

The Cabinet Office and  
Premier's Department

# Risk Management Policy

---

October 2022



OFFICIAL

# Document management

## Publication details

Document type(s) (select all that apply)	Yes/No
Policy	Yes
Procedures	
Guidelines	
Standard	
Fact sheet	

Responsible branch	Document owner	Document reviewer
Cabinet & Governance	Governance Team	Senior Advisor, Governance

Publication (select all that apply)	Yes/No
Not for publication	No
Intranet	Yes
NSW Government website	Yes
Other (please specify)	

Approved by	Date of approval
TCO Secretary	
PD Secretary	
Executive Committee	24 October 2022

## Review record

Date	Action	Version
June 2010	Publication	1.0
May 2011	Publication	2.0
June 2012	Publication	3.0
January 2013	Publication	4.0

Date	Action	Version
March 2014	Publication	5.0
November 2016	Publication	6.0
November 2017	Publication	7.0
February 2020	Publication	8.0
October 2022	Publication	9.0 (Risk Appetite Statement added as appendix - Feb 2023) (Section 3 and 6.1.3 amended to reflect changes in Premier's Department organisational structure – Aug 2023)

# Contents

1	Scope and purpose .....	1
2	Definitions .....	1
3	Roles and responsibilities.....	3
4	Key principles .....	Error! Bookmark not defined.
4.1	[Summary of principal] .....	Error! Bookmark not defined.
4.2	[Summary of principal] .....	Error! Bookmark not defined.
5	Procedures .....	7
6	Contacts.....	7

# 1 Scope and purpose

It is the policy of the Departments to identify, manage and treat risks that arise in the pursuit of the strategic objectives and priorities of the Departments, its staff and stakeholders. This means all risks should be managed within the boundaries defined in our Risk Appetite Statement. In support of our commitment and accountability the Departments will comply with the NSW Treasury Internal Audit and Risk Management Policy for the General Government Sector (TPP20-08), ISO Risk Management Standard 31000:2018 and all relevant legislation and public sector requirements.

This policy aims to ensure that there is a systematic process to identify, analyse, assess, manage and monitor risk.

This policy:

- Enhances the Departments ability to seize opportunities while reducing the impacts of risk to the lowest practicable level
- Establishes the principles by which the Departments will identify, assess and manage risk
- Provides for the appropriate allocation of responsibilities for managing risks
- Enhances risk management decisions by providing a robust, uniform approach to identifying, assessing and evaluating risk, and selecting from multiple risk mitigation options having regard to the costs, the benefits and the appetite for the relevant risk.
- Defines the accountabilities and responsibilities for risk management across the Departments.
- Aligns risk appetite and strategy to enable the leadership to consider the Departments risk appetite when evaluating strategic alternatives in investment decisions.

# 2 Definitions

<b>Consequence</b>	The potential impact of the risk event on the Departments objectives and priorities if the risk event were to occur (i.e. insignificant, minor, moderate, major, severe).
<b>Control</b>	Processes, policies, devices, practices or other actions that act to minimise negative risks.
<b>Departments</b>	Means The Cabinet Office ( <b>TCO</b> ) and the Premier's Department ( <b>PD</b> ).
<b>Enterprise Risk Register</b>	TCO and PD risk register established and maintained by the Chief Risk Officer.
<b>Employee</b>	All employees (ongoing, temporary and casual, and those on secondment to the departments); contractors (including employees, agents or subcontractors engaged by a contractor) and agency staff engaged to perform work for, or provide services on behalf of the departments; work experience

students; and volunteers and consultants where their engagement requires adherence to the Code of Conduct.

<b>Event</b>	An event could be one occurrence, several occurrences, or even a non- occurrence (when something doesn't happen that was supposed to happen). It can also be a change in circumstances. Events are sometimes referred to as incidents or accidents.
<b>Inherent Risk</b>	The value of the consequence and likelihood of a risk, before applying any risk treatment plans or controls.
<b>Likelihood</b>	The probability of the risk event occurring (i.e., rare, unlikely, possible, likely, almost certain).
<b>Key Risk Indicators (KRIs)</b>	Measure and metrics that relate to a specific risk and demonstrate a change in the likelihood or consequence of a risk occurring.
<b>Local Risk Register</b>	A risk register relating to a group, branch or project established and maintained by the head of the group, branch or project sponsor.
<b>Objectives (strategic)</b>	Measurable and achievable goals, which may relate to a project, activity, program or an entire Group or organisation.
<b>Residual Risk</b>	The value of the consequence and likelihood of a risk, after applying controls (i.e., the risk remaining).
<b>Risk</b>	The effect of uncertainty on objectives. Risk is measured in terms of the consequence of the risk event if it were to occur and the likelihood of the risk event occurring.
<b>Risk Management</b>	A series of coordinated activities to assist management in the creation and protection of value through controlling activities with regard to risk.
<b>Risk Matrix</b>	Risk Matrix defines the likelihood and consequence criteria and overall risk rating used by the Departments to evaluate the identified risks, and subsequently monitor and treat higher rated risks.
<b>Risk Rating</b>	Risk Rating is assessing the risks involved in the daily activities of a business and classifying them (low, moderate, significant, high risk) on the basis of the impact on the business.

