NSW Treasury

Risk Management Toolkit

May 2025

NSW GOVERNMENT

Acknowledgement of Country

We acknowledge that Aboriginal and Torres Strait Islander peoples are the First Peoples and Traditional Custodians of Australia, and the oldest continuing culture in human history.

We pay respect to Elders past and present and commit to respecting the lands we walk on, and the communities we walk with.

We celebrate the deep and enduring connection of Aboriginal and Torres Strait Islander peoples to Country and acknowledge their continuing custodianship of the land, seas and sky.

We acknowledge the ongoing stewardship of Aboriginal and Torres Strait Islander peoples, and the important contribution they make to our communities and economies.

We reflect on the continuing impact of government policies and practices, and recognise our responsibility to work together with and for Aboriginal and Torres Strait Islander peoples, families and communities, towards improved economic, social and cultural outcomes.

Artwork:
Regeneration by Josie Rose

Contents

Introduction

Background and Context

All agencies will encounter risks which have the potential to impact their ability to successfully delivering their objectives. The *Government Sector Finance Act 2018* (GSF Act) requires all accountable authorities of government agencies (Secretaries, Chief Executives) to establish and maintain effective systems for risk management, internal control and assurance for their agency.

To increase the likelihood of meeting these objectives efficiently and effectively, it is vital for all agencies to maintain an appropriate risk management function. The risk management approach taken by each agency will vary depending on several factors, such as their size and risk profile. The international standard *ISO 31000* provides guidance on how to establish a risk management framework and an approach to designing effective risk management processes.

The aim of this toolkit is to:

- Provide an overview of the ISO principles as they may apply to NSW government agencies
- Help agencies to understand what 'good risk management' looks like, and how this can be achieved
- Provide risk managers with a set of tools and resources to support their work and meet their obligations under the GSF Act and *TPP20-08 Internal Audit and Risk Management Policy for the NSW Public Sector* (TPP20-08)
- Highlight the importance of risk management and how it supports an agency in achieving objectives

The toolkit has been structured to provide key information, with links to appendices containing additional resources to help support your risk management function.

1 Risk Management Guiding Principles

Risk management helps agencies to identify, assess, and address potential risks. Maintaining a sound risk management function ensures the agency is equipped to manage uncertainties in a proactive manner. This delivers benefits to the agency, such as improved decision making and efficiency, while protecting resources and reputation.

The principles of risk management outlined in this toolkit are aligned with the *AS ISO 31000: Risk Management Guidelines*. This toolkit provides agencies with guidance and tools in various aspects of risk management to assist them in meeting their legislative obligations under the *Government Sector Finance Act 2018* (GSF Act), *TPP20-08 Internal Audit and Risk Management Policy for the General Government Sector* (TPP20-08), and the governance and reporting requirements in *TPG23-10 NSW Treasury Policy and Guidelines – Annual Reporting Requirements* (TPG23-10).

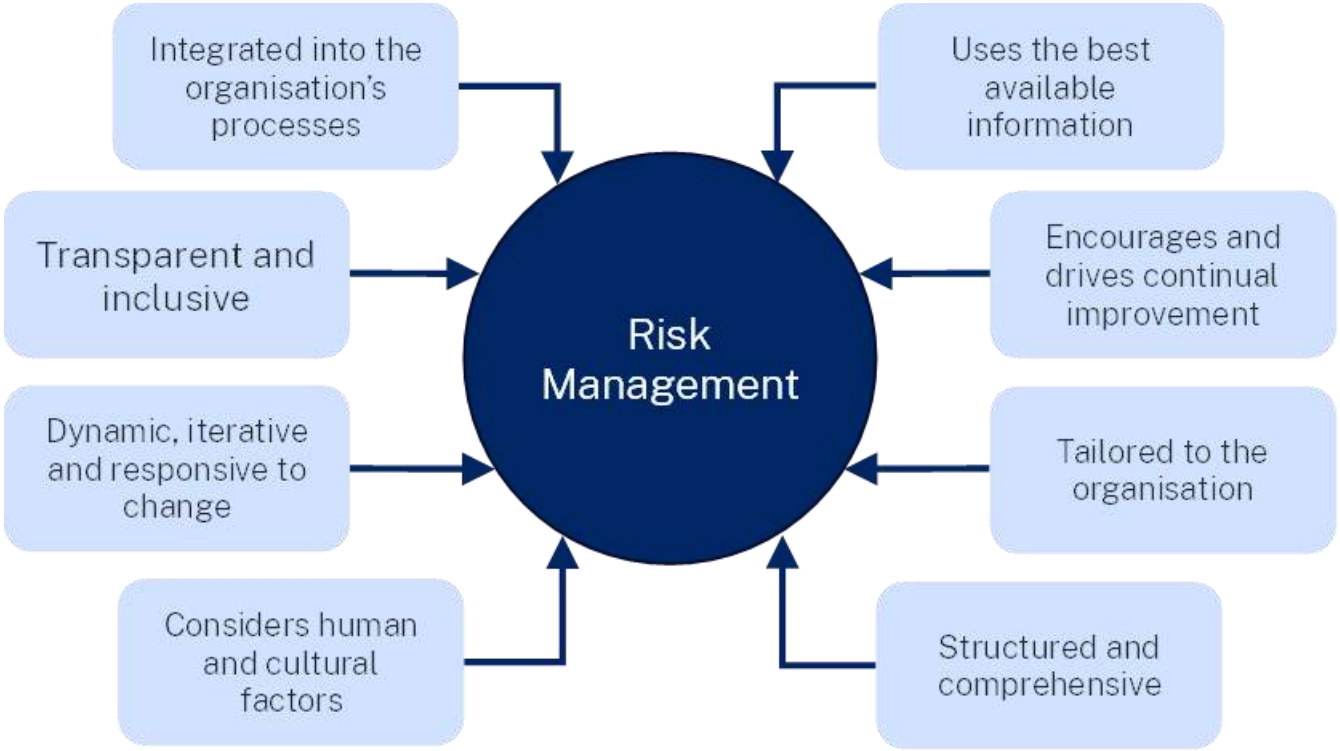

Fig. 1 The principles of risk management

1.1 What is risk?

Risk is the 'effect of uncertainty on objectives', as defined in *ISO 31000*.

When an activity is undertaken by an agency, risk represents the threats that the activity may not proceed as planned or will potentially lead to an unexpected outcome. Often people think that risks only have negative effects, however sometimes they can have positive effects, or a combination of the two.

Risk should be considered for all activities and decision making undertaken by an agency. This supports an agency in ensuring that their activities have the best chance to achieve positive outcomes in the face of uncertainties.

1.2 What is risk management and why is it important

The purpose of risk management is to create and protect value within the agency. Risk management refers to the steps taken by an agency to identify and manage risks which may impact their activities and achievement of objectives.

Risk management is a systematic and transparent process which aids the agency in making decisions and achieving its goals.

Critical elements of effective risk management include:

- establishing clear ownership of risks, controls, and actions
- building strong risk practices and positive risk-aware behaviours
- considering risk from the start of a process, and either avoiding, mitigating, or accepting it within a set risk appetite
- involving risk management in any decision-making, business strategy, and operational choices, and
- exploring worst-case scenarios and deciding if they are acceptable within your risk appetite.

