NSW GOVERNMENT | The Treasury

Risk Management Toolkit for NSW Public Sector Agencies

Executive Guide

Policy & Guidelines TPP12-03a

NSW Treasury
ISBN 978-0-7313-3567-1

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: TPP12-03a

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.

NSW Treasury has developed a *Risk Management Toolkit for NSW Public Sector Agencies* (the Toolkit), which comprises guidelines, templates and a case study. The Toolkit is a comprehensive guide to the current international risk management standard (ISO 31000) and is designed to support agencies across the NSW public sector to develop effective and integrated risk management frameworks and processes.

This executive guide complements the Toolkit and provides a navigation aid to the detailed guidance it contains. Each section of this guide is cross-referenced to the Toolkit.

Philip Gaetjens
Secretary
NSW Treasury
August 2012

Treasury Ref: **TPP12-03a**
ISBN: **978-0-7313-3567-1**

Contents

Toolkit References
for more information

Risk management in the NSW public sector – an overview

NSW Treasury's *Internal Audit and Risk Management Policy for the NSW Public Sector* (TPP 09-05):

- introduced corporate governance requirements to ensure the real and perceived independence of the Audit and Risk Committee (ARC), the Chief Audit Executive and the internal audit function
- adopted the current standards for professional practice in internal audit and risk management.

Core Requirement 5 of TPP 09-05 requires department heads and governing boards of statutory bodies to establish and maintain a risk management process that is consistent with the current Australian/New Zealand (AS/NZS) standard on risk management. Standards Australia has adopted the international standard (ISO 31000), which it has titled *AS/NZS ISO 31000: Risk management – Principles and guidelines* (referred to in the Toolkit and this Guide as ISO 31000).

The current risk management standard

ISO 31000 consists of a set of principles, frameworks and processes aimed at improving decision making about risks and their management by reducing uncertainty and increasing the likelihood that organisational objectives will be achieved. It is not a compliance standard, but instead provides principles-based guidance on best practice.

Risk management, like your agency's other management systems, should be designed to meet your specific needs. The Toolkit offers detailed and practical advice on the various elements of ISO 31000 so you can manage risk efficiently and effectively by implementing a risk management framework[1] appropriate to your agency's own needs.

What is risk?

Risk, in ISO 31000, is defined as the effect of uncertainty on your agency's objectives. This can mean both negative and positive effects on your objectives. While risk is inevitable, it can and must be managed.

Chapter 2 Section 2.1
What is risk?

[1] The application of risk management to all aspects and levels of an organisation is sometimes referred to as 'enterprise risk management'. This term is not used in the Toolkit or this executive guide, but it is an implied requirement of ISO 31000 that an agency must develop a whole-of-agency view of its risks. It is mentioned in TPP 09-05 and is a condition of compliance with that policy.

Toolkit References
for more information

What is risk management and why do I need to manage risks?

Managing your risks means managing the effect of uncertainty to provide greater assurance that your agency will achieve its objectives by minimising threats and seizing opportunities. This requires directing, controlling and holding your agency accountable for:

- systematically identifying the risks in all aspects of your agency's operations that can affect achieving your objectives
- making informed decisions about these risks.

