Parliamentary Counsel's Office

Risk Management Policy

May 2023

Approved by Parliamentary Counsel, Annette O'Callaghan

Contents

Policy Owner / Contact

Corporate Services

Review Record

Date	Action	Version
April 2022	Published	1.0
May 2023	Review	1.1

1. Introduction

Risk is the effect of uncertainty on our objectives. Risk management refers to coordinated activities that direct and control an organisation in relation to risk. Effective risk management across the NSW Parliamentary Counsel's Office (PCO) helps us to achieve our objectives through risk-based decision-making.

In 2020, NSW Treasury released *TPP 20-08 Internal Audit and Risk Management Policy for the General Government Sector*, which provides for the effective implementation of risk management practices across NSW Government agencies. Its component requirements align with the Australian/New Zealand Standard (AS/NZS) *ISO 31000: 2018 Risk management – Principles and guidelines*.

This document sets out PCO's Risk Management Policy, and details the key principles, policies and processes that underpin effective risk management across the agency.

2. Roles and responsibilities

Role	Key responsibility
Parliamentary Counsel	Ultimately responsible and accountable for risk management in PCO. Articulates the level of risk PCO is willing to accept. Promotes a positive risk culture.
Other members of the PCO Leadership Team	Identify, assess and manage risks relating to the operations of their teams. Ensure staff are aware of relevant policies and approaches to risk management. Promote a positive risk culture. If applicable, inform updates to the strategic risks on the Enterprise Risk Register and implement any delegated management actions from the Parliamentary Counsel.
Chief Audit Executive (Director, Corporate Services)	Designs, implements and responsible for the continuous improvement of the Risk Management Policy so it is appropriate for PCO's operating environment. Manages and coordinates PCO's risk management reporting process, including regular reporting to the Audit and Risk Committee. Administer and establish the Risk Management Policy.
Audit and Risk Committee	Provides independent advice to the Parliamentary Counsel and Chief Audit Executive on PCO's governance and risk management processes. Reviews the Enterprise Risk Register and provides advice to the Parliamentary Counsel and Chief Audit Executive. Oversees the application of the Risk Management Policy within PCO and challenges the adequacy of PCO's processes for managing risk.
All Employees	Ensure familiarity with the Risk Management Policy. Ensure day to day identification and management of risk within PCO and report and escalate risks and concerns to the PCO leadership team.

3. Risk Management Framework

PCO recognises that effective management of risk is integral to good management and business practice. It is important to consider risk, not only as adverse consequences but as providing potential opportunities that can be achieved through proactive management. Risk management is integrated into PCO's operations and governance, including business planning, business continuity and business performance reporting.

2.1 Principles of risk management

Risk management at PCO is guided by the following principles:

- **Comprehensive**: risk management applies to all PCO activities and staff.
- **Proportionate**: the level of response to a risk needs to be proportionate to the level of risk and PCO's risk appetite.
- **Proactive**: risk management is used proactively to make informed decisions.
- The Parliamentary Counsel is responsible for ensuring the implementation of an appropriate risk management policy within PCO. However, all PCO employees have a responsibility to identify and manage risks in line with this Policy.