Incorporating risk management into all areas of the agency results in greater resilience, which helps you respond to change, seize opportunities, and make informed choices.

1.3 The Three Lines Model

It is important that everyone in your organisation is aware of their responsibilities in managing risk. The Three Lines Model was developed by the Institute of Internal Auditors (IIA) to show the role of different areas of an organisation in managing risk. The responsibility of the three lines is as follows:

- The **first line** contains all staff who are accountable for work to deliver the objectives of the agency. Their role within the first line is to observe and own any risks which arise from their work, communicate these risks, and manage them appropriately with the support of the second line. Additionally, the first line is responsible for day-to-day risk management decision-making involving risk identification, assessment, mitigation, monitoring and management. This line will have processes in place to maintain effective internal controls and ensure a continual focus on risk management.
- The **second line** relates to functions that specialise in risk management and compliance. This line provides risk management support to the first line. Their role includes reviewing and monitoring the effectiveness of risk management, internal controls, and activities. They may have broad responsibilities such as enterprise risk management, or specialist risk responsibilities such as cyber, climate change, or work health and safety. Oversight of the level of risk in the agency and its relationship to risk appetite and any necessary reporting and escalation to the executive and relevant committees'.
- The **third line** relates to functions that provide independent assurance and advice to the Accountable Authority (the AA) regarding the adequacy and effectiveness of the first and second lines. This is the line where internal and external audit sit.

If the agency has an Audit and Risk Committee (ARC), this sits outside of the three lines and has an oversight role. An ARC provides advice and guidance to the AA with input from the Chief Audit Executive (CAE) and Internal Audit team. While the Chief Risk Officer (CRO) and the risk management team report functionally within the agency, they also provide information to the ARC to support their oversight role.

A visual representation of the Three Lines Model for NSW can be seen below:

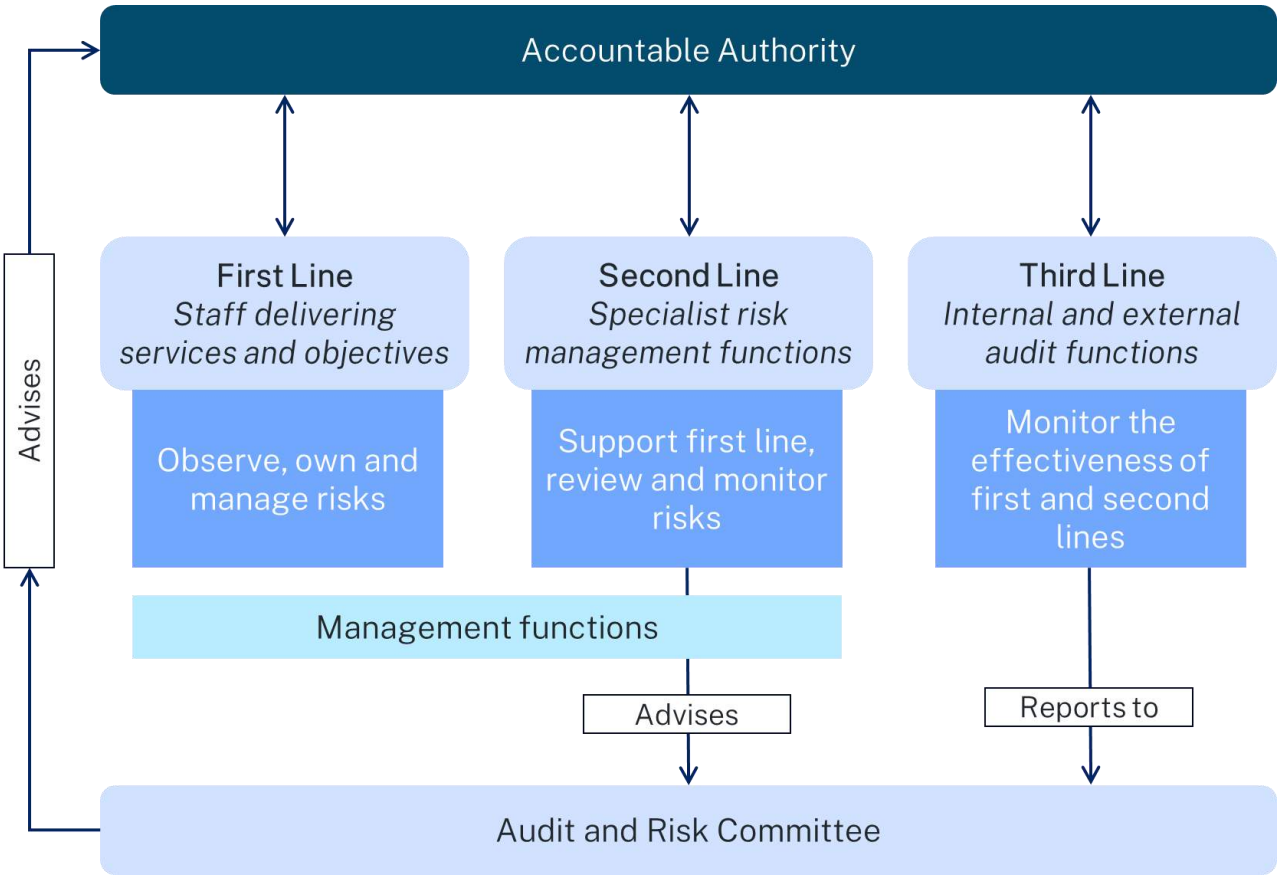

Fig 2. NSW model of Three Lines

1.4 Risk Management Frameworks

A risk management framework is the foundation established by an organisation on which their risk management process is built. A well-designed and implemented risk management framework will provide the agency with a blueprint to use when designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization.

The purpose of a risk management framework is to embed risk management throughout the agency and provide a structure that facilitates the use of a consistent process to manage risk whenever decisions are made. This assists the agency in integrating risk management into all activities and functions.

Establishing a risk management framework is an ongoing process. The framework will evolve over time to reflect changes in the agency's size, complexity, risks, and objectives.

A diagram of the development cycle of this framework, taken from *ISO 31000* can be seen below:

Fig 3. Extract from *ISO 31000 Risk Management Guideline*

A risk management framework helps the agency to make more informed decisions, however it is not fail-proof. Human error can occur, internal controls can be circumvented or may not be effective and cause poor management of risk, as well as purposeful circumvention of controls, and management can override decisions. This means no risk management framework can provide absolute assurance that the agency will achieve its objectives. However, with a robust risk management framework the agency is more likely to achieve its objectives.

2 Risk Governance

Good governance, as it applies to the public sector, is a set of responsibilities, policies and procedures, exercised by an agency's executives to provide strategic direction, ensure objectives are achieved, manage risks, and use resources responsibly. Creating and providing an architecture by which the agency considers and manages risk ensures that the aims of the agency are central to all risk-related decisions.

