |
|-----------------------|--|----------------|----------------|
| RISK #: | 5 | PLAN REF #: | 1 |
| RISK NAME: | Failure to adequately report to the regulator resulting in potential fines and penalties | DATE LOGGED: | June 2012 |
| COMPILED BY: | Financial Controller | REVIEW DATE: | July 2012 |
| TREATMENT PLAN OWNER: | Financial Controller | TARGET DATE: | September 2012 |
| REVIEWER: | Chief Executive Officer | PRIORITY H/M/L | H |

| | |
|------------------------|---|
| TREATMENT PLAN: | Review and strengthen the reporting system and include in the audit process |
|------------------------|---|

| | |
|--|---|
| Treatment Plan Objective(s): | To reduce the potential threat of fines and penalties arising from the risk of failure to adequately report in a timely manner |
| 1 Proposed actions: | <ul style="list-style-type: none"> • Review existing process • Review reporting mechanism • Develop draft change to process • Obtain CEO approval for revised process • Implement new reporting system |
| 2 Resources required: | <ul style="list-style-type: none"> • Time (approximately 15 working days) • No additional financial resources required – part of management time |
| 3 Responsibilities: | Financial Controller reporting to the Chief Executive Officer |
| 4 Timing for implementation: | Three months |
| 5 Monitoring requirements (i.e. weekly/monthly): | Monitor progress on risk treatment plan monthly as part of the existing management process |