NSW GOVERNMENT | The Treasury

Risk Management Toolkit for NSW Public Sector Agencies

Volume 1: Guidance for Agencies

Policy & Guidelines

TPP12-03b

August 2012 © Crown Copyright 2012
NSW Treasury
ISBN 978-0-7313-3568-8

General inquiries concerning this document should be initially directed to the Financial Management and Accounting Policy Branch of NSW Treasury.

This publication can be accessed from the NSW Treasury website: www.treasury.nsw.gov.au.
NSW Treasury reference: TPP12-03b

Preface

In a globally connected world, both the types and magnitude of risk we face are increasing, while our tolerance for ineffective risk management is diminishing. Simply put, many more things can go wrong and with more far-reaching consequences. At the same time, the community increasingly expects public sector agencies to manage these risks to minimise any negative consequences. But increased uncertainty in the world today can also offer possibilities. Recognising and responding to opportunities, as well as effectively managing for things that could go wrong, will not only support the success of your agency in meeting its objectives but also ensure that your agency remains relevant and resilient into the future.

Effective risk management is a core requirement for all NSW public sector departments and statutory bodies under the Internal Audit and Risk Management Policy for the NSW Public Sector (TPP 09-05). Core Requirement 5 of TPP 09-05 requires agencies to 'implement a risk management process that is appropriate to the needs of the department or statutory body and consistent with the current risk standard'.

NSW Treasury has developed this *Risk Management Toolkit for NSW Public Sector Agencies* (the Toolkit) to provide a comprehensive reference to the current international risk management standard, ISO 31000. It contains guidelines, templates and a case study based on a hypothetical agency. It may be particularly useful for those agencies that are just embarking on the risk management journey.

The Toolkit consists of two volumes:

- Volume 1 – Guidance for Agencies (this volume)
- Volume 2 – Templates, examples and case study.

These two volumes are complemented by an Executive Guide which provides a navigation aid to the detailed guidance in the Toolkit.

The Toolkit has been developed in consultation with agency representatives from across the NSW public sector as well as Audit and Risk Committee members. The toolkit also draws on the standards developed and endorsed by professional associations and the policies and practices of exemplar public sector organisations.

The toolkit is not prescriptive. These guidelines will help agencies design and implement a risk management framework and process that is customised for their circumstances.

I encourage departments and statutory bodies to familiarise themselves with the content of this toolkit and integrate these guidelines and templates into their management systems as appropriate.

Philip Gaetjens
Secretary
NSW Treasury

Treasury Ref: **TPP12-03b**
ISBN: **978-0-7313-3568-8**

Acknowledgements

A number of organisations and individuals have contributed content and expert advice to developing this toolkit, including:

Suncorp Risk Services

NSW Self Insurance Corporation

Public Sector Risk Management Association

Treasury's Internal Audit and Risk Management Policy Reference Group

Audit and Risk Committee Independent Members and Chairs discussion forum

Risk Management professionals from:

- Department of Education
- Ministry of Health
- Department of Attorney General and Justice
- Sydney Ports
- Internal Audit Bureau

Contents

Risk Management Toolkit for the NSW Public Sector

Chapter 1 – Introduction

All public sector agencies are concerned with successfully delivering their objectives. The effect of uncertainty in achieving objectives is known as risk. Risk is inherent and unavoidable in all activities. All agencies must take action to manage their risks.

To manage risk, an agency must create an environment where informed decisions about the risks affecting its activities – including delivering on policy initiatives and objectives – can be made in an open and transparent manner. It is this principle that underpins Core Requirement 5 of NSW Treasury Policy Paper 09-05 *Internal Audit and Risk Management Policy for the NSW Public Sector*. Core Requirement 5 requires departments and statutory bodies to establish and maintain an appropriate risk management process. The risk management process should be consistent with the current Australian and New Zealand standard on risk management.

1.1 The current risk management standard

In 2009, the International Organization for Standardization (ISO) released ISO 31000:2009 *Risk Management – Principles and Guidelines*. Standards Australia has adopted this standard, which it has titled 'AS/NZS ISO 31000:2009 (ISO 31000)'. ISO 31000 describes a generic approach for managing any form of risk in a systematic, transparent and credible manner, and within any scope and context.[1] This standard forms the basis of, and is continually referred to in, this toolkit. ISO 31000:

- establishes a generic set of principles that organisations need to satisfy to manage risk effectively
- lists the benefits to organisations of adopting a consistent, systematic and integrated approach to managing risk
- sets out the concepts that organisations should adopt in designing and implementing a risk management framework
- emphasises that the process of managing risk should be integrated into an organisation by creating and continuously improving a risk management framework.

ISO 31000 is a set of principles and guidelines rather than a compliance standard. How your agency applies ISO 31000 will depend on its size, nature, complexity and objectives, and your agency's maturity in risk management. ISO 31000 supersedes AS/NZS 4360:2004 Risk Management. It builds upon the process described in the latter standard and includes more guidance on implementing and integrating risk management into organisational systems, processes and activities by designing and continuously improving a risk management framework. It is important to note that if your agency has existing risk management processes in place, there is no need to 'reinvent the wheel'. Instead, use this toolkit to benchmark your risk management practices, and improve and align them with ISO 31000.

[1] Standards Australia AS/NZS ISO 31000:2009 Risk management – Principles and guidelines.

1.2 What is the purpose of this toolkit?

This toolkit was developed to help agencies interpret ISO 31000. It is intended to support the ongoing development of a risk management framework that suits agencies' specific organisational needs. The risk management framework should be integrated with an agency's other management systems and processes.

The purpose of this toolkit is to help NSW public sector agencies answer the question:

'How should my agency interpret ISO 31000 to develop and implement a risk management framework that is consistent with this standard?'

The aim of this toolkit is not to prescribe an approach but provide advice on how an agency might achieve consistency with ISO 31000. It should be read in conjunction with ISO 31000 and other related risk management standards.

The risk management concepts in this toolkit can be applied at the strategic, divisional, operational and project levels within agencies. The guidance it contains recognises that agencies differ greatly in size and complexity and in the nature of the services they deliver.

It also recognises that agencies have different levels of maturity in their approach to managing risk, and that while some have developed comprehensive risk management frameworks, others are yet to do so.

Volume 1 of this toolkit contains guidance to help agencies develop and implement a risk management framework and process. Volume 2 contains templates and a case study with examples to help agencies implement ISO 31000.

1.3 Who is the target audience for this toolkit?

This toolkit is targeted at a wide set of stakeholders. It is intended for use by:

- the Head of the Authority who is responsible for internal controls, risk management and establishing the right organisational culture with regard to risk management
- senior executive and operational management teams responsible for managing risks
- the Chief Risk Officer or equivalent who is responsible for embedding, coordinating and maintaining risk management in an agency
- staff members engaged to undertake training and development regarding risk management in their agency
- staff members engaged to review the efficacy of risk management arrangements
- other stakeholders, such as the Audit and Risk Committee and Internal Audit.

The way that an agency assigns specific responsibility for its risk management activities will depend on its structure, risk management needs and risk management maturity. This toolkit refers to the person or persons with these specific responsibilities as 'you' rather than prescribing a specific position within the agency. It is recognised that in many instances, this position will be held by the Chief Risk Officer or coordinator within an agency.

1.4 Risk management glossary

ISO Guide 73:2009 Risk Management – Vocabulary (Guide 73) sets out a generic glossary to help develop a common understanding of risk management concepts and terms. The ISO released this guide and ISO 31000 concurrently, so the definitions in ISO Guide 73 are used in ISO 31000. While you should refer to ISO Guide 73 for a full list of terms, these terms are more fully explained throughout this toolkit. Some of the key terms used in ISO Guide 73 and their definitions are set out in Table 1.1 below.

Table 1.1 – Key risk management terms

Term	Definition
Consequence	The outcome of an event affecting objectives
Control	A measure (including a process, policy, device, practice or other action) that is modifying risk
Event	An occurrence or change of a particular set of circumstances
Level of a risk	The magnitude of a risk or combination of risks, expressed as a combination of consequences and their likelihoods
Likelihood	The chance of something happening
Risk	The effect of uncertainty on objectives
Risk acceptance	An informed decision to take on a particular risk
Risk assessment	The overall process of risk identification, risk analysis and risk evaluation
Risk description	A structured statement of risk containing the following elements: source, events, causes and consequences
Risk identification	The process of finding, recognising and describing risks in terms of the source, event, cause and potential consequence
Risk management	Coordinated activities to direct and control an organisation with regard to risk
Risk management framework	The set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout an organisation
Risk management policy	A statement of the overall intentions and direction of an organisation in regard to risk management
Risk management process	The systematic application of risk management policies, procedures and practices to the tasks of: communication, consultation, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk
Risk profile	A description of any set of risks
Risk register	A record of information about identified risks
Risk tolerance	An organisation or stakeholder's readiness to bear the risk after the risk has been treated, to achieve the organisation's or stakeholder's objectives
Risk treatment	A process to modify risk
Residual risk	The risk remaining after risk treatment

In addition to the definitions in ISO Guide 73, this toolkit uses the terms set out in Table 1.2 below.

Table 1.2 – Other key terms

Term	Definition
Audit and Risk Committee (ARC)	An Audit and Risk Committee established in accordance with the requirements of Treasury Policy Paper 09-05 *Internal Audit and Risk Management Policy for the NSW Public Sector* (TPP 09-05)
Chief Risk Officer (CRO)	The person that has designated responsibility for designing the agency's risk management framework and for the day-to-day activities associated with coordinating, maintaining and embedding the framework. The Chief Risk Officer is a primary risk champion (see below)
Chief Audit Executive (CAE)	Refers to the role of Chief Audit Executive established in accordance with TPP 09-05
Executive	The Head of Authority and his or her direct reports
Head of Authority (HOA)	As defined in section 4 of the *Public Finance and Audit Act 1983*
Risk sponsor	The person with ultimate accountability for managing risk in an agency. Section 11(1) of the *Public Finance and Audit Act 1983* requires the Head of the Authority (HOA) to ensure there is an effective system of internal control over the authority's financial and related operations. Accordingly, the HOA is the risk sponsor
Risk champion	The person(s) tasked with promoting risk management either across the agency, or specifically within a particular agency function or aspect of risk. A risk management champion provides training and education and helps improve the 'risk competence' of an agency
Risk owner	The person accountable and authorised to manage a particular risk
Senior management	Heads of business units, divisions or branches with ultimate accountability for delivering business unit, division or branch objectives
Risk management plan	A plan identifying the strategy, activities, resources, responsibilities and timeframes for implementing and maintaining risk management in an agency

Chapter 2 – Risk and risk management

2.1 What is risk?

Risk is defined in ISO Guide 73 as the 'effect of uncertainty[2] on objectives, where an effect is the deviation from what is expected'. In other words, risk is the potential for either a positive or negative deviation from the objective(s) your agency expects to achieve. Risk is often expressed in terms of an event's consequences and the likelihood of its occurrence.

Risk is inevitable and all agencies must take action to manage it. Risk management encompasses all organisational objectives and should address all uncertainties, both negative (threats) and positive (opportunities).

Organisational objectives cover the full range of activities undertaken by an agency and include:

§ strategic – high-level objectives aligned with the organisation's mission
§ operational – effective and efficient use of resources, including safeguarding assets from misappropriation or misuse and the mitigation of hazards
§ reporting – ensuring the reliability and timeliness of financial and management information
§ compliance – adherence to internal policies and procedures, and laws and regulations
§ projects – ensuring project objectives are met.

2.2 What is risk management and why is it important?

ISO Guide 73 defines risk management as 'coordinated activities to direct and control an organisation with regard to risk'. Risk management should occur in a systematic, transparent and disciplined way that will contribute to your agency's success in delivering its stated purpose.[3]

Risk management:

§ provides a framework for addressing risk in methodical, consistent ways
§ creates an environment where informed decisions about your agency's risks are made in an open and transparent way
§ gives you confidence you can reduce uncertainty in achieving your objectives by:
  - effectively managing threats to an acceptable/tolerable level
  - making informed decisions about exploiting opportunities, where they exist.

[2] ISO Guide 73 defines uncertainty as 'the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood'.

[3] TPP 09-05 uses the term 'enterprise risk management' in Core Requirement 5 to describe risk management. The use of the term 'enterprise' denotes a more complete risk management process in terms of its application across the agency, at every level and functional unit and the reporting of risk at a whole-of-agency level. ISO 31000 (which was issued after TPP 09-05 and AS/NZS 4360:2004) takes, by definition, a whole-of-organisation view of risk. Accordingly, the term 'enterprise risk management' is not used in this toolkit as it is implied in the new standard.

2.3 What are the key principles for effective risk management?

ISO 31000 discusses the key principles of effective risk management. It is important that your agency's senior management endorses these principles.

The principles state that risk management should:

- **create and protect value** to help your agency achieve its objectives. Some benefits of risk management are detailed in Figure 2.2 in section 2.5
- **be an integral part of your agency's activities and processes,** including planning, project and change management
- **be part of decision making** as every decision you make has an element of risk. Effective risk management can help you make informed choices, prioritise actions and select between alternative options
- **deal explicitly with uncertainties** inherent in all agency activities
- **be systematic, structured and timely** to facilitate repeatable and reliable outcomes
- **be based on best available information** with inputs to the risk management process drawing on objective data able to be independently verified wherever possible. Such inputs may include historical data, experience, feedback, observation, forecasts or expert judgment. Assumptions must be stated clearly
- **be tailored** to your agency and consider its objectives, capabilities, the environment in which it operates and the risks it faces
- **take human and cultural factors into account** by recognising the perceptions of internal and external stakeholders, including staff members' capabilities and attitudes towards risk management
- **be transparent and inclusive** about how risk is identified and assessed, how decisions are reached and how risks are treated. Senior management and relevant decision makers should be regularly consulted to ensure they can provide input into the criteria used to evaluate the effectiveness of the risk management process
- **be dynamic, iterative and responsive** as the internal and external environments in which your agency operates change. You need to monitor these environments to determine which risks are still relevant and to identify any new and emerging risks. Your agency's risk management framework and processes needs to be responsive to changes
- **facilitate your agency's continual improvement and enhancement**, through regular reviews of and improvements to your risk management framework and processes.

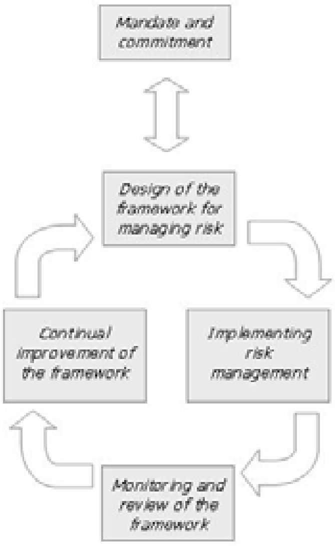
2.4 What is a risk management framework?

ISO Guide 73 defines a risk management framework as a set of components that provide the foundations and organisational arrangements for designing, implementing and monitoring, reviewing and continually improving risk management throughout an organisation.

The purpose of a risk management framework is to embed risk management throughout your agency and provide a structure that facilitates the use of a consistent process to manage risk whenever decisions are made.

Figure 2.1 outlines the components that comprise the risk management framework as described in ISO 31000. These components need to be active in your agency's wider management system and be regularly maintained if risk management is to be effective.

Figure 2.1 – ISO 31000 risk management framework components


Mandate and commitment
Design of the framework for managing risk
Implementing risk management
Monitoring and review of the framework
Continual improvement of the framework

Implementing a risk management framework is an iterative process and may take several years to effectively implement. The sophistication of the framework you adopt will evolve over time to reflect changes in your agency's size, complexity, risks and objectives.

2.5 What are the benefits of a risk management framework?

By adopting a formal risk management framework, you can help ensure that risks to your agency's objectives are identified and managed effectively, efficiently and coherently.

A formal risk management framework will, among other things:

§ provide the Head of Authority and other officers in your agency with knowledge of the risks inherent in your agency's operations, and an understanding of the process used to manage those risks

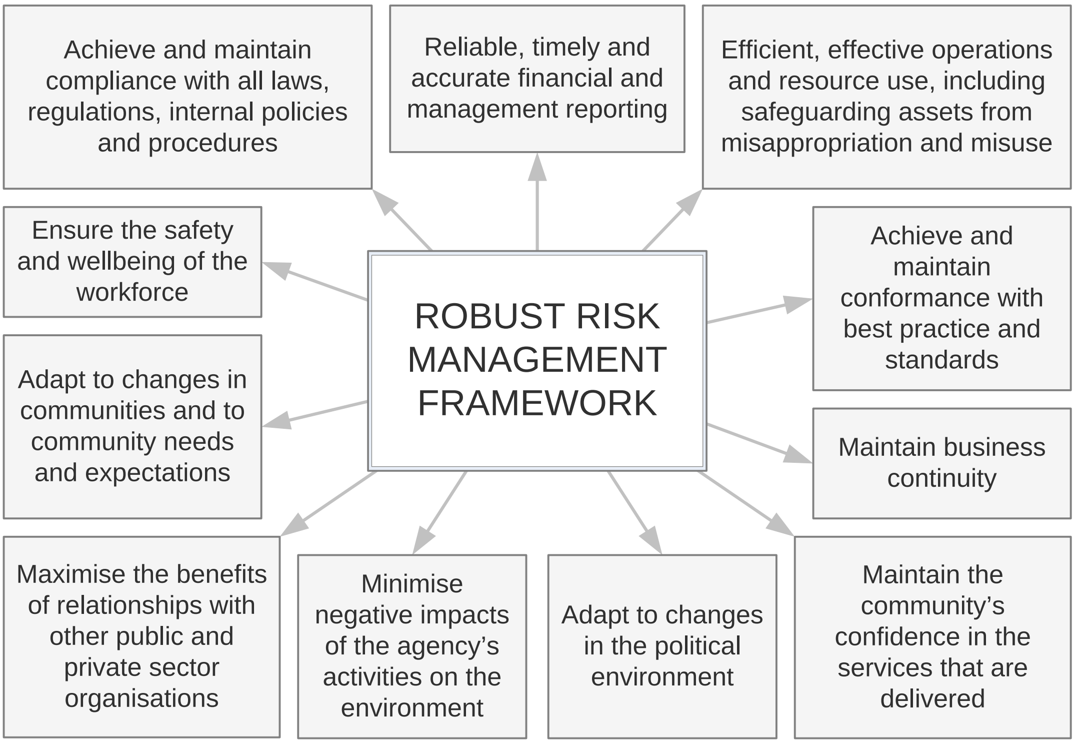
§ identify who will 'own' the risk

§ allow you to monitor how effective your agency is at responding to risk

§ provide stakeholders with increased confidence in your agency's governance and ability to achieve its objectives.

The benefits of a robust risk management framework are described in ISO 31000. Some of these benefits are presented in Figure 2.2 below.

Figure 2.2 – Benefits of a robust risk management framework



ROBUST RISK MANAGEMENT FRAMEWORK

Achieve and maintain compliance with all laws, regulations, internal policies and procedures

Reliable, timely and accurate financial and management reporting

Efficient, effective operations and resource use, including safeguarding assets from misappropriation and misuse

Ensure the safety and wellbeing of the workforce

Achieve and maintain conformance with best practice and standards

Adapt to changes in communities and to community needs and expectations

Maintain business continuity

Maximise the benefits of relationships with other public and private sector organisations

Minimise negative impacts of the agency's activities on the environment

Adapt to changes in the political environment

Maintain the community's confidence in the services that are delivered

A risk management framework helps you make more informed decisions. However, management systems are not fail-proof. Agencies need to be aware that human error can occur, internal controls can be circumvented through collusion, and management can override decisions. This means no risk management framework can provide absolute assurance that your agency can achieve its objectives.

2.6 What is the relationship between governance, risk management and compliance?

The NSW Auditor-General's 2011 report *Corporate Governance—Strategic Early Warning System* identified sound risk management as essential to good corporate governance.

Governance, risk management and compliance are three related but distinct disciplines:

§ **Governance** provides the direction and structure required to meet organisational objectives and enables your agency to properly manage its operations

§ **Risk management** provides the policies and procedures that enable your agency to function effectively in a changing environment

§ **Compliance** is adherence to both external and internal requirements.

Each of these disciplines plays an important role in organisational control and each focuses on achieving objectives. Your agency will find it difficult to meet its objectives if one of these disciplines is either ineffective or missing.

Governance, as it applies to the public sector, is defined as '…the set of responsibilities and practices, policies and procedures, exercised by an agency's executive, to provide strategic direction, ensure objectives are achieved, manage risks and use resources responsibly with accountability'.[4]

A complete discussion on public sector governance is outside the scope of this toolkit.5 Broadly speaking, governance is about:

§ **performance:** where an agency uses governance arrangements to contribute to its overall performance in the delivery of its services

§ **conformance:** where an agency uses governance arrangements to ensure it meets legal and policy compliance obligations, community expectations of probity, and accountability and transparency.

Risk management underpins your agency's governance arrangements. It is a fundamental component of your internal control framework that supports good governance by providing reasonable assurance that your agency will be able to meet its objectives without exceeding its ability to accept or tolerate risk.

Compliance complements governance and risk management by providing assurance that control strategies are working and objectives will be met.

The manner in which your agency coordinates its governance, risk management and compliance activities will depend on its size, the complexity of operations, the services it delivers and the resources available to it. By coordinating your governance, risk management and compliance activities, your agency can streamline processes to optimise resource use and improve information quality and consistency. Your agency's Chief Audit Executive (CAE), Audit and Risk Committee (ARC) and Chief Risk Officer should direct the coordination of these activities with the support of your agency's executive team.

[4] ANAO and Department of the Prime Minister and Cabinet, *Implementation of Programme and Policy Initiatives: Making Implementation Matter, Better Practice Guide*, Commonwealth of Australia, Canberra, 2006, p 13.

[5] For further information on public sector governance, refer to 2003 ANAO *Better Practice Guide Public Sector Governance*.

2.7 How should project risks be managed?

Projects are characterised by:

§ a defined start and end date
§ specific deliverables in terms of time, cost, quality and scope.

The objective of risk management at the project level is to increase the likelihood and impact of positive events and mitigate the likelihood and impact of negative events, to enhance the project's chance of success.

There are industry-standard frameworks and methodologies such as the Project Management Book of Knowledge (PMBOK) and PRINCE2 that integrate risk management with project management. Alternatively, your agency may have its own project management methodology in place that fulfils the same purpose.

NSW Treasury's Total Asset Management (TAM) policy, Capital Business Case Guidelines, Economic Appraisal Guidelines and NSW Gateway guidance material provide further guidance on considering risks in capital planning processes, including developing robust business cases.

Sound project governance arrangements are key to managing project risk. Your agency needs to manage project risks in the same manner as all other risks. The risk management process used to manage project risks needs to be consistent with and linked to your agency's risk management framework, to ensure project risks are visible, rather than being managed as a discrete activity. By making project risks visible, your agency will be better able to manage the impact of the project if it falls across several divisions.

By integrating specific project risks into a wider risk management framework, your agency will be able to identify – and manage in a coherent way – common project risks such as those related to poor project governance, flawed scope definition or sub-optimal resourcing arrangements.

2.8 How should interagency risks be managed?

Risks involving other agencies should be formally communicated to the affected agency as soon as they are identified. Implementing a common standard for risk management and establishing the roles of Chief Audit Executive and Chief Risk Officer should help coordinate and communicate risk management information among agencies.

Communication can be established through the Chief Risk Officer or the Chief Audit Executive and their counterparts in other agencies.

For major projects involving a number of agencies, the project steering committee or equivalent should assume responsibility for managing risks. In some instances, it may be necessary to establish interdepartmental risk management committees with senior level representation.

Managing interagency risk will need to evolve in line with new approaches to departmental structures and service delivery in the NSW public sector.

Chapter 3 – Implementing a risk management framework

3.1 How do I develop and implement a risk management framework?

Risks must be managed consistently in various organisational contexts, ranging from whole-of-enterprise risks to those that apply to only a single business unit or specific function.

A risk management framework provides a structure that will enable the use of a consistent risk management process no matter where decisions are being made in your agency.

ISO 31000 provides generic guidance on implementing and integrating risk management into organisational systems, processes and activities through the creation and continuous improvement of a risk management framework.

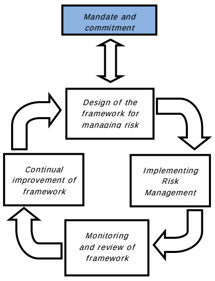
This chapter discusses the components of a risk management framework as outlined in ISO 31000, including:

- developing a mandate and securing commitment
- designing the framework for managing risk
- implementing risk management
- monitoring and reviewing the framework
- implementing measures for continual improvement of the framework.

The ISO 31000 framework is intended to help your agency integrate risk management into your overall management system. You should adapt the risk management framework to meet the specific needs of your agency.

Agencies that adopt the approach described in this toolkit will be aligned with the risk management–related requirements of TPP 09-05 and well-positioned to realise the benefits of risk management, illustrated in Figure 2.2 in section 2.5.