Some organisational actions which demonstrate good governance around risk are:

- the AA and senior management consistently demonstrating a commitment to identifying and managing risks, creating a positive and risk aware 'tone from the top', and an overall positive risk culture
- a commitment to risk ownership from all stakeholders with clearly defined roles and responsibilities
- enabling and facilitating responsible risk behaviours across the organisation
- ensuring that sufficient resources are committed to implementing the risk management framework in the organisation
- ensuring risks are appropriately identified, assessed and managed, and
- regular functionally-independent reviews of risk management processes

2.1 Risk Behaviours

It is important to facilitate responsible risk behaviours across the organisation. Activities that support this include:

- ensuring the AA has endorsed the risk management policy
- communicating the benefits of risk management to all staff
- ensuring that all staff feel comfortable reporting risks, and risk management strategies
- identifying performance indicators that will enable you to measure how well the agency manages risk, and
- ensuring that decisions are made in accordance with the agency's risk appetite.

2.1.1 Risk appetite and the Risk Appetite Statement

Defining an agency's risk appetite through a Risk Appetite Statement (RAS) is one way for an agency to support a common stance towards risk through an agency. A RAS defines the amount of risk that the agency is willing to take in pursuit of its strategic objectives.

An agency's risk appetite may vary depending on the strategic objective, or the type of risk. Risk appetite can also vary over time.

A RAS is most effective when it has been agreed by an agency's Executive team, communicated through the agency, is used to drive decision-making, and is regularly refreshed so it remains relevant.

2.2 Roles, resourcing and capacity

Clear role descriptions, expectations and lines of accountability are an essential part of both good governance and good risk management. The Three Lines model provides a systematic approach that may be used to help clarify the specific roles and responsibilities that are necessary for the effective management of risks.

Leadership is ultimately responsible for ensuring the agency has sufficient capable and competent staff to implement and maintain your risk management framework. They must ensure that all staff:

- have job descriptions that clearly define and assign accountabilities in their job descriptions
- receive sufficient training and development to build their risk-related competencies
- review risk accountabilities and responsibilities during performance appraisals, and
- are empowered to take ownership of and escalate risks throughout the agency.

Different roles in the agency will have significantly different risk responsibilities. To ensure these are clearly communicated, a capability matrix can be used to record for each 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.

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.

Guidance is available in Appendix A on the different roles which may be found in the agency, and their risk related responsibilities. Not all roles will be necessary in all agencies.

2.3 Training and development

Training and development are central to uplifting and maintaining the risk-related capability of staff and increasing awareness of risk management throughout the agency. In conjunction with leadership, your risk management function should identify and address the agency's training needs.

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

Programs are most successful when they:

- are tailored to suit the needs of the agency and the varied risk management capability needs of your staff,
- use a range of training delivery mechanisms, and
- are regularly reviewed and developed as risk management capability improves and the needs of the agency change.

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

Training needs should consider roles, competencies and capacity (see 2.2 above).

3 Risk Culture

Risk culture is the combination of values, beliefs, knowledge and attitudes shared by the agency which shape how staff identify and manage risk. This influences the approach taken to decision-making across the organisation.

Many factors influence risk culture, including the tone at the top, the code of conduct, and human resource policies.

Tone from the top is particularly important because it sets the fundamental attitude towards risk management within the agency. This is because leadership is responsible for demonstrating and driving good risk behaviours. If senior staff do not exhibit a good risk culture themselves, this can spread through the organisation and undermine risk management efforts.

Positive risk culture is based on creating a risk-aware workplace where employees at all levels manage risk as part of their job. Some core behaviours of an organisation with a positive risk culture are:

- consistently demonstrating that risk management is valued
- open communication and consultation
- learning and continuous improvement
- a clear and understood appetite for risk
- encouraging everyone to proactively report risks, and
- ensuring there is accountability and transparency.

Positive risk culture should be consistently present throughout all levels of the agency to support sound risk management.

3.1 Understanding the agency's risk culture

It is important to understand and monitor the agency's risk culture so that action can be taken to improve risk culture when necessary. Some methods and tools which can be used to gain insight into the risk culture of an entity are:

- Interviewing executives and the AA to understand their needs and expectations from risk management
- Conducting periodic staff surveys to identify trends in risk culture. For example, a question on risk management is included in the annual *PMES for the NSW Public Service*.
- Using the *NSW Treasury Risk Maturity Assessment tool*[1] as a measurable way to track changes in risk maturity. This tool helps identify your current level of risk culture maturity and what level of risk culture maturity is most appropriate (i.e. target maturity). It also helps to target specific areas and activities that can be used to improve risk culture maturity.

These insights will likely show that people at different levels in an organisation see risk management differently. This is why it is important to get input from everyone – frontline staff, risk practitioners, executives, and the AA – when assessing risk culture.

[1] Treasury Risk Maturity Assessment Tool | NSW Treasury

3.2 Tone from the top

Tone from the top recognises the importance of a leadership team in promoting risk culture in an agency, and in enabling good risk management as a result.

Maintaining a tone from the top that is consistent with the agency's values is vital to ensuring that the agency's risk framework is effective. Whilst the risk management function of the agency can support leadership in informing and monitoring risk, this will be ineffective if the decisions made by leadership do not align with the risk management function.

An agency's leadership sets the tone from the top. To support effective tone from the top the leadership team should:

- model and actively promote commitment to risk management
- recognise the need to resource the management of risk in order to achieve the agency's objectives
- ensure that any strategic direction taken by the organisation does not conflict with policies and controls implemented to manage risk,
- model ethical behaviour, and ensure compliance with policies and procedures
- establish methods for employees to report unethical behaviour, and
- clearly communicate the values of the organisation to employees.

3.3 Practical steps to promote positive risk culture

The introduction of any new risk management initiatives requires widespread organisational support. Management must consider the risk culture of the agency when driving change in risk management.

The desired risk management culture should align with the agency's strategic goals and be part of the organisational culture, internal policies and decision-making processes. Performing a gap analysis of the current and desired state of risk culture is the first step to successfully promoting positive risk culture, as discussed in section 3.1.

Actions to promote positive risk culture include:

- Executive and senior managers embedding the importance of risk management in the agency, by championing and demonstrating their commitment to it through their behaviour,
- Communicating that all staff in the agency are part of the risk management process, for example including responsibilities in role descriptions
- Encouraging managers and staff to develop and invest in risk management knowledge and skills
- Training and supporting staff in incorporating risk management into everyday roles and responsibilities, such as business planning, budgeting, project management, and.
- Ensuring sufficient time and resources are allocated to risk management activities to strengthen and enhance resilience and success.

For further drivers and possible actions to influence risk culture please see Appendix B.

4 Integrating Risk Management

Risk management should be considered in all of an organisation's practices and processes. This means that, in addition to being part of a dedicated risk function (if resources permit), risk management activities should be embedded into the policies, daily operations and decision-making processes of the organisation. By doing so, organisations can ensure that risk considerations are consistently applied across all functions and levels, leading to more effective and proactive risk management and better decision making.