**Risk Register**

A document or collection of documents containing a record of information about identified risks.

## 3 Roles and responsibilities

The TCO and PD Secretaries ultimately responsible for ensuring that appropriate risk management responsibilities are delegated and carried out within the Departments.

**The Secretaries**

- Have ultimate responsibility and accountability for risk management in the Departments
- Promotes a positive risk culture
- Articulates the level of risk the agency is willing to accept or tolerate through risk appetite
- Approve the Risk Management Policy
- Are responsible for ensuring that managers and decision makers at all levels in the agency understand that they are accountable for managing risk within their sphere of authority and in relation to the decisions they take
- Are responsible for ensuring that all staff (permanent, temporary or contract) are aware they are accountable for managing risk in their day to day roles
- Monitor and receives reports on Department risks and their management
- Are responsible for ensuring that risks are adequately considered when setting the Departments objectives and priorities

**Deputy Secretaries, Chief Digital and Information Officer, and Chief Financial and Operations Officer**

- Set and communicate good risk management practices and culture
- Ensure risk capability is developed and maintained within their respective areas to enable effective risk management
- Ensure their respective areas manage risk in line with the Risk Management Policy
- Oversee the allocation of resources to enable effective risk management
- Is responsible for ensuring Group (where relevant) and Branch risk registers are completed as part of the Group/Branch Business Plan.
- Report on key risks and their management to the Risk and Governance Committee, Audit and Risk Committee and PD and TCO Executive

**Executive Directors and Directors**

- Identify, assess and manage risks relating to the operations of their Branch/Teams and assign day to day responsibility for risk management within the teams reporting to them

- Ensure that their staff are aware of the relevant Department policies and approaches to risk management and have the necessary skills to manage risks related to their particular area of work
- Promote a positive risk culture
- Update and maintain Project and Branch Risk Registers for operational risks
- Where applicable, inform updates to the strategic risks on the Enterprise Risk Register and implement any delegated management actions from Enterprise Risk Owners
- Monitor and review the management of risks within their Branch/Team, and consider new and emerging risks on a regular basis
- Report and escalate significant and high risks to the relevant Deputy Secretary (or Secretary, in the case of the Chief Digital and Information Officer and Chief Financial and Operations Officer) in accordance with the Risk Management Policy

#### All Employees

- Be familiar with the Risk Management Policy
- Ensure day to day identification and management of risk in their role, including carrying out their roles and responsibilities in accordance with relevant policies and procedures
- Where appropriate, report and escalate risks and concerns to the appropriate level of management within the remit of their position

#### Chief Risk Officer

- Design, implement and be responsible for the continuous improvement of the risk management Policy so it is dynamic to the internal and external environment within which the Departments operate
- Manage and coordinate the Departments risk management reporting process, and reporting on strategic and emerging risks
- Administer and establish the Risk Management Policy
- Support the Secretary in articulating and embedding the risk appetite statement
- Challenge the completeness and accuracy of risk information
- Ensure that the risk assessment process is consistently applied across all branches of the Departments
- Build risk management capabilities throughout the Departments



- Work collaboratively with branches to provide a second line of defence (appendix two) to the Executive and Secretary to ensure that risk is appropriately managed
- Facilitate risk management knowledge and best practice sharing
- Oversee the delivery of risk management training

### **Chief Audit Executive**

- Provide assurance and advice on the Departments risk management activities, including the design and effectiveness of controls
- Develop and implement risk-based audit action plans
- Monitor and report on progress of implementation action plans to the Audit and Risk Committee

### **Risk Owners** (as a minimum, risk owners are Director level and above)

- Responsible for ensuring that risks are managed, monitored and reported, without taking away the ultimate responsibility of the Secretary
- Consider the risks assigned to them
- Identify, assess and manage risks relating to their respective area or project and communicate these to the relevant Director, Executive Director and/or Executive member
- Devise and implement appropriate risk management plans
- Review progress of implementing management strategies and updating the Enterprise Risk Register for significant and high risks, and maintaining a Local Risk Register for other operational and project risks
- Design and implement appropriate risk treatments (risk mitigation plans) to manage the risk within the boundaries of the Departments Risk Appetite and have a designated responsibility for monitoring the risk(s) on an ongoing basis.
- Report and escalate as appropriate any identified risks that cannot be properly managed consistently within the Risk Management Policy

### **Risk and Governance Committee**

- Oversee the design, implementation, operations and monitoring of the Departments governance, compliance and risk framework
- Monitor the execution of sound risk practices to enhance the overall risk maturity of the Departments
- Understand and review the material enterprise risks facing the Departments, the actions (controls) being implemented to manage the risk, their effectiveness and options for further actions being considered and/or undertaken by the risk owner

- Regularly review the Enterprise Risk Register and high and significant risks reported across operational and project risk registers and report key risks to the PD and TCO Executive