Mandate and Commitment


Mandate and commitment
Design of the framework for managing risk
Implementing Risk Management
Monitoring and review of framework
Continual improvement of framework

3.2 Mandate and commitment

Introducing risk management and ensuring its ongoing effectiveness in your agency requires strong and sustained commitment by your agency's senior management and support at all levels of management. Management must be genuine in their commitment to risk management. If not, many staff will disregard its importance.

It is management's responsibility to set a mandate and commit to implement, operate, maintain and continually improve your risk management framework.

3.2.1 Define and endorse a risk management policy

A risk management policy is a statement of the intentions and direction of your agency with regard to risk management. The Head of Authority (HOA) is responsible for defining and endorsing a risk management policy.

The policy should clearly state your agency's objectives for, and commitment to, risk management. Your policy is central to developing a common understanding of risk and its management within your agency. It provides your agency with the opportunity to articulate its risk management vision and to describe the benefits that it derives from managing risk.

Your agency's risk management policy should typically include:

- your vision and rationale for managing risk – why it is important to manage risk
- how your risk management policy fits in with your agency's policies and objectives
- who is accountable and responsible for managing risk (refer section 3.2.6)
- your commitment to make necessary resources available to assist those accountable and responsible for managing risk
- how you will measure and report your performance on risk management
- your commitment to regularly review and improve the risk management policy and framework in response to events or changed circumstances
- glossary of terms[6]
- whom you should contact (for example, the Chief Risk Officer) and their contact details, for questions about the policy.

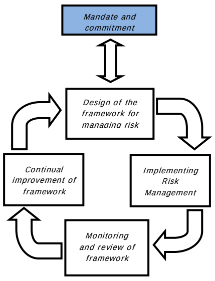
Refer to Volume 2 for an example of a risk management policy.

Actions such as establishing, maintaining and communicating a risk management policy demonstrate your agency's commitment to risk management. The HOA has access to resources to commit the agency to risk management policies and procedures, and to require your senior management and staff to comply with those risk management policies and procedures.

However, management and staff commitment to risk management can be developed only where the HOA also creates and sustains a risk management culture.

[6] It may also be beneficial to keep the definitions in a single document, such as an agency-specific risk management dictionary, and refer to this in your agency's other documents, including the risk management policy.

Mandate and Commitment


Mandate and commitment
Design of the framework for managing risk
Implementing Risk Management
Monitoring and review of framework
Continual improvement of framework

The HOA's approach will establish the fundamental attitude towards risk management within the agency. If the HOA is indifferent to, or does not visibly support, risk management, this indifference will manifest throughout your agency and undermine its risk management efforts. An analysis of recent organisational failures has linked those failures to an absence of management commitment.[7]

3.2.2 Ensure that your agency's culture and risk management policy are aligned

ISO 31000 recognises that organisational culture is an important component of risk management. Organisational culture refers to the basic values, norms, beliefs and practices that characterise the functioning of a particular institution. Culture drives organisational performance and embodies both the written and the unwritten rules of conduct. At the most basic level, organisational culture defines the assumptions that employees make as they carry out their work: that is, 'the way we do things around here'. An organisation's culture is a powerful force that persists despite reorganisation and the departure of key staff.

Many factors influence organisational culture, including the tone at the top, the code of conduct, and ethics and human resource policies. The HOA, the senior leadership team and the Audit and Risk Committee both model and drive the right behaviour with regard to risk.

Organisational culture often comprises a series of subcultures. These may be associated with an organisational system (e.g. work health and safety culture), particular business units or workgroups, or a geographical location. The introduction of any new system or process requiring widespread organisational buy-in, such as a risk management framework, needs to consider both the prevailing organisational culture and any subcultures that may affect the implementation and continuing success of the initiative.

Risk management culture is the accepted way of applying risk management within an agency. It drives how people recognise and respond to risk. If your agency does not have a culture that emphasises at all levels the importance of managing risk as part of each person's daily activities, your risk management policy cannot be effectively implemented.

Some of the actions that can influence and support a positive risk management culture in your agency are set out in Table 3.1 below.

[7] Caplain, B (2008). *Risk Management: Why it Failed, How to Fix It*, Internal Auditor. http://www.theiia.org/intAuditor/free-feature/2008/risk-management-why-it-failed-how-to-fix-it-ii/

Mandate and Commitment

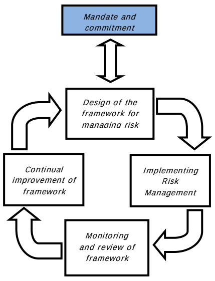

Mandate and commitment
Design of the framework for managing risk
Implementing Risk Management
Monitoring and review of framework
Continual improvement of framework

Table 3.1 – Actions supporting a positive risk management culture

Drivers	Action
Values Statement	Include reference to risk and risk management in any Values Statement approved by the HOA; for example, by stating that 'We value communication of risk information and the management of risk'.
Management commitment	Management must take every opportunity to demonstrate commitment to risk management and model expected risk management behaviours.
Systems and processes	Design agency-specific, fit-for-purpose tools, systems and processes to help people manage risk. Provide guidance to staff in the agency that use these tools and nominate the person they should contact for further assistance.
Organisational structure	Ensure the organisational structure allows responsibility for risks and risk treatment to be delegated.
Job design and performance	Create support for your risk management framework by nurturing suitable competencies, attitudes and behaviours in your staff. Ensure job descriptions refer to accountabilities and responsibilities for risk management. Assign leadership roles in risk management. Do not tolerate poor risk management behaviours. Review these behaviours as part of the staff appraisal process. Recognise and incentivise those who effectively identify or manage risk
Performance agreements	Articulate risk management responsibilities in performance agreements.
Desired versus actual behaviours	Encourage and support staff in managing risks. Incorporate measures of risk management culture and attitude into organisational climate surveys and performance management systems.
Effective communication	Ensure that your agency communicates its reasons for managing risk and that these are commonly understood and agreed. All staff should feel comfortable discussing risk management issues, encouraging effective two-way communication about risks and their management. Ensure that staff understand your agency's tolerance for risk and when and to whom risks should be escalated.

3.2.3 Align risk management objectives with your agency's objectives and strategies

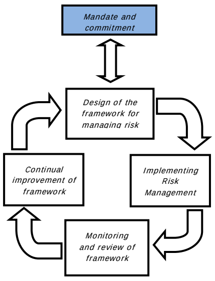
In many organisations, risk management has traditionally been focused at the operational level, limited to financial and physical asset risks, and managed within silos or business units.

ISO 31000 elevates risk management beyond these traditional risks to include risks at the strategic level, that is, those risks that critically impact on an agency's ability to achieve its objectives.

Your agency's executive is responsible for setting organisational objectives and priorities. These should include objectives and priorities for risk management, which should be aligned with your agency's overall objectives.

Achieving your risk management objectives should enable you to better achieve your agency's overall objectives.

Mandate and Commitment


Mandate and commitment
Design of the framework for managing risk
Implementing Risk Management
Monitoring and review of framework
Continual improvement of framework

3.2.4 Determine risk management performance indicators that align with your agency's performance indicators

Once you have set your agency's risk management objectives, you should also develop performance indicators that measure the extent to which your risk management framework is contributing to achieving your agency's objectives.

By working with your agency's executive, Audit and Risk Committee, Chief Audit Executive and Internal Audit, your Chief Risk Officer or risk management function should develop a suitable set of indicators to measure the success of your risk management. It may be possible to select measures already used in your agency to measure overall business performance.

If performance against a specific measure improves after risk treatment, then there is evidence that your risk management is contributing to achieving your agency's objectives. For example, if you have put in place risk treatments to reduce fraud, and there is evidence that the size and frequency of incidents have been reduced, then this is a good indicator that your risk management framework is working.

The International Standards for the Professional Practice of Internal Auditing (IIA Standards) require Internal Audit to 'evaluate the effectiveness and contribute to the improvement of risk management processes'.[8] Determining whether risk management processes are effective is based on an internal auditor's assessment of whether:

§ organisational objectives support and align with the organisation's mission
§ major risks are identified and assessed
§ appropriate risk responses are selected that align risks with the organisation's ability to accept or tolerate risk
§ relevant risk information is captured and communicated in a timely manner across the organisation, enabling staff, management, and the executive or governing board to carry out their responsibilities.

You can also use indicators that measure compliance with your risk management policy.

3.2.5 Ensure legal and regulatory compliance

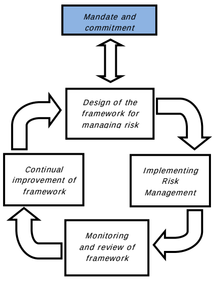
Compliance is defined as 'adhering to the requirements of laws, industry and organisational standards and codes, principles of good governance and accepted community and ethical standards'.[9] The context for compliance depends on your agency's legal and regulatory obligations, including those created by case law.

Various laws, regulations and policies create an obligation for agencies to manage risk in the NSW public sector. A complete list of legislative obligations that drive the management of risk in the NSW public sector is not within the scope of this guidance. Agencies need to individually identify the legislative and policy requirements that they are required to comply with. However, some key components of the financial management framework in NSW and attendant obligations are as follows.

[8] Institute of Internal Auditors 2010 International Standards for the Professional Practice of Internal Auditing (Standards), http://www.iia.org.au/technicalResources/knowledgeitem.aspx?ID=180

[9] Standards Australia Committee QR-014 Compliance Systems, 2006, *AS 3806-2006 Australian Standards Compliance Programs*, Standards Australia, Sydney, p5.

Mandate and Commitment


Mandate and commitment
Design of the framework for managing risk
Implementing Risk Management
Monitoring and review of framework
Continual improvement of framework

Public Finance and Audit Act 1983

The purpose of the *Public Finance and Audit Act 1983* (PFAA) is primarily 'to make provision with respect to the administration and audit of public finances' in NSW, including matters relating to the Auditor-General of NSW.

Section 11(1) of the PFAA requires the Head of Authority to ensure that there is an effective system of internal control[10] over the financial and related operations of the authority. Internal controls, by definition, are any action taken by management to manage risk and increase the likelihood that established objectives will be achieved.

While the PFAA is not explicit on risk management matters, it is implicit in section 11(1) that in order to ensure an effective system of internal control, an agency should have an effective system to establish its objectives and identify its risks. This is a necessary precursor to the design and implementation of internal controls.

Annual Reports Acts

Annual Reports (Departments) Regulation 2010 and Annual Reports (Statutory Bodies) Regulation 2010 require an agency, as part of its report of operations, to report on risk management, and the insurance arrangements and activities that affect the agency.

Annual reports enable those responsible for governance to discharge their accountability by communicating relevant information, including financial information, to external stakeholders and interested users. This information includes an overview of the agency, its strategic objectives and challenges, and any other information required by users to assess the agency and its ability to fulfil its mandate.

Although there is no prescribed format for reporting risk-related matters in the Annual Report, agencies should consider including:

§ an overview of risk management, including the agency's approach and commitment
§ roles and responsibilities for risk management
§ significant risks and management strategies.

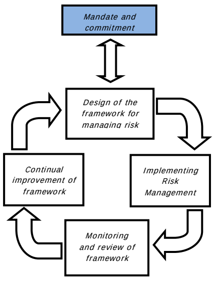
The Government Information (Public Access) Act 2009 (GIPA Act)

The GIPA Act encourages the routine and proactive release of government information, including information held by providers of goods and services contracted by government agencies.

The GIPA Act applies to all NSW government agencies. Section 5 of the GIPA Act states that 'there is a presumption in favour of disclosing government information unless there is an overriding public interest against disclosure'. Documents related to the management of risks in your agency are subject to the GIPA Act. You should seek advice from the officer in your agency who is responsible for dealing with GIPA matters.

[10] Institute of Internal Auditors, 2012, Full Standards – Glossary (http://www.theiia.org/guidance/standards-and-guidance/ippf/standards/full-standards/?i=8317)

Mandate and Commitment


Mandate and commitment
Design of the framework for managing risk
Implementing Risk Management
Monitoring and review of framework
Continual improvement of framework

Treasury Policy Paper TPP 09-05 Internal Audit and Risk Management Policy for the NSW Public Sector

The purpose of TPP 09-05 *Internal Audit and Risk Management Policy for the NSW Public Sector* is to ensure that the Head of Authority establishes and maintains organisational arrangements that will provide additional assurance, independent from operational management, on internal audit and risk management.

TPP 09-05 does this by:

- introducing corporate governance requirements to ensure the real and perceived independence of the Audit and Risk Committee, the Chief Audit Executive and the internal audit function
- drawing on best practice in the public and private sector
- adopting the current risk management standard
- adopting the current standards for the professional practice of internal audit (set out in the International Professional Practice Framework of the Institute of Internal Auditors) and risk management.[11]

Other requirements

Examples of other legislation and policies that require risks to be managed are:

- *Work Health and Safety Act 2011*
- *Protection of the Environment Operations Act 1997*
- *Independent Commission Against Corruption Act 1988*
- NSW Government Procurement Frameworks.

In addition, Independent Commission Against Corruption and the Auditor-General reports identify sector-wide risks from time to time.

Compliance

Standards Australia and the NSW Government Better Regulation Office have each developed and published guidance on achieving legal and regulatory compliance.

The Better Regulation Office, in its guidance Risk Based Compliance[12], provides information about regulatory practice. The compliance approach adopted by this guidance is risk-based, focusing resources on high-risk areas.

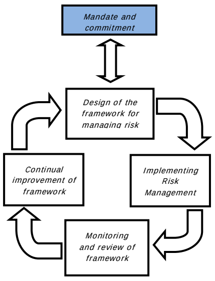
Australian Standard 3806:2006 *Compliance Programs* was developed to assist both public and private organisations to ‘identify and remedy any deficiencies in their compliance with laws, regulations and codes, and develop processes for continual improvement in this area’. The Standard provides 12 principles for the development, implementation and maintenance of effective compliance programs.

You are encouraged to refer to these guidance materials in developing your agency’s compliance programs.

[11] TPP09-05 *Internal audit and risk management for the NSW public sector*, dated August 2009, refers to AS/NZS 4360:2004 *Risk management*. This standard was replaced by AS/NZS ISO 31000:2009.

[12] The Better Regulation Office, NSW Department of Premier and Cabinet 2008, *Risk-based Compliance*, http://www.dpc.nsw.gov.au/__data/assets/pdf_file/0019/30862/01a_Risk-Based_Compliance.pdf.

Mandate and Commitment


Mandate and commitment
Design of the framework for managing risk
Implementing Risk Management
Monitoring and review of framework
Continual improvement of framework

3.2.6 Assign accountabilities and responsibilities at appropriate levels in your agency

Your agency should ensure that there is clear accountability and authority for managing risks. All staff assigned with responsibility for risk management must have the appropriate competencies, attitudes and behaviours.

Key stakeholders include:

- Head of Authority
- governing board of a statutory body
- Audit and Risk Committee
- executive or management committees
- risk management function
- Chief Risk Officer
- risk champion
- managers
- risk owners
- staff and contractors
- Internal Audit function and Chief Audit Executive
- External Audit function.

Head of Authority

The Head of Authority (HOA) has ultimate responsibility for risk management and is the risk sponsor.

Section 11 of the *Public Finance and Audit Act 1983 (PFAA)* requires the HOA to, among other things, ensure that an effective system of internal control over the financial and related operations of the authority, and an internal audit function are established.[13]

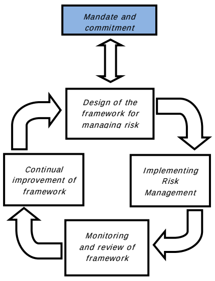
While retaining complete accountability for compliance with section11 of the PFAA, the HOA may delegate certain tasks, including the development and implementation of the risk management framework, to members of the senior leadership team and others.

Your HOA is also responsible for determining and articulating your agency's ability to accept or tolerate risk, approving your agency's risk management plan, ensuring your agency's risk management policy is implemented and reviewed regularly, and reviewing recommendations from your agency's Audit and Risk Committee.

The HOA's responsibilities extend to ensuring that risk management is included in job descriptions, staff induction programs and performance agreements, and is considered as part of performance appraisals.

[13] The *Public Finance and Audit Act 198*3 uses the term 'Internal Audit Organisation'. Various interpretations have been applied to the term 'organisation' pursuant to section 11(2). NSW Treasury has taken the term to mean an 'Internal Audit function' on the basis that the attendant responsibilities listed in section 11(2) denote an internal audit *function*.

Mandate and Commitment


Mandate and commitment
Design of the framework for managing risk
Implementing Risk Management
Monitoring and review of framework
Continual improvement of framework

To provide assurance that risks are being managed in the NSW public sector in a manner consistent with the current Australian/New Zealand standard on risk management, TPP 09-05 requires the department head or governing board of a statutory body to formally attest, every year, to NSW Treasury that they have implemented arrangements that are operating in all material respects in conformance with the policy, and to publish that attestation in the agency's annual report.

Governing board of a statutory body

TPP 09-05 similarly requires the governing board of a statutory body to ensure that a risk management process that is appropriate to the statutory body has been established and maintained, to attest to compliance with the policy, and publish that attestation in the agency's annual report.

Audit and Risk Committee

TPP 09-05 requires the department head or governing board of a statutory body to establish an Audit and Risk Committee (ARC). The ARC's responsibilities include the oversight of risk management processes of the department or statutory body.

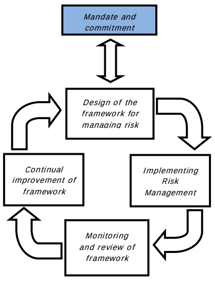
The ARC must:

- review whether management has in place a current and appropriate risk management process, and associated procedures for effective identification and management of financial and business risks, including fraud and corruption
- review whether a sound and effective approach has been followed in developing and implementing risk management strategies in relation to major projects or undertakings
- review the impact of the risk management process on the department's or statutory body's control environment and insurance arrangements
- review whether a sound and effective approach has been followed in establishing business continuity planning arrangements, including whether disaster recovery plans have been tested periodically
- review the fraud control plan and satisfy itself that the department or statutory body has appropriate processes and systems in place to capture and effectively investigate fraud-related information.

The ARC may seek assurance from multiple sources, including management, and the agency's Internal and External Audit function. The ARC may request:

- written reports and other risk management reports from senior management including risk registers
- the results of control self-assessments
- senior management to present at ARC meetings to discuss their activities and risks.

Mandate and Commitment


Mandate and commitment
Design of the framework for managing risk
Implementing Risk Management
Monitoring and review of framework
Continual improvement of framework

In this way, the ARC exercises an important role in setting an appropriate tone within the agency with regard to risk and driving risk management.

Executive or management committees

Executive or management committees in agencies have a role in risk management. Their responsibilities should include the review and scrutiny of:

§ agency approach and activities with regard to risk management
§ risk treatment plans and risk management reports, including risk registers, assessed for completeness (at a business-unit level and agency-wide), accuracy, consistency and use of a common language
§ internal controls for efficiency and effectiveness.

Executive or management committees may also have the executive authority to manage risks.

These responsibilities should be specified in your agency's executive or management committee terms of reference.

Risk management function

The risk management function is responsible for facilitating and assisting responsible officers with their risk management obligations. The risk management function should be independent of line management.

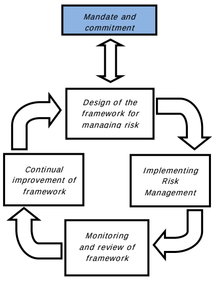
The risk management function should report to either the Head of Authority or a direct report to the Head of Authority, such as a member of the executive with responsibility for governance or planning, so that independence of risk management from line management is maintained. Providing this independence reduces the potential for management to influence the risks that are reported on. When you are determining the level to which your risk management function reports, you should consider the ability of the risk management function to provide 'frank and fearless' advice about risks and how they are managed.

The size of the risk management function will depend on the size of the agency. This may range from an officer nominated to undertake this role in addition to their existing duties, or a single dedicated Chief Risk Officer, or to a risk management team.

The role of the risk management function includes:

§ developing or leading the development of the risk management policy and strategy for risk management
§ acting as the primary champion for risk management at the strategic and operational level
§ designing and reviewing the processes for risk management
§ building a risk management culture within the agency, including appropriate staff training and development (refer to section 3.2.2)
§ providing advice and tools to staff to assist them in managing risk
§ co-ordinating the various functional activities relating to risk management within the agency

Mandate and Commitment


Mandate and commitment
Design of the framework for managing risk
Implementing Risk Management
Monitoring and review of framework
Continual improvement of framework

- working with risk owners to ensure compliance with the risk management framework
- collating and reviewing risk registers for completeness and accuracy
- preparing risk management reports for the ARC (refer to section 3.3.6).

It is important to emphasise that the risk management function does not own the risks. Risk owners are responsible and accountable for risks, and this accountability must form part of their job descriptions (refer to the separate description of ‘Risk owners’ below in this section).

Chief Risk Officer

A Chief Risk Officer (CRO) should be appointed to lead the risk management function. This officer is also a primary risk champion. The CRO is responsible for designing your agency’s risk management framework and for the day-to-day activities associated with coordinating, maintaining and embedding the framework in your agency.

The role of a CRO is a technical role. Wherever practical, it is recommended that staff with an appropriate skillset be assigned the responsibility for risk management. The role does not have to be a dedicated one. It is common for a staff member who has operational responsibility for some risks (e.g. Work Health and Safety or Project Management), and who understands risks and risk management, to be assigned the role of a CRO.

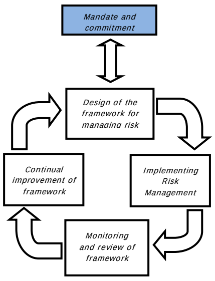
The role of the CRO is different from the role of the Chief Audit Executive (CAE). In some circumstances, for example in smaller agencies, the CAE may fulfil the role of the CRO. However, this may not be the optimal choice. For example, the CAE may not possess the required risk management competencies. Appropriate safeguards must also be put in place to address the threats to independence of both roles.

Risk champion

It may be beneficial for your agency to nominate one or more risk champions in addition to your Chief Risk Officer. Risk champions are people who promote risk management across the agency, or specifically within a particular agency function or project. They can help embed risk management into your agency’s other systems and processes. Champions can also help ensure that functional and project areas are using your agency’s risk management processes consistently.

A risk champion may hold any position within your agency, but is generally a person who:

- has the skills, knowledge and leadership qualities required to support and drive a particular aspect of risk management
- has sufficient authority to intervene in instances where risk management efforts are being hampered by a lack of cooperation or through lack of risk management capability or maturity
- is able to add value to the risk management process by providing guidance and support in managing difficult risk or risks spread across functional areas.


Mandate and commitment
Design of the framework for managing risk
Implementing Risk Management
Monitoring and review of framework
Continual improvement of framework

Managers

Managers at all levels of your agency are responsible for managing risk and ensuring that their staff perform their duties within the constraints of your agency's ability to manage risk. This include being responsible, within the sphere of their authority, for:

- establishing an environment that promotes an awareness of internal controls and responsibility for individual risks
- identifying uncertainties that will affect the achievement of agency objectives
- establishing policies, operating and performance standards, budgets, plans, systems and procedures to address identified risks and reduce them to an acceptable or tolerable level
- monitoring the effectiveness of controls
- carrying out self-assessments (where directed) to certify the effectiveness of controls addressing risks for which they are responsible (e.g. internal control self-assessments[14], which are completed by operating units, could be a mechanism that management can use to demonstrate this aspect of the internal control structure).

NSW Treasury requires Chief Financial Officers (CFOs) to certify to their respective Heads of Authority that they have 'effective systems, processes and internal controls to ensure that the monthly and annual financial information provided to Treasury is reliable'; that is, that they have designed and instituted effective internal controls to address financial reporting risk.

CFO certification must be supported by a process that seeks evidence and assurance from line managers regarding the quality of financial information.

Risk owners

A risk owner is the person who has responsibility for designing, implementing and monitoring risk treatments for a particular risk. Risk owners are accountable for ensuring that the risk is managed in accordance with the agency's ability to accept or tolerate risk. The risk owner must be knowledgeable about the process or activity for which risks are being assessed, but may not necessarily be the person who implements the internal control, that is, takes action to address the identified risk.

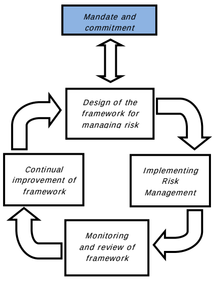
Staff and contractors

All staff and contractors must be aware of their responsibilities in managing risk in their day-to-day roles. This includes carrying out their roles in accordance with all policies and procedures, identifying risks and reporting these to relevant risk owners in accordance with reporting protocols. Staff and contractors should also report ineffective or inefficient controls.

All staff and contractors should be aware of the risks that relate to their roles and activities.