4.1 Integrating Risk Management into Policies, Procedures and Operations

Your agency should have dedicated risk policies and procedures in place. In addition, even policies and procedures which do not directly address risk should consider uncertainties that might impact their goals. This means identifying risks early and putting measures in place to handle them. Integrating risk management into your policies and procedures ensures risk is part of decision-making at all levels.

Policies need to be flexible and regularly updated to deal with new risks and changing circumstances.

Risk management practices should be embedded in the agency's operations. Examples of this include

- Developing standard templates and/or frameworks that guide staff through articulating and capturing risk requirements ad risks in a structured way
- Providing risk-related training and support to front-line staff and risk owners
- Clear communication protocols and feedback loops between the risk function and business
- Clearly defined roles and responsibilities in risk management between the different internal parties

4.2 Integrating Risk Management into Planning

Risk management should be embedded into strategy development, planning and decision making. Planning is the process of determining a desired outcome, establishing objectives and then designing a course of action to achieve that outcome.

There is a clear link between planning and risk management. When setting up a strategic plan, an organisation's risk appetite should be considered. Strategic objectives can be put forward, discussed and if they are found to sit outside the organisations risk appetite, either rejected or with a modification to the Risk Appetite Statement.

As part of the business planning process, the agency should identify and assess the operational risks linked to your business and operational objectives. Where risks are identified as beyond your risk appetite, the agency should treat these risks to bring them to a level that the agency can accept or tolerate. Resources for managing risks should also be part of the planning process.

Fig 4 –Linkages between risk management and the objectives.

Incorporating risk management into the agency's strategic planning process may involve the following:

- **Strategic assessment.** Develop a general understanding of all sources of risks that affect the agency. Consider both the external and internal factors that could impact on the agency's ability to achieve its objectives. This can involve exercises such as horizon scanning.
- **Strategic development and planning**. When developing your strategic objectives, you must consider the associated risks and opportunities. Risk assessment plays a crucial role in this step, as it allows you to analyse the effectiveness of current controls and identify residual risks. Based on the assessment results you can adjust delivery plans, policies, and procedures to support the achievement of strategic objectives. Additionally, reviewing the existing risk profile, Risk Appetite Statements, and merging risks on a periodic basis can embed risk management into the strategic process.

Another benefit of integrating risk assessment at the strategy development and planning stage is that it helps to assign risk owners and identify performance indicators before implementing processes.

4.3 Risk Management in Projects

Effective project governance is essential for managing project risks. Project risks should be visible within the overall risk management process of the agency and managed alongside other ongoing risks, rather than in isolation. Following the completion of a project, risks identified during the project should be reviewed and assessment made on next steps. If a risk does not close at the end of a project, then the risks should be handed over to BAU. Project risk management aligns with the agency's wider risk management framework. By aligning project risk management with your agency's wider risk management framework, the agency will be able to identify and manage common project risks such as those related to poor project governance, flawed scope definition, or sub-optimal resourcing arrangements.

NSW Treasury's Investment Framework guidance material provides further guidance on considering risks in capital planning processes, including developing robust business cases.[2] Risks identified in business cases should not just be captured in business cases – instead they should be integrated into organisational risk management for ongoing monitoring and reporting.

4.4 Specialist risk management

An agency may have specialist risk management functions, such as climate change, cyber, work health and safety, or organisational resilience. Where an agency maintains specialist risk management functions, the specialist risk management framework should align with the agency's broader risk management framework.

[2] https://www.treasury.nsw.gov.au/information-public-entities/centre-for-economic-evidence/investment-framework

5 Risk Management Process

A risk management process is the application of the steps an organisation takes to identify, analyse, evaluate and treat risks. These steps should be done with stakeholders in collaboration with the risk management function. Each step in the process should be continuously monitored.

To be effective the risk management process must be:

- an integral part of the agency's operations,
- embedded in the agency's culture and practices,
- tailored to the agency's business processes, including your strategic, business and project planning processes, and
- developed and implemented with input from across the organisation, so that a diverse range of skills, experiences and perspectives contribute to the process.

Risk management is dynamic and ongoing, with the risk management process triggered by a variety of situations, but it is always in response to new information or conditions. Examples include:

- major changes to operating conditions, such as a local or macro-organisational restructure (e.g. Machinery of Government changes), the establishment of new organisational functions, or the introduction or removal of major policies
- the commencement of programs or projects
- as part of business case development
- in response to the release of updated data (eg. climate change projections or research)
- in response to a major external enquiry
- during business planning and strategic planning cycles
- if legislation affecting the agency has been introduced or amended

5.1 Steps of the risk management process

The following steps describe the risk management process. These steps align with the process outlined in *ISO 31000* and are explained further in the following sections:

1. **Establishing the context:** defining the internal and external parameters to be considered when managing risk and setting the scope of the agency's risk management process. This includes specifying the level and type of risk that it may or may not take, and defining the criteria used to evaluate the significance of risks.
2. The risk identification, analysis and evaluation stages are collectively known as **risk assessment**.
    a. **Risk identification:** finding, recognising and describing risks
    b. **Risk analysis:** understanding the nature and level of risks so you can make decisions about whether a risk needs to be treated
    c. **Risk evaluation:** deciding what action, if any, to take in relation to a risk

3. **Risk treatment:** identifying, selecting and implementing responses to risks that fall outside the levels the agency is prepared to accept or tolerate
4. **Communication and consultation:** exchanging information about risk management with internal and external stakeholders
5. **Monitoring and review:** continually checking each component of the risk management process is performing as desired
6. **Recording and reporting:** the risk management process and its outcomes should be documented and reported appropriately through the agency

5.1.1 Establishing scope, context and criteria

Scope and context inform the other elements of the risk management process, including deciding what types of risk will be considered, how they will be measured, and establishing criteria to decide if a risk is acceptable or tolerable. The scope and context should be consistently referred to throughout a risk management framework and process. All risk conversations and decisions should aim to assist the agency in achieving its objectives.

To establish the scope and context of the risk management process an entity should consider both internal and external variables which may impact the risk environment:

- External variables are the environment or setting in which the agency operates. This includes political, economic, social, technological, legal, climate, and environmental settings.
- Internal variables are environments within the agency, such as culture, governance and other structures, processes, and accountabilities.

A risk appetite statement (RAS) specifies the level and type of risk that it is prepared to accept, relative to its objectives.

Criteria to evaluate identified risks

Defining your risk criteria helps you to ensure that you are consistent in deciding the significance of the risks that the agency is facing and supports effective decision-making. This includes a consistent approach to defining and measuring the consequences and likelihoods or risks, and the agency's capacity to take risks.

The criteria that are needed to form an understanding of the level of a risk are:

- The consequence, or impact, of the risk
- The probability, or likelihood, of the risk occurring
- How probability and consequence combine to determine the overall risk rating.

Example risk criteria that you can adopt for the agency's risk management process can be found in Appendix C.

5.1.2 Risk Assessment

Risk assessment is a structured approach consisting of three discrete stages: *risk identification*, *risk analysis* and *risk evaluation*.

Risk assessment stages	
1. **Risk identification**	What can happen and why?
2. **Risk analysis**	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?
3. **Risk evaluation**	Is the current level of risk acceptable or tolerable compared with established criteria? If not, what further measures are needed to manage the risk?