#### **Audit and Risk Committee**

- Provide independent assistance to the Secretary on the Departments governance and risk management processes
- Review the Enterprise Risk Register and provide advice to the Secretary
- Challenge the adequacy of the Departments processes for managing risk
- Make recommendations on risk management within the Departments
- Have oversight on the application of the risk management policy across the Departments
- Endorse the Risk Management Policy
- Monitor and receive reports on risks and their management

#### **Governance Team**

- Administration and establishment of the Risk Management Policy
- Support the Secretary in embedding the Risk Appetite Statement across the Departments, including promoting a positive risk culture
- Provide guidance to staff on risk management processes
- Support the Chief Risk Officer and Chief Audit Executive in risk activities
- Support the Departments leadership to embed a mature, positive risk culture
- Manage and coordinate risk management reporting process, and reporting on strategic and emerging risks
- Aggregate the risks of Department groups and branches into the Enterprise Risk Register for reporting by the Chief Risk Officer to the Risk and Governance Committee, PD and TCO Executive and Audit and Risk Committee
- Ensure that the risk assessment process is consistently applied across all branches of the Departments
- Work collaboratively with branches to provide a second line of defense to the Executive and Secretary to ensure that risk is appropriately managed
- Delivery of risk management training

---

## 4 Risk Management Structure

[Each section here will be a subheading]

## 4.1 Governance

The Departments governance structure supports the management of risks through regular risk assessment, monitoring and reporting. The Secretary is responsible for ensuring that appropriate risk management responsibilities are delegated and carried out in the Departments. However, all employees have a responsibility to identify and manage risk in line with this Policy.

## 4.2 Risk Appetite

The Risk Appetite Statement defines the risks the Departments are willing to accept (its risk appetite), and events and/or actions that are considered acceptable in the pursuit of its objectives.

In considering appropriate tolerance for its risks, the Departments will have regard to the following:

- The importance of providing leadership in policy development through its statutory and strategic role of identifying and managing risk to the NSW Government.
- Sustaining an effective relationship with the Departments stakeholders.
- Assisting in the development and forward planning of Government policy and the setting and achievement of the NSW Government's priorities.
- Protecting the health and safety of its staff and visitors.
- Ensuring compliance with all relevant legislation and public sector accountability requirements.
- Maintaining key services where disruption to business continuity is threatened.

### *What is it?*

Risk appetite sets out and communicates the type and level of risk the Departments are willing to accept in pursuit of its priorities and objectives.

- For example, the Departments may accept a level of project failure where it seeks to invest and lead the sector in innovative program delivery models.

---

# 5 Risk Management Approach

the Departments are committed to embedding a proactive approach to identifying, assessing, prioritising and managing risks that could affect our stakeholders and strategic objectives and priorities.

Figure 3.0 below summarises the Departments risk management process.



Figure 3.0 – Simplified Risk Management process is in line with the ISO 31000 Risk Management Standard

## 5.1 Communication and Consultation

The management of risk is a continuous cycle that ensures risk is actively considered. Planning, communication and consultation is important to ensure that risk management activities are directed at the right stakeholders and organisational context. The risk management process may start by:

- Development of a Group/Branch Business or Project Plan to define objectives and deliverables
- Business plans are a space to capture key Group/Branch objectives, projects and initiatives.

Then a risk assessment is undertaken to identify what events could occur that could negatively (or positively) impact our objectives. We do this by:

- Defining and communicating the objectives and context of the risk assessment; and
- Identifying who the relevant stakeholders are for consultation and input

The above can be performed through either individual or group consultations, or in a workshop environment led by a facilitator. The Risk Assessment Template (Appendix 3) is available on the intranet.

Depending on the risk being assessed, consideration should also be given to whether an additional assessment, such as a cyber security risk assessment (in the case of a new IT system being

implemented) or a privacy impact assessment (in the case of a new project/initiative where data is being collected), is appropriate.

## 5.2 Identify

The purpose of risk identification is to determine a comprehensive list of risks which may affect the Departments objectives and priorities. Consideration will be given to the source of the risk, the event that could trigger the risk and the impact on the Departments objectives. Comprehensive risk identification should include risks whether or not they are under the control of the Departments.

### **Examples:**

The Premier may request that the Departments perform a detailed risk assessment of the cyber security threats (objective) that impact the Departments (context). Relevant stakeholders could be staff, NSW citizens and any parties engaged by the Departments.

### **OR**

the Departments reputation may be affected if Project X (objective) is not delivered on time/budget (context). Consultation with relevant stakeholders include community reference groups, client agencies.

### **“What event could occur in the future that will impact our objectives?”**

The Departments identifies and manages risks at different levels throughout the organisation:

- Department level
- Group level
- Branch level
- Project level

Questions you may ask:

- What has happened in the past?
- What could go wrong?
- How could it happen?
- Who could it impact?

At the Department level, the Chief Risk Officer will facilitate the risk identification and assessment process with the PD and TCO Executive to identify and assess the key strategic risks. This information will be captured in a risk register format. This Enterprise Risk Register will be sent to the Audit and Risk Committee for endorsement on a quarterly basis

The risk management process should establish the context in which the sources that create risks and opportunities for the Departments can be understood. This means establishing the strategic, organisational and risk management context in which the rest of the process will take place.