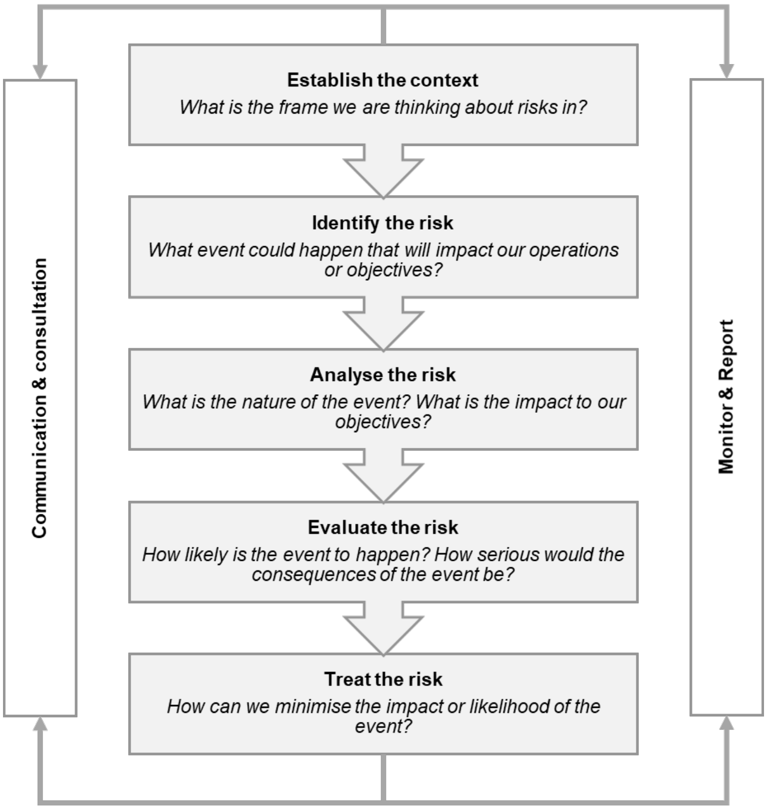
2.2 Risk appetite

Risk appetite defines the areas of risk PCO will and will not accept as part of achieving its objectives. In the context of risk appetite, PCO will prioritise:

- 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 by a natural disaster, infrastructure failure, a pandemic or another incident.

4. Risk management approach

This section provides a general overview of the methodology to be applied across PCO in its management of risks. This methodology is based on the ISO:31000 Risk Management Standards and requirements under TPP20-08 and is illustrated below. Further detail on each step is provided in the following sections.


Establish the context
What is the frame we are thinking about risks in?
Identify the risk
What event could happen that will impact our operations or objectives?
Analyse the risk
What is the nature of the event? What is the impact to our objectives?
Evaluate the risk
How likely is the event to happen? How serious would the consequences of the event be?
Treat the risk
How can we minimise the impact or likelihood of the event?
Communication & consultation
Monitor & Report

4.1 Establish context

Context is important in the risk assessment process as it establishes the environment in which PCO operates and aids in identifying events that could become risks for PCO.

Both internal and external factors must be considered, incorporating the objectives, priorities, and operating environment of, and emerging threats to, PCO. Analytical approaches such as SWOT (strength, weakness, opportunities and threats) can be used to help establish the context in which risks and opportunities are considered.

4.2 Identify risks

Risk identification is performed to define potential threats to PCO's strategic objectives. Factors to consider in performing the risk identification process include changes in both the internal and external environment, assumptions of stakeholders and the vulnerabilities and capabilities of PCO.

Defining risks vs issues: Risk management is focused on prevention and mitigation rather than remediation.

- ✓ A RISK describes an event of uncertainty; an event that could happen
- ✓ An ISSUE describes an event that has happened

4.3 Risk analysis

Risk analysis aims to qualitatively identify root cause and define the nature of the risk to inform impacts, both short and long-term. Robust risk analysis enables better targeted controls and allocation of resources into further mitigations that address the primary causes of the risk. Some common tools and techniques that can be used to help risk analysis include bow tie analysis, root cause analysis and strengths, weakness, opportunities and threats ("SWOT") analysis.

4.4 Risk evaluation

The risk evaluation process quantifies the scale of possible impacts against a likelihood of the impacts eventuating and assigns a rating that helps to prioritise the risks and their management. It assists to understand how controls and further mitigating actions act to address either the risk impact or likelihood. A Risk Assessment Tool is available in Appendix 2 to support this.

A. Determining the risk rating

PCO's risk evaluation criteria considers:

- **Consequence**: the level or outcome or impact of the identified risk event, including the magnitude of the impact of the event occurring.
- **Likelihood**: the probability of a risk event and assessed level of impact occurring.

The resultant rating is mapped against PCO's risk matrix (refer to Appendix 1) and the risk recorded on the Enterprise Risk Register.

Risk ratings can be evaluated with or without reference to the controls currently in place as follows:

- **Inherent** risk evaluation: the assessed level of risk before applying controls
- **Residual** risk evaluation: the assessed level of risk after taking into consideration controls. Residual risk ratings provide a more practical assessment of the risk exposure and can be applied against the risk appetite to determine if the risk exposure is acceptable or otherwise.

B. Assessing the design and operating effectiveness of the controls

Controls (see section 5) are the existing policies, processes or systems that minimise risk impact or likelihood. Controls can be predictive, detective, automated, manual, hard (documented) or soft (behavioural).