[14] Control self-assessments are a method that allows managers to self-assess risks and controls in place. They may assist in clarifying organisational objectives and risks, and may also be used by internal auditors for the purpose of identifying high-risk areas and provide a basis for the efficient allocation of internal audit resources.

Mandate and Commitment


Mandate and commitment
Design of the framework for managing risk
Implementing Risk Management
Monitoring and review of framework
Continual improvement of framework

Internal Audit and Chief Audit Executive

Your agency's internal audit function plays a major role in organisational compliance and risk management. These responsibilities are set out in the TPP 09-05 model Internal Audit Charter, and they include providing assurance that:

- risk controls are appropriately designed and effectively implemented
- your agency's risk management framework is effective.

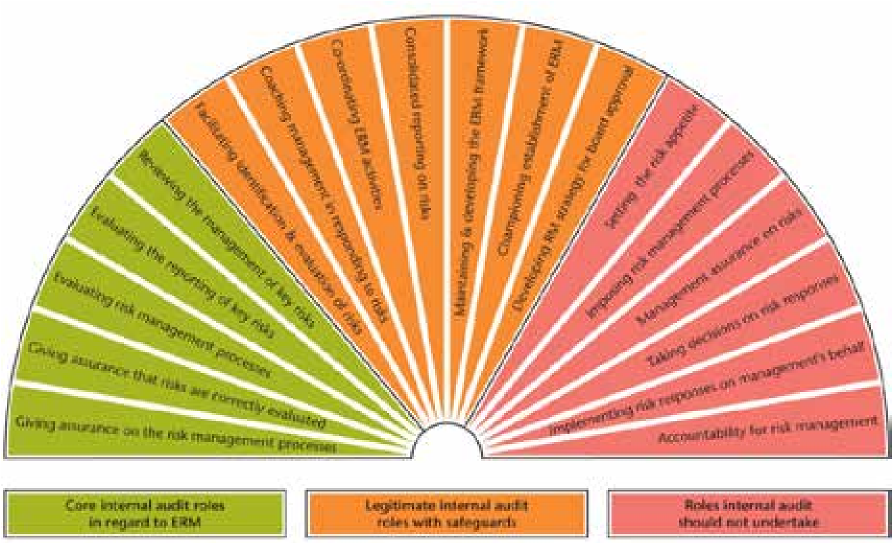
One of the responsibilities of the ARC is to gain assurance that processes are operating within defined parameters to achieve defined objectives. The Chief Audit Executive (CAE) should understand the ARC's assurance requirements.

Internal Audit provides objective assurance of the adequacy and effectiveness of control processes to the Head of Authority through the ARC, by bringing a systematic, disciplined approach to evaluating and improving the effectiveness of governance, risk management and internal control processes.

In some agencies formal risk management functions may not exist. In such cases, Internal Audit may, in addition to its assurance function, provide risk management consulting services. However, where internal auditors accept operational responsibility for functions that are subject to periodic internal audit assessments, their independence and objectivity may be impaired.

Figure 3.1 presents the range of risk management activities that an internal audit function may and may not undertake, as identified by the Institute of Internal Auditors in a paper entitled 'The role of internal auditing in enterprise risk management'.[15]

Figure 3.1 – Internal Audit's role in risk management

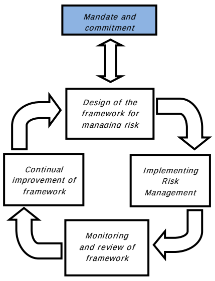

Giving assurance on the risk management processes
Giving assurance that risks are correctly evaluated
Evaluating risk management processes
Evaluating the reporting of key risks
Reviewing the management of key risks
Facilitating identification & evaluation of risks
Coaching management in responding to risks
Co-ordinating ERM activities
Consolidated reporting on risks
Maintaining & developing the ERM framework
Championing establishment of ERM
Developing RM strategy for board approval
Setting the risk appetite
Imposing risk management processes
Management assurance on risks
Taking decisions on risk responses
Implementing risk responses on management's behalf
Accountability for risk management
Core internal audit roles in regard to ERM
Legitimate internal audit roles with safeguards
Roles internal audit should not undertake

This diagram is taken from "Position Statement: The Role of Internal Audit in Enterprise-wide Risk Management", reproduced with the permission of the Institute of Internal Auditors – UK and Ireland. For the full Statement visit www.iia.org.uk.

© The Institute of Internal Auditors – UK and Ireland Ltd, July 2004

[15] Institute of Internal Auditors (IIA) 2009, 'The role of internal auditing in enterprise risk management', Position Paper. IIA, https://na.theiia.org/standards-guidance/Public%20Documents/IPPF_PP_Role_of_IA_in_ERM_01-09.pdf. Note all references to enterprise risk management in the IIA position paper should be read as reference to risk management.

Mandate and Commitment



Mandate and commitment
Design of the framework for managing risk
Implementing Risk Management
Monitoring and review of framework
Continual improvement of framework

External Audit

External Audit is 'the examination by an independent third party of the financial report of a company or other organisation, resulting in the publication of an opinion on whether the financial report is presented fairly, in all material respects, and has been prepared in accordance with an applicable financial reporting framework'.[16]

External auditors are not part of the agency, and they are responsible to external stakeholders. External auditors are required to make those charged with governance or management aware of material weaknesses in the design or implementation of internal controls that come to their attention during the audit.[17]

In the NSW public sector, the Audit Office of NSW carries out the external audit function. The Auditor-General may, when considered appropriate, conduct an audit of all or any particular activities of an authority (including risk management) to determine whether the authority is carrying out those activities effectively, economically, efficiently and in compliance with all relevant laws. A performance audit is separate from, and does not affect, any other audit required or authorised by or under the *Public Finance and Audit Act 1983* or any other Act.

3.2.7 Ensure that necessary resources are allocated to risk management

Your agency needs to allocate sufficient resources to develop and implement a risk management framework, which includes allocating an adequate budget as well as appropriate technical and human resources. Resources are discussed further in section 3.3.5.

3.2.8 Communicate the benefits of risk management to all stakeholders

It is important for all stakeholders to appreciate the benefits of risk management, which are presented in Figure 2.2 in section 2.5 so they remain committed. A variety of strategies for communicating with both internal and external stakeholders is outlined in the discussion on effective internal and external communication (refer to section 3.3.6).

For more on communication about risk, refer to the Standards Australia companion handbook to AS/NZS ISO 31000 called *HB 327:2010 Communicating and consulting about risk*.

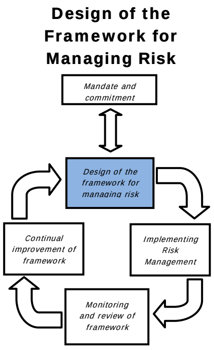
3.2.9 Ensure that your risk management framework continues to remain appropriate

Your agency's commitment to risk management should extend to regular review and maintenance of your framework to ensure it remains fit for purpose. Reviews can allow you to assess if your agency's risk management activities remain both relevant and effective. Reviews may result in the need to make some changes from time to time.

The more consistently you apply your risk management framework, the better positioned your agency will be to realise the benefits in Figure 2.2 in section 2.5. Your agency's Audit and Risk Committee should set the schedule for your risk management framework review.

[16] Auditing and Assurance Standards Board (AASB) 2007, Auditing Standard ASA 200 *Objective and general principles governing an audit of a financial report*, AASB, Melbourne.

[17] Auditing and Assurance Standards Board (AASB) 2006, Auditing Standard ASA 315 *Understanding the entity and its environment and assessing the risks of material misstatement*, AASB, Melbourne.


Design of the Framework for Managing Risk
Mandate and commitment
Design of the framework for managing risk
Implementing Risk Management
Monitoring and review of framework
Continual improvement of framework

3.3 Design of the framework for managing risk

This section describes what you need to do to design a risk management framework that is tailored to your agency's needs.

3.3.1 Understand your agency and its context

The first step in designing your framework is to consider the internal and external factors specific to your agency that could affect the design of the framework.

Your external context is the environment or background in which your agency operates, including the political, economic, social, technological and legal environment. Understanding the external environment allows you to identify external stakeholders and the impact they might have on your agency achieving its objectives. Take particular note of the legal and regulatory requirements (your compliance obligations – refer to section 3.2.5) and your stakeholder expectations.

The internal context is the environment within your agency. It includes the culture, governance and other structures, roles and accountabilities in your agency, and considers both its formal and informal structures.

The internal and external context should be considered again, in more detail, when you establish the risk management process for your agency (Chapter 4).

3.3.2 Establish a risk management policy

Your risk management policy is a statement of your agency's intentions and direction in risk management. It sits within your agency's broader policy framework, and it supports, and should be supported by, all your other policies. In this way you can demonstrate the integration of risk management into your organisational processes. Your agency's HOA should define and endorse your risk management policy (refer to section 3.2.1).

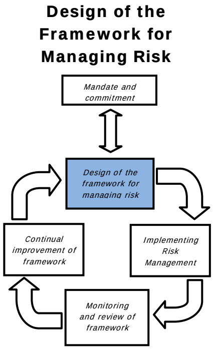
3.3.3 Assign accountability

Your agency should ensure that key stakeholders have clear accountability and authority for managing risks. Stakeholders and their roles and responsibilities are discussed in section 3.2.6.

3.3.4 Integrate risk management into all of your agency's processes

In many organisations, risk management has historically been limited to well-recognised risks, such as work health and safety, insurable risks, business continuity and disaster recovery planning. In other instances, risk management has been practised in silos – that is, it has been limited to particular areas, divisions or projects in an organisation.

ISO 31000 recommends that risk management should be part of, and not separate from, an organisation's practices and processes. The relationship between risk management, governance and compliance has been previously discussed (refer to section 2.6). Your agency's approach to managing risk should be embedded in your agency's planning processes, decision-making structures and operational procedures.


Design of the Framework for Managing Risk
Mandate and commitment
Design of the framework for managing risk
Implementing Risk Management
Monitoring and review of framework
Continual improvement of framework

Your agency policies should consider uncertainties that may affect the achievement of policy objectives and include sufficient controls to ensure that policy objectives will be achieved. Designing policies in this way allows you to demonstrate the integration of risk management into all of your organisational processes.

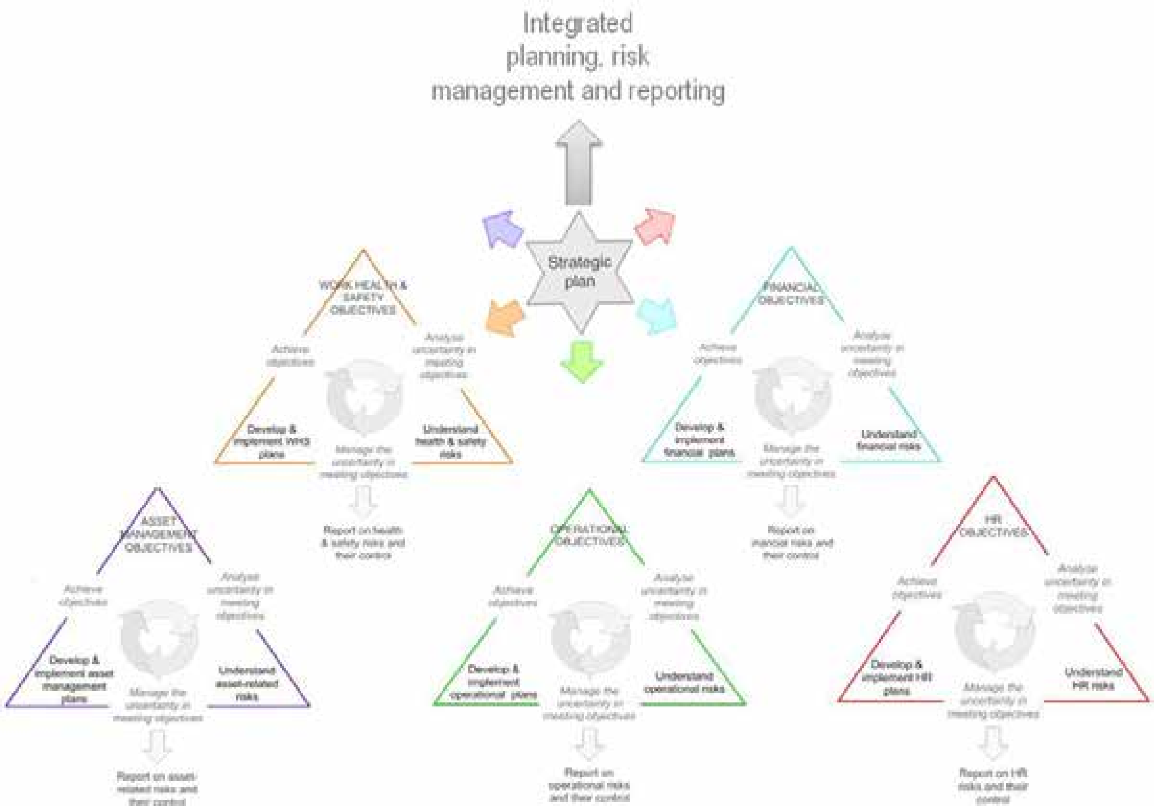
Risk management issues should be considered across all levels and activities so that you can develop an agency-wide view of risks that can impact on the achievement of your agency's objectives.

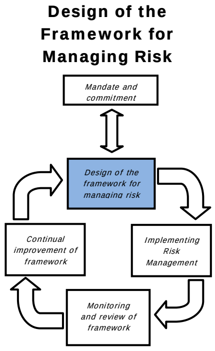
Planning

Risk management must be embedded into strategy development and planning. Planning is the process of determining a desired outcome, establishing objectives and then designing a course of action to achieve that outcome. Since the purpose of risk management is to deal with the uncertainty associated with the achievement of objectives, there is an intrinsic link between planning and risk management. Figure 3.2 demonstrates many of these linkages.

An agency generally develops its strategic objectives as part of its corporate planning process.

Figure 3.2 – Integrated planning and risk management


Integrated planning, risk management and reporting
Strategic plan
WORK HEALTH & SAFETY OBJECTIVES
Achieve objectives
Analyse uncertainty in meeting objectives
Develop & implement WHS plans
Understand health & safety risks
Manage the uncertainty in meeting objectives
Report on health & safety risks and their control
FINANCIAL OBJECTIVES
Achieve objectives
Analyse uncertainty in meeting objectives
Develop & implement financial plans
Understand financial risks
Manage the uncertainty in meeting objectives
Report on financial risks and their control
ASSET MANAGEMENT OBJECTIVES
Achieve objectives
Analyse uncertainty in meeting objectives
Develop & implement asset management plans
Understand asset-related risks
Manage the uncertainty in meeting objectives
Report on asset-related risks and their control
OPERATIONAL OBJECTIVES
Achieve objectives
Analyse uncertainty in meeting objectives
Develop & implement operational plans
Understand operational risks
Manage the uncertainty in meeting objectives
Report on operational risks and their control
HR OBJECTIVES
Achieve objectives
Analyse uncertainty in meeting objectives
Develop & implement HR plans
Understand HR risks
Manage the uncertainty in meeting objectives
Report on HR risks and their control


Design of the Framework for Managing Risk
Mandate and commitment
Design of the framework for managing risk
Implementing Risk Management
Monitoring and review of framework
Continual improvement of framework

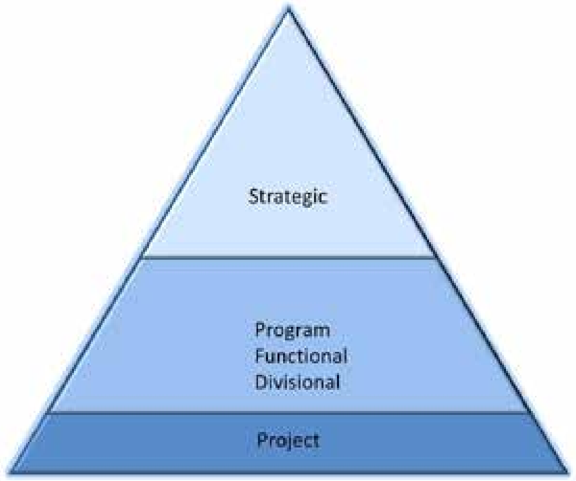
Integrating risk management into your agency's strategic planning process may entail the following:

- **Strategic assessment.** Develop a general understanding of all sources of risks that affect your agency in this phase. Consider both the external and internal contexts that could impact on your agency's ability to achieve its objectives.
- **Strategy development and planning.** When developing your strategic objectives and your approach to achieving these objectives, you should undertake a risk assessment, that is, identify potential events that may affect your agency achieving its desired objectives; analyse your current control effectiveness; identify the residual risks; and determine how you will treat these risks. You should also assign risk owners (refer to section 3.2.6) and identify performance indicators (refer to section 6.1.3) at this stage.

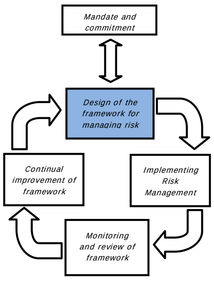
Similarly, as part of your business planning process, your agency can identify and assess the operational risks associated with your business and operational objectives (which derive from your strategic objectives). Where risks are identified as high during the planning process, your agency can treat these risks to bring them to a level that your agency can accept or tolerate.

At the end of the strategic and business planning processes, your agency may end up with a hierarchy of integrated plans, as shown in Figure 3.3. Each of these plans should contain strategies and activities for managing identified risks.

Figure 3.3 – A typical hierarchy of plans



Design of the Framework for Managing Risk


Mandate and commitment
Design of the framework for managing risk
Continual improvement of framework
Implementing Risk Management
Monitoring and review of framework

Depending on the size and complexity of your agency, such plans may include:

- your agency’s strategic plan
- your agency’s corporate plan
- whole-of-agency functional plans, such as those for human resource management, asset management, financial management and risk management
- whole-of-agency activity plans, such as those for procurement, communications, information management, work health and safety, business continuity and security
- divisional business plans, such as regional service delivery plans
- project plans
- individual work plans.

If you develop an integrated hierarchy of plans and risk assessments, you can optimise the benefits of both planning and risk management, which can help ensure risks are managed at the appropriate level in your agency.

3.3.5 Allocate appropriate resources for risk management

Your agency needs to commit sufficient resources to implement its risk management framework.

Human resources

The allocation of dedicated human resources, with defined roles, responsibilities and competencies, is a vital component of your agency’s risk management framework. In order for risks to be managed, you must ensure that accountability is clearly defined, assigned and reflected in job descriptions.

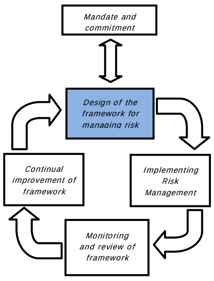
People skills, experience and capabilities

Risk management is effective only when all staff and contractors are accountable and responsible for the management of risk. Staff and contractors should have the confidence to take ownership of, and escalate, risks throughout the agency. They should possess risk-related competencies (skills and experience, complemented by training and development) and appropriate resources (including time). Their risk accountabilities and responsibilities should be reviewed as part of their performance appraisals.

Staff and contractors will need different capabilities and levels of competence in risk management depending on their role. You can use a capability matrix to record, for each relevant position or level in the agency:

- the risk management roles undertaken
- the capability required to perform these roles
- how to develop this capability, including induction, and ongoing learning and development.

Design of the Framework for Managing Risk



Mandate and commitment
Design of the framework for managing risk
Continual improvement of framework
Implementing Risk Management
Monitoring and review of framework

A comprehensive capability matrix for risk management should include specialist risk practitioners, those with a governance role in risk management, those with responsibility for managing specific risks as part of their general duties and, where appropriate, contractors.

For many operational or front-line staff, the capability required may simply be an understanding of your agency's approach to risk management and knowledge of key operating procedures, work health and safety, and hazard reporting systems. (Refer to Volume 2 for a template and an example of a capability matrix.)

Training and development

Training and development are central to improving the capability of staff who have risk responsibility and increasing awareness of risk management throughout your agency. Your risk management function or your primary risk champion (Chief Risk Officer or equivalent) should identify your agency's training needs and develop the appropriate training content.

Training may be delivered through your internal learning and development area, or by an external provider. Training should form a mandatory component of continued professional development within your agency.

Agencies generally deliver training through learning and development programs, including appropriate staff induction and hands-on activities, such as participation in risk assessment workshops and incident debriefs.

Programs are most successful when they:

- are tailored to the requirements of the work environment, as well as to the risk management capability needs of your staff
- use a range of training delivery mechanisms, such as face-to-face courses, workshopping real activities, internal seminars, and on-line learning to reach as many staff as possible
- are regularly reviewed for continuing relevance and developed as risk management capability improves and the organisation's risk management culture matures.

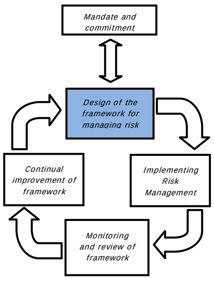
Capability can also be developed by providing opportunities for staff who exhibit an interest or ability in risk management. For example, you might provide opportunities for staff to act in higher duties or in other roles within the agency, or to participate in specific risk management-related projects.

Monitoring organisational capability as part of your agency's performance management program can help you ensure that learning and development, induction and other programs are providing the required capabilities and that those capabilities are being attained.

Risk information

You should design your agency's risk management framework to ensure that information about risks and their management are reported and used as a basis for decision making and accountability at all levels within your agency.

Design of the Framework for Managing Risk


Mandate and commitment
Design of the framework for managing risk
Implementing Risk Management
Monitoring and review of framework
Continual improvement of framework

Risk information includes information used to:

- identify, measure and report on the nature and level of risks
- make decisions about treating risks
- monitor consistency in the decisions that are being made about risks and their treatment
- monitor risks and the strategies in place to manage them
- monitor the effectiveness of the risk management framework.

Risk information can be qualitative or quantitative. Your agency may wish to use information from a range of sources to inform your risk management activities, including:

- results of environmental scanning activities, such as SWOT analyses
- service delivery information
- internal human resources and industrial relations information
- Australian Bureau of Statistics data
- reports of compliance infringements
- asset maintenance reports
- insurance data
- risk registers
- incident reports, critical incident debriefs and decision review meetings
- audit findings and reports.

To be useful, risk information needs to be:

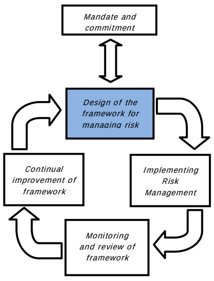
- relevant – to the needs of individual stakeholders
- reliable – it contains current, accurate information
- timely – it is produced when needed
- understandable – by users
- complete – it has an appropriate level of detail
- consistent – it is captured in a form that ensures all users interpret it in the same way.

Risk management information systems

In developing an effective risk management framework, you will need the right tools and technology to capture data about risks, analyse the data, and report and communicate relevant and reliable information in a timely manner to internal and external stakeholders. A risk management information system (RMIS) used consistently throughout your agency, based on a common language and definition of key terms, can aid and develop communication, understanding and management of risks.

An RMIS is a system designed around the risk management process to manage your risk-related information and documents. While an RMIS is a valuable supporting tool for risk management, it is *not* a proxy for a risk management framework.

Design of the Framework for Managing Risk



Mandate and commitment
Design of the framework for managing risk
Continual improvement of framework
Implementing Risk Management
Monitoring and review of framework

The size, complexity and risk management maturity of your agency, and the nature of its risks will influence your RMIS requirements. For medium-sized and smaller agencies, or agencies in the early stages of implementing risk management, the cost of acquiring and maintaining a proprietary package may be prohibitive. In that case, the use of Microsoft Excel or Word documents to record, report and communicate risk information may be appropriate. (Reporting templates and examples are provided in Volume 2.) Larger or more risk-mature agencies may consider purchasing proprietary software or developing their own RMIS.

Acquiring an RMIS is a decision for your agency executive.

An RMIS may be implemented centrally, within the risk management function, or distributed throughout the agency to multiple users. In distributed systems, users should have the appropriate level of access to information systems commensurate with their risk management role. Like all organisational information, risk information needs to be stored with an appropriate level of security. An audit trail of access and changes to the master files is essential. If multiple systems are used, you must ensure sufficient integration so that information is consistent and duplication, particularly in data entry, is minimised.

Irrespective of the technology your agency selects, your system should ideally be able to:

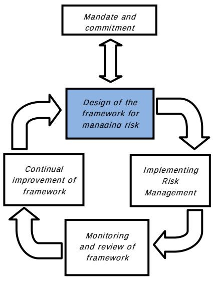
- store risk management policy and procedures documents and related information
- categorise risks according to likelihood and consequence
- rank risks
- capture risk treatment options (controls) and resource requirements
- monitor risks
- produce reports such as risk profiles (refer to Volume 2 for examples)
- track progress and implementation of risk treatment
- record details of control weaknesses and failures
- capture actual losses or gains and near-miss events
- conduct trend analysis.