### **Example:**

- Internal context – the Departments strategic priorities and objectives, business plans and values
- External context – the wider environment in which the Departments operate including the regulatory environment, contractual agreements, funding agreements and other agencies
- Stakeholder context – the consideration of our internal and external stakeholders who may be impacted by the Departments decisions

### **Example:**

A cyber-attack (identified risk) on the data held by the Departments on third parties and staff (context) as a result of an anonymous party breaching the data security protocols in place (cause), resulting in a privacy breach and reputational damage to the Departments (consequence).

## 5.3 Analyse

### **“What is the nature of the risk event, and how could it impact our objectives?”**

When analysing risks, we need first to understand the consequence and likelihood of the risk, and the effectiveness of the current control environment in managing the risk.

It is also important to consider what positive opportunities can be realised when analysing risks. As well as looking how to mitigate and avoid negative risk we should assess positive impacts of risks to enhance the delivery of your work.

**Example:**

A TCO or PD branch sees an opportunity for NSW to drive a reform nationally that will achieve better outcomes for NSW if done as part of a national initiative. The team assesses that it would require a small team to work on the initiative for 6 months, with a 50:50 chance of success at convincing other jurisdictions to participate. Given the scope of the upside if successful, the team assesses the project as worthwhile but uses the risk framework to engage senior executives in the risk/opportunity assessment.

It is important to understand the possible causes and impacts to build an accurate understanding of the issues surrounding the risk(s) identified and how the business objectives could be impacted. It also helps to ensure that the risk is described in a level of detail such that people who are not fully familiar with the background will understand the risk. Once we have determined both the consequence and the likelihood, we have determined the **inherent risk rating**.

It is also important to consider the controls in place which could reduce the consequence or likelihood of the risk event. Controls should be considered and evaluated to determine how effective they are in reducing risk. Controls include any policy, procedure, practice, process, technology, technique, method or device that modifies or manages an existing risk and these controls should be identified for all levels of risk – i.e. Department, group, branch, and project. The table below outlines how control effectiveness should be rated.

**Example:**

How often are the Departments, its groups, branches, and/ or projects going to be subject to cyber-attacks (likelihood)? And what is the greatest likely level of impact of this risk event to reputation and operations (consequence)?

Effectiveness	Description
Effective	Controls are well designed, and are effectively implemented thus significantly reducing risk exposure
Partially effective	The design and/or implementation of controls requires some improvement to effectively mitigate the underlying risk exposure
Ineffective	Controls (if in place) are poorly designed and implemented. The risk's likelihood and/or consequence is not mitigated

After analysing the consequence and likelihood of the risk event, and any mitigating factors such as controls that reduce the consequence or likelihood, we are left with the residual risk.

**Example:**

How effective are the current controls in place to reduce the likelihood and/ or consequence of the risk event? For example does the current cyber security policy (control) reduce the likelihood of a cyber-attack? Does the current system (control) design reduce the likelihood or consequence of a cyber-attack?

**Note:**  
 Your analysis will be documented in the respective Department, branch or project risk register. Your risk register will include:

- Risk Event and Description
- Cause(s)
- Impact(s)
- Controls in place
- Likelihood
- Consequence

Refer to Appendix 2 for the risk assessment template

## 5.4 Evaluate

“How serious an effect could the event have on our objectives?”

Now that the context of the identified risk event has been defined, and the range of potential causes and consequences analysed, evaluation of the risk event should be performed and documented.

The evaluation of the identified risks is performed at the residual risk level i.e., the risk that remains once all existing controls are taken into account (see 5.3).

Evaluation involves combining the overall residual risk likelihood and consequence to produce an **residual risk rating** (i.e., low, moderate, significant or high) using the Risk Matrix at Appendix One.

This Risk Matrix defines the likelihood and consequence criteria and overall risk rating used by the Departments to evaluate the identified risks, and subsequently monitor and treat higher rated risks.

**Example:**

The Departments have identified the risk of a cyber-attack that may impact the Departments financially, operationally and reputationally. Considering the current cyber security controls in place the impact of such a risk event is likely to attract negative media attention and disrupt core business activities (major consequence). Given the increasing trend of such attacks on large organisations, this is considered to have the potential to occur in the next 12 months (possible likelihood).

Based on the Departments risk assessment, a combination of a major consequence and a possible likelihood gives a total rating of ‘significant’ to the risk of a cyber-attack. (Refer to Appendix One for risk assessment detailed criteria).