The table below defines how controls are evaluated for effectiveness in mitigating identified risks:

Effectiveness	Description
Ineffective	• The control design does not meet the control objective • The control is not being applied or is applied incorrectly
Partially effective	• The control design mostly meets the control objective. • Control is normally operational. However, is occasionally not being applied or is occasionally applied incorrectly.
Effective	• The control design meets the control objective. • The control is operational a majority of the time and is being correctly applied (test evidence).

4.5 Risk treatment

Once a risk has been assessed subject to the effectiveness of controls in place, a decision needs to be made as to whether additional action is required to further mitigate to acceptable levels. This decision needs to be considered considering PCO's risk appetite.

Risk treatment options include:

- **Accept the risk**: the residual risk is within appetite and PCO is comfortable. Investment in additional mitigations is not required.
- **Mitigate the risk**: the residual risk is outside of appetite and investment in additional mitigations is required to bring the risk to within appetite.
- **Transfer the risk**: the residual risk may be within or outside of appetite. However, due to limited controllability, the risk is better managed by a different owner.

Should risk treatment plans be required, the plans should capture as a minimum, the following information:

- **Treatment description**: what are the key activities or phases of work that will be performed and how will it target the risk exposure?
- **Treatment owner**: allocation of an accountable person to own the progress of the treatment actions.
- **Treatment due date**: nomination of a realistic timeframe to completion will assist in ensuring good governance and accountability.

4.6 Monitoring and reporting

It is necessary to monitor risks and the effectiveness and appropriateness of the strategies and management systems in place to ensure the strategies and systems continue to be effective. This means reviewing the performance of the business process and changes to business initiatives and other internal processes which may affect the performance of the business process. The table below summarises the risk monitoring and reporting processes:

Recipient	Frequency	Item	Purpose
PCO Audit and Risk Committee	Quarterly	Enterprise risk update	To review and endorse periodic updates for PCO on: • Significant movements in strategic risks • Key potential operational or project level risks • Progress update on risk treatment plans • Emerging risks and issues
	Annually	Enterprise Risk Management Performance Report	To review and endorse the annual risk management performance activities: • Review of and updates to the Enterprise Risk Management Framework • Key risk management achievements and progress on risk maturity initiatives
	Annually	Strategic Risk Profile Review	To review and endorse PCO's strategic risk profile
Parliamentary Counsel	Quarterly	Quarterly Enterprise Risk Report	To review, discuss and approve: • Significant movements in strategic risks • Key risks with potential impacts on PCO • Progress update on risk treatment plans • Emerging risks and issues

5. Internal controls

Implementation and maintenance of internal controls are a key element of robust risk management. There are several factors to consider in determining the effectiveness of a control, which must be routinely considered to ensure the controls in place remain effective:

- Does the control address the risk it is intended to address?
- Does the control address the entire risk or only a part of the risk?
- Will the control reliably address the risk every time with the same level of impact?
- How quickly will the control impact the consequence or likelihood of a risk? Is it fast enough?
- Are there enough people with the right skills to effectively operate the control?
- Is the performance of the control able to be effectively analysed?

PCO's approach to internal control leverages the benefits of a small agency with centralised processes and deploys the following principles to control design and operation:

- **Consistency**: if possible, extend application of internal controls to external parties, such as contractors, to enhance consistency in process and assurance.
- **Currency & relevance**: develop principles-based policies and frameworks, supported by processes that are periodically reviewed and updated.
- **Proportionate**: design processes and controls to manage the level of risk exposure.
- **Quality assured**: regularly 'check' controls to ensure the controls are still working as intended. This should act as a pre-cursor to independent assurance activities.

Appendix 3 provides examples of key internal controls in place. Details of controls as related to specific risks are detailed in PCO's risk register.

6. Further information

References:

TPP 20-08 Internal Audit and Risk Management Policy for the General Government Sector.