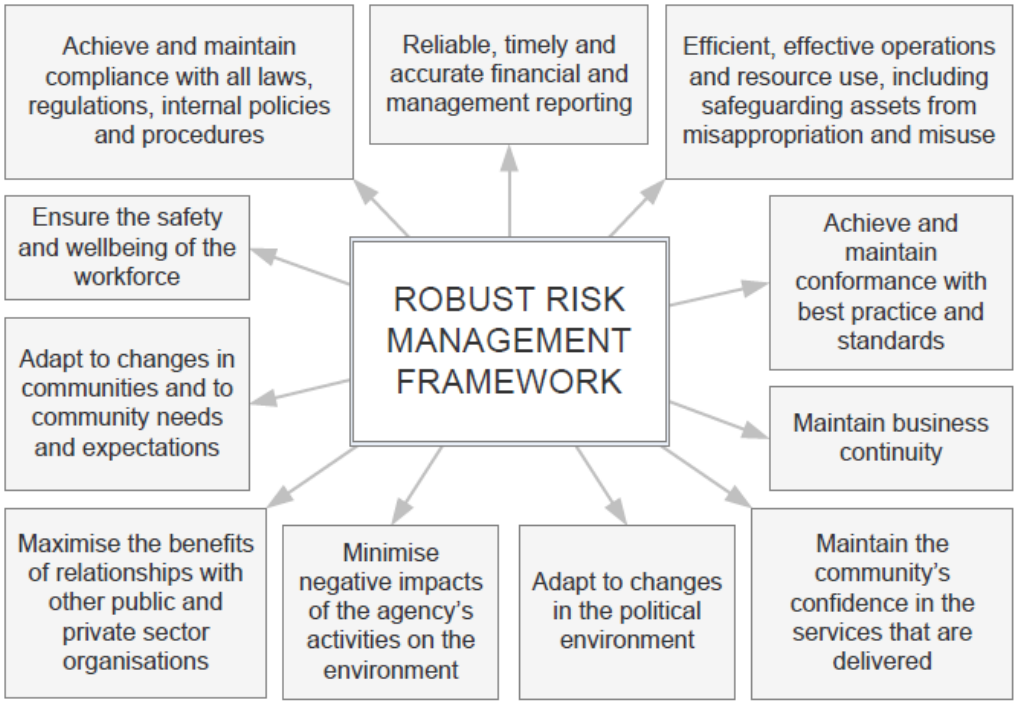
Successful management of risks will, amongst other things:

- reduce foreseeable threats to a level that your agency is willing to accept
- enable you to maximise opportunities that may present themselves.

In essence, the successful management of risks will increase the likelihood of your agency achieving its objectives, both in the short and longer term. A robust risk management framework, by increasing your agency's resilience and capacity to learn, will support the sustainability of your agency. Other benefits of a robust risk management framework are summarised in Figure 1.

Chapter 2 Section 2.5
What are the benefits of a risk management framework?

Figure 1 – Benefits of a robust risk management framework



Risk management is integral to good governance and good management. It is also required by NSW government policy (TPP 09-05) and legislation such as the *Public Finance and Audit Act 1983*, *Work Health and Safety Act 2011*, *Environmental Planning and Assessment Act 1979*, and *Protection of the Environment Operations Act 1997*.

Toolkit References
for more information

Under Annual Reports Regulations, NSW public sector agencies are required to report on their risk management and insurance arrangements and activities. Agencies are also required to publish an annual attestation of compliance with the Core Requirements of TPP 09-05.

A risk management framework

A risk management framework provides a structure that will facilitate the use of a consistent risk management process wherever decisions are being made in your agency. This includes all projects, functions and activities, at all levels of your agency.

Chapter 2 Section 2.4
What is a risk management framework?

ISO 31000 provides a risk management framework to embed the process for managing risk throughout your agency, including your overall governance, strategy, planning, budgeting, management, and reporting processes and policies.

This means, for example, that you should formally consider risks:

- in your strategic, business and workforce planning processes
- in your budgeting processes
- when developing and implementing:
  - new or revised policies or programs
  - new strategies, projects or activities
  - significant changes to an initiative, project or level of activity
- in all capital projects
- in procurement processes.

Your agency's attitude to risk management should be reflected in the statement of values and culture of your agency.

Does my agency's risk management framework align with ISO 31000?

While the specifics will vary, frameworks developed in accordance with ISO 31000 will display some common features. These include:

Chapter 3
Implementing a risk management framework

- an executive that is committed to risk management and clearly communicates and demonstrates this commitment
- a risk management process that is well understood, and consistently used, by all decision makers
- a system to monitor and report on risks to the appropriate level
- clear accountabilities for managing risks
- a process to continuously review and improve the framework.