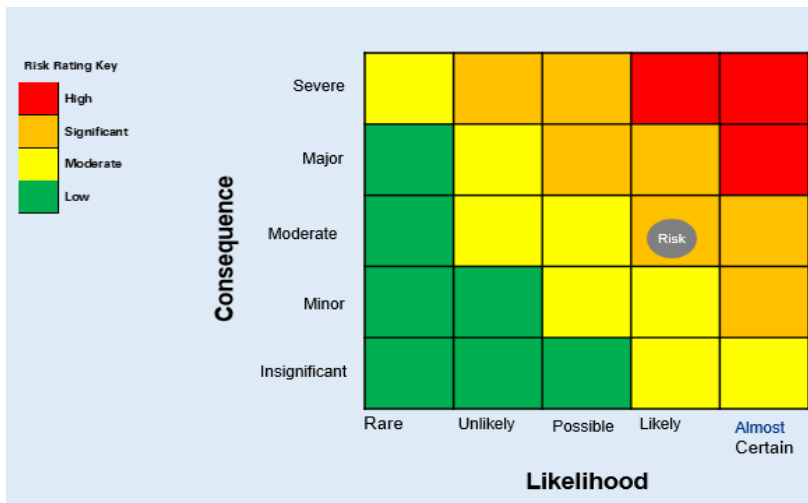


Figure 4.0 – The Departments Risk Assessment Matrix

The residual risk rating is used to assist the Departments in prioritising the effort, resources, monitoring and reporting of its risks.

## 5.5 Treat



### “How can we minimise/modify the event impact on our objectives?”

Once the level of residual risk has been determined, and it remains outside the Departments risk appetite, then risk treatment can be applied. Treatment may include ceasing the activity that creates the risk, managing the risk, accepting the risk, sharing or transferring the risk.

Accept and monitor low priority risks. For other risks identified, develop and implement specific management plans including the resources allocated to manage the risks to an acceptable level. Risk treatments become part of the routine business process

- Questions you may ask:
  - Is the control design effective to address the risk?
  - Do the controls operate effectively?
  - Are there monitoring activities and if so are they effective?
- Is there a better control that could be more effective to address the risk?

#### Types of risk treatments include:

- control implementation – can be detective, preventative or corrective
- training around the risk and risk event
- policy and procedures – new or redesigned policies and/ or procedures to help reduce/ eliminate the risk

#### Example:

The Departments have a number of existing measures in place that reduce the likelihood of a cyber security attack, however there are options to strengthen the existing controls, and create new controls that may reduce the likelihood and consequence of an attack. These may include:

- Increase regular staff training on cyber security awareness
- Engage an independent cyber security expert to assess and implement actions that would reduce the consequence and likelihood of attacks on the Departments
- Prepare a response plan in the case of a cyber-attack
- Update the design of existing controls to ensure they are still relevant to the current operating environment

## 6 Monitoring and Reporting

### 6.1 Risk Registers

The Chief Risk Officer must establish and maintain the Enterprise Risk Register for the Departments.

The Enterprise-wide Risk Register must document the key strategic risk events that would likely impact the Departments as a whole.

The following must also establish local risk registers:

- the head of a Group, in relation to that Group
- the head of a Branch, in relation to that Branch
- the executive sponsor, in relation to a project.

Local risk registers must document key risk events that would impact the group, branch or project. The Departments Risk Register template is available on the Hub.



## 6.1.1 Monitoring and Review of Risk Registers

Monitoring and review is an essential and integral part of managing risk. It is necessary to monitor risks and the effectiveness and appropriateness of the controls and treatment plans (i.e. management actions) to ensure these continue to be effective.

Tracking progress made against management actions provides an important accountability measure. Risk reporting should incorporate the tracking of items that are above the Departments acceptable level of risk to ensure they are addressed and actioned within the agreed target date.

## 6.1.2 Reporting Frequency

Frequency	Report	Content of report	Committee
<b>Every two years</b>	Review of Risk Management Policy	<ul style="list-style-type: none"> <li>Revise and update Risk Appetite Statement and Risk Management Policy</li> </ul>	Audit & Risk Committee PD and TCO Executive Risk & Governance Committee
<b>Annual</b>	Risk Management performance	<ul style="list-style-type: none"> <li>Review of the enterprise risk management activities, how they support the Departments priorities and plan for the year ahead</li> </ul>	Audit & Risk Committee Risk & Governance Committee
<b>Quarterly</b>	Enterprise Risk Register (ERR) Review	<ul style="list-style-type: none"> <li>Revised and updated ERR with commentary on the mitigation activities to date, planned and emerging risks</li> </ul>	Audit & Risk Committee PD and TCO Executive Risk & Governance Committee
<b>Quarterly</b>	Risk Management update	<ul style="list-style-type: none"> <li>Report on the status of ERR, including trend, mitigation actions implementation status, and any other key updates</li> <li>Report on any new or emerging risks / issues, including systemic and interdependent risks</li> </ul>	Audit & Risk Committee PD and TCO Executive Risk & Governance Committee
<b>Ad hoc</b>	Risk Deep Dive	<ul style="list-style-type: none"> <li>Individual risk report on a specific risk, presented by risk owners</li> </ul>	Audit & Risk Committee Risk & Governance Committee

### 6.1.3 Risk Escalation and Responsibilities

The table below provides high level guidance on how risks should be reported on, treated, escalated and monitored based on the residual risk rating.