Risk identification

Risk identification involves finding and recognising uncertainties that could impact the agency's objectives. Both threats and opportunities should be considered, and existing controls identified. Risk identification must be ongoing, adapting as objectives and environments change. Current information is critical.

A variety of tools and techniques can be used to identify risks. You should select the methods best suited to the 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 to articulate its objectives and identify potential events that could affect the achievement of the objectives.

Risk Analysis

Risk analysis is the process of coming to an understanding about the nature and level of risks so that a decision can be made about whether the risk can be accepted. It should be undertaken with stakeholder consultation. This analysis involves:

- **Determining the level of each risk** – The agency must use the consequences and likelihood tables alongside the risk matrices which they have developed (as discussed in 5.1.1) to determine the level of each risk. This is often called the 'inherent risk rating'.

  Rules should be established for how to manage and rate risks which have more than one consequence. It is also good practice to analyse the level of risk in both current case and worst-case scenarios.
- **Analysis of existing controls –** Once a risk has been identified, any existing controls must be identified and assessed using the control effectiveness criteria that were established in the scope and context stage.

- **Identifying and documenting uncertainties and sensitivities –** These should be identified and documented when interpreting and communicating the results of the risk analysis. This information can also be included in the risk register.

Risk analysis can be difficult, especially when events are highly uncertain. Risk analysis can also be influenced by assumptions, the quality of information used, opinions and biases. These should be documented as part of the analysis.

Risk analysis is an input into risk evaluation and decision-making.

Risk evaluation

The evaluation process determines if the risk should be accepted or if additional actions are required to treat the risk and lower the residual risk rating. The residual risk rating is the level of risk that remains after controls have been put in place. This process is used to prioritise risks and to focus the attention of management. Evaluating a risk will lead to one of the following decisions:

- **Treat** - Reduce the risk using treatment actions and additional controls.
- **Accept** - Accept the risk and take no further action or controls to reduce the risk, reviews to ensure currency. The risk cannot be realistically reduced any further.
- **Avoid** - This means that no actions can reduce the risk to an acceptable level. Therefore, the objective must be reviewed and possibly changed or, if necessary and/or possible, abandoned.
- **Share** - Share the risk with another party e.g. by outsourcing or insurance

The proposed risk rating is the anticipated rating once all identified treatment actions have been implemented. This is not the desired rating, but a realistic predicted risk rating once any treatment activities have been completed.

5.1.3 Risk Treatment

Risk treatment is the process of identifying, selecting and implementing responses to the risks that have a higher risk rating than the agency finds acceptable. Whether a risk rating is 'acceptable' will depend on whether it exceeds the target ratings agreed by the agency. The evaluation of existing controls helps to determine whether these controls can be modified, or if new controls need to be introduced.

Risk treatment is cyclical. If the level of risk remains unacceptable after it has been treated then additional actions should be identified such as escalating the risk, before the risk is assessed again.

Treatment options include taking action to:

- change the consequence, or
- change the likelihood

Risk treatments should be developed by, or under the direction of, a risk owner. Stakeholders should be consulted during the development and implementation of risk treatments.

If there are no treatment options, or the options do not modify the risk to an acceptable level, the risk should be recorded and kept under review. Regular and careful monitoring is essential to ensuring the effectiveness of any risk treatment.

Example control design and implementation tables can be seen in Appendix D.

5.1.4 Communication and consultation

Each team in the agency will often only have control over certain aspects of a risk. It is therefore extremely important for leaders to collaborate by articulating the risk context and agreeing on ownership, responsibilities, and actions. These discussions should identify:

- Which senior leader is accountable for delivery of the objectives potentially impacted by the risk? This is usually the best indicator of risk ownership.
- Who is best placed for implementing and managing each control and treatment action, including their design, implementation, and management?
- The shared mechanisms and responses that need to be implemented if the risk materialises.

5.1.5 Monitor and review

As well as monitoring and reviewing individual risks, it is important to monitor and review your overall 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 risks are still relevant
- you can capture lessons learnt from your risk management activities, including near misses and actual losses or gains, and
- the expected results of the agency's risk management process are being achieved.

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

- management reviews - for example, the use of self-assessments
- 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.

The monitoring and review phase can be supported by using a process elements model to check each element of the process. A generic example has been included in Appendix D.

5.1.6 Recording and reporting

Recording and reporting the risk management process and its outcomes provides:

- information for decision making
- a way of communicating risk management activities and outcomes, and
- support for engagement with stakeholders

5.2 Measuring the performance of the Risk Management Process

Reviews may indicate that your risk management process needs refinement. Any changes to the agency's risk management process or your risk management framework should be formally documented and approved in accordance with your risk management policy.

The responsibility for monitoring and performing reviews of the elements of the risk management process within the agency should be clearly assigned when roles and responsibilities are defined in your risk management framework. You should document the outcomes of your monitoring and review and regularly report these to your AA and the ARC.

6 Collaboration and Best Practice

Collaboration is a central focus of improving risk management across the sector. By breaking down silos and collaborating, we can use risk management to detect and respond to changes in a timely manner. Information and perspectives should be supplemented by further enquiry as necessary, should reflect changes over time, and should be appropriately evidenced.

Communication and consultation should:

- bring together different functions and areas of professional expertise in the management of risks
- ensure that different views are appropriately considered when defining risk criteria and when analysing risks
- provide sufficient information and evidence to facilitate risk oversight and decision making
- build a sense of inclusiveness and ownership among those affected by risk
- raise the profile of the risk conversation and keep consideration of risk at front of mind

6.1 Risk Registers

Risk registers are an effective way to ensure key stakeholders are aware of the full range of risks that the agency faces, how these risks might evolve, and the risk control strategies in place to manage them.

A risk register is a list of the risks that the agency has identified and assessed as part of its risk management process. Large or complex agencies may benefit from developing a hierarchy of multiple risk registers. By having this holistic view, key stakeholders can make more informed decisions in how these risks are managed. Keeping up to date risk registers also helps the agency to meet their information obligations to Audit and Risk Committees, Boards, and other relevant stakeholders.

Responsibility for maintaining the risk register should be assigned at each level of the agency. For example, the whole-of-agency risk register should be compiled and maintained by your CRO. It is important to maintain an audit trail of when changes are made to the risk register.

For further information on how a risk register is developed and the information it might contain, please see Appendix E.

6.2 Risk Reporting

Risk reporting is the regular sharing of risk information with decision makers to enable them to fulfil their risk management obligations.[3] Accurate and timely reporting of risk information is an essential part of good governance.

In some situations it can be helpful to focus not just on current risks, but also on 'worst-case risks' which enable stakeholders to make decisions while being aware of all possible outcomes.

Risk reports should be aligned with the governance arrangements of the agency and be customised to reflect your structures, committees and functions. This will inform things such as:

- The frequency and timeliness of reporting
- How reporting is integrated with planning and performance management processes
- Links to organisational objectives
- The method and format of reporting
- The scope of strategic risk updates
- The requirements of stakeholders

6.3 Types of Reporting

There are multiple different types of report which each serve different purposes in risk reporting. These include strategic risk reports, operational risk reports, emerging risks, and deep dive reports. The CRO is usually responsible for producing these reports and optimising the frequency and content of the reports to meet the needs of the agency.