A risk management framework established in accordance with ISO 31000 consists of a set of components that provide the *foundations* and *arrangements* for designing, implementing, monitoring, reviewing and continually improving risk management.

Toolkit References
for more information

The questions below will help you assess whether your agency already has, or needs to put in place, these components.

Foundations

The foundations of a risk management framework are a risk management policy, clear risk management objectives, and a mandate and commitment to risk management. Questions to test if these foundations are in place are listed below.

Policy

§ Does your agency have a risk management policy in place that sets out its objectives and commitment to risk management?

Objectives

§ Have you set clear objectives for risk management in your agency?
§ Do these risk management objectives align with your agency's overall objectives?

Mandate and commitment

§ Has your Head of Authority endorsed your risk management policy?
§ Have you communicated the benefits of risk management to staff and stakeholders?
§ Do you have a culture in which your staff and management are comfortable in reporting risks or suggesting risk management strategies?
§ Have you identified performance indicators that will enable you to measure how well your agency is managing risk?

Arrangements

The arrangements for implementing a risk management framework consist of plans, building relationships, assigning accountabilities, allocating resources, implementing a risk management process, and activities such as risk reporting and reviewing your framework. Questions to test if these arrangements are in place are listed below.

Plans

§ Do you have an overall plan to ensure your risk management policy is implemented?
§ Do you have plans in place to manage individual risks?

Relationships

§ Have you communicated and consulted with your internal and external stakeholders in developing your risk management policy, plans and risk management process?

Toolkit References
for more information

Accountabilities

- Do all staff and management understand they have a role in managing risk?
- Have you clearly assigned the accountabilities for your risk management implementation plan?
- Have you clearly assigned accountabilities for managing individual risks?

Resources

- Have you allocated the necessary resources to manage risk properly, including training or otherwise building staff competencies in risk management?

Processes

- Is there a commonly accepted and consistent way in which risks are identified and managed in your agency?
- Is this method integrated with your other policies, practices and processes?

Activities

- Does your agency have formal risk monitoring and reporting mechanisms in place so risk information is escalated to the right level in your agency?
- Do you regularly review your agency's risk management framework to ensure it remains current?

The Toolkit provides guidance on how you can put in place foundations and arrangements consistent with ISO 31000 and appropriate for your agency.

A risk management process

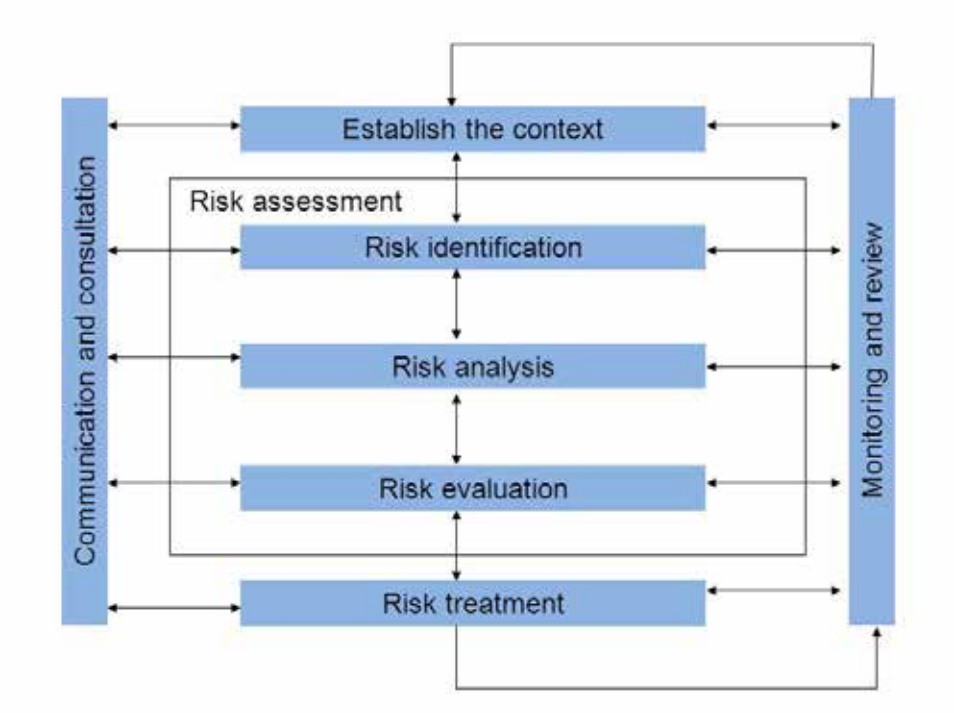
A risk management process is a systematic way of establishing the context in which your agency operates, and identifying, analysing, evaluating and treating your risks, while communicating and consulting with stakeholders, and continuously monitoring and reviewing the elements of the process. It is a generic process that can be applied at any level in your agency.