#### Risk Actions and Escalation Points

Residual Risk Rating	Risk Delegations	Action required for risk	Risk Escalation
<b>High</b>	Management strategies must be approved by the Secretary	Action required: Immediate attention required by direct Management to reduce residual risk or cease activity if risk cannot be appropriately controlled.	Inform the Minister about the risk. Escalate to the Secretary and ARC.  Control strategy monitored by the PD and TCO Executive
<b>Significant</b>	Management strategies must be approved by relevant Deputy Secretary / Chief Digital and Information Officer / Chief Financial and Operations Officer	Action required: Outside of appetite without appropriate risk management in place. Tolerated if there is appropriate risk management in place.	Escalate to the Secretary and ARC.  Control strategy developed and monitored by the PD and TCO Executive
<b>Moderate</b>	Management strategies must be approved by the relevant Senior Executive reporting directly to Deputy Secretary/Secretary for approval	Potential action: Risks will be treated as long as the costs do not outweigh the benefits.	Manage at functional or branch level Escalate to the relevant Deputy Secretary/Secretary for information
<b>Low</b>	Management strategies must be approved by the relevant Executive reporting directly to Executive Director for approval	No action: Acceptable risks requiring no further treatment. Should be monitored for significant changes in risk rating.	Executive Director to be kept informed on management of risk

## 6.2 Key Risk Indicators

Key Risk Indicators (KRIs) are measures and metrics that relate to a specific risk and demonstrate a change in the likelihood of a consequence of the risk occurring.

KRIs do not measure how well something is being done, they measure and trend the possibility of a future adverse impact. KRIs provide an early warning to identify potential events.

In addition to risk registers the Departments sets and reports on KRI's quarterly to the Risk and Governance Committee, PD and TCO Executive and Audit and Risk Committee via the Enterprise Risk Register reporting. The KRI's are set by the PD and TCO Executive and are informed by the Departments Risk Appetite Statement and emerging risks in the Enterprise Risk Register.

---

## 7 Contacts

---

Governance Team

[governance@tco.nsw.gov.au](mailto:governance@tco.nsw.gov.au)

## 8 Appendices

### Appendix One – Risk Matrix

#### Consequence

The consequence(s) of a risk event must be assessed and given a rating using the consequence descriptors below. A risk event may have more than one consequence where the overall consequence rating for the risk event will be the highest. For example, if a risk event could have a “moderate” impact in terms of excellence but a “major” impact in terms of our reputation, the overall rating will be “major”. This matrix is not exhaustive, please consult with the Governance Team for further assistance.

Rating	Management Effort	Financial	Safety & Wellbeing	Reputation	Compliance
<b>Severe</b>	Premier and Secretary involved in efforts to rectify or reduce the event, engaging external assistance is likely to ensure the Departments are able to continue operating	Loss or variation in the Departments or project by more than \$20 M or 10% of Divisional Budget; requiring additional financial assistance	Significant fatality(ies) or injury (mental or physical) requiring priority medical treatment resulting in medium to long term incapacitation of person(s)	Irreparable reputational damage causing long-term, sustained loss of public and Government confidence in the Departments. Premier is included in coverage.	Illegal activity or significant negligent or intentional acts of non-compliance with regulatory, contractual or internal governance obligations.
<b>Major</b>	Impact on core business significantly disrupting normal routines requiring Secretary intervention – may need to engage external assistance to continue core functions	Loss or variation in the Departments or project by more than \$10 M but less than \$20 M; or More than 5% but less than 10% of Divisional Budget	Significant injury (mental or physical) requiring priority medical treatment resulting in short to medium term incapacitation of person(s)	Significant negative media attention that impacts our reputation causing sustained loss of public and Government confidence. Premier is included in coverage.	Major fines or penalties imposed for non-compliance. Serious one-off breach of regulatory, contractual or internal governance obligations.
<b>Moderate</b>	Functions of the Departments could be subject to significant review or changes to operations, resulting in additional effort from Deputy Secretaries and their teams	Loss or variation in the Departments or project by more than \$5 M but less than \$10 M; or More than 2% but less than 5% of Divisional Budget	Injury (mental or physical) requiring medical treatment resulting in days off work	Negative media attention that impacts our reputation with stakeholders and other Government agencies but does not cause long term damage. Premier is aware of the issue.	Breaches rectifiable with management effort, fines or penalties imposed for non-compliance that do not significantly impact business operations, reputation or future funding opportunities.
<b>Minor</b>	A threat to the efficiency or effectiveness of some aspects of the Departments operations, but at a level that can be dealt with internally with minimal additional resources	Loss or variation in the Departments or project by more than \$1 M but less than \$5 M; or More than 1% but less than 2% of Divisional Budget	Minor injury (mental or physical), may require first aid	Isolated and minor impact on our reputation with customers and other stakeholders, Premier may not be aware.	Minor breaches or governance issues rectifiable with minimal effort.

<b>Insignificant</b>	The consequences can be dealt with by routine operations	Loss or variation in the Departments or project less than \$0.5 M; or Less than 1% of Divisional Budget	<i>Intentionally Blank</i>	Negligible impact, no external coverage	Negligible impact, minor internal policy breaches
----------------------	--	---	----------------------------	---	---

**Likelihood**

Analysing risks requires an assessment of their frequency of occurrence. The following table provides descriptions relevant to the Departments used to support risk likelihood ratings.