Please see Appendix F for examples of strategic and operational risk reports, and their purposes.

[3] Risk reporting is governed by the *State Records Act 1998*; *State Records Regulation 2015*; *C2021-05Managing Records in NSW Government*; *Privacy and Personal Information Protection Act 1998 (NSW)*; *Privacy and Personal Information Protection Regulation 2019 (NSW)* (PPIP Regulation).

7 Continual Improvement

Continual improvement is an important part of risk management as it helps the agency adapt to changing circumstances and situations. Agencies are operating in an increasingly volatile and complex environment, with new threats emerging quickly. Transparency and accountability are more important than ever when managing the impacts of risks.

By regularly and proactively updating risk management strategies, the agency can ensure that potential threats are identified efficiently - even with frequent changes in technology, regulations, and government priorities. In addition to safeguarding assets and ensuring compliance, this approach promotes a culture of resilience and innovation, and is a key driver for meeting community expectations and ensuring long-term success.

7.1 Monitoring, Review and Evaluation Process

Continual improvement can be achieved by utilising the agency's monitoring, review and evaluation processes to identify changes to improve the efficiency and efficacy of your risk framework. The agency should:

- Periodically review the performance of the risk management framework against its purpose, implementation plans, indicators and expected behaviour; and
- Determine whether elements of the framework remain suitable and effective in supporting the objectives of the agency.

Evaluations can be in the form of self-assessments, management reviews, or independent audit. Some questions which may be considered in the evaluation include:

- Does your risk management framework demonstrate good practice, and is it aligned with the standard (*ISO 31000*) and the needs of the agency?
- What are the background indicators telling us about the performance of systems and operations, and are they effective in measuring performance?
- Is the framework effectively implemented, and how well is it integrated into operations?
- Does the framework support the effective identification, management, and review of critical risks?
- Does the agency have an effective continuous improvement program? How are improvement opportunities identified, prioritised, implemented and monitored?
- How do the agency's senior leadership promote a positive risk culture?
- What can we learn from any incidents that have occurred previously and how can these learnings be implemented?

Key Risk Indicators

Key Risk Indicators (KRIs) provide a way to effectively monitor and review the progress and performance of the risk management activities adopted by the agency and provide early warning of potential future events.

KRIs are most effective when they relate directly to agency objectives, are embedded in the agency's performance management and reporting system, and provide actionable information.

It can also be useful to monitor the progress of implementing risk treatment plans as a qualitative performance measure. As the agency's 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, the agency can monitor:

- **Changes to the consequence or likelihood of a risk:** If the 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 may be an indicator of the likelihood, and therefore overall risk, of not delivering the project
- **Changes to the effectiveness of your controls:** If the agency's firewall is your major control against the risk of being hacked, the number of failed attempted firewall breaches can be an indicator of effectiveness of your firewall
- **Processes and activities as they are performed or implemented:** You can monitor the controls implemented by individual risk owners to ensure that risks are being managed most appropriately.

KRIs should be included in risk management reports to the executive and, where relevant, the agency's ARC.

7.2 Continual Improvement

When improvement opportunities are identified, the agency should develop plans and assign tasks to those accountable for implementation. Small improvements can be done on a continuous basis as they are less likely to require major changes.

Any actions taken should contribute to improving risk management in the agency. Below are some useful tools to support continual improvement of the risk management framework.

7.2.1 Lessons Learnt

Continuous risk management learning enhances risk management performance, as it uses your agency's existing knowledge and recent experiences to achieve agency-wide behavioural and cultural change.

This knowledge can be sourced from both previous risk management decisions and from the experiences of other agencies. This kind of knowledge can be shared through working groups, information sessions, learning events, newsletters and other publications.

These lessons should be continually captured, evaluated, and acted upon.

7.2.2 TPP20-06 Treasury Risk Maturity Assessment Tool

The *TPP20-06 Treasury Risk Maturity Assessment Tool* aims to support the improvement of risk management, culture and capability across the NSW public sector.

The tool is a good starting point to identify the current level of the agency's risk maturity, and how you can reach your desired level of risk maturity. It provides a uniform approach to self-assessment.

Your risk maturity assessment should result in a program of activities that will support the agency in lifting its level of risk maturity.

8 Glossary

Term	Definition
Accountable Authority (AA)	For an agency, has the same meaning as in section 2.7(2) of the GSF Act, which is, unless otherwise specified in the GSF Act, the Secretary of the Department if the agency is a Department, or the head of the agency if the agency is not a Department.
Audit and Risk Committee (ARC)	The Committee established in accordance with NSW Treasury policy requirements to monitor, review and provide advice and guidance about the agency's governance processes, risk management and internal control frameworks and external accountability obligations
Chief Audit Executive (CAE)	The most senior position in the agency with the primary responsibility and accountability for the audit function of the agency, including monitoring and verifying the adequacy, effectiveness and correct operation of the internal control system, and sharing findings and relevant insights from audit projects.
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.
Circumvent	To find a way around an obstacle or to avoid something
Consequence	The outcome of an event affecting objectives
Control	A measure (including a process, policy, device, practice or other action) that is modifying risk
Enterprise Risk Management	The integrated process of identifying, assessing, managing, and monitoring risks across an organisation to minimise negative impacts and maximise opportunities.
Governance	Set of responsibilities and practices, policies and procedures, exercised by an agency's executives, to provide strategic direction, ensure objectives are achieved, manage risks and use resources responsibly with accountability
Independent Assurance	The process of providing an objective evaluation of an organisation's processes, procedures, and controls
Internal Controls	The processes and procedures implemented by an organisation to ensure the integrity of financial and accounting information, promote accountability, and prevent fraud
Iterative	The process of repeating a sequence of steps or actions to gradually improve or refine the outcome
Key Risk Indicators	Measurable metrics used to identify potential risks that could impact an organisation's strategic objectives enabling proactive decision-making
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

Term	Definition
Objectives	Specific and measurable goals that an organisation aims to achieve within a defined timeframe
Process Elements Model	Framework that defines the various components or elements that make up a process
Risk	The effect of uncertainty on objectives
Risk Appetite	The level of risk an organisation is willing to accept in pursuit of their goals
Risk Assessment	The overall process of risk identification, risk analysis and risk evaluation
Risk Culture	Combination of values, beliefs, knowledge and attitudes shared by an agency which shapes how staff identify and manage risk, and influences the approach taken to decision-making
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 Process	The systematic application of the steps an entity undertakes to identify, analyse, evaluate and treat risks
Risk Maturity	The degree of development and effectiveness with which an organisation identifies, assesses, monitors, and manages risks
Risk Ownership	Responsibility assigned to an individual or group, accountable for managing a specific risk by ensuring it is identified, assessed, mitigated, and monitored effectively.
Risk Rating	Evaluating the risks associated with an organisation's operations and categorizing them as low, medium, or high based on their potential impact on the business
Risk Register	A record of information about identified risks
Risk Reporting	The process of sharing risk information with decision makers
Risk Treatment	The process of identifying, selecting and implementing measures to mitigate the risks

9 Appendix

9.1 Appendix A – Risk-related Accountabilities, Roles and Responsibilities

The table below outlines example risk-related responsibilities for various roles which may exist in the agency. Please note that this list is not fully comprehensive and only includes responsibilities related to risk.