3.3.6 Establish internal and external communication mechanisms

Effective communication is critical to successful risk management to ensure that the right information is communicated to the right people at the right time. The success of your agency's risk management approach relies on all stakeholders having a common understanding of:

- your agency's reasons for, and commitment to, risk management
- your agency's risk management policy, risk management plan and risk management priorities
- how much risk your agency will accept or tolerate
- who is responsible for what in managing risk
- how risks should be identified, assessed and managed

Design of the Framework for Managing Risk


Mandate and commitment
Design of the framework for managing risk
Implementing Risk Management
Monitoring and review of framework
Continual improvement of framework

- who needs to know what about a risk and the way it is being managed
- where to find support when undertaking risk management activities
- what to do if the risk management process isn't working
- your agency's risk management performance and lessons learnt.

Communication about risks and their management is most effective when it is tailored to the needs of your stakeholders. Ensuring the communication is clear and consistently understood means your stakeholders can draw informed conclusions about the impact that a risk management decision will have on them and their work.

Two-way risk communication facilitates consultation and common understanding. Undertaking a stakeholder analysis as part of the development of your agency's risk communication strategy can provide a good understanding of the needs and expectations of your stakeholders. (Refer to Volume 2 for templates to document the needs of your stakeholders and develop your communication strategy.)

Using a common risk language can improve the way risks and their management are communicated and understood. Using a common risk language should also reduce the possibility of miscommunications and misunderstandings, and oversights when managing risks.

Essential components of a common risk language include:

- a risk management vocabulary
- a common view of the agency in terms of its operating units, support units and sources of risk
- a clearly defined risk management process
- a defined process for communicating information about risks.

Effective internal communication

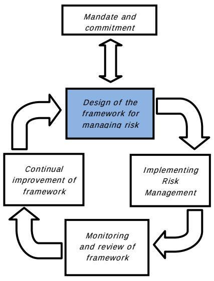
Your agency's internal stakeholders will have different information needs. For example, the Head of Authority and the Audit and Risk Committee need to know:

- the significant risks that affect the ability of your agency to achieve its objectives
- how the agency will manage crises
- the importance of communication and the best methods to use to communicate with external and internal stakeholders
- whether risk management is operating effectively.

Business units and senior management need to know:

- which risks fall into their area of responsibility
- the potential impacts that risks in their area may have on other areas within the agency and on other agencies
- their responsibilities in identifying potential, and managing actual, crises
- what key risk and control indicators are in place
- reporting requirements.

Design of the Framework for Managing Risk


Mandate and commitment
Design of the framework for managing risk
Implementing Risk Management
Monitoring and review of framework
Continual improvement of framework

Individuals need to know:

- their accountability for certain risks
- that risk management is a part of organisational culture
- how to report new or emerging risks
- changes in risk profiles of known risks, including control failures.

Your agency can use a number of mechanisms to communicate risk information with internal stakeholders. These include:

- policies and procedures documents
- education and training programs
- formal risk reports and briefing documents
- Audit and Risk and other committee minutes
- corporate and other plans
- risk-related forums and briefing sessions with committees, project teams, work groups and other stakeholder groups
- electronic methods, such as internet and intranet sites, and including newsletters, webcasts and e-mail
- your agency's Annual Reports.

Effective external communication

The objective of external communication is to communicate with your external stakeholders about risk management issues that may affect them.

Your external stakeholders include suppliers, trade creditors, users of services, the community and other entities (both public and private sector) that may be affected by or interested in the services provided by your agency.

A key mechanism for communicating information to external stakeholders is through your agency's Annual Report. The Annual Report Acts and Regulations (Departments and Statutory bodies) set out the requirements for the content, publication and dissemination of agency Annual Reports. Agencies are required to report on their risk management activities and the insurance arrangements affecting the agency.

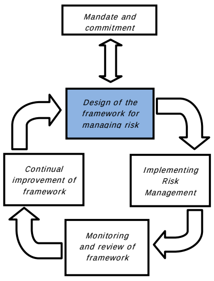
Your agency's internet site can also be used to communicate with external stakeholders.

Risk management reporting

Risk management reporting is the regular provision of risk information to enable decision makers to fulfil their risk management obligations.

Accurate and timely reporting of risk information, particularly to internal stakeholders, is essential to good corporate governance. Information on current and emerging risks, and treatment and monitoring plans should be used in strategic planning, divisional, operational and project management processes to provide reasonable assurance that your agency's objectives will be met.

Design of the Framework for Managing Risk


Mandate and commitment
Design of the framework for managing risk
Implementing Risk Management
Monitoring and review of framework
Continual improvement of framework

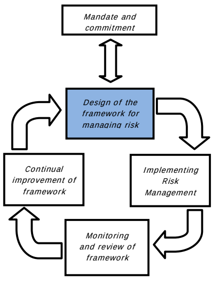
The Chief Risk Officer or equivalent has the responsibility for producing reports. The frequency and content of reports should be tailored to the needs of individual stakeholders. An illustrative list of strategic and operational risk reports is provided in Table 3.2 and Table 3.3 below.

While ISO 31000 focuses on residual risk (risk remaining after risk treatment), in reporting and documenting risks it may sometimes be good practice to also consider 'worst-case risks'[18] (risks assuming no related controls), in addition to 'current risks' (risks after current controls) and residual risks. This will provide stakeholders, including the Audit and Risk Committee, with a complete picture of all risks and a position on which to challenge management on the effectiveness of controls. (Refer to Volume 2 for a Risk Register Template and worked example.)

Table 3.2 – Examples of strategic risk reports

Report type	Users	Frequency	Purpose and content
Attestation statement in accordance with TPP 09-05 *Internal Audit and Risk Management Policy for the NSW Public Sector*	Treasury and users of annual reports	Annually	The attestation statement requires the department head or the governing board of a statutory body to attest, among other things, that risk management processes consistent with the current Australian/New Zealand standard have been implemented. The template for the attestation is prescribed in TPP 09-05.
Annual report	External and internal stakeholders	Annually	As discussed in section 3.2.5, the *Annual Reports (Departments) Regulation 2010* and *Annual Reports (Statutory Bodies) Regulation 2010* requires agencies to report on the risk management activities and insurance arrangements affecting the agency. Information in the annual reports should possess the requisite qualitative characteristics of relevance, reliability and comparability, and be easily understood.

[18] This is similar to the concept of 'Potential Exposure' defined in *HB 158-2010 Delivering assurance based on ISO 31000:2009 - Risk Management – Principles and guidelines* as the total plausible maximum impact on an organisation arising from a risk without regard to controls.


Mandate and commitment
Design of the framework for managing risk
Implementing Risk Management
Monitoring and review of framework
Continual improvement of framework

Report type	Users	Frequency	Purpose and content
Reports to the Audit and Risk Committee (ARC)	Head of Authority Governing boards of statutory bodies ARC Senior management Internal Audit	As per frequency of ARC meetings	Reports can include: § Risk register § Significant risks: information provided on these risks include risk owner, risk treatment, additional treatments and timeframes and any other information § Risk trends: trend analysis can only occur where there is frequent and regular assessment of risks. Trend reports can: – cover movements in risks, identifying those which are getting worse or better – show the effect of treatments on risk – identify risks that need further treatment. § New or emerging risks: by conducting regular assessments, reports on new or emerging risks should be able to be compiled § Risks with ineffective controls: the provision of this information will allow the ARC and the HOA to identify potential points of business failure requiring urgent response or action § Risk categories: generic risk categories are strategic, operational, compliance and reporting (both financial and management) § Risk profiles: refer to section 5.5.2.

Design of the Framework for Managing Risk

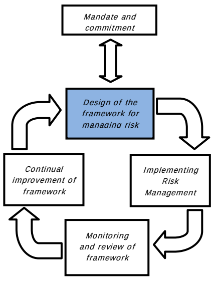
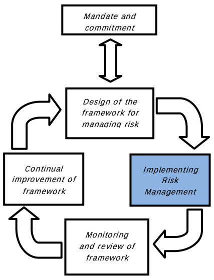

Mandate and commitment
Design of the framework for managing risk
Continual improvement of framework
Implementing Risk Management
Monitoring and review of framework

Table 3.3 – Examples of operational risk reports

Report type	Users	Frequency	Purpose and content
Operational risk reports	Functional business unit managers Project managers Staff responsible for managing risks	Monthly or quarterly	Production and dissemination of tailored reports to risk owners. (Where risks are not assigned to an owner, operational risk reports will provide management with details of risks that have not been treated or risks that are not being monitored. Providing risk reports to risk owners allows an opportunity for staff to view the risks and treatments that they are required to oversee.)
Incident report	Risk manager Internal Audit Functional business unit manager	Ad hoc as they occur Summary reports monthly	Communicate risks realised, including control failures.
Staff communication	All employees	As required	Includes but not limited to risk management policy, training and development.

Implementing Risk Management


Mandate and commitment
Design of the framework for managing risk
Continual improvement of framework
Implementing Risk Management
Monitoring and review of framework

3.4 Implementing risk management

Once you have designed your agency's risk management framework, you need to develop a plan to implement it in your agency.

3.4.1 Risk management plan

Your risk management plan can be developed through your agency's planning processes and should set out how you will implement your risk management framework and policy. The focus of the plan should be to integrate risk management into your agency's management systems.

Depending on the size, complexity and nature of your agency, you may require a single risk management plan or a hierarchy of linked plans (for example, branch risk management plans that underpin your agency's risk management plan).

Articulating a high level risk management strategy in a risk management plan enables your agency to promote a common understanding of the agency's approach to risk management.

The risk management plan should outline the activities associated with pursuing your risk management strategy. It should also include:

- roles, accountabilities and responsibilities
- timeframes for risk management activities
- change-management strategies
- resourcing requirements (people, IT and physical assets)
- training and development
- performance measures
- review processes.

Communicating the plan to internal and external stakeholders demonstrates your agency's commitment to risk management.

Since the aim is to involve all staff in relevant risk management activities, full implementation of your agency's risk management plan may take some time – it may take years rather than months to reach a high level of maturity. You should regularly monitor progress against the plan. Your ARC and executive must approve any changes to your agency's risk management plan.

Refer to Volume 2 for an example of a risk management plan.

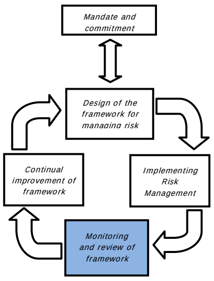
3.4.2 Develop a risk management process

A risk management process is a core component of your risk management framework. The risk management process advocated by ISO 31000 is a systematic way of establishing the context in which your agency operates, and identifying, analysing, evaluating and treating your risks, while communicating and consulting with stakeholders, and continuously monitoring and reviewing the elements of the process (see Figure 4.1 in section 4.1).

You need to develop a process based on ISO 31000 that can be applied consistently across your agency to support risk management decision making.

Your risk management implementation plan should cover how this process will be implemented and maintained in your agency. For detailed guidance on the risk management process and its implementation, refer to Chapter 4.

Monitor & Review of the Framework


Mandate and commitment
Design of the framework for managing risk
Implementing Risk Management
Monitoring and review of framework
Continual improvement of framework

3.5 Monitoring and review of the framework

Monitoring and reviewing your risk management framework is essential in ensuring it remains fit for purpose and assessing whether your agency's approach to risk management remains consistent with its objectives. You can use the results of the reviews to prioritise improvement strategies and to inform your attestation regarding compliance with Core Requirement 5 of TPP 09-05.

ISO 31000 recommends that you should:

- measure performance against risk management indicators (refer to section 3.2.4); these indicators should, in turn, be regularly reviewed to ensure they remain appropriate
- periodically measure your progress against your risk management plan
- periodically review changes in your agency's internal and external environments that may affect your agency's risk management framework[19]
- report on risk and compliance with your risk management policy.

The review method you choose will depend on many factors, including the level of maturity of your risk management framework, the resources available and the aspect of the framework being assessed. Review methods include self-assessment tools and internal audit processes. More frequent reviews may be needed if rapid changes affect your risk management framework, your agency and your agency's environment. Two possible methods that you may consider to review the effectiveness of your risk management framework are described below.

3.5.1 Risk management maturity model

Annex A of ISO 31000 describes the attributes of enhanced risk management. Your agency can use these attributes to monitor the alignment of its risk management framework with this standard and test the maturity of your framework against a set of success indicators for each attribute. These attributes are:

- continual improvement
- full accountability for risks
- application of risk management in all decision making
- continual communications about risk
- full integration into your agency's governance structures

Refer to Volume 2 for an example and a template applying this approach.

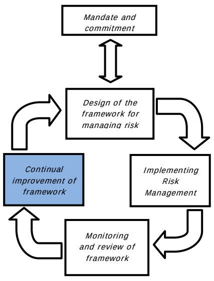
3.5.2 Key principles approach

Alternatively, you can conduct an audit of your framework's effectiveness based on the 11 principles set out in ISO 31000 (refer to section 2.3). This approach is based on the premise that your framework will be more effective if you adopt those principles. The main benefit of this approach is that it is flexible and allows you to develop your own indicators. It is also suited to agencies at varying levels of risk maturity.

For more information on this approach, refer to *HB 158-2010*: *Delivering assurance based on ISO 31000:2009 Risk management – Principles and guidelines* (HB 158-2010).

[19] NSW Auditor General's Report Volume 2 2011, *Corporate governance – strategic early warning system*, (http://www.audit.nsw.gov.au/ArticleDocuments/191/05_Vol_2_2011_Corp_Governance.pdf.aspx) suggests that your risk management policy should be reviewed at least once every five years or within one year of a significant restructure.

Continual Improvement of the Framework


Mandate and commitment
Design of the framework for managing risk
Implementing Risk Management
Monitoring and review of framework
Continual improvement of framework

3.6 Continual improvement of the framework

Continual improvement is about enhancing your risk management framework and moving to a higher level of risk maturity. This can be achieved by identifying, through your agency's monitoring and review processes, changes that should be made so that elements of your framework, such as your risk management policy and risk management process, work more effectively.

Continual improvement of your framework may require specific initiatives, which should be documented in your risk management plan. You may also want to include a section in your risk management policy that explains your agency's commitment to continually improve the way it manages risk (refer to Volume 2). Your risk management performance indicators (refer to section 3.2.4) should also support the continual improvement of your risk management framework by enabling your agency to measure improvements that have occurred.

Continuous risk management learning, often referred to as 'lessons learnt', is about leveraging existing knowledge and capacity or recent experiences to achieve organisation-wide behavioural and cultural change, and increased risk management performance.

Your agency can use lessons learnt from previous risk management decisions and apply these to its current decision-making processes through critical incident debriefings, decision review processes and minutes of meetings. It is also important to learn from other organisations with similar service delivery goals and operating environments, in addition to considering your agency's own incidents, near-misses and risk experiences.

You need to establish a process so these lessons learnt are communicated to relevant stakeholders. Your agency can facilitate risk management learning through working groups, information sessions, learning events, newsletters and other publications. You can also use these mechanisms to celebrate improvement in your agency's risk management performance and risk management success stories.

Chapter 4 – The risk management process: establishing the foundation

4.1 What is a risk management process?

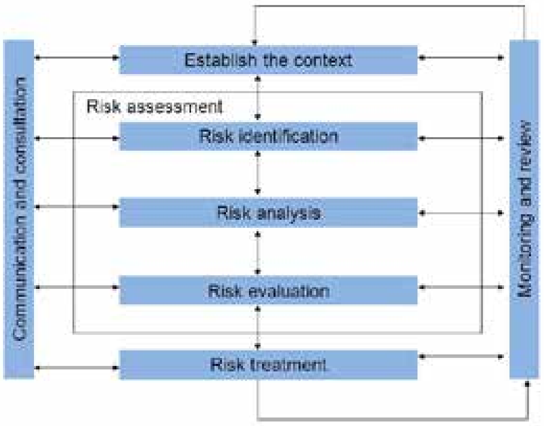
A risk management process is a systematic way to establish the context in which your agency operates, and identify, analyse, evaluate and treat your risks, while communicating and consulting with stakeholders and continuously monitoring and reviewing the elements of the process.

ISO 31000 identifies seven distinct but interrelated elements in the risk management process, as shown in Figure 4.1. These elements are:

- **Communication and consultation:** exchanging information about risk management with internal and external stakeholders
- **Establishing the context:** defining the internal and external parameters to be considered when managing risk and setting the scope of your agency's risk management process
- **Risk identification:** finding, recognising and describing risks
- **Risk analysis:** understanding the nature and level of risks so you can make decisions about whether a risk needs to be treated
- **Risk evaluation:** deciding which risks require further treatment by comparing against established risk criteria, and in what order
- **Risk treatment:** identifying, selecting and implementing responses to risks that fall outside the levels your agency is prepared to accept or tolerate
- **Monitoring and review:** continually checking each component of the risk management process is performing as desired.

The risk identification, analysis and evaluation stages are collectively known as **risk assessment**.

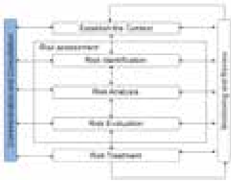
Figure 4.1 – The risk management process



The risk management process must be an integral component of your agency's operations, embedded in your agency's culture and practices, and tailored to your agency's business processes, including your strategic, business and project planning processes.

ISO 31000 recommends taking a team-based approach to developing and implementing a risk management process. Working as a team enables you to take advantage of different skills, experience and organisational perspectives when developing and implementing your agency's risk management process.

To be effective, development and implementation should be facilitated by your risk management team or your agency's Chief Risk Officer, that is, by the person to whom your agency has assigned responsibility for the design of its risk management framework.



4.2 Communication and consultation

You should communicate and consult with your stakeholders at all stages of the risk management process. Effective communication and consultation mechanisms will support the effective implementation of your risk management process.

You may wish perform a stakeholder analysis to develop a deeper understanding of the issues that most concern your stakeholders, their level of influence and the impact your agency has on them. You can conduct a stakeholder analysis for the whole agency, a specific directorate or business unit, or as part of the development and implementation of a particular initiative (refer to Volume 2 for examples and templates).

4.2.1 Consultation

You need to consult with your internal and external stakeholders so that:

- the context in which your agency is operating is fully understood
- the interests of stakeholders are understood and considered
- all risks are identified
- different areas of expertise are drawn on when analysing and evaluating risks
- different views are considered
- you can secure endorsement and support for risk treatment plans.

Consultation can be formal or informal. Formal consultation processes may include strategic planning sessions; presentations to the executive internal memoranda; minutes from relevant risk evaluation meetings; surveys; and focus groups. Formal consultation ensures stakeholder needs and concerns are addressed in a structured environment, and establishes an audit trail of decisions.

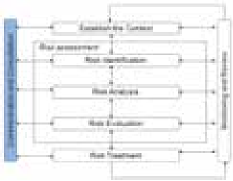
Informal consultation may include less formal meetings, workshops, emails, updates, reports, briefings and interviews.

4.2.2 Communication

Clear and effective communication is necessary to ensure that the right people receive the right information at the right time, so they can make the best decisions and carry out their risk management responsibilities.

Different people within your agency will have different information needs. For example, staff who are accountable for carrying out actions to deal with risk will need to understand their accountabilities, the rationale for decisions and why these actions are required.

Other internal stakeholders such as the Head of Authority, governing boards of statutory bodies, advisory committees such as the Audit and Risk Committee and senior management will have their own unique information needs, such as an understanding of how risks are managed and reported.



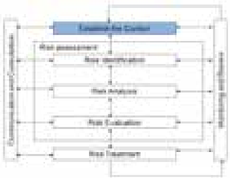
You also need to communicate information about risks and how they are being managed to external stakeholders, for example through your agency's annual report.

Communication with your stakeholders should be continuous, and should permeate the risk management process.

You need to develop plans to identify what, how, when and to whom you will communicate information about risks and the risk management process. These communication plans should be developed early in your agency's risk management process. Your plans should be regularly reviewed and revised to ensure they reflect changes in your agency's external, internal and risk management contexts.

You can develop different risk communication plans for internal and external stakeholders that include both formal and informal approaches, as informed by your stakeholder analysis (refer to Volume 2 for examples and templates).

Establishing the context

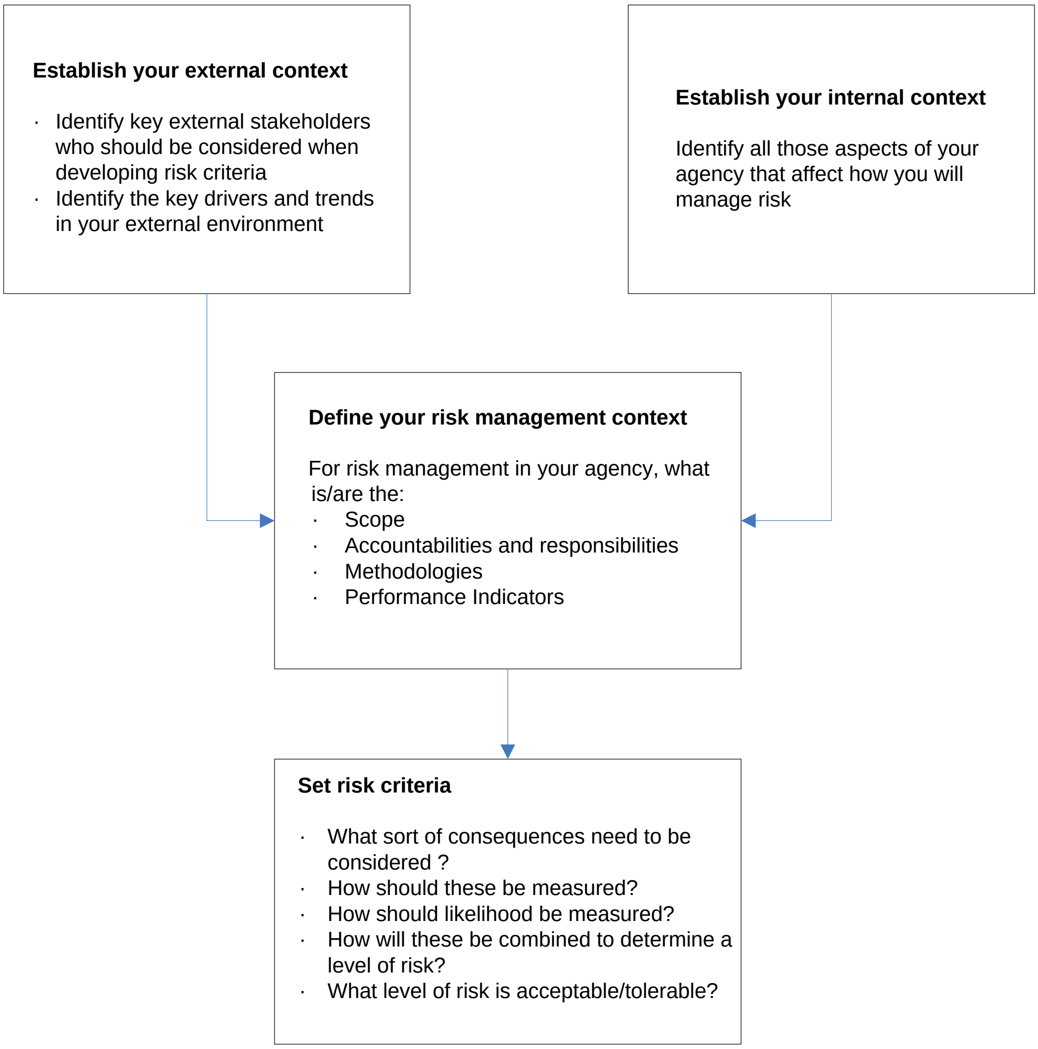


4.3 Establishing the context

Establishing the context is about defining the external and internal parameters to be considered when managing risk and setting the scope of your agency’s risk management process.

You must establish the context so that you can understand the business environment your risk management process operates in. In turn, this understanding informs the definition of a scope and structure for the remaining components of the risk management process, including determining what types of risk will be considered and how these will be measured, and establishing criteria to decide if a given risk is acceptable or tolerable. Figure 4.2 illustrates the key steps in establishing a context for your risk management process.

Figure 4.2 – Establishing the context for the risk management process



Establish your external context

- Identify key external stakeholders who should be considered when developing risk criteria
- Identify the key drivers and trends in your external environment

Establish your internal context

Identify all those aspects of your agency that affect how you will manage risk

Define your risk management context

For risk management in your agency, what is/are the:

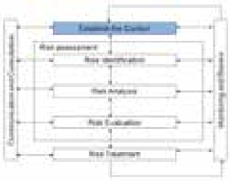
- Scope
- Accountabilities and responsibilities
- Methodologies
- Performance Indicators

Set risk criteria

- What sort of consequences need to be considered ?
- How should these be measured?
- How should likelihood be measured?
- How will these be combined to determine a level of risk?
- What level of risk is acceptable/tolerable?

Parameters to be considered in establishing the context are similar to those considered in the design of a risk management framework. However, when establishing the context for the risk management process, these parameters need to be considered in more detail, particularly how they relate to the scope of your agency’s risk management process.