Chapter 4 Section 4.1
What is a risk management process?

The seven elements of the ISO 31000 risk management process and their interrelationships are shown in Figure 2 below. Each of these elements are briefly discussed in the rest of this section.

Toolkit References
for more information

Figure 2 – The risk management process



Risk identification, analysis and evaluation are collectively termed 'risk assessment'.

Chapter 4 Section 4.2
Communication and consultation

Communication and consultation

You should communicate and consult with your stakeholders at all stages of the risk management process.

Communication

Communication is necessary to ensure that the right people receive the right information at the right time to make the best decisions or carry out their risk management responsibilities.

Different levels in 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, senior management and other individuals will have their own unique information needs, which will include an understanding of how risks are managed and reported.

You also need to communicate to external stakeholders about risks, and how they are being managed, for example through annual report disclosures.

You must identify your internal and external stakeholders and their information needs in relation to risk management, and develop a way to meet those needs.

Toolkit References
for more information

Consultation

You must 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 upon when analysing and evaluating risks and different views are considered
- you can secure endorsement and support for risk treatment plans.

Establishing the context

Establishing the context is about understanding your business environment and setting the scope for your agency's risk management process.

Identifying your activities, objectives and stakeholders

Chapter 4 Section 4.3
Establishing the context

Before you can conduct a risk assessment, you need to develop a complete understanding of your agency's external and internal operating environment.

The external environment creates risks that must be addressed. External factors include both current and emerging social, political, economic, environmental, technological and legal elements and influences.

The internal environment includes your agency's mandate, the activities you undertake and your structure, strategies and objectives.

This process of understanding the context (internal and external) will yield an understanding of, among other things:

- your agency's key activities
- the objectives of each activity
- your key stakeholders
- factors that could have a positive or negative effect on achieving your objectives.

Defining your risk criteria

Chapter 4 Section 4.3.3
Establishing the context of the risk management process

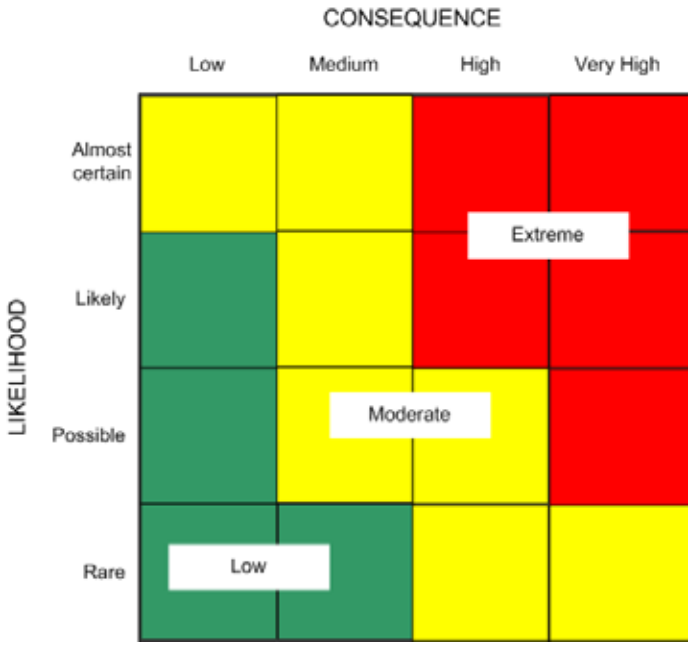
To prioritise your risks, you need to have a scale or terms of reference to evaluate them against; these terms of reference are defined in ISO 31000 as 'risk criteria'. You must define your risk criteria before conducting a risk assessment.