NSW Audit Office Risk Management Framework

Appendix 1: Risk evaluation criteria

Risk Likelihood Table

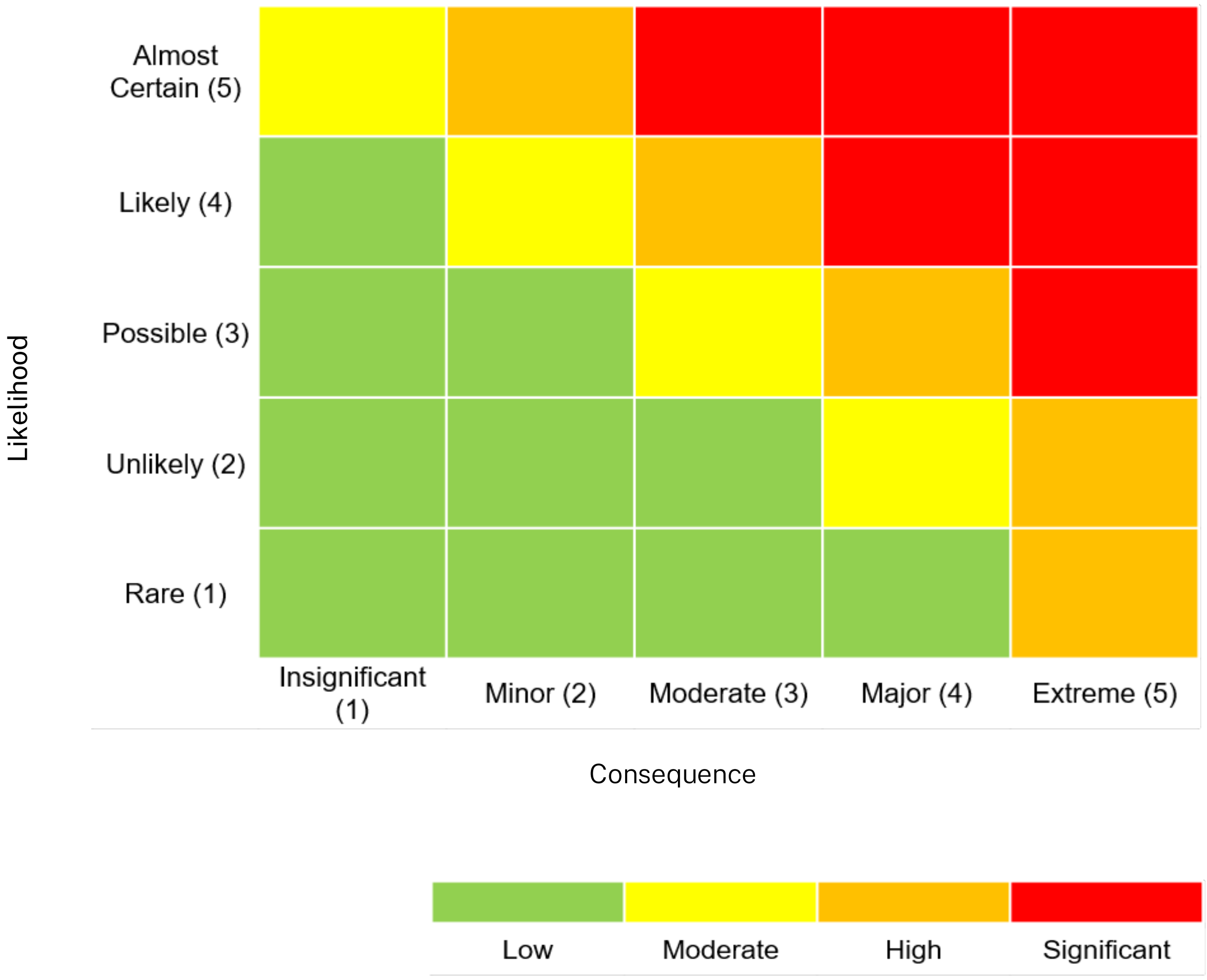
Rating	Description	Definition	Probability
1	Rare	• The event may occur only in exceptional circumstances (5-10 years). • Almost no opportunity to occur.	<10%
2	Unlikely	• The event could occur at some time (2 to 5 years). • No known incidents recorded or experienced. • Little opportunity or means to occur.	>10% to 50%
3	Possible	• The event could occur at some time over 12 months. • Few infrequent, random occurrences recorded/experienced. • Some opportunity and means to occur.	>50% to 75%
4	Likely	• The event will probably occur during the year. • Regular incidents known (records/experience). • Considerable opportunity and means to occur.	>75% to 95%
5	Almost Certain	• The event is expected to occur in most circumstances (multiple times a year). • High level of known incidents (records/experience). • Strong likelihood of re-occurring, with high opportunities/means to occur.	>95% to 100%