These roles and responsibilities can support development of your agency's risk management policy. Not all agencies will need all the roles set out in this table.

Role	Responsibilities
Accountable Authority/Governing Board of a Statutory Body	• Has the ultimate responsibility for risk management and is the risk sponsor • Ensures that there is an effective system of internal control over the financial and related operations of the entity • Ensures that internal audit functions are established • Determines the entity's risk tolerance and appetite • Ensures the implementation and regular review of the entity's risk management plan • Ensures that risk management is included in job descriptions, staff induction programs and performance agreements, and is considered as part of performance appraisals. • Ensures compliance with current Australian/New Zealand standards and NSW public sector policies on risk management
Audit & Risk Committee (ARC)	• Reviews whether management has a current and appropriate risk management process in place, and associated procedures for effective identification and management of financial and business risks, including fraud and corruption • Reviews whether a sound and effective approach has been followed in developing and implementing risk management strategies in relation to major projects or undertakings • Reviews the impact of the risk management process on the entity's control environment and insurance arrangements • Reviews whether a sound and effective approach has been followed in establishing business continuity planning arrangements, including whether disaster recovery plans have been tested periodically

Role	Responsibilities
	• Reviews the fraud control plan to confirm that the entity has appropriate processes and systems in place to capture and effectively investigate fraud-related information.
Executive/Management Committees	• Reviews activities with a focus on risk management • Reviews risk treatment plans and risk management reports, including risk registers, and assessing them for completeness, accuracy, consistency, and use of a common language • Reviews internal controls for efficiency and effectiveness • May also have the executive authority to manage risks
Risk Management Function	• Develops/leads the development of the risk management policy and strategy for risk management • Acts as the primary champion for risk management at the strategic and operational level • Designs and reviews the processes for risk management • Builds a risk management culture within the agency, including appropriate staff training and development • Provides advice and tools to staff to assist them in managing risk • Co-ordinates the various functional activities relating to risk management within the agency • Works with risk owners to ensure compliance with the risk management framework • Collates and reviews risk registers for completeness and accuracy • Prepares risk management reports for the ARC 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.
Chief Risk Officer (CRO)	• Leads the risk management function as the primary risk champion, including designing the entity's risk management framework and managing the day-to-day activities associated with coordinating, maintaining and embedding the framework. The role does not have to be a dedicated one. In smaller agencies 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	Responsibilities
	role of a CRO. More complex agencies may benefit from a dedicated role to ensure comprehensive and focused risk management. • The role of the CRO is different from the role of the CAE. Appropriate safeguards should be in place to address the threats to independence of both roles.
Risk Champion	• Promoting risk management across the agency, or specifically within a particular agency function or project. • Embeds risk management into the agency's other systems and processes. • Ensures that functional and project areas are using the agency's risk management processes consistently. A risk champion may hold any position within the agency, but is generally a person who: • Is responsible for supporting and driving particular aspects 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
Managers	• Managing risk and ensuring that their staff perform their duties within the constraints of the agency's ability to manage risk. • This includes being responsible, within the sphere of their authority, for: o establishing an environment that promotes an awareness of internal controls and responsibility for individual risks o identifying uncertainties that will affect the achievement of agency objectives o establishing policies, operating and performance standards, budgets, plans, systems and procedures to address identified risks and reduce them to an acceptable or tolerable level o monitoring the effectiveness of controls o 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, which are completed by operating units, could be a mechanism that

Role	Responsibilities
	management can use to demonstrate this aspect of the internal control structure).
Chief Financial Officers	• The person primarily responsible for financial management within an agency including preparation of financial information. • Oversees the management of financial risk within the agency. • Advises the Accountable Authority, who is accountable for financial performance. • Oversees a program of internal controls to provide assurance on financial systems and information. This is required to be annually certified to the Accountable Authority that they have 'effective systems, processes and internal controls to ensure that the monthly and annual financial information provided to Treasury is reliable'.
Risk Owners	• Designs, implements and monitors risk treatments for a particular risk. • Ensures 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
Staff, workers and contractors	• All staff, workers 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, workers and contractors should also report ineffective or inefficient controls. • All staff, workers and contractors should be aware of the risks that relate to their roles and activities.
Chief Audit Executive (CAE)	• Oversees the planning and management of the agency's annual internal audit program, and ensuring effective reporting of internal audit findings to the accountable authority, responsible executives and the ARC. • Provides assurance that: ○ risk controls are appropriately designed and effectively implemented

Role	Responsibilities
	○ the agency's risk management framework is effective. ○ control processes are effective and adequate • Understanding the ARC's assurance requirements.

9.2 Appendix B - Drivers for improving risk culture

Drivers	Action
Values Statement	Including risk and risk management in a Values Statement, or similar, approved by the Accountable Authority. For example, by stating that 'We value communication of risk information and the management of risk'.
Management demonstrating commitment to risk management	• Communicating to staff the consequences of not demonstrating expected risk management behaviours • Ensuring that risk is included on the agenda in relevant project or team meetings • Conducting regular review of risk status, risk reporting and follow up actions • Actively monitoring key risk indicators
Systems and processes	• Designing agency-specific, fit-for-purpose tools, systems and processes to help people manage risk. • Providing guidance to staff in the agency that use these tools and ensuring support is available
Organisational structure	• Ensuring the organisational structure allows responsibility for risks in all levels, and risk treatment to be delegated.
Roles and responsibilities	• Ensuring job descriptions refer to accountabilities and responsibilities for risk management • Assigning leadership roles in risk management • Addressing poor risk management behaviours and reviewing these as part of the staff appraisal process.
Performance agreements	• Articulating risk management responsibilities in performance agreements
Desired versus actual behaviours	• Measuring risk management culture and attitude through surveys into organisational climate surveys and performance management systems. • Analysing results and recognise those who effectively identify or manage risk.
Effective communication	• Ensuring that the agency communicates its reasons for managing risk and that these are commonly understood and agreed.

Drivers	Action
	• Creating an environment where all staff feel comfortable discussing risk management issues, encouraging effective two-way communication about risks and their management. • Ensuring that staff understand the agency's tolerance for risk and when and to whom risks should be escalated.

9.3 Appendix C - Tools to support the risk management process

9.3.1 Methods or tools to identify risks

Methods or tools to identify risks:

- 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
- risk assessment workshops

Risks can be **identified through these business activities:**

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

Some actions for risk identification:

- consider possible sources of risk for the 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 in a risk register and the risk identification process that was used as well as stakeholders involved in the process.

Each method has strengths and limitations. Previous experience can guide risk identification, but may not be reliable for new processes, systems, or policies. Therefore, the agency should follow a systematic and disciplined approach that isn't limited by past experience.