Establishing the context



Your agency should consider its external, internal and risk management contexts, as discussed below. These contexts should be regularly examined when your agency's risk management framework and processes are reviewed to ensure that any changes are identified in a timely manner and treatments and priorities for risk treatment can be revised if necessary.

4.3.1 Establishing the external context

The external context is the external environment in which your agency operates. Defining this context requires you to consider the impacts that external factors may have on your agency's operations and your agency's ability to achieve its objectives. Consider these factors at a local, regional, national and international level. Examples include:

- **political:** change of government, change in government policies
- **economic:** economic growth, commodity prices, interest rates
- **socio-cultural:** population growth, impact of demographic change on demand for services, change in stakeholder expectations, pressure groups
- **technological:** technological change, cost of updating technology, obsolescence of systems
- **laws and regulations:** legislation, regulations and standards
- **environmental:** impacts that your agency's operations have on the built or natural environment, climate change.

You must identify the key trends and drivers that may affect your agency's ability to achieve its objectives.

Your agency should also consider stakeholder perceptions and values, and how they influence your agency's ability to achieve its objectives (refer to Volume 2 for a template and a worked example of a stakeholder analysis matrix).

4.3.2 Establishing the internal context

The internal context is the internal environment in which your agency operates. Defining your agency's internal context requires you to consider, amongst other things, your agency's objectives, structure, capabilities, processes, resources and stakeholders.

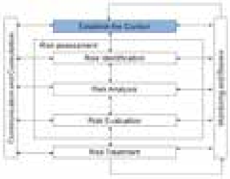
4.3.3 Establishing the context of the risk management process

The risk management context refers to the parameters established for your risk management process based on a consideration of your agency's external and internal environment. It covers all the activities in your risk management process.

Establishing the risk management context for your agency requires you to consider, and determine, for example:

- your agency's goals, objectives, strategies, resources and accountabilities for its risk management activities
- the risk assessment methodologies you will use

Establishing the context



- the risk criteria you will use to measure risk and determine if a given risk is acceptable or tolerable
- the performance metrics you will use to evaluate your risk management performance.

You must use consistent terminology and language when establishing your risk management context. The following terms (defined in the glossary in section 1.4, but reproduced here for ease of reference[20]) are commonly used in risk management:

- **consequence:** the outcome of an event affecting objectives
- **control:** a measure (including a process, policy, device, practice or other action) that modifies risk
- **event:** an occurrence or change of a particular set of circumstances
- **level of risk:** the magnitude of a risk, or combination of risks, expressed as a combination of consequences and their likelihoods
- **likelihood:** the chance of something happening
- **risk:** the effect of uncertainty on objectives
- **risk tolerance:** an organisation's or stakeholder's readiness to bear the risk that remains after risk treatment in order to achieve their objectives.

Developing risk criteria

One of the reasons for establishing the context is to allow you to develop risk criteria for your agency. You need a set of standard criteria so that everyone in your agency has a common understanding of how to evaluate the significance of a risk. These criteria could be informed by product or service specifications, accepted industry standards or legal requirements. Once developed, your risk criteria should be documented and communicated to stakeholders.

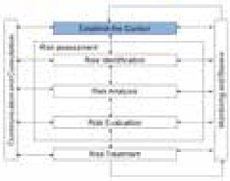
As shown in Table 4.1 below, your risk criteria consist of scales to measure consequence, likelihood, control effectiveness and the overall level of risk, and to determine your response to different levels of risk.

Table 4.1 – Risk criteria

Risk criteria	Used in
Consequence levels: the scale you will use to assess consequences of a risk	Risk analysis
Consequence table: a matrix where consequence levels are described for different types of consequences	Risk analysis
Likelihood table: the scale you will use to assess the likelihood of a risk	Risk analysis
Control effectiveness: the scale you will use to assess risk controls	Risk analysis Risk evaluation
Risk matrix: a technique used to combine consequence and likelihood to determine the level of a risk	Risk analysis
Risk actions and escalation points: describes the escalation actions required for each risk level	Risk evaluation
Risk tolerance table: defines your response to risk depending on whether or not you accept or tolerate the risk	Risk evaluation

[20] As defined in International Organization for Standardization (ISO) 2009, *ISO Guide 73:2009 Risk management - vocabulary*, ISO, Geneva.

Establishing the context



Although risk criteria are initially developed as part of establishing the context for risk management, they should also be further developed and refined as particular risks are identified, and risk analysis techniques are chosen, or as your agency's risk management maturity grows.

Your agency's executive must be involved in developing, and must approve, your risk criteria.

Measuring consequences

There are many techniques for measuring consequences. Advantages and disadvantages of each technique are discussed in IEC/ISO 31010:2009, *Risk management – risk assessment techniques* (ISO 31010). Techniques range from qualitative methods, which use a set of descriptors of the level of risk (e.g. very high, high, medium, low), to quantitative techniques, which are based on statistical analysis of historical data.

If you want to use quantitative techniques to measure consequences, you may need good historical data or the estimation of a multitude of conditional probabilities. You may also need specialist skills to apply quantitative techniques, but they can offer a disciplined and systematic analytical framework in risk management. Quantitative techniques may not be suitable for all agencies; for example, agencies whose core business is policy. Qualitative techniques are likely to be more subjective, but they are simple to apply.

The method you choose will depend on your agency's decision-making needs, the type and reliability of the data available and the capabilities and experience of those who will be conducting this analysis.

A detailed discussion of the various techniques is not in the scope of this toolkit. However, one of the most commonly used qualitative techniques for measuring consequences is a consequence table.

Designing consequence tables

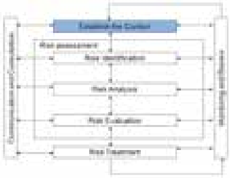
A consequence table enables you to measure consequences using a consistent, predetermined scale. It consists of a matrix that defines consequence levels for each consequence type.

The three main steps in creating a consequence table are:

1. Identify types of consequences that should be included in your table.
2. Determine how many levels of consequences you need in your table to differentiate severity.
3. Describe each consequence level for each consequence type.

The steps for creating consequence tables are discussed in detail below.

Establishing the context



Step 1: Identify types of consequences that should be included in your table

The first step is to identify all the types of consequences that will affect your agency's ability to achieve its objectives. Consequence tables need to include the most relevant types of consequence that may be experienced by your agency, based on your understanding from establishing the context.

Both tangible (such as financial) and intangible (such as reputational) types of consequences should be considered.

Some common consequence types include:

- financial
- service delivery
- work health and safety
- community
- environment
- stakeholder satisfaction
- reputation and image
- exposure to fraud and corruption
- exposure to litigation
- legal and regulatory.

Step 2: Determine how many levels of consequences you need in your table

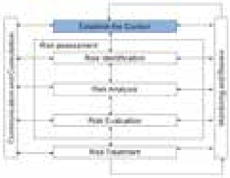
The next step is to determine the number of levels required to describe severity for each of the consequence types identified in step 1. The aim is to define enough levels for you to clearly differentiate levels of severity for each consequence. If you specify too many levels, it will be difficult to choose the most appropriate consequence level, particularly between adjacent levels. Similarly, if there are too few levels, it may also be difficult to choose the most appropriate level. Most organisations that use consequence tables define between three and five levels.

Consequence levels must be determined to suit your agency's circumstances. For example, four consequence levels have been defined in Table 4.2.

Table 4.2 – Typical consequence levels and descriptors

Consequence level	Consequence level description
Very high	Affects the ability of your entire agency to achieve its objectives and may require third party intervention
High	Affects the ability of your entire agency to achieve its objectives and requires significant coordinated management effort at the executive level
Medium	Affects the ability of a single business unit in your agency to achieve its objectives but requires management effort from areas outside the business unit
Low	Affects the ability of a single business unit in your agency to achieve its objectives and can be managed within normal management practices

Establishing the context



Step 3: Describe each consequence level for each consequence type

The next step is to describe each consequence level for each consequence type. Consequences should be described so they are easily understood and can be distinguished from each level of consequence above or below it. For example, the descriptions you use should allow anyone in your agency to understand exactly what you are defining as a '*high* financial consequence' and how this differs from a '*medium* financial consequence'. Descriptions must be tailored to your agency's circumstances and should flow from your understanding of your agency's context.

Consequences selected should be comparable across each consequence type. For example, the highest level of consequence for a financial consequence type must be broadly comparable to the highest level of consequence for a stakeholder satisfaction consequence type. The examples in Table 4.3 and Table 4.4 respectively illustrate how consequences can be developed for threats and opportunities.

Table 4.3 – Consequence table: threats

Consequence type	**Consequence level**			
	Low	**Medium**	**High**	**Very high**
Financial loss	Does not exceed 0.1% of budget	Greater than or equal to 0.1% but less than or equal to 0.5% of budget	Greater than or equal to 0.5% but less than or equal to 2% of budget	Exceeds 2% of budget
Service delivery	Service failure across a single service group's services that can be managed within the service group	A significant disruption to business continuity across a single service group's service, requiring resources from other areas of your agency	A major disruption to business continuity across multiple services that your agency provides	A significant disruption in business continuity across all major services provided by your agency
Work health and safety	1 staff member or contractor lost-time injury	1–5 staff member or contractor lost-time injuries	More than 1 staff member or contractor left with a permanent disability injury and/or 5–25 staff member or contractor lost-time injuries	Fatality; 5 or more staff members or contractor permanent disability injuries and/or 25 or more staff member or contractor lost-time injuries

Establishing the context

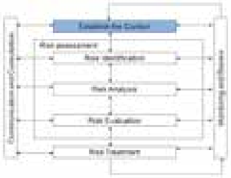


Table 4.4 – Consequence table: opportunities

Consequence type	Consequence level			
	Low	Medium	High	Very high
Financial gain	Savings or benefit up to 1% of the budget	Savings or benefit of 1–5% of the budget	Savings or benefit of 5–10% of the budget	Savings or benefit greater than 10% of the budget
Service delivery	Minor improvement in program/ project/ service outcomes	Moderate improvement in program/project/ service outcomes	Major improvement in program/ project/service outcomes	Substantial improvement in program/project/ service outcomes
Reputation	Visible satisfaction from public; and/or limited/ localised media interest	Short-term state-wide positive publicity; and/or public interest in agency	Sustained state-wide positive publicity; and/or sustained community satisfaction; and/or supportive Ministerial comments; and/or positive reinforcement in Parliament	Significant recognition leading to major improvement in community and stakeholder support; and/or broad and sustained public interest

Note that while a qualitative consequence table is relatively simple to use, the results will be subjective and should be interpreted as indicative and not definitive. It is also worth considering that a qualitative consequence table does not lend itself to consideration of the combined consequence of multiple interrelated risks.

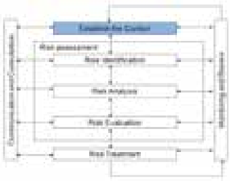
Likelihood tables

Just as a table with descriptors can be used to define consequence levels, a likelihood table can be used to define the levels of likelihood of a given event that you will use to analyse risks.

Likelihood can be defined quantitatively or qualitatively. It can be based on statistical data, or predictive or simulation techniques, or expert opinion, using structured techniques.[21] Your agency needs to select the most appropriate tools and techniques given the level of your agency's risk management maturity.

[21] Tools and techniques are discussed in International Organization for Standardisation (ISO) 2009, *ISO/IEC 31010:2009 Risk management – risk assessment techniques*, ISO, Geneva.

Establishing the context



Likelihood table design

The three main steps in defining likelihood are:

1. Determine how many levels of likelihood you need in your table.
2. Decide how to describe the likelihood.
3. Describe the levels of likelihood in a table.

The steps for creating a likelihood table are discussed in detail below.

Step 1: Determine how many levels of likelihood you need in your table

As with consequences, the aim in step 1 is to define sufficient levels so that each risk can be assigned an appropriate likelihood rating. If you specify too few levels it will make it hard to differentiate between likelihoods. If you have too many levels, it will make it difficult to select the most appropriate likelihood rating, particularly when a risk straddles two likelihood levels. Most organisations that use likelihood tables define between three and five levels. You don't have to have the same number of consequence and likelihood levels. For example, you could decide to give greater emphasis to consequences and have more consequence levels than likelihood levels.

Step 2: Decide how to describe the likelihood

Likelihood tables usually use terms such as rare, possible, likely and almost certain to describe the chance of something happening. A likelihood table describes each of these terms based on:

- frequency – the number of times that something might happen in a given timeframe, and/or
- probability – the chance of something happening on a scale from 0 per cent (the event will not occur) to 100 per cent (the event will certainly occur).

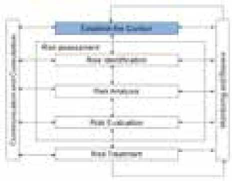
As with consequence tables, the method you use will be influenced by your agency's risk management maturity and the nature of its business, the type and reliability of data available, and the capabilities and experience of those who will be interpreting and analysing the data.

To define the likelihood of a risk, you need to consider all the sources of the risk that could cause the risk to emerge. To avoid inconsistencies in creating likelihood tables, you should specify the timeframe to be considered when making a judgement on likelihood. For example, if your agency's strategic planning horizon is five years, you may wish to specify a five-year timeframe for judging the likelihood of events occurring. You can also describe likelihoods in terms of how often a risk will occur within a defined planning cycle, such as the annual budget cycle.

Step 3: Describe the levels of likelihood in a table

Each level on the likelihood scale should be described so it is easily understood and unambiguous, using the method you chose in step 2. Each likelihood level should be clearly distinguished from the level above or below it.

Establishing the context



If you choose to describe likelihood levels in terms of both frequency and probability, you need to ensure that the descriptions for each level, whether in terms of frequency or in terms of probability, are broadly comparable.

Just like consequence tables, likelihood tables should be tailored to your agency's circumstances. An example of a typical likelihood table is shown in Table 4.5 below.

Table 4.5 – Likelihood table

Likelihood table		
Likelihood level	**Frequency**	**Probability**
Almost certain	The event is expected to occur in most circumstances, and frequently during the year	More than 99%
Likely	The event will probably occur once during the year	More than 20% and up to 99%
Possible	The event might occur at some time in the next five years	More than 1% and up to 20%
Rare	The event could occur in exceptional circumstances	Less than 1%

Measuring the effectiveness of your controls

You need to establish criteria to measure the effectiveness of your existing risk controls. Once you have identified existing controls, you will have to determine:

§ whether the controls are well designed – for example, are they capable of managing the risk and maintaining it at an acceptable or tolerable level?

§ whether the controls are operating as intended. Have they been, or can they be, proven to work in practice? Are they cost-effective?

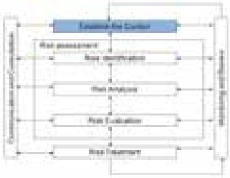
Your assessment of existing controls can be qualitative, semi-quantitative or quantitative, depending upon the data available. In many instances, a simple set of descriptors can be used to qualitatively assess control design and operating effectiveness as shown in the example[22] (Table 4.6) below.

Table 4.6 – Control effectiveness table

Control effectiveness table			
Level	**Description and further action**	**Design effectiveness**	**Operational effectiveness**
Substantially effective	Existing controls address risk, are in operation and are applied consistently. Management is confident that the controls are effective and reliable. Ongoing monitoring is required.	Y	Y
Partially effective	Controls are only partially effective, require ongoing monitoring and may need to be redesigned, improved or supplemented.	N	Y
		Y	N
Largely ineffective	Management cannot be confident that any degree of risk modification is being achieved. Controls need to be redesigned.	N	N

[22] Standards Australia 2010, *HB 158-2010 Delivering assurance based on ISO 31000:2009: risk management principles and guidelines,* Standards Australia, Sydney, provides another example of how control effectiveness can be qualitatively assessed.

Establishing the context



Where a control (or a suite of controls) has been assessed as ineffective, your analysis should also help you decide whether it would be better to improve the existing control(s) or replace them with another treatment.

There may be more than one control for a particular risk. It may be more useful to assess the effectiveness of all the controls taken as a whole for a particular risk rather than to individually assess the effectiveness of each control separately and try to combine the results.

Internal Audit can provide objective assurance of the adequacy and effectiveness of control processes.

Determining a risk level

The next step is to develop a method to combine consequences and likelihood to determine a risk level. Various techniques are available including:

- qualitative methods[23]
- semi-quantitative methods, which may use numerical scales and combine them using a formula
- quantitative methods to estimate practical values for likelihood and consequence and produce a value for the risk in specific units
- a combination of any of these techniques.

As with consequence and likelihood, the choice of technique for combining likelihood and consequence depends on your agency’s risk management maturity, staff capabilities and the availability and quality of data. For many agencies, including those just starting on their risk management journey, simple qualitative techniques may be adequate.

A common qualitative technique is the use of a risk matrix (see Figure 4.3 for an example). A risk matrix provides a graphic representation of the relationship between consequence, likelihood and the resulting risk level. Each square in the matrix represents a unique pairing of consequence and likelihood and, therefore, a risk level.[24]

In Figure 4.3 the risk matrix has been designed to assess threats. A similar approach could be used to analyse opportunities. To use the matrix to determine the level for a specific risk, find the appropriate consequence level from your consequence table and the corresponding likelihood from your likelihood table. The level of risk can then be read off the matrix.

[23] Tools and techniques are discussed in ISO/IEC 31010.

[24] A similar matrix can also be used to plot all of your agency’s risks to create a risk profile – refer to section 5.5.2. This is known as a heat map (see figure 5.7).

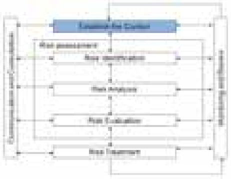
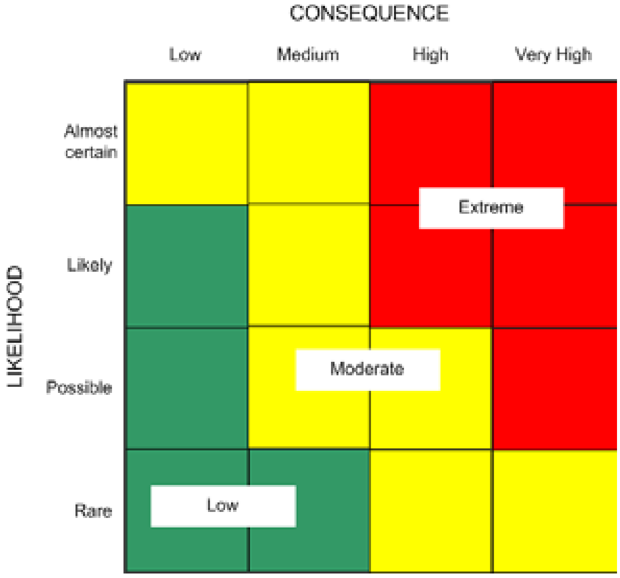


Figure 4.3 – Example of a risk matrix



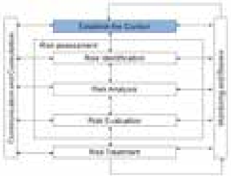
In Figure 4.3, multiple risk levels have been grouped and colour coded into extreme, moderate and low categories. Each grouping is associated with a decision rule, such as treat the risk to bring it to an acceptable level, treat the risk only under certain circumstances or accept the risk.

These groupings can also provide escalation points for risk management decisions, ensuring that risks are visible to, and managed at, the appropriate level in your agency. For example, the red, yellow and green groupings can be aligned with risk escalation points as shown in Table 4.7.

Table 4.7 – Risk actions and escalation points

Risk actions and escalation points			
Group	**Group description**	**Action required for risk**	**Escalation**
Red	Extreme	Action required: risks that cannot be tolerated and require treatment	§ Escalated to the Head of Authority and executive § Control strategy developed and monitored by the Head of Authority or executive
Yellow	Moderate	Potential action: risks that will be treated as long as the costs do not outweigh the benefits. Risk after treatment is As Low As Reasonably Practicable (ALARP)[25]	§ Managed at functional or service group level § Escalated to relevant direct report to the Head of Authority for information
Green	Low	No action: acceptable risks requiring no further treatment. May only require periodic monitoring	§ No action required § Monitoring within functional area or business unit

[25] Refer to ISO/IEC 31010.



The risk actions and escalation table reflects your agency's risk tolerance (refer to the discussion on determining your agency's tolerance for risk later in this section).

In designing a similar matrix for your own agency, you should:

- divide your matrix into the minimum number of groups required to express different levels of actions
- clearly specify the appropriate actions and escalation for each group
- colour squares in a way that minimises the chance of misrepresenting the level of actions required.

The example shows a 4 x 4 matrix with three escalation points. This can be adapted to your needs – for example, you may choose to use a 5 x 5 matrix with four escalation points.

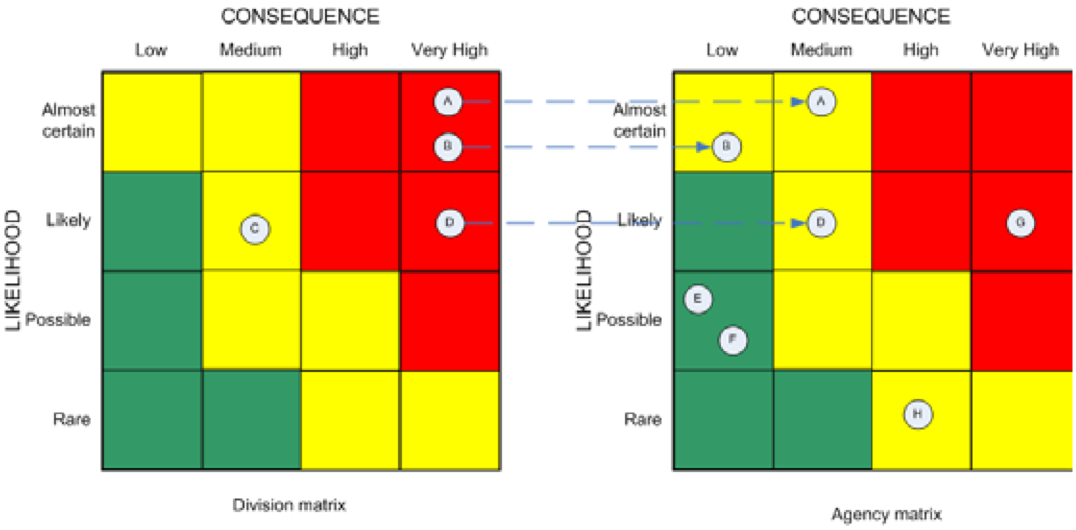
Your agency may be able to undertake all of its risk assessments using a single set of tables and matrix or you may require a number of sets. If more than one set is used, you need to design them so that risks assessed using the different sets are broadly comparable within one level of your agency.

Developing a hierarchy of risks in your agency

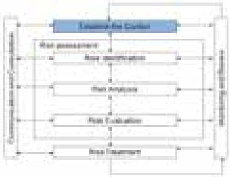
Each function or division of your agency should identify risks through their planning processes and their day-to-day operations (refer to section 3.3.4). To analyse and evaluate such functional or divisional risks, you should develop consequence and likelihood tables and risk matrices that are appropriate to their individual circumstances.

However, what may be rated as an extreme risk at one level of your agency, such as a division, may be rated as moderate or low risk at a higher level of management, such as the executive. Escalation points in each risk matrix should be set so that risks are escalated to the appropriate level of management, depending on delegations.

Figure 4.4 – Different levels of risk



Establishing the context



In figure 4.4, A, B and D refer to individual risks. A, B and D were assessed as very high risks at the divisional level but as low and medium risks at the whole-of-agency level.

If project risks are evaluated in the same way as overall agency risks, the impact of a particular project may be inappropriately managed. For example, if a small project goes over budget by 100 per cent, this may not be considered a high consequence compared with the consequence levels set at the agency level. You should design project-specific consequence tables and set escalation levels to ensure that major project risks are also brought the attention of your agency's executive.

Determining your agency's tolerance for risk

All organisations are exposed to a range of risks (both opportunities and threats) of varying severity arising from a number of internal and external sources. While you can avoid or mitigate some threats, it is usually necessary to tolerate a level of risk in order to achieve a level of benefit.

You need to determine the level at which your agency is prepared to accept or tolerate a specific risk without developing further strategies to modify the level of risk. This is generally a decision for your agency's executive and will depend on your agency's internal and external context, including such factors as:

- the nature of the services that your agency delivers
- your operating environment
- your legal and public sector obligations
- the type of consequence from the risk (e.g. to reputation, finances, safety, service delivery)
- your internal and external stakeholders, their perceptions of risk and how much risk they are prepared to allow your agency to accept.

It is important to ensure that there is a common awareness of the level of risk that your agency is prepared to accept or tolerate. This will enable consistent decision making when managing risk.

Your risk tolerance is expressed practically in the risk actions and escalation points in your risk matrix.

Organisations that exhibit a high level of risk management maturity understand, and clearly define, where the balance between loss and gain lies for the context in which they operate. By clearly defining the risks that your agency will accept or tolerate, your agency can improve its ability to deliver on services by:

- providing input for your decision-making processes
- showing how different resource allocation strategies can add to or reduce the total burden of risk
- identifying specific areas where risk should be removed
- increasing the transparency and consistency of business decisions.