<b>Rating</b>	<b>Definition</b>	<b>Frequency</b>
<b>Almost Certain</b>	The future event is expected to occur within the year	Likely to occur frequently, and probably more than once per year. Greater than 90% chance of occurring in any year.
<b>Likely</b>	The future event is highly likely to occur	Likely to occur at least once per year. 51% to 90% chance of occurring in any year.
<b>Possible</b>	The future event could occur at some time	Likely to occur once in 2-5 years. 21% to 50% chance of occurring in any year.
<b>Unlikely</b>	The chance of the future event occurring is slight or remote	Likely to occur once in 5-10 years. 10% to 20% chance of occurring in any year.
<b>Rare</b>	Risk will only occur in exceptional circumstances	Greater than 10 year event. Less than 10% chance of occurring in any year.

## Assessment Matrix

The likelihood and consequence ratings for a risk event will be used to assess the overall impact of the risk using the risk evaluation matrix:

<b>Consequence</b>	Severe	Yellow	Orange	Orange	Red	Red
	Major	Green	Yellow	Orange	Orange	Red
	Moderate	Green	Yellow	Yellow	Orange	Orange
	Minor	Green	Green	Yellow	Yellow	Orange
	Insignificant	Green	Green	Green	Yellow	Yellow
		Rare	Unlikely	Possible	Likely	Almost Certain
		<b>Likelihood</b>				

Red	<b>High</b>
Orange	<b>Significant</b>
Yellow	<b>Moderate</b>
Green	<b>Low</b>

## Appendix Two – Glossary of Terms

The following terms and definitions used in the Policy are included below.

Term	Description
<b>Corrective (mitigating) Control</b>	Controls are designed to correct errors or issues that have already occurred, and prevent future occurrences of the error or issue.
<b>Detective Control</b>	Controls that are designed to find errors or issues and highlight these within the specific process or activity.
<b>Frequency</b>	A measure of likelihood expressed as the number of occurrences of an event in a given time.
<b>Hazard (Cause)</b>	A source of potential harm, or a situation with potential to give rise to negative consequences.
<b>Preventative Control</b>	Controls that are designed to keep an error or issue from occurring.
<b>1<sup>st</sup> Line of Defence</b>	The 1st Line of Defence is concerned with owning and managing the risks. It is provided by operational managers and frontline staff. Operational management is responsible for maintaining effective internal controls and for executing risk and control procedures on a day-to-day basis.
<b>2<sup>nd</sup> Line of Defence</b>	The 2nd Line of Defence centres on risk oversight and involves some level of real-time activity and is mandated to review 1st Line of Defence activities. This encompasses the work of specialists like risk management, technical and regulatory compliance, and safety. The aim is to confirm the effectiveness of governance and compliance arrangements, and to identify and action improvements.
<b>3<sup>rd</sup> Line of Defence</b>	The 3rd Line of Defence involves independent assurance that evaluates the adequacy and effectiveness of both 1st Line and 2nd Line risk management. This is traditionally performed by Internal Auditors, to independently verify governance and compliance effectiveness, and to recommend improvements and enhancements.



## Appendix Three – Risk Assessment Template

The following assessment template provides a working document that follows the risk management process, for recording of identified risks, analysis, evaluation and treatment within the applicable risk register.

In practice:

Copy this template out of the Departments Risk Management Framework and complete either in an excel document or word document. The information you populate in here will translate directly into the Departments, Branch or Project risk register. .

1. Planning & Consultation		
Risk Assessment Context		<i>Document within Step 1 the individuals, groups and or organisations involved in the risk assessment. As well as the context of the risk assessment. Refer to Section 5.1 of the Policy for detailed guidance.</i>
Identified Stakeholders		<i>Document within Step 1 the individuals, groups and or organisations involved in the risk assessment. As well as the context of the risk assessment. Refer to Section 5.1 of the Policy for detailed guidance.</i>

2. Identify				
Define and describe the risk(s) identified:	Risk One	Risk Two	Risk Three	<i>The template includes columns for identifying more than one risk, add/ remove columns based on the specific scenario.</i>
What are the key potential causes of the risk?				<i>Identify and describe the factors that may be causing the risk.</i>

<b>2. Identify</b>				
What are the key potential consequences of the risk?				<i>Identify and describe each of the potential impacts on the Departments if the risk event were to occur.</i>