Risk identification should be integral to your strategic, business, operational, change management, and project planning processes. It should be part of daily activities, involving knowledgeable stakeholders. All risks should link to the agency's objectives, identified when establishing context. This process should be continuous to identify new risks and validate existing ones.

9.3.2 Likelihood and Consequence Tables

These tables provide a foundation for an agency to tailor them to their own circumstances in development of their risk rating methodology.

Likelihood Rating	General Description	Historical	Probability
Almost Certain	Expected to occur in most circumstances involving normal operations.	Large number of known incidents within the department. Occurs regularly in the industry.	Predicted to occur in almost every operation of this kind (>90%)
Likely	Considerable opportunity and means to occur. Could happen at any time.	Regular incidents known within the department. Has occurred many times in the industry	Likely to occur in more than 1-in-2 operations of this kind (50%-90%)
Possible	Some opportunity and means to occur.	Few infrequent, random occurrences recorded within the department. Has occurred several times in the industry.	Likely to occur between 1-in-2 and 1-in-4 operations of this kind (25-50%)
Unlikely	Little opportunity or means to occur. Might happen, but not expected to occur.	No known incidents recorded or experienced within the department. Has occurred once or twice in the industry	Likely to occur between 1-in-4 and 1-in-20 operations of this kind (5%-25%)
Rare	Almost no opportunity to occur. Might happen, but probably never will.	Not known or reported to have ever occurred in the industry.	Highly unlikely to occur (<5%)

Figure 4. Likelihood scale

Category	**Insignificant** Minimal impact requiring only marginal remediation activities/management	**Minor** Small, local effects easily contained	**Moderate** Some impact or impact requiring remediation	**Major** Significant impacts/costs with some objectives not met	**Extreme** Catastrophic event threatening viability of function and objectives
Example 1: Financial/Built Assets	Barely noticeable financial impact easily absorbed within project or program budget	One-off under or overspend up to $10M or 5% of your budget	One-off under or overspend up to $25M or 15% of your budget	One-off under or overspend up to $100M or 25% of your budget	One-off under or overspend over $250M or 30% of your budget
Example 2: Health, Safety & Wellbeing	Physical or psychological Injury/ Illness requiring notification or treatment up to First Aid only.	Physical or psychological Injury/ Illness requiring professional medical treatment	Physical or psychological Injury/ Illness resulting in moderate temporary impairment or disability (up to 6 months).	Physical or psychological Injury/ Illness resulting in partial permanent disability or long-term temporary impairment (more than 6 months)	Single or multiple fatalities. Physical or psychological Injury/ Illness resulting in irreversible, total permanent impairment or disability

Figure 5 – Example Consequence Table

9.3.3 Risk Matrix

The risk matrix shows the outcome of the combined likelihood and consequence.

The example below can be customised for the specifics of your agency.

	CONSEQUENCE	Insignificant	Minor	Moderate	Major	Extreme
LIKELIHOOD	5 Almost Certain	Moderate 5	High 10	Extreme 15	Extreme 20	Extreme 25
	4 Likely	Moderate 4	High 8	High 12	Extreme 16	Extreme 20
	3 Possible	Low 3	Moderate 6	High 9	High 12	Extreme 15
	2 Unlikely	Low 2	Moderate 4	Moderate 6	High 8	High 10
	1 Rare	Low 1	Low 2	Low 3	Moderate 4	Moderate 5

9.4 Appendix D - Control Effectiveness Ratings Tables

Rating Category	Control Design
Very Strong	• Will substantially reduce risk. • High degree of automation or documented formalised processes.
Strong	• Will substantially reduce risk. • High degree of automation or documented formalised processes. • Rare exceptions. • Places reliance on knowledge/actions of key persons.
Adequate	• Designed in such a way it will reduce risk. • Expected to fail at times, however within acceptable appetite. • Places reliance on knowledge/actions of key persons.
Limited	• Designed in such a way it will reduce some aspects of risk. • Likely to fail requiring remedial effort and actions. • Places heavy reliance on knowledge/actions on persons to manually address exceptions/incidents.
Weak	• Poor design even when used correctly. • It provides little or no protection. • Only addresses part of the risk requiring additional work arounds or manual processes to make up for deficiencies. • Extreme reliance on knowledge/actions of key persons.

Rating Category	Implementation
Very Strong	• The control operates consistently as intended and is being correctly applied by the vast majority of users. • Never known to fail in the past, highly unlikely to fail in a short to mid-term.
Strong	• The control operates on a mostly consistent basis and is being applied correctly by most users. • Control is mature and unlikely to fail significantly within 12-month period. • Has significantly addressed the risk.
Adequate	• The control operates as intended at least half of the time by sections of control users. • The control has experienced a failure in the past 12 months but is not expected to experience more in the immediate future.
Limited	• The controls are not operating consistently and/or effectively or have not been implemented in full. • The control has experienced failures in the past 12 months and is expected to experience more, potentially more frequently. • Rates of failure are deemed to be unacceptable.
Weak	• Consistently not operating as intended, immature, operating inappropriately or inconsistently. Rates of failure are significant and deemed unacceptable.

Figure 6 – Example Control implementation / operational effectiveness table

		Implementation				
		Very Strong	Strong	Adequate	Limited	Weak
Control Design	Weak	Partially Effective	Partially Effective	Ineffective	Ineffective	Ineffective
	Limited	Partially Effective	Partially Effective	Partially Effective	Ineffective	Ineffective
	Adequate	Substantially Effective	Substantially Effective	Partially Effective	Partially Effective	Ineffective
	Strong	Effective	Substantially Effective	Substantially Effective	Partially Effective	Ineffective
	Very Strong	Effective	Effective	Substantially Effective	Partially Effective	Partially Effective

Figure 7 – Control Matrix example

9.5 Appendix E - Risk Register

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, their owners and their effectiveness
    - the current consequence, likelihood and risk level
    - whether the risk is acceptable or tolerable
    - additional treatments, their owners, and treatment due dates if the risk is not acceptable or tolerable
    - the residual risk level once additional treatments have been implemented.
- risk owner – who is accountable 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)
- target risk rating and due date

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

For further guidance on how to best create a risk register that suits the agency's needs, try answering the following questions for guidance:

- Have risk owners been assigned?
- Have control owners been assigned?
- Have controls been assessed (effective, partially effective, ineffective)?
- Have risk ratings been reviewed and updated?
- Have treatment actions been implemented as planned?
- Are treatment actions being monitored?
- Are there mechanisms in place to review and update the risk regularly?

The agency's risk register can be developed or set out in many ways. The content of your risk register should be customised for the agency and the information needs of key stakeholders. In more complex organisations, additional technical or specific information may be needed.

The agency decides 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.

9.6 Appendix F - Strategic Risk Report

Report type	Users	Frequency	Purpose and content
Attestation statemen in accordance with *TPP20-08: 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 TPP20-08.
Annual report	External and internal stakeholders	Annually	The GSF Act and Treasurer's Direction TD23-10 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.
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 AA 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)

Figure 8 – 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.