As previously discussed, risks can be divided into those that require no further action, those that may require action, and those that demand action. Table 4.8 presents an example of how whole-of-agency risks can be classified into these three categories.

Establishing the context

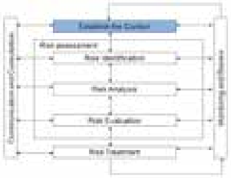


Table 4.8 – Risk tolerance

Risk tolerance table		
Response	**Threat**	**Opportunity**
Action required	Unacceptable risks Threats that your agency **cannot tolerate** at their current levels because their consequences, coupled with their likelihood, are unacceptably high	Opportunities whose positive consequences, coupled with their likelihood, are so large that your agency **must pursue** them because it cannot afford to forgo the benefits associated with them
Potential action	ALARP risks Threats that your agency is **prepared to tolerate** at their current levels if the costs associated with implementing additional control measures outweigh the associated benefits	Opportunities that your agency **may wish to pursue**, as the benefits outweigh the costs associated with implementing the strategies required to realise the opportunity
No action required	Acceptable risks Threats that your agency **can accept** at their current levels after existing controls	Opportunities that your agency will **give a low priority to**, as the benefits are not sufficient to expend resources on pursuing

The overall risk your agency faces is a combination of all of the individual risks that it has to deal with as it strives to meet its objectives. Your agency's overall risk should not exceed the total burden of risk that you are prepared to accept or tolerate. It is therefore important to take a holistic view of all your risks.

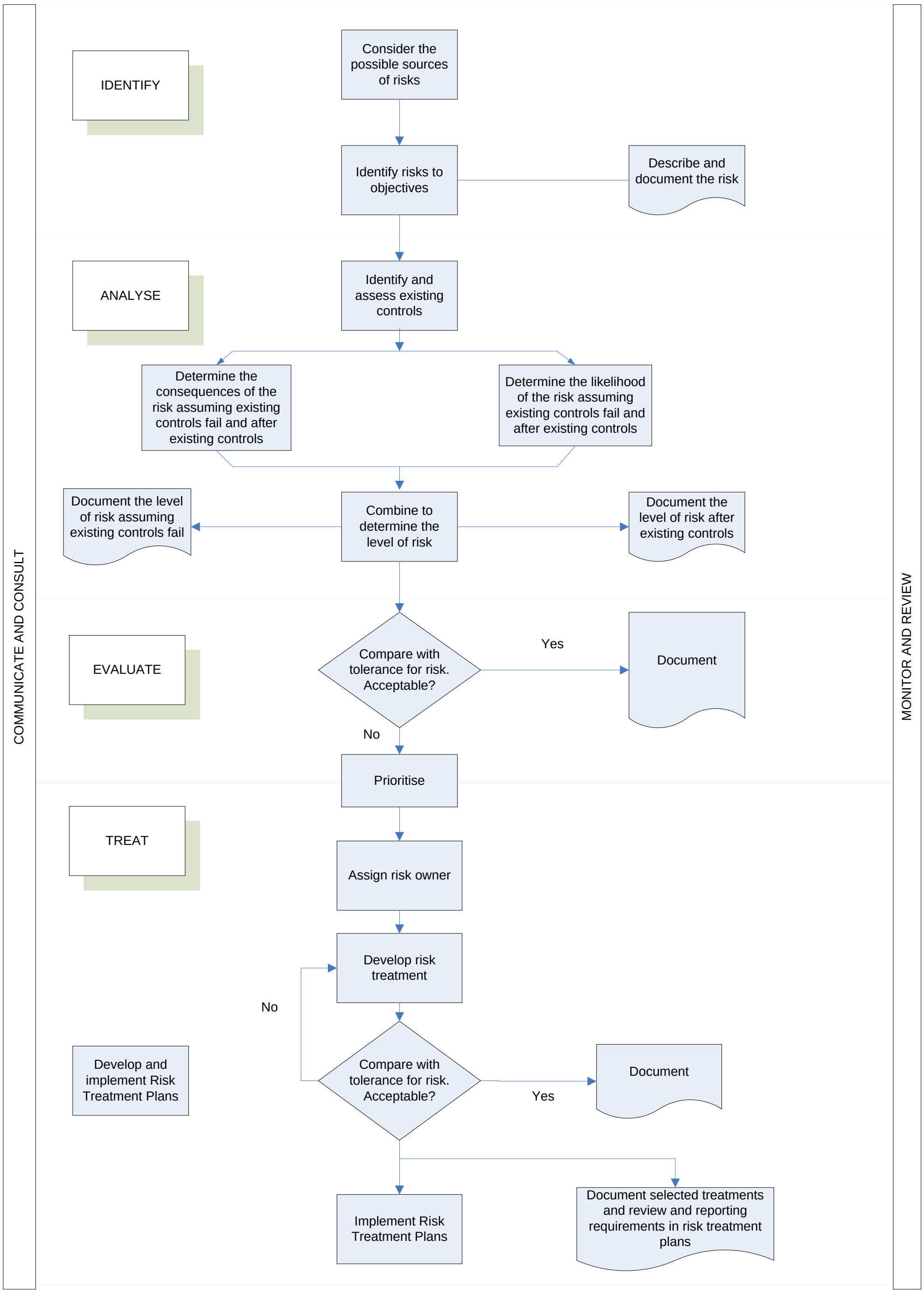
Understanding the level of risk that your agency is prepared to accept or tolerate is generally an evolving process, where changes occur over time, and with changing staff, systems, community expectations, cultures and technology. Executive and senior management levels must conduct regular discussions to ensure that risk management strategies remain appropriate. All staff in your agency should be aware of the actions required at different levels of risk.

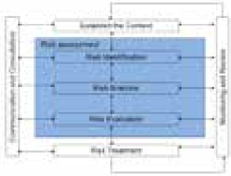
Chapter 5 – The risk management process: assessment and treatment

5.1 Risk assessment and treatment

Once the foundation of the risk management process has been established, you should be in a good position to undertake risk assessment and treatment. This chapter will lead you through the steps involved in these stages of the risk management process, as outlined in Figure 5.1.

Figure 5.1 – Risk assessment and treatment


COMMUNICATE AND CONSULT
MONITOR AND REVIEW
IDENTIFY
Consider the possible sources of risks
Identify risks to objectives
Describe and document the risk
ANALYSE
Identify and assess existing controls
Determine the consequences of the risk assuming existing controls fail and after existing controls
Determine the likelihood of the risk assuming existing controls fail and after existing controls
Document the level of risk assuming existing controls fail
Combine to determine the level of risk
Document the level of risk after existing controls
EVALUATE
Compare with tolerance for risk. Acceptable?
Yes
Document
No
Prioritise
TREAT
Assign risk owner
Develop risk treatment
No
Develop and implement Risk Treatment Plans
Compare with tolerance for risk. Acceptable?
Yes
Document
Implement Risk Treatment Plans
Document selected treatments and review and reporting requirements in risk treatment plans



5.2 Risk assessment

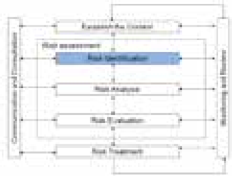
Risk assessment is a structured approach to identify and analyse the uncertainties that exists in meeting your agency's objectives. Risk assessment consists of three discrete stages: *risk identification*, *risk analysis* and *risk evaluation*.

Risk assessment aims to answer the questions set out in Table 5.1.

Table 5.1 – Risk assessment

Risk assessment		
Risk identification	**Risk analysis**	**Risk evaluation**
What can happen and why?	What are the consequences? How likely are the risks to occur? Are there any measures currently in place that act to reduce the consequences or the likelihoods of the identified risk? How reliable are these measures? What happens if they fail?	Is the current level of risk acceptable or tolerable compared with established criteria? If not, what further measures are needed to manage the risk?

The International Standards Organization has produced guidance on risk assessment techniques in addition to ISO 31000. IEC/ISO 31010: 2009, *Risk management – risk assessment techniques* (ISO 31010) provides an overview of each step in the risk assessment process and advice on the tools that can be used to perform these steps. ISO 31010 aims to reflect current good practice in the selection and use of risk assessment tools in a way that applies across a range of sectors and types of systems. It is a valuable resource for additional information on assessment tools and techniques.

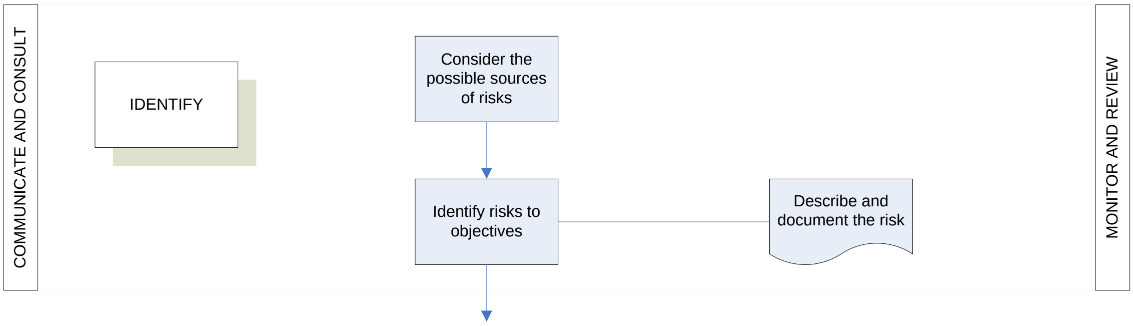


5.3 Risk identification

Risk identification is the process of finding, describing and recognising uncertainties that might enhance or inhibit your agency's ability to achieve its objectives. Identified risks form the basis of further analysis, evaluation and treatment. Risk identification is therefore a critical aspect of your agency's risk management process.

In identifying risks, you must consider not only threats, but also the risks associated with not pursuing an opportunity, such as reducing crime by increasing the number of police officers on patrol. Once the risk is identified, any existing controls should also be identified at the same time.

Figure 5.2 – The first stage of risk assessment: risk identification


COMMUNICATE AND CONSULT
IDENTIFY
Consider the possible sources of risks
Identify risks to objectives
Describe and document the risk
MONITOR AND REVIEW

5.3.1 Areas of risk

Each agency needs to determine the risks that are most relevant to itself. As part of establishing your context, you should have developed an understanding of your agency's objectives, and the key trends and drivers that might affect your ability to achieve these objectives.

It may be useful to think about some or all of the following areas, in terms of what positive or negative effects there could be on your agency's objectives.

§ **Governance**: failure to meet compliance and accountability requirements; inadequate or unclear definition of roles and responsibilities; lack of effective and transparent decision-making processes; inadequate control and procedural frameworks; the robustness of any third-party systems and processes

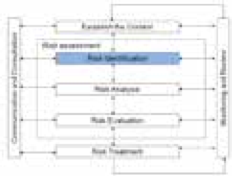
§ **Fraud and corruption**[26]**:** potential losses due to fraud or behaviour contrary to your agency's code of conduct; underlying political, business and community culture and attitudes

§ **Resources**: financial, human, physical assets, systems, including their adequacy or threats to them, as well as opportunities created through efficiencies

§ **Legislative and contractual compliance:** failure to comply with legislation and contract requirements; or opportunities created by changes to legislation

[26] For detailed information on corruption risks, refer to ICAC resource 'Knowing your risks' at http://www.icac.nsw.gov.au/preventing-corruption/knowing-your-risks.

Risk identification



- **Policies, programs and projects:** events that could impair or enhance the delivery of the policy, program or project on time and within budget, or the quality of its outcomes; events that could lead to damage to your agency's assets or compromise the security of sensitive information
- **Continuity of operations and services:** events that could cause disruption to services or operations
- **Environmental damage:** events that could damage the environment
- **Work health and safety:** events that could result in injury or death to staff, clients, contractors or others
- **Procurement:** failure to meet compliance with relevant requirements, including probity and achieving value for money outcomes, as well as positive outcomes leading to savings and efficiencies
- **Reporting:** reliability and timeliness of financial and other information.

5.3.2 How to identify risks

Many tools and techniques can be used to identify risks. Select a method or methods best suited to your agency's objectives, capabilities, risk management maturity and the nature of risks faced. Possible approaches to risk identification include the following:

- **Risk self-assessment:** each division of the agency reviews its own activities, objectives and events that can influence achieving its objectives. Risk assessments may be conducted in formalised workshops facilitated by either the risk manager or a professional facilitator.

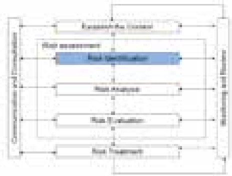
- **Commissioned risk review:** a team is established to review the operations and activities of the agency in order to articulate its objectives and identify the potential events that could affect the achievement of the objectives.

These approaches are not mutually exclusive and a combination of approaches may also be used.

A simple process, which could be led by the agency's Chief Risk Officer or risk management team to identify risks, is to:

- consider possible sources of risk for your agency (or business unit, policy, program, project, etc.)
- discuss possible areas of risk with key individuals, within and outside the organisation, including people who have a sound knowledge of the business (e.g. staff and management, external stakeholders and clients, and other subject matter experts); discussions could take the form of structured or semi-structured interviews, facilitated workshops or brain-storming sessions, informed by relevant and up-to-date information
- identify potential risks to the organisation (or business unit, policy, program, project etc.) based on this consultation
- document the identified risks and the risk identification process that was used as well as stakeholders involved in the process.

Risk identification



A number of other methods can be used to identify risks[27], including:

- checklists (lists of hazards, risks and control failures, based on experience, such as previous risk assessments or past failures)
- self-assessment questionnaires
- evidence-based methods, such as reviews of historical data
- systematic team-based approaches involving experts
- more specialised techniques, such HAZOP (Hazard and Operability studies)
- audits or physical inspections.

Risks can also be identified through the formal planning processes and normal organisational activities in your agency, such as:

- assessment against standards
- records of incidents or complaints
- investigations
- internal or external audit, or both
- routine team meetings.

Volume 2 describes another technique – the Source–Pathway–Target methodology – that you could use to identify risks in a workshop or brain-storming session.

Each of these methods has its strengths and limitations. For example, previous experience can be an important guide to identifying potential risks. However, previous experience may not be a reliable guide in considering risks associated with new and unfamiliar business processes or systems, or with the development and implementation of new policies, programs and projects. It is therefore important that your agency follow a systematic and disciplined approach to identifying risk that is not limited by previous experience.

Irrespective of the technique your agency selects, risk identification should be integral to your strategic, business, operational, change management and project planning processes. It should be part of your day-to-day activities. Knowledgeable stakeholders should be involved. All risks should be linked to your agency's objectives, which should have been identified when you established the context (refer to section 4.3). Risk identification should be a continuous process to identify new risks as they emerge and confirm the continued validity of previously identified risks.

5.3.3 How to describe risks

Once identified, risks should be described and documented so that:

- the source, the event and the impact on your agency's objectives are consistently and clearly defined and differentiated
- those who were not involved in the assessment process can understand the risk.

An example of a risk description could be as shown in Figure 5.3.

[27] Refer to ISO 31010 for a more comprehensive description of tools and techniques.

Risk identification

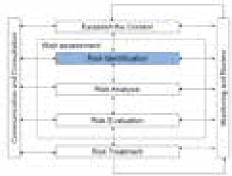
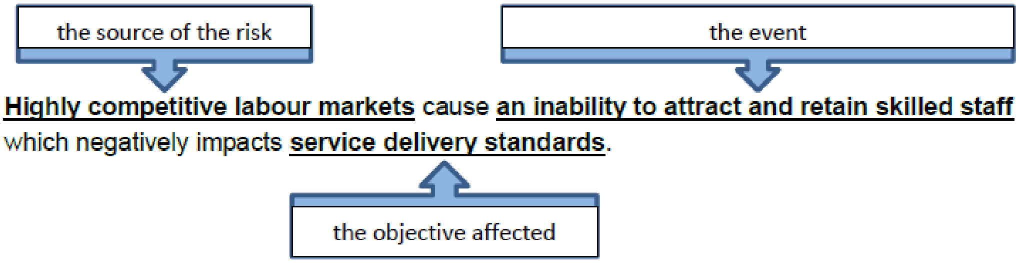


Figure 5.3 – Example of a risk description



Highly competitive labour markets cause **an inability to attract and retain skilled staff** which negatively impacts **service delivery standards**.

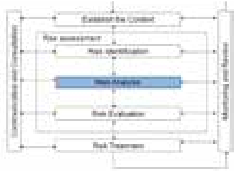
Risks often have more than one cause, and you may need to determine whether the risk is better described and analysed by being combined or identified separately.

Once risks are identified, organisations commonly classify them into categories, for example, Financial, Service Delivery, Safety, Environmental, based on either:

- the objectives affected
- the selected consequences criterion (which may be the same).

Categorising your risks enables risk information to be searched or filtered across multiple criteria.

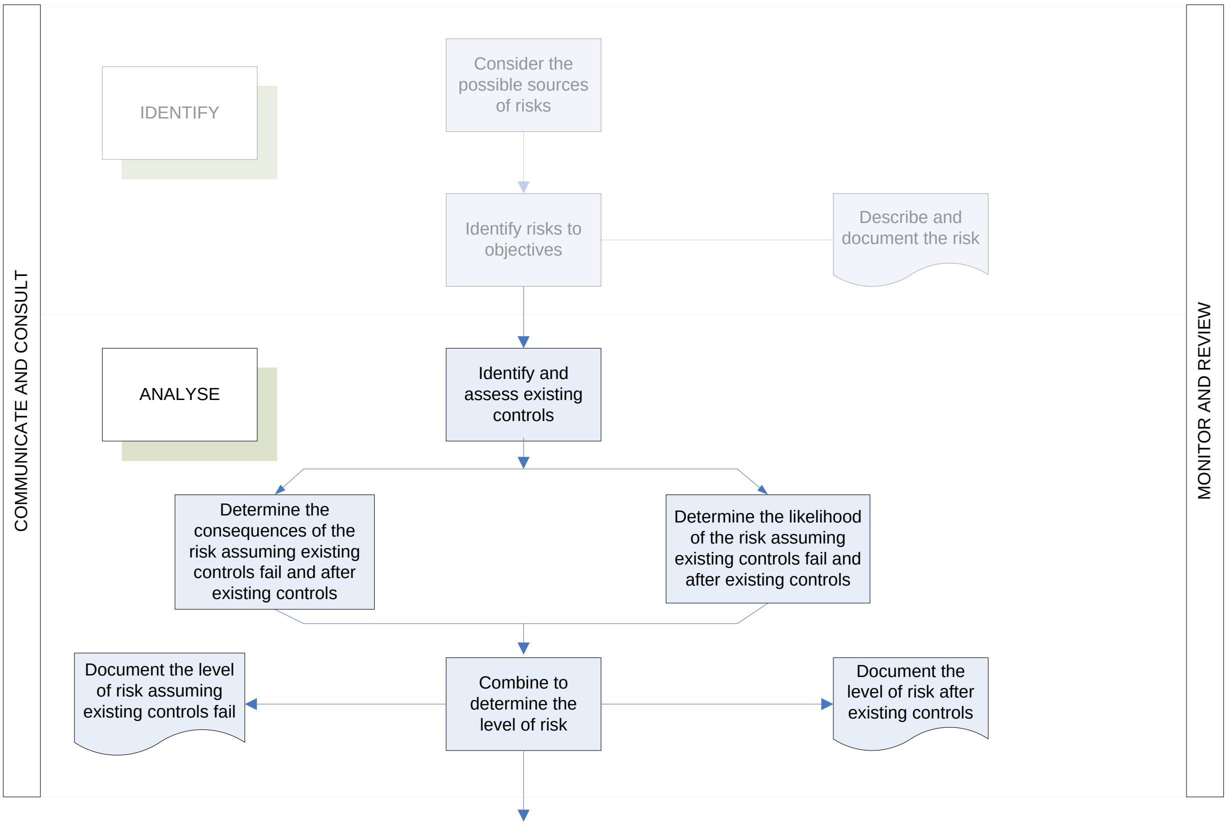
Assessment - Risk Analysis



5.4 Risk analysis

Risk analysis is the process of coming to an understanding about the nature and level of risks so you can make decisions about whether a risk needs to be treated. You should document each step of your risk assessment process for each risk. (Refer to Volume 2 for a template that you can use to document your risk assessment.)

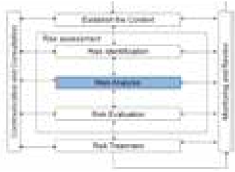
Figure 5.4 – The second stage of risk assessment: risk analysis


COMMUNICATE AND CONSULT
IDENTIFY
Consider the possible sources of risks
Identify risks to objectives
Describe and document the risk
ANALYSE
Identify and assess existing controls
Determine the consequences of the risk assuming existing controls fail and after existing controls
Determine the likelihood of the risk assuming existing controls fail and after existing controls
Document the level of risk assuming existing controls fail
Combine to determine the level of risk
Document the level of risk after existing controls
MONITOR AND REVIEW

5.4.1 Analysis of existing controls

Once you have identified risks, the next step is to identify controls that currently exist to minimise or prevent negative consequences, or reduce the likelihood of a potential event (or enhance positive consequences or likelihood of an opportunity). You then need to assess the effectiveness of current controls using the control effectiveness criteria that you determined as part of establishing the context (refer to section 4.3).

Assessment - Risk Analysis



5.4.2 Determining the level of risk

The consequences and likelihood of the risks identified through the risk identification process should now be estimated and combined to determine the level of a risk.

Use the consequence and likelihood tables and the method of combining these (i.e. your risk matrix) that you developed as part of establishing your risk management context (see section 4.3.3) for risk analysis.

A single risk may have more than one consequence. You need to establish a business rule on how you will deal with such instances. For example, you may decide to carry out further analysis based on only the consequence type with the most serious credible outcome. Naturally, the likelihood relevant to the selected consequence should be used when determining the risk level.

It is often good practice to analyse consequences and likelihoods and the level of risk in both the worst case (assuming current controls fail completely), and the current case, that is, after considering the effectiveness of existing controls. (Refer to the risk assessment templates in Volume 2.)

5.4.3 Uncertainty and sensitivities

Since the risk analysis process has inherent uncertainties, it is important that uncertainties and sensitivities are also identified and documented when you are interpreting and communicating the results of risk analysis. This information can also be included in your risk register (see section 5.5.1 and refer to Volume 2 for a worked example).

5.4.4 Cognitive bias

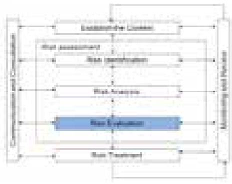
The effectiveness of risk management is dependent on sound risk assessments. Even if your agency has all the well-designed processes, methods and tools for risk management, risk assessment is ultimately an activity that requires subjective judgement. Although there may be other causes for faulty risk assessments, cognitive biases can be particularly pervasive.

If unchecked, these biases can lead to systematic decision-making errors and faulty risk assessments. Cognitive biases include:

- **Anchoring:** relying too heavily, or ‘anchoring’, on one aspect or piece of information when making decisions
- **Bandwagon (or herd) effect:** doing (or believing) something because many other people do (or believe) the same
- **Confirmation bias:** looking for evidence to justify preconceived ideas
- **Framing effect bias:** arriving at conclusions based on how information is presented
- **Optimism (or over-confidence):** overestimating the likelihood of favourable outcomes.

Recognising these biases is the first step in minimising their impact on your risk assessment.