The level of a risk depends on the consequence(s) of an event and the likelihood of that event occurring. You therefore need to establish scales for measuring consequence and likelihood and a consistent way of combining these to arrive at a level of risk.

The risk criteria you need to define include:

- the type of consequences that will impact on objectives
- how you will measure these consequences (for example, using a consequence table that describes the severity of consequences using descriptors such as low, medium, high and very high)
- how you will define likelihood (for example, using a likelihood table that describes the chance of an event occurring within a relevant time horizon as rare, possible, likely and almost certain)
- how you will measure the effectiveness of your risk controls
- how you will combine likelihood and consequence to determine a level of risk (agencies typically use a risk matrix for this purpose, see Figure 3)
- what level of risk your agency is prepared to accept or tolerate (this is usually a matter for the Head of Authority to determine).

Figure 3 – Example of a risk matrix



Note: the colours in each cell in the figure represent a level of risk.

Risk assessment

Risk assessment is a structured approach to identifying and analysing the uncertainties that exist in meeting your agency's objectives. Risk assessment consists of three stages: risk identification, risk analysis and risk evaluation.

Toolkit References
for more information

Risk identification

Chapter 5 Section 5.3
Risk assessment Stage 1: Risk identification

The first step in the risk assessment process is to identify all the risks that might affect your agency's ability to achieve its objectives.

You will need to consider the source of risk, the event that could trigger the risk and the impact on your agency's objectives. You also need to document these in a way that is easy for others to understand (even if they were not involved in the risk assessment process).

Many techniques can be used to identify your risks, including:

- checklists
- questionnaires
- individual interviews
- group methods, such as brainstorming sessions or commissioned reviews
- risk assessment workshops
- internal and external audit findings.

You may identify strategic and operational risks that affect your objectives in areas such as:

- service delivery
- reputation
- people and culture
- finance
- fraud and corruption
- health and safety
- stakeholder
- business continuity
- security
- compliance with legislative requirements.

Risk management is iterative: your list of risks will not be static and will evolve over time. Do not be overly concerned that you may not have identified all your risks when you begin – you need to start somewhere. A risk management framework consistent with ISO 31000 should eventually yield a comprehensive listing of all your risks. The process of monitoring and reviewing should also provide assurance of the reliability of your risk assessments.

Toolkit References
for more information

Risk analysis and risk evaluation

Once you have identified your agency's risks, you need to prioritise them to determine which ones need more active management than others. For each risk you have identified, you need to:

Chapter 5 Section 5.4
Risk assessment Stage 2: Risk analysis

- identify the consequence(s) – the impact, if the event occurs, on your agency's objectives
- identify the likelihood – the chance of the event happening
- identify any controls already in place or included in approved plans to prevent the event from occurring or limit the impact of possible consequences if the event occurs
- assess whether these controls are adequate
- use your risk matrix to determine a risk level for each risk based on your assessment of consequence and likelihood after taking account of existing controls.

Chapter 5 Section 5.5
Risk assessment Stage 3: Risk evaluation

There is a subjective element to the assessment of risk. While it is not an exact science, there must be a basis behind the assessment. You need to be able to articulate all assumptions and be accountable for each assessment. For this reason, you must document each risk assessment.