Risk Consequence Table:

Consequences Category	Insignificant	Minor	Moderate	Major	Extreme
Overall description	An occurrence, the impact of which can be absorbed through business-as-usual activity	An occurrence, the impact of which can be absorbed but potential reallocation of resources is required	An occurrence that requires additional management effort or resources to minimise the impact	An occurrence that requires changes in management, or significant management effort or additional resources	An occurrence so severe in nature it could lead to a significant restructure of the organisation or collapse of the organisation
Reputation			Internal staff lose confidence in PCO	Credibility of PCO among agencies is compromised	Sector-wide loss of confidence in PCO Premier expresses dissatisfaction with PCO
Legal / Compliance			Compliance issues that can be managed internally	Breach of legislation or other regulation impacting PCO's operations	Ministerial inquiry or Parliamentary scrutiny
Service Delivery		Service delivery affected but resolved by routine operations	Some impact on efficiency or effectiveness in service delivery that can be managed internally	Significant review / changes to operations required to enable service delivery	Critical services are not delivered
Financial	Negative impact on budget of 1-2%	Negative impact on budget of 2-5%	Negative impact on budget of 5-9%	Negative impact on budget of 10-15%	Negative impact on budget of over 15%
People		Staff working above capacity temporarily An injury not requiring hospitalisation Low level of complaints from staff	Staff are regularly working at full capacity / working additional hours Increasing staff turnover Temporary and reversible disabling illness to one or more persons Increase in request for sick leave / increasing complaints about workload	Staff exhibiting symptoms of burnout Significantly increased turnover Serious injury or irreversible disability to one or more persons	Substantial loss of staff across PCO One or more fatalities Staff requiring psychological assistance

Risk Matrix

The following risk matrix should be used to determine the risk rating for each risk.



Likelihood

	Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Extreme (5)
Almost Certain (5)	🟨	🟧	🟥	🟥	🟥
Likely (4)	🟩	🟨	🟧	🟥	🟥
Possible (3)	🟩	🟩	🟨	🟧	🟥
Unlikely (2)	🟩	🟩	🟩	🟨	🟧
Rare (1)	🟩	🟩	🟩	🟩	🟧

Consequence

🟩	🟨	🟧	🟥
Low	Moderate	High	Significant

Appendix 2: Risk assessment template

The below template may be used to assess identified risks.

RISK		
Date of risk assessment	Original assessment: Last review and assessment:	
Responsibility		
1. OPERATING ENVIRONMENT AND CONTEXT		
2. RISK IDENTIFICATION		
Risk description		
3. RISK ASSESSMENT		
Likelihood factors		
Consequences		
Inherent likelihood rating	Inherent consequence rating	Inherent risk rating
Existing controls		
Control rating		
Residual likelihood rating	Residual consequence rating	Residual risk rating
4. RISK TREATMENT		
Management action		
Additional risk management strategies/controls		
Responsibility		
Timetable		

Appendix 3: Key internal controls

The table below outlines key internal controls in place at PCO. Details of controls related to specific risks are detailed in PCO's risk register.

AREA	CONTROL EXAMPLES
Accounting	Monthly operating statements are prepared showing actual and budgeted revenue and expenditure for the month and year to date, and variances and unusual movements are investigated and explained.
Confidentiality	LEGIS access is only provided to those staff who need it (predominantly Drafting and Legislation, Editing and Access staff) and access to sensitive projects within LEGIS is further restricted to staff working on the project.
Fraud and corruption	All staff complete annual training on fraud and corruption, with additional specific training for finance staff provided as necessary.
Legislative drafting	All legislation is reviewed by at least several people, other than the drafter, before being finalised, with the review process recorded on LEGIS.
Payments	All payments from PCO are authorised in the bank portal by two finance staff.
Procurement	All procurement of goods and services are processed through the SAP finance system or purchasing card system (Expense8).
Purchasing cards	Purchasing card expenses are approved in Expense8 by officers with appropriate financial delegation.
Records management	Hard copies of records are only disposed of with the approval of the Director, Corporate Services (corporate documents) or Director, Legislation, Editing and Access (legislative documents), using shredders or secure destruction bins if the contents are confidential.
System access	SAP access listings are reviewed regularly by the Director, Corporate Services and necessary changes made.