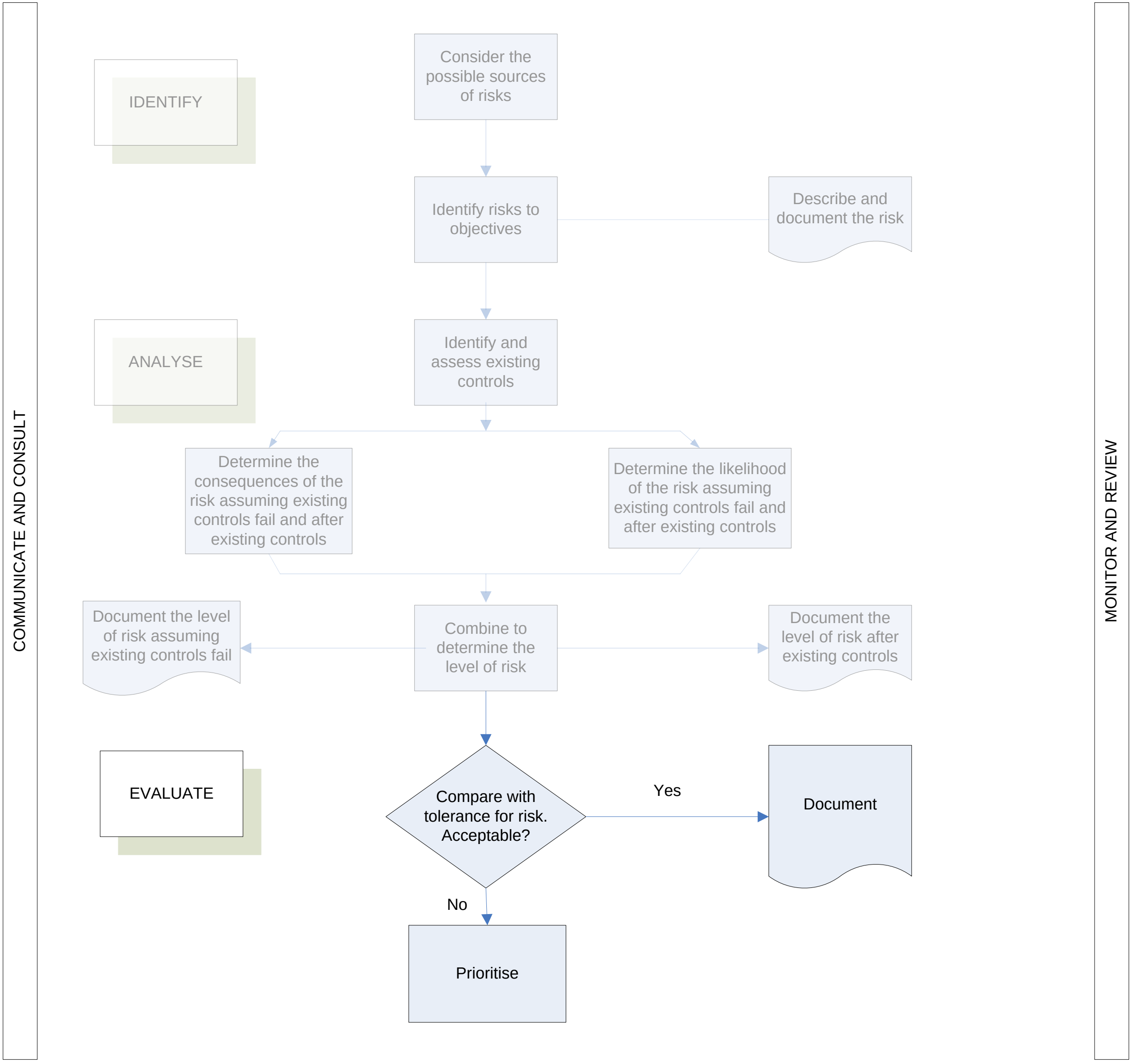
Risk Assessment - Risk Evaluation



5.5 Risk evaluation

Risk evaluation is the process of deciding which risks require further treatment and in what order. It is based on the outcomes of risk analysis. It involves determining where a particular risk, after existing controls are applied, sits compared with the level of risk your agency is prepared to accept or tolerate, and the need for and priority of further treatment.

Figure 5.5 – The third stage of risk assessment: risk evaluation

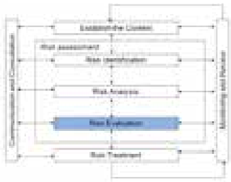

COMMUNICATE AND CONSULT
MONITOR AND REVIEW
IDENTIFY
Consider the possible sources of risks
Identify risks to objectives
Describe and document the risk
ANALYSE
Identify and assess existing controls
Determine the consequences of the risk assuming existing controls fail and after existing controls
Determine the likelihood of the risk assuming existing controls fail and after existing controls
Document the level of risk assuming existing controls fail
Combine to determine the level of risk
Document the level of risk after existing controls
EVALUATE
Compare with tolerance for risk. Acceptable?
Yes
Document
No
Prioritise

ISO 31010 recommends that risks be screened to identify the most significant and exclude the least significant, based on the criteria developed when establishing the context. It may be necessary to revisit the criteria now that more is known about the risk. The least tolerable risks should be given highest priority.

This evaluation of risks could lead to a decision to:

- treat the risk without further analysis, or
- consider the risk as insignificant and not warrant treatment, or
- continue to undertake a more detailed analysis of the risk.

Risk Assessment - Risk Evaluation



Using the qualitative risk matrix technique described in section 4.3.3 allows risks to be prioritised according to their likelihood and consequence. It does not, however, provide an objective method of distinguishing or prioritising risks that have been assessed as having the same consequence and likelihood. Such risks may have to be subjectively ranked.[28]

5.5.1 Risk registers

To manage risk effectively across your entire agency, key stakeholders must have full knowledge of the range of risks your agency faces, including how these risks might change with time, and the associated risk control strategies.

The most common way to document this information is by using one or more risk registers. A risk register is simply a list of the risks that your agency has identified and assessed using its risk management process. It provides a holistic view of the risks faced by your agency and enables key stakeholders to make informed decisions regarding risks and their management. A risk register also helps meet the information needs of the Audit and Risk Committee, members of the boards, executives and other relevant stakeholders.

You could use a risk register to document and manage all the risks faced by your agency, including strategic risk, as well as risks within a particular project or activity. Large and complex agencies might find it helpful to develop a hierarchy of risk registers to support and reflect their planning framework. Responsibility for maintaining the risk register should be assigned at each level of your agency. For example, your whole-of-agency risk register should be compiled by your Chief Risk Officer.

A comprehensive risk register typically contains the following information:

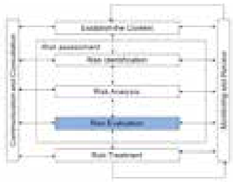
§ risk ID (this is a unique identifier)
§ entry date (into risk register)
§ name of the person(s) who did the assessment
§ description of the risk
§ objective(s) that will be affected by the risk
§ risk assessment information, such as:

  – the worst case consequence, likelihood and risk level
  – the current controls and their effectiveness
  – the current consequence likelihood and risk level
  – whether the risk is acceptable or tolerable
  – additional treatments if the risk is not acceptable or tolerable
  – the residual risk level once additional treatments have been implemented.

§ risk owner – who is responsible for managing the risk
§ monitoring information – how and when the risk and its controls will be reviewed and reported
§ the date the risk register was last updated
§ risk category (e.g. Financial, Service Delivery, Work Health and Safety).

[28] HB 158-2010 suggests using Potential Exposure (defined as 'the total plausible maximum impact on an organisation arising from a *risk without regard to controls*') as a basis to rank risks (emphasis added).

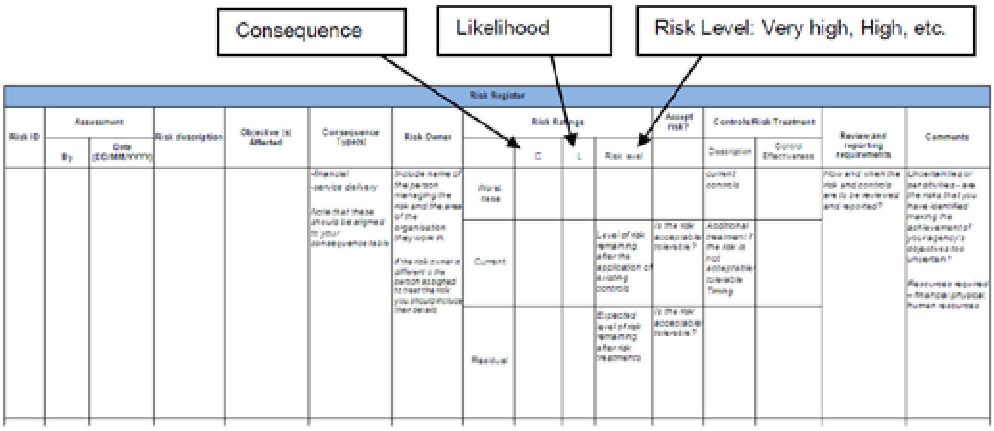
Risk Assessment - Risk Evaluation



The information captured in your risk register can be extremely useful in helping your agency prioritise risks and make the best use of its resources.

Your agency's risk register can be developed or set out in many ways. The content of your risk register must be customised for your agency and the information needs of key stakeholders. Figure 5.6 shows just one example of a risk register. In more complex organisations, additional technical or specific information may be needed (refer to Volume 2 for a template and a worked example of a risk register).

Figure 5.6 – An example of a risk register


Consequence
Likelihood
Risk Level: Very high, High, etc.

Risk Register

Risk ID	Assessment		Risk description	Objective (s) Affected	Consequence Type(s)	Risk Owner	Risk Ratings				Accept risk?	Controls/Risk Treatment		Review and reporting requirements	Comments
	By	Date (DD/MM/YYYY)						C	L	Risk level		Description	Control Effectiveness		
					-financial -service delivery Note that these should be aligned to your consequence table	Include name of the person managing the risk and the area of the organisation they work in. If the risk owner is different to the person assigned to treat the risk you should include their details	Worst case					current controls		How and when the risk and controls are to be reviewed and reported?	Uncertainties or sensitivities – are the risks that you have identified making the achievement of your agency's objectives too uncertain? Resources required – financial, physical, human resources
							Current			Level of risk remaining after the application of existing controls	Is the risk acceptable/ tolerable?	Additional treatment if the risk is not acceptable/ tolerable Timing			
							Residual			Expected level of risk remaining after risk treatments	Is the risk acceptable/ tolerable?				

Your agency needs to decide whether risks that are no longer relevant are removed from the register and archived, or remain on the register but are marked as no longer applicable. Both strategies have their benefits: archiving helps to restrict the length of the register to a manageable level, while retaining all risks on the register can help maintain corporate knowledge.

It is important that there is an audit trail of changes to the risk register, so there is a record of when changes are made and who has made them.

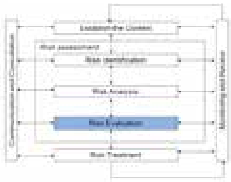
5.5.2 Risk profiles

Risk profiles are summaries used to present an overview of information contained in risk registers. The aim of the risk profile is to promote consistent organisational understanding of significant risks and their controls. Risk profiles can:

§ summarise and add value to the information in risk registers for risk owners, members of boards or executives, Audit and Risk Committees, and other relevant stakeholders
§ help identify the objectives associated with the greatest uncertainty (i.e. most at risk)
§ highlight significant risks and key controls
§ track progress on the implementation and effectiveness of controls
§ track how the organisation's risks change over time
§ inform continuous improvement in organisational performance.

Risk profiles can be developed for any level in your agency, such as at corporate or divisional level, as long as you can map the risks at that level against a set of relevant objectives.

Risk Assessment - Risk Evaluation



What information should your agency's risk profile contain?

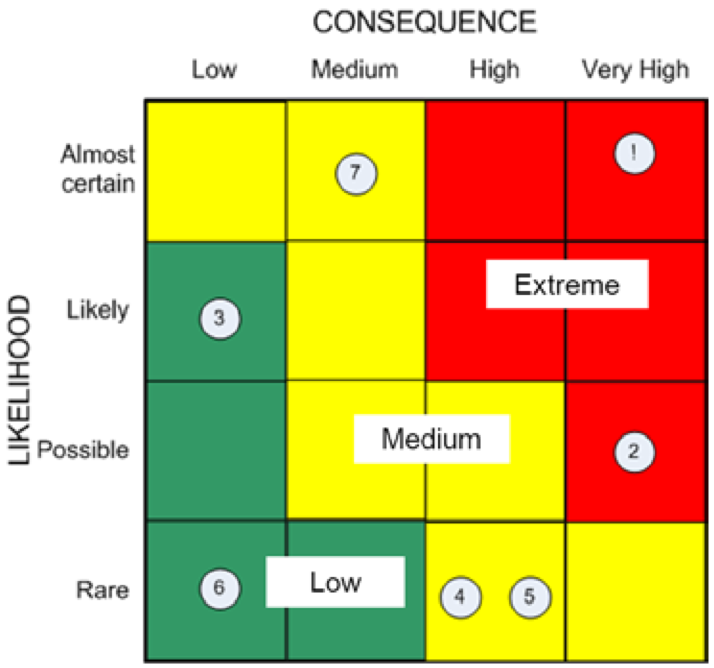
Information in the risk profile falls into two categories: information that focuses on risk and information that focuses on risk controls. Your agency can use a mix of diagrams and tables to aggregate and summarise the information and to highlight areas that require consideration. Some of the ways risk information can be summarised in risk profiles include heat maps, risks by objective, control effectiveness maps, and reports on significant risks.

Heat maps

Heat maps are tools used to graphically present an agency's risk levels compared with its risk tolerance.

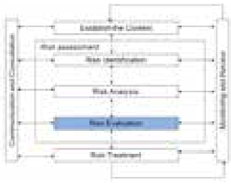
A heat map is produced by plotting multiple risks on your agency's risk matrix. In the example in Figure 5.7, each number represents a risk. This number corresponds with the risk identifier in the risk register. Each risk is plotted on the matrix based on the consequence and likelihood ratings given to the risk in the risk assessment. In Figure 5.7, residual risks have been plotted on a 4 x 4 matrix with three risk groupings. Risk number 1 has a *very high* rating on the consequence scale and has an *almost certain* rating on the likelihood scale, and therefore falls in the red grouping as an extreme risk (unacceptable or intolerable risks requiring treatment).

Figure 5.7 – Example of a heat map



You can also increase the amount of information displayed in the heat map. For example, you could use different graphics, in addition to the risk identification number, to identify risks associated with different objectives.

Risk Assessment - Risk Evaluation

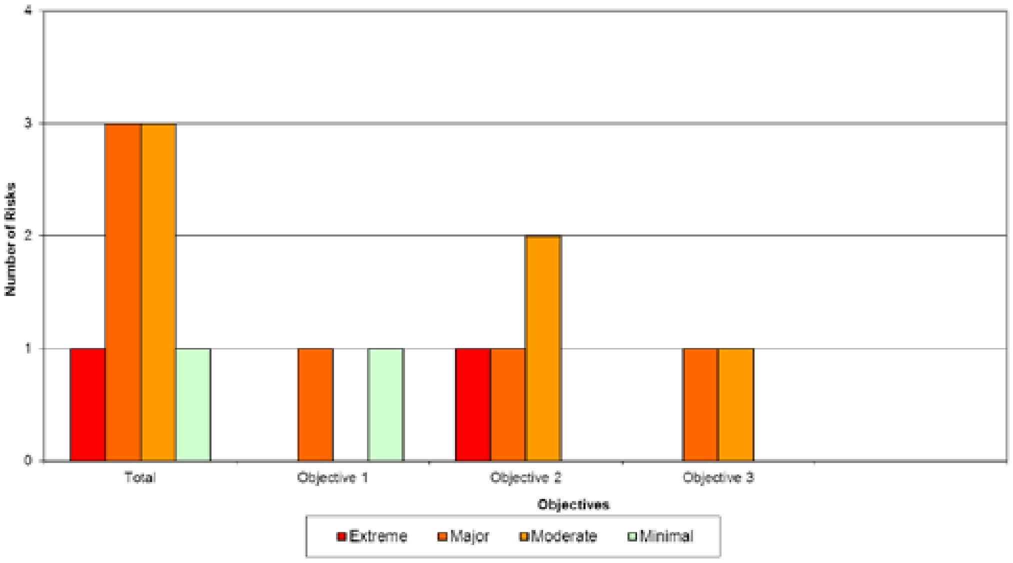


Risks by objective

The relationship between risks and objectives can be visually represented by graphing the number of risks associated with each objective. This gives your agency an overview of the level of uncertainty associated with each objective.

In the Figure 5.8, the number of risks, by level, has been plotted against each objective.[29] In this instance, the greatest uncertainty is associated with objective 2.

Figure 5.8 – Profile of risks affecting strategic objectives



Control effectiveness map

You can graphically show how the levels of your agency's risks have changed because of current controls. Each risk identifier in Figure 5.9 represents a risk in the risk register and the direction of the arrow depicts the effect of current controls on the worst case level of the risk. Note that in this example of a 4 x 4 matrix, some risks are shown with only one symbol without an arrow. In such instances, the current controls for the risk are non-existent or ineffective. Using this risk profile can help your agency identify where it might need to modify its control strategies.

[29] Note in this example four risk groupings have been used-Extreme, Major, Moderate and Minimal

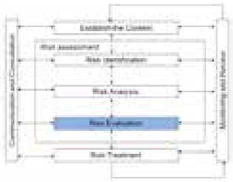
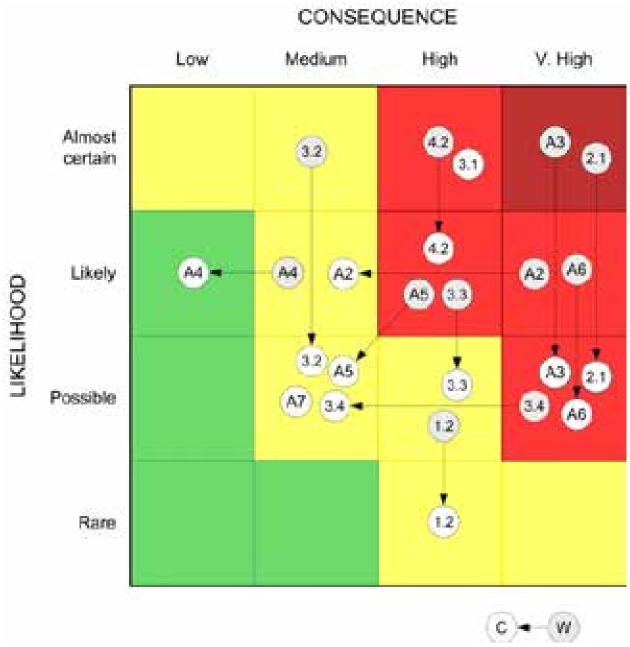


Figure 5.9 – Example of a control effectiveness map graphing worst case and current level of risk



Legend: C = current risk level, W = worst case risk level

You can also graphically show how the current risk levels of your agency's risks are anticipated to change because of additional risk treatments that have been introduced.

Each risk identifier in Figure 5.10 represents a risk in the risk register and the direction of the arrow depicts the effect of risk treatments on the current risk level. Note that in this example some risks, where additional treatments are non-existent or ineffective, are shown with only the identifier and no arrow. Using such a risk profile can help your agency identify where it might need to modify its control strategies.

Risk Assessment - Risk Evaluation

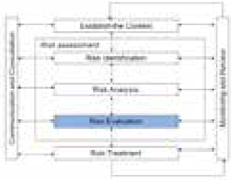
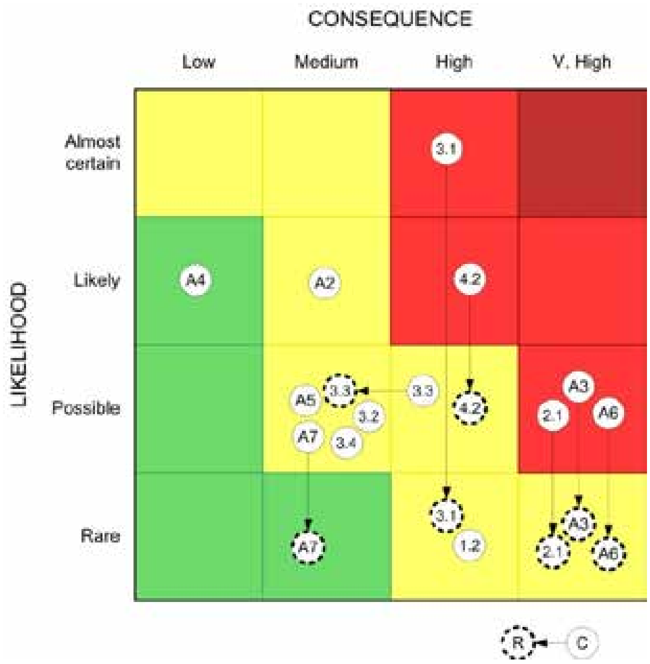


Figure 5.10 – Example of a control effectiveness map graphing current level and residual risk



Legend: C = current risk level, R = residual risk level

Status reports monitoring significant risks

In addition to using heat maps to present information on the level of your agency's risks and their relationships to its objectives, your agency can capture information on the strategies it is using to monitor its significant risks (including significant emerging risks) and their status.

In Figure 5.10, significant risks are those that have a worst case risk level of high or very high, where the consequence rating is very high.

One way to capture this information is to summarise it in a table, under the following headings:

- the risk and the objective(s) it affects
- the worst case level of the risk
- the current level of risk
- when the risk was last assessed
- the risk owner
- how you are monitoring the risk
- the status of your monitoring strategy.

An example is shown in Figure 5.11.

Risk Assessment - Risk Evaluation

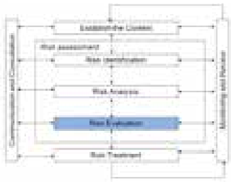
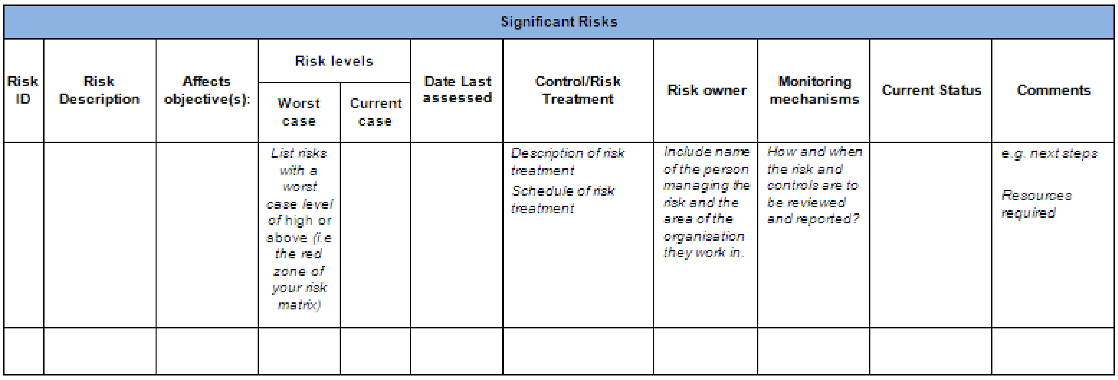


Figure 5.11 – Sample table for monitoring risks



Significant Risks										
Risk ID	Risk Description	Affects objective(s):	Risk levels		Date Last assessed	Control/Risk Treatment	Risk owner	Monitoring mechanisms	Current Status	Comments
			Worst case	Current case						
			List risks with a worst case level of high or above (i.e the red zone of your risk matrix)			*Description of risk treatment* *Schedule of risk treatment*	*Include name of the person managing the risk and the area of the organisation they work in.*	*How and when the risk and controls are to be reviewed and reported?*		*e.g. next steps* *Resources required*

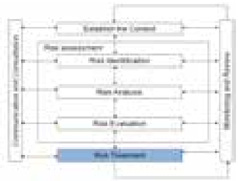
You could include traffic light indicators in the table (e.g. red for urgent attention, orange for warning and green for acceptable), or otherwise flag risks that require immediate attention or closer monitoring.

5.5.3 Documenting the risk assessment process

Individual risk assessments should be documented (e.g. using the risk assessment template in Volume 2). All risks should be collated in your risk register (see section 5.5.1). You should also document other aspects of your risk management process, including:

- the internal and external and risk management context
- your risk identification methodology
- risk criteria, including your likelihood and consequence tables and risk matrix, describing the terms and levels used
- sources of information, assumptions and limitations.