It can be good practice to assess your risks for both worst case (assuming there are no controls in place), and for current case (after existing controls).

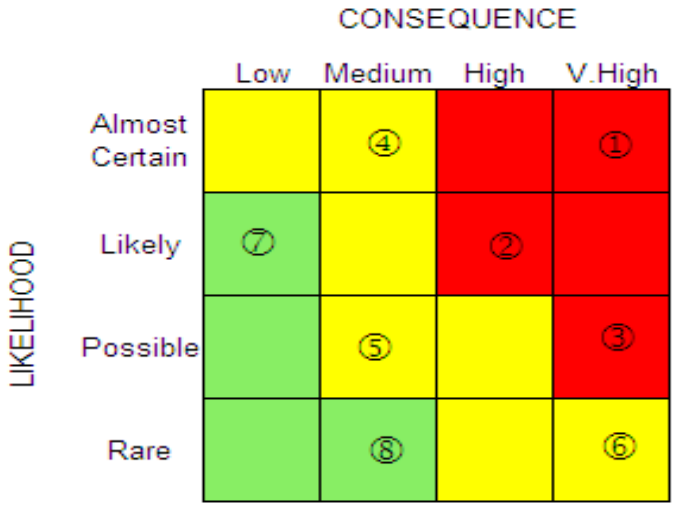
Organisations commonly plot their risks on a heat map, which allows the relative level of risks to be easily visualised. In Figure 4, multiple risk levels have been grouped into colour-coded categories. Each category is associated with a decision that needs to be made to manage the risk – for example:

- the red category indicates risks that must be treated
- the yellow category represents risks that will be treated if the benefit exceeds the cost
- the green category represents risk that are acceptable without further treatment.

These categories can also be associated with escalation points. For example, you could set a business rule that all red category risks are to be escalated to your agency's executive.

Toolkit References
for more information

Figure 4 – Example of a heat map



Note: each number in the heat map represents a unique risk.

Risk treatment

Once you have prioritised your agency's risks and decided which risks require further treatment, you must decide how you will treat them. Approaches to risk treatment include:

Chapter 5 Section 5.6
Risk treatment

- ceasing the activity that creates the risk
- mitigating the risk (in the case of a threat) to reduce the likelihood and/or consequence or, in the case of an opportunity, to enhance the likelihood and/or consequence
- accepting the risk
- sharing or transferring the risk[2].

Risk treatments need to be cost effective, practicable and commensurate with the level of the risk.

Your chosen response to each risk, including your rationale for the approach and its impact on both likelihood and consequence, must be documented. The risk treatments – including specific strategies, timeframes, accountabilities and responsibilities – need to be clearly described.

Risk assessments and risk treatment information should be documented in a risk register that will provide a whole-of-agency view of risk. A risk register is simply a list of the risks that your agency has identified and assessed using its risk management process. It enables key stakeholders to make informed decisions regarding risks and their management.

[2] This can be a good option to reduce your agency's exposure in certain areas such as financial risks or risks to assets. However, it is important to note that outsourcing of activities to third party service providers, whether within the government sector or outside, may not result in the complete transfer of risk. Also, outsourcing creates a new risk: that the organisation with which the risk has been shared or to which it has been transferred may not manage the risk effectively.

Toolkit References
for more information

Relevant information in your risk register should be summarised and reported regularly to your key stakeholders – for example, to your Audit and Risk Committee and your agency's executive. A well-developed risk register provides critical input into the development of a risk-based internal audit plan.

Risk management reporting

Chapter 3 Section 3.3
Design of the framework for managing risk

Accurate and timely reporting of risk information is essential to good corporate governance. It provides a means of ensuring that those with responsibility for decision making in your organisation have the best information about current and emerging risks to hand. It also provides a way to ensure that risks are being properly managed by monitoring the implementation and effectiveness of treatment plans, as well as the ongoing effectiveness of controls.