<b>3. Analyse &amp; Evaluate</b>				
How likely is the risk to occur?	5 - Almost Certain 4 - Likely 3 - Possible 2 - Unlikely 1 - Rare	5 - Almost Certain 4 - Likely 3 - Possible 2 - Unlikely 1 - Rare	5 - Almost Certain 4 - Likely 3 - Possible 2 - Unlikely 1 - Rare	<i>Make reference to the detailed risk assessment criteria contained within Appendix One of the Policy for guidance on selecting the appropriate likelihood and consequence rating.</i>
What is the greatest potential consequence of the risk?	5 - Almost Certain 4 - Likely 3 - Possible 2 - Unlikely 1 - Rare	5 - Almost Certain 4 - Likely 3 - Possible 2 - Unlikely 1 - Rare	5 - Almost Certain 4 - Likely 3 - Possible 2 - Unlikely 1 - Rare	<i>Your analysis and evaluation is performed at the residual risk level. Refer to section 5.4 Evaluate for more information.</i>
What is the overall risk rating?	5 - Almost Certain 4 - Likely 3 - Possible 2 - Unlikely 1 - Rare	5 - Almost Certain 4 - Likely 3 - Possible 2 - Unlikely 1 - Rare	5 - Almost Certain 4 - Likely 3 - Possible 2 - Unlikely 1 - Rare	<i>The overall rating will be defined by the likelihood and consequence rating – refer to the assessment matrix within Appendix One.</i>
What controls exist? And; What is their current effectiveness?	Control: Effectiveness:	Control: Effectiveness:	Control: Effectiveness:	<i>Control effectiveness and assessment is performed in line with the guidance in section 5.3 Analyse of the Policy.</i>
Who is the risk owner?				<i>Your analysis and evaluation is performed at the residual risk level. Refer to section 5.4 Evaluate for more information.</i>

4. Treatment				
Summary of Steps 1 – 3	Risk:  Overall Rating:	Risk:  Overall Rating:	Risk:  Overall Rating:	<i>Define a treatment plan for the identified risk that is directed at reducing the likelihood and/ or consequence. Refer to section 5.5 Treat of the Policy for detailed guidance.</i>
What are the management actions to treat the risk?				<i>Define a treatment plan for the identified risk that is directed at reducing the likelihood and/ or consequence. Refer to section 5.5 Treat of the Policy for detailed guidance.</i>
Who will be responsible for management actions?				
What is the timeline for the management actions?				

Summary	
Risk assessment undertaken by:	
Date of review:	
Date communicated/ actioned to the relevant risk register:	

## Appendix Four - Risk Appetite Statement 2023

The Department's Risk Appetite Statement defines the risks the Department is willing to accept (its risk appetite), and the boundaries of events and/or actions that are considered acceptable in the pursuit of its objectives (its risk tolerance).

### Governance and compliance



**Governance structure:** we have no appetite for project or service delivery that is not supported by a governance structure that defines accountability and is underpinned by formal risk management.



**Compliance:** we have no appetite for actions, projects or activities that would lead to a breach of legislation, regulation, probity or internal compliance requirement.

### Service delivery



**Innovative delivery:** we have a high appetite to accept 'big ideas' and 'quick to fail' projects and initiatives to enhance the lives of, and secure the best outcomes for, the people of NSW.



**Partnerships and integration:** we have a high appetite to invest in partnerships with others and harmonise our culture by respecting the difference in values of incoming agencies as a result of Machinery of Government changes.



**Reputation:** we have a moderate appetite for short-term (up to 3 months) negative impact on the department's reputation related to new policy or project delivery in untested areas, provided the activities are within the Department's authority.



**Challenge:** we have a high appetite to provide full and frank advice that challenges conventional wisdom and ways of working for better outcomes.



**Cyber security:** we have no appetite for data loss or a breach of sensitive information.



We have a low appetite for impacts to the availability of information and systems due to cyber attacks

### People and culture



**Staff wellbeing:**

We have no appetite for activities that may cause serious physical or psychosocial harm to our staff



We have a high appetite for activities that positively impact staff wellbeing and safety







**Workplace behaviour:**

We have no appetite for bullying or harassment within the Department

## Risk Appetite Criteria

The following criteria sets out the definition of the 4 levels of the Department's risk appetite and the action to be taken.

	Appetite Action		Definition
	No	Don't do/ Stop	<p>Unacceptable conduct that conflicts with the Department's principles and would lead to harm to the Department or stakeholders and result in breaches or disciplinary action. Activity must not commence.</p> <p>If the Department inadvertently breaches a no appetite measure, immediate action must be undertaken to cease activity as soon as practically and safely possible. In addition, mitigating controls should be considered to prevent the incident being repeated. The Department should seek to return to its target level as soon as possible.</p>
	Low	Fix	<p>Activity with the potential to harm the Department. Management must take action in the short-term to return the activities to within target. The Department would not deliberately make a decision or enter into a commitment knowing that it would lead to such a breach.</p>
	Moderate	Enhance	<p>The Department can take action to take measured risks to operate and enhance the operations to within appetite providing adequate controls and contingency plans have been established.</p>
	High	Pursue	<p>Management must explore opportunities that improve the Department's ability to deliver outcomes in programs and services within appetite.</p>

# The Cabinet Office and Premier's Department

52 Martin Place  
Sydney NSW 2000

GPO Box 5341  
Sydney NSW 2001

T: 02 9228 5555

W.[nsw.gov.au/the-cabinet-office](http://nsw.gov.au/the-cabinet-office)  
[nsw.gov.au/premiers-department](http://nsw.gov.au/premiers-department)



OFFICIAL