Risk Treatment

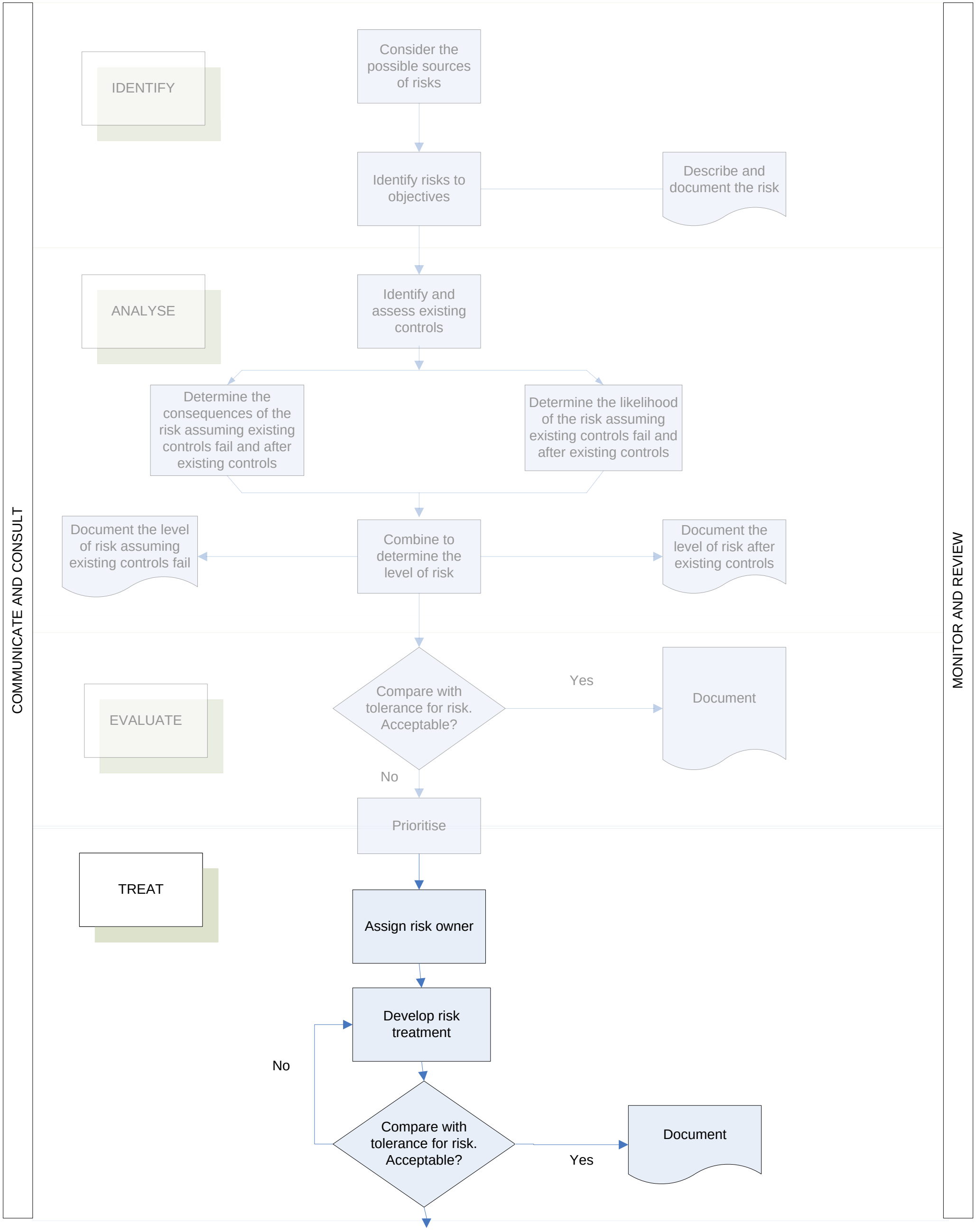


5.6 Risk treatment

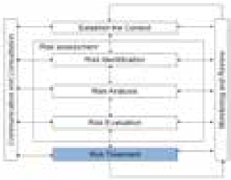
Risk treatment is the process of identifying, selecting and implementing responses to risks that fall outside the risk levels your agency is prepared to accept or tolerate. These risks will have been identified as part of the risk evaluation process (discussed in section 5.5).

This part of the risk management process seeks to control these risks by developing a treatment that addresses underlying causes, assesses the treatment's effectiveness and, if the residual risk is still considered unacceptable or intolerable, generates an alternative treatment.

Figure 5.12 – Risk treatment


COMMUNICATE AND CONSULT
MONITOR AND REVIEW
IDENTIFY
Consider the possible sources of risks
Identify risks to objectives
Describe and document the risk
ANALYSE
Identify and assess existing controls
Determine the consequences of the risk assuming existing controls fail and after existing controls
Determine the likelihood of the risk assuming existing controls fail and after existing controls
Document the level of risk assuming existing controls fail
Combine to determine the level of risk
Document the level of risk after existing controls
EVALUATE
Compare with tolerance for risk. Acceptable?
Yes
Document
No
Prioritise
TREAT
Assign risk owner
Develop risk treatment
No
Compare with tolerance for risk. Acceptable?
Yes
Document

Risk Treatment



Risk treatments should be developed by, or under the direction of, a risk owner. Like risk assessments, risk treatments may be developed by a team – either the team that conducted the risk assessment or a different team. It may be beneficial to review the risk assessment before deciding on risk treatment options.

The evaluation of the effectiveness of existing controls, which should have been carried out as part of the risk assessment process, can assist in determining whether existing controls should be modified or new treatments introduced.

A number of generic options (which are not necessarily mutually exclusive) can be considered for treating risks, including:

§ **Avoiding the risk:** Where the level of risk is unacceptable or intolerable and the means of control are either not viable or not worthwhile, it might be possible to avoid the risk, for instance, by not proceeding with an activity that could generate the risk

§ **Changing the likelihood:** Developing and implementing strategies to change the likelihood of the risk occurring, either to reduce the chance of negative outcomes or increase the chance of positive outcomes

§ **Changing the consequence:** Developing and implementing strategies to reduce the size of negative outcomes or increase the magnitude of positive outcomes

§ **Taking the opportunity:** Developing and implementing strategies to recognise, and benefit from, circumstances that offer opportunities, as well as strategies to exploit possible benefits while mitigating threats

§ **Sharing the risk:** The responsibility for treating risk can be either shared or transferred to other parties, for example, contracting or other arrangements with a third party, such as other agencies or insurance companies. This can be a good option to reduce your agency's exposure to financial risk or asset risk. It is important to note, however, that outsourcing may not result in the complete transfer of a risk[30].

§ **Accepting or tolerating the risk based on informed decision:** This may be appropriate where the remaining risk levels are insufficient to justify potential treatment options or where it is not possible or is not cost-effective to treat the residual risk.

The risk treatment itself could introduce secondary risks. For example, sharing or transferring risks raises a new risk in that the organisation or division within your agency with which the risk has been shared or transferred to may not manage the risk effectively. Secondary risks like this should not be treated as new and separate risks, but should be considered along with the original risk when developing a risk treatment.

Regular and careful monitoring is essential to ensure the effectiveness of any risk treatment.

[30] While the responsibility for treating some risk as well as the financial impact to your agency may be outsourced agencies remain ultimately accountable for the successful delivery of their objectives and therefore accountable for managing their risks. In addition, it is important to note that some risks are not able to be transferred such as risks to reputation or corruption risks.

Risk Treatment

5.6.1 Selection of risk treatment options

It may not be possible to eliminate all risk relating to your agency's operations. Risk treatments need to be cost-effective, practicable and commensurate with the level of the risk, especially when addressing risks in the yellow (or moderate) category of your risk matrix (refer to section 4.3.3).

In selecting the most appropriate treatment or combination of treatments, you need to balance the costs and resource requirements against the likely benefits. Both financial and non-financial costs and benefits should be considered in making this assessment.

Grouping risks into categories, such as Financial, Service Delivery, Safety and Environmental, may also help in the development of cost-effective treatments. Since a chosen treatment might affect multiple risks, you should review the suite of proposed treatments to resolve any conflicts and eliminate any duplication.

Apart from cost–benefit analysis, the other important consideration in selecting risk treatment options is the perception of key stakeholders. Your key stakeholders should be consulted so you can consider and understand a range of perspectives and experiences before deciding on a control.

5.6.2 Develop and implement risk treatment plans

Once selected, chosen risk treatments should be developed by risk owners into detailed risk treatment plans so that:

§ risk treatments can be implemented effectively and in a timely manner
§ performance and success measures can be assigned for the risk treatment so that your agency can monitor and review its ongoing effectiveness
§ your agency is able to demonstrate the application of risk management in the organisation.

Information documented in risk treatment plans should include:

§ the rationale for selection of treatment, and the expected outcome of the treatment; it is important that decision makers are kept informed of the residual risk
§ accountabilities and responsibilities – it would be typical, for example, for the accountability for strategic risks to be assigned to a direct report to the Head of Authority, who may in turn choose to delegate implementation responsibilities to others
§ the actions to be undertaken to practically implement the selected treatment
§ budgets and other resources required (e.g. physical assets, human resources)
§ performance measures – measures to evaluate the effectiveness of the controls and evaluation criteria
§ timeframe and critical implementation milestones
§ reporting, review and monitoring protocols.

Risk Treatment

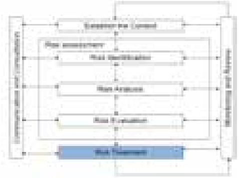
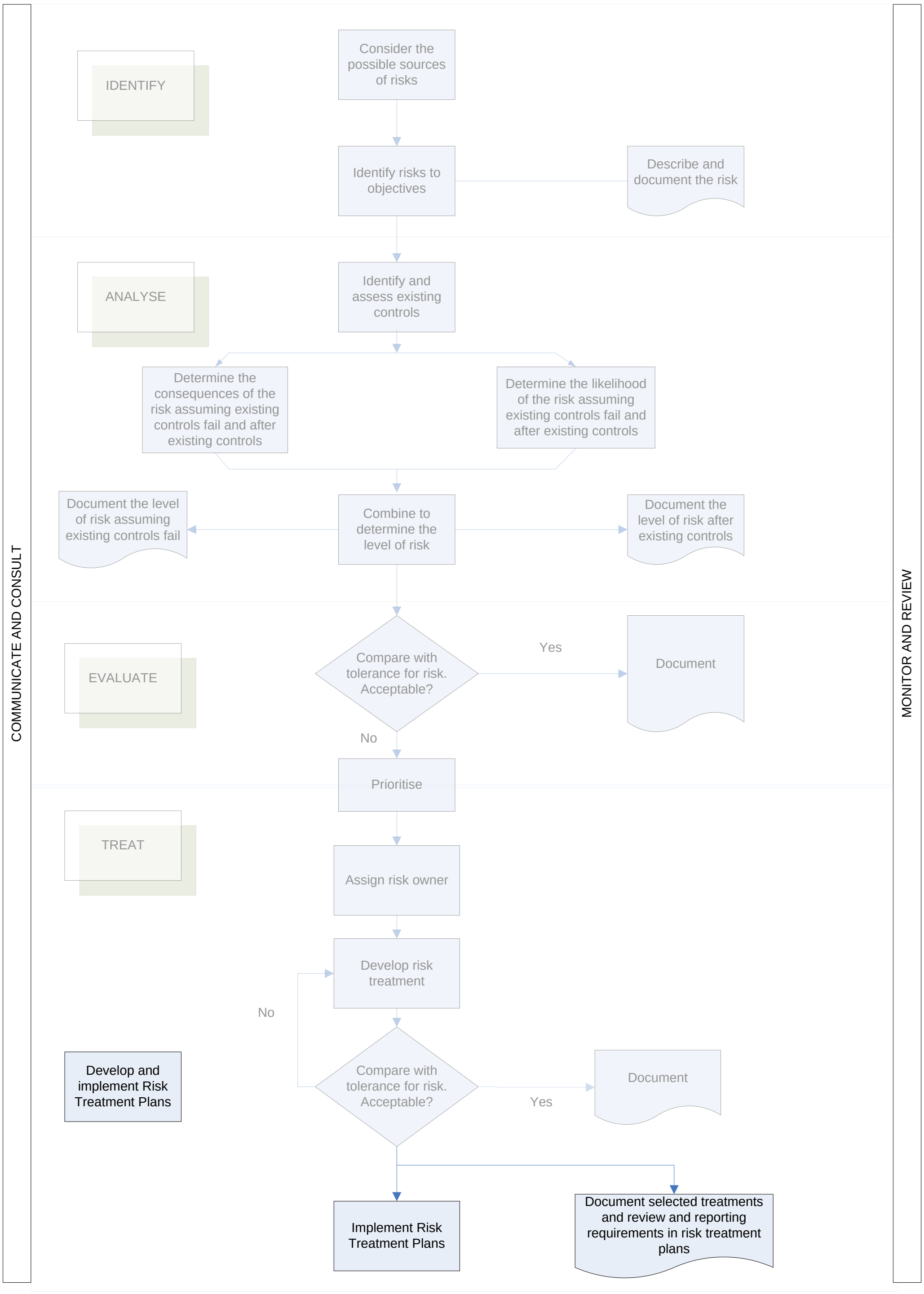
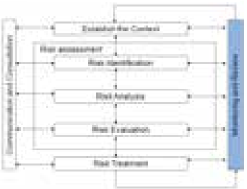


Figure 5.13 – Developing and implementing risk treatment plans


COMMUNICATE AND CONSULT
MONITOR AND REVIEW
IDENTIFY
Consider the possible sources of risks
Identify risks to objectives
Describe and document the risk
ANALYSE
Identify and assess existing controls
Determine the consequences of the risk assuming existing controls fail and after existing controls
Determine the likelihood of the risk assuming existing controls fail and after existing controls
Document the level of risk assuming existing controls fail
Combine to determine the level of risk
Document the level of risk after existing controls
EVALUATE
Compare with tolerance for risk. Acceptable?
Yes
Document
No
Prioritise
TREAT
Assign risk owner
Develop risk treatment
No
Develop and implement Risk Treatment Plans
Compare with tolerance for risk. Acceptable?
Yes
Document
Implement Risk Treatment Plans
Document selected treatments and review and reporting requirements in risk treatment plans

Monitor and review



Chapter 6 – The risk management process: monitor and review

It is vital to monitor and review your risk management process to ensure that:

- it remains relevant as your external and internal context changes
- it is operating effectively
- the criteria you use to evaluate risk are still relevant
- you are able to capture lessons learnt from your risk management activities, including near misses and actual losses or gains
- expected results of your agency's risk management process are being achieved.

6.1 Monitoring and review mechanisms

Monitoring and review can either be carried out formally or informally. Mechanisms include:

- **management reviews:** for example, the use of self-assessments and other types of management reviews
- **independent reviews:** for example, by internal or external audit
- **continuous informal reviews:** for example, discussing the progress of your risk management activities in workgroups or meetings.

6.1.1 Process elements model

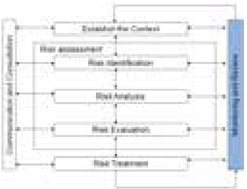
HSB 158-2010 *Delivering assurance based on ISO31000:2009 Risk management – Principles and guidelines* recommends the use of a process elements model to check whether each element of the risk management process is in place. A generic example of this approach is shown in Table 6.1. In this example[31], the requirements that should be in place for each element and evidence that could substantiate (prove) that the element is being satisfied in practice have been listed.

Table 6.1 – Example of the use of a process elements model

Process element	Requirements	Evidence that would substantiate process element is in place
Communication and consultation	§ Have key stakeholders been consulted? § Has a communication plan been developed? § Has accountability been assigned for risks and controls? § Is there ownership of risks and controls?	§ Stakeholder management and communications plans, e.g. stakeholder analysis matrix, stakeholder needs analysis, stakeholder communication strategy (either dedicated to risk management or part of a broader agency plan) § Communications that have been provided to stakeholders § Job or role descriptions for evidence of allocation of risks and controls to responsible officers

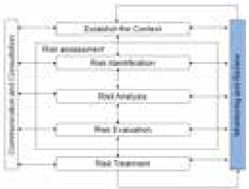
[31] Note: Adapted from HB 158-2010, pp. 57-59.

Monitor and review



Process element	Requirements	Evidence that would substantiate process element is in place
Establish the context	Is there a process to obtain an understanding of: § external context? § internal context? § risk management context?	§ Analysis undertaken such as SWOT (strengths, weaknesses, opportunities, threats) or PESTLE (political, economic, social, technological, legal and environmental) analysis § Consequence, likelihood, risk tolerance, control effectiveness, escalation tables
Risk assessment § Risk identification	§ Is risk identification a part of all agency activities, i.e. strategic, divisional, operational and project planning? § Does the agency have an ongoing, comprehensive and systematic approach to identify its risks? § Are staff involved in the risk identification process knowledgeable about the area under review? § Are identified risks allocated to responsible officers (risk owners)? § Has your agency considered the history of incidents that have occurred?	§ Strategic and business plans § Business cases § Project plans § Presentations on planning § Risk registers
§ Risk analysis	§ Is there a means of assessing control effectiveness? § Are critical risks and related controls allocated to specific individuals? § Is there a process for the analysis of risk for both consequence and likelihood? § Are the right people involved in the risk analysis to determine a risk rating?	§ Internal and external audit reports § Risk registers § Risk treatment plans § Control self-assessments § Internal control questionnaires
§ Risk evaluation	§ Are risks evaluated using a consistent process? § Are risks assessed against pre-established criteria?	§ Risk registers § Risk assessment sessions § Risk assessment template § Evidence of assessment of risks against established risk criteria § Evidence of discussion and approval of risk treatment In addition, general background information such as session notes, meeting minutes and presentations

Monitor and review

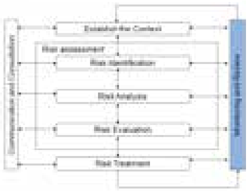


Process element	Requirements	Evidence that would substantiate process element is in place
Risk treatment	§ Are risk treatment plans formulated for risks? § Does your risk treatment plan include consideration of benefits, costs, resources and timing? § Does the risk register record the person responsible for overseeing the risk treatment (the risk owner)?	§ Risk registers § Risk treatment plans/risk register indicate resources and timing § Risk owners clearly identified
Monitoring and review	§ Is there regular review and monitoring of the risk management process? § Has the operation and design effectiveness of controls and risk treatments been validated? § Have the risk management processes been applied systematically at all levels of the agency? § Where activities are outsourced, have third-party certifications been sought to implement risk management activities? § Is the risk register updated throughout the year to reflect changes in risks and emerging risks?	§ Internal audit reports[32] § Risk reports § Risk registers § Risk treatment plans § Minutes of meetings where risk reports are tabled and discussed

The process elements model approach can confirm whether all the process elements are in place. However, assessment using the process elements model should not be conducted in isolation but should be accompanied by regular reviews of your risk management process, as discussed in section 6.1.2.

[32] Internal audit reports provide assurance on the design effectiveness and operation of internal controls and the completeness of management's risk assessment.

Monitor and review



6.1.2 Reviewing the risk management process

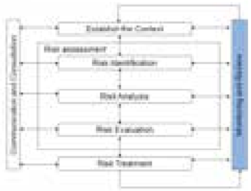
You should continually review your entire risk management process to ensure your agency's risk management strategies are appropriate and up to date. You can do so by considering issues at each stage of the risk management process, including those listed in Table 6.2.

Table 6.2 – Reviewing your risk management process

Process element	Issues for review
Establishing the context	§ Have there been changes in the external or internal context, and does your agency's risk management context need to change to remain relevant? § Have the stakeholders who should be considered changed? § Have your stakeholders' preferences changed with regard to how you manage risk?
Risk identification	§ Are the sources of information used to identify risks still relevant and reliable? § Are changes required to the risk identification processes? What effect will these changes have on the identification of future risks? § Are there any new or emerging risks that should be considered?
Risk analysis	§ Are the assumptions about risk, and the assumptions upon which your risk assessment is based, still valid? § How fit for purpose are the tools your agency uses in the risk analysis process? Are they are still relevant? Are they being correctly applied? § Are those responsible for analysing risk and assessing controls doing so in a consistent manner? § Has there been any change in the likelihood or consequence of risks? § Is there any need to modify your agency's risk assessment process based on actual experience?
Risk evaluation	§ Are those responsible for evaluating risks doing so in a consistent manner? § Have your risks changed in priority reflecting any changes to your agency's context?
Risk treatment	§ How effective are your agency's risk treatment plans? - Are the controls effective and fit for purpose? - Does the risk require further treatment or do you need to change your agency's control strategy? § Are staff following procedures? Is the control strategy supported by appropriate communication including documentation and training? Do the benefits of the risk treatment continue to justify the costs of the treatment?

As a result of such reviews, you may find that your risk management process needs refinement. You may also find that the monitoring and review of the risk management process can be used as an input into a review of your risk management framework. Any changes to your agency's risk management plan or your risk management framework should be formally approved in accordance with your risk management policy and documented.

Monitor and review



Responsibilities for monitoring and performing reviews of the elements of the risk management process within your agency should be clearly assigned when you define roles and responsibilities in your risk management framework (refer to section 3.2.6). For example, risk owners who have accountability for the effectiveness of risk controls should drive the assurance activities associated with the risks for which they have responsibility.

Your Audit and Risk Committee should establish the review schedule for your agency.

You should document the outcomes of your monitoring and review and regularly report these to your executive and the Audit and Risk Committee.

6.1.3 Measuring your risk management performance

To be able to effectively monitor and review the progress and performance of the risk management activities adopted by your agency, you need to develop appropriate key risk performance indicators.

Key risk performance indicators are most effective when they relate directly to agency objectives and are embedded in your agency's performance management and reporting system.

Progress in implementing risk treatment plans is a qualitative performance measure that can be incorporated into your agency's overall performance management and reporting systems.

In addition, as your risk management maturity increases, you can develop other key risk performance indicators that measure the level of performance of a particular item or activity.

For example, your agency can monitor:

- **Changes to the consequence or likelihood of a risk:** If your agency requires a certain number of staff with specialised skills to be recruited within a particular timeframe to deliver a project, your actual recruitment rate can be an indicator of the likelihood, and therefore overall risk, of not delivering the project
- **Changes to the effectiveness of your controls:** If your agency's firewall is your major control against the risk of being hacked, the number of firewall breaches can be an indicator of effectiveness of your firewall
- **Processes and activities as they are performed or implemented**: You can monitor the ownership of risks and controls to ensure that risks are being managed most appropriately.

Key risk performance indicators should be included in risk management reports to the executive and the Audit and Risk Committee.

Useful resources

Audit Office of New South Wales 2011, *NSW Auditor-General's 2011 Report Corporate Governance – Strategic Early Warning System,* vol. 2, Audit Office of New South Wales, Sydney

Auditing and Assurance Standards Board (AASB) 2006, Auditing Standard ASA 315 Understanding the entity and its environment and assessing the risks of material misstatement, AASB, Melbourne

Australian National Audit Office (ANAO) 2003, *Public Sector Governance*, Better Practice Guide, ANAO, Canberra

Australian National Audit Office (ANAO) 2007, *Public Sector Internal Audit: An Investment in Assurance and Business Improvement*, Better Practice Guide, ANAO, Canberra

Australian Public Service Commission 2007, *Building Better Governance*, Commonwealth of Australia, Canberra

British Standards Institution (BSI) 2011, *BS 31100:2011 Risk management – Code of practice and guidance for the implementation of BS ISO 31000*, BSI (purchase required), London

Comcover 2008, *Better Practice Guide – Risk Management*, Commonwealth of Australia, Canberra

Committee of Sponsoring Organizations of the Treadway Commission (COSO), Guidance on Enterprise Risk Management*,* http://www.coso.org/guidance.htm

Fraser, J & Simkins, B 2010, *Enterprise risk management*, John Wiley & Sons Inc, Hoboken, New Jersey

HM Treasury 2004, *The Orange Book: Management of Risk – Principles and Concepts*, October, Norwich

Independent Commission Against Corruption (ICAC) 2008, *Corruption risk management – tip sheet,* ICAC, Sydney
http://www.icac.nsw.gov.au/component/docman/doc_download/1276-corruption-risk-management-tip-sheet.pdf

ICAC, 'Knowing your risks' internet resource at
http://www.icac.nsw.gov.au/preventing-corruption/knowing-your-risks

Institute of Internal Auditors 2009, *International Standards for the Professional Practice of Internal Auditing*
https://na.theiia.org/standards-guidance/Pages/Standards-and-Guidance-IPPF.aspx

International Organization for Standardisation (ISO) 2009, *ISO Guide 73:2009 Risk management – vocabulary*, ISO (purchase required), Geneva

Useful resources (continued)

International Organization for Standardisation (ISO) 2009, *ISO/IEC 31010:2009 Risk management – risk assessment techniques*, ISO (purchase required), Geneva

NSW Better Regulation Office 2008, *Risk-based compliance*, NSW Better Regulation Office, Sydney

NSW Treasury 2009, *Internal audit and risk management policy for NSW public sector*, Policy Paper 09-05 http://www.treasury.nsw.gov.au/__data/assets/pdf_file/0020/15077/tpp09-5_dnd.pdf

Praxiom Research Group, *ISO 31000 2009 Translated into Plain English*, Praxiom Research Group (purchase required), Alberta

Public Finance and Audit Act 1983 (NSW)

Queensland Treasury and Trade 2011, *A Guide to Risk Management*, Queensland Treasury and Trade, Brisbane

RiskCover – Insurance Commission of Western Australia (RiskCover) 2011 (2nd Edition), *WA Government Risk Management Guidelines*, August, RiskCover, Perth

Standards Australia 2006, *AS 3806-2006 Australian Standards Compliance programs*, Standards Australia (purchase required), Sydney

Standards Australia 2010, *HB 158-2010 Delivering assurance based on ISO 31000:2009 Risk management – principles and guidelines,* Standards Australia (purchase required), Sydney

Standards Australia 2010*, HB 327:2010 Communicating and consulting about risk (Companion to AS/NZS ISO 31000:2009),* Standards Australia (purchase required), Sydney

Standards Australia/Standards New Zealand 2009, *AS/NZS ISO 31000:2009 Risk management – principles and guidelines*, Standards Australia/Standards New Zealand (purchase required), Sydney

Victorian Managed Insurance Authority 2010, *Risk Management: Developing and Implementing a Risk Management Framework*, Victorian Managed Insurance Authority, Melbourne

Williams, Graham 2011, *Everything you wanted to know about Management of Risk (M_o_R®) in less than 1000 words,* The Stationary Office, London

Williams, Graham 2010 (3rd Edition), *Management of Risk: Guide for Practitioners,* The Stationary Office, London