The frequency and content of reports should be tailored to the needs of individual stakeholders. Those stakeholders will include your Head of Authority or governing board, your agency's executive, and the Audit and Risk Committee.

Monitoring and review

Chapter 6
Monitor and review

To ensure that risk management is operating as intended, you must put in place a monitoring and review process so that you can:

- ensure that risk treatments have been implemented as planned
- assess whether risk treatments are effective
- continually review risk information on the risk register to ensure that it remains relevant to the agency; risks do change, and some risks may cease[3] and new risks may emerge
- periodically measure the agency's progress against the risk management plan.

There are a range of mechanisms that can be used to monitor and review your risk management process. A useful way to provide independent assurance on risk management to your executive and the Audit and Risk Committee is through periodic internal audit.

Barriers to effective risk management

Despite universal acknowledgement of risk management as a fundamental component of good governance, anecdotal evidence indicates that some organisations, despite the investment of considerable resources, have failed to realise the benefits from risk management.

[3] While risks may become obsolete, it is important that a list of all risks, past and present, be maintained. Risks deemed obsolete should be archived or flagged as such in the risk register. In this way you are able to maintain within your agency a complete listing of all the risks it faces or has faced.

Toolkit References
for more information

Risk management is unlikely to be effective if:

- **You do not strongly link it to your objectives:** If the risk management effort is focused solely on achieving regulatory or legislative compliance, there will be significant gaps. Risk management should focus on, and support, the achievement of your agency's objectives.
- **You do not have the right culture:** In addition to a strong commitment, and sustained and visible support from senior management, there should be broad engagement with risk management across your agency. Risk management should be seen as the responsibility of all managers and staff (not just the responsibility of the Chief Risk Officer). Your culture should support and encourage individuals to actively identify and report risks.
- **You do not commit the required resources:** Sufficient time, training and other resources must be devoted to risk management. In addition, your risk management process should be supported by a system to properly and effectively manage risk information.
- **You make risk management processes too complex:** If risk documentation and processes are unnecessarily complex, managers, staff and other stakeholders will be less likely to support implementation. Risk documentation and processes should consider and reflect the needs of your stakeholders.
- **Your risk treatments are not commensurate with the risk:** Treatments need to be cost effective, practicable and commensurate with the level of risk. Without a cost–benefit analysis, it is likely that you will over-control some risks and under-control others. Money saved by not over-controlling risks can be diverted to risks more worthy of attention.
- **You do not identify the right risks:** Risk management should support good decision making. If the risks listed in your risk register are described incorrectly or are too broad or too low level, they will not support good decision making. It will be difficult for decision makers to make the correct decisions if they are overwhelmed by detail. Your agency's key decision makers need a concise list of risks that accurately reflects the most significant risks your agency faces.
- **You do not acknowledge the likelihood of cognitive bias in decision making:** Decision-making errors and faulty risk assessments will result from risk identification and assessment that reflect subjective judgements that have not been challenged or tested. Sometimes these errors can persist for years. Recognising bias is the first step in minimising its impact on your risk assessment.
- **You do not set clear responsibilities:** Risks and their management need to be clearly assigned to risk owners.
- **You do not get independent assurance of the effectiveness of risk management:** You must identify and implement ways of determining whether your risk management efforts are providing real and ongoing benefits.

Toolkit References
for more information

Where do I begin?

To successfully introduce risk management to your agency, as with any management initiative, you need:

- clear objectives for risk management
- a risk management policy that sets out your agency's commitment and intention for risk management, endorsed by the Head of Authority
- a plan, clearly assigned responsibilities and a timeframe for implementing your risk management policy
- a risk management process that is understood by all decision makers
- targeted training
- ongoing communication with stakeholders
- a way to monitor and report compliance and results that will also inform ongoing improvement.

The Toolkit provides guidance on each of these aspects to help you develop an effective and integrated risk management framework that meets the needs of your agency now and into the future.