NSW GOVERNMENT Parliamentary Counsel's Office

Policy

Risk Management

Policy Reference: 12/22

Approved by Parliamentary Counsel: Annette O'Callaghan, 3 March 2022

Introduction

The Parliamentary Counsel's Office (PCO) is a Public Service executive agency that provides a comprehensive and integrated range of services for the drafting, development, and publishing of legislation to Government and non-government Members of Parliament. PCO also provides public access to legislation through the authorised NSW legislation website and provides advice and information about legislation. PCO provides the secretariat for the Australasian Parliamentary Counsel's Committee (PCC). PCO is a small agency consisting of a staff of approximately 55 people. The Parliamentary Counsel is responsible for the management of risk at PCO.

It is recognised that effective corporate governance arrangements are essential to the performance, integrity and transparency of public sector organisations. In 2015, NSW Treasury released *TPP 15-03 Internal Audit and Risk Management Policy for the NSW Public*. The aim of the policy is to support effective and efficient management by promoting the use of best practice standards and frameworks and tailoring those frameworks for agencies to implement, further develop and manage. In this regard, the core requirements concerning risk management have been largely modelled on Australian/New Zealand Standard (AS/NZS) *ISO 31000: 2009 Risk management – Principles and guidelines*. Risk management is a critical component of governance arrangements at PCO and is integrated into PCO's governance, planning (including business planning, business continuity and project planning) and reporting framework.

PCO's risk management system comprises a policy and framework, as detailed in this document. PCO also maintains a Risk Register that identifies risks across PCO. The Risk Register also records the key risks that have been identified for PCO.

A. RISK MANAGEMENT POLICY

This Policy aims to:

- Support the embedding of risk management into PCO's management practices to optimise the achievement of goals and objectives
- Provide a framework for the identification, mitigation and control of risk at PCO
- Establish protocols for how risk should be managed within PCO
- Inform PCO employees about:
    - their roles, responsibilities and accountabilities for managing risk in their work area,
    - the approach to be followed in managing risks at PCO,
    - obtaining guidance and assistance with the management of risk, and
    - the context for the management of risk in PCO's business processes.

The Risk Management Policy outlines:

- PCO's approach to risk management – how risks are to be identified, assessed and managed at PCO,
- Responsibilities of all levels of staff in identifying, assessing and managing risks that relate to their particular area of work,
- PCO's appetite for risk,

- Delegations for approval of risk assessments and risk management strategies,
- When risk management is to be used on a formal basis within PCO,
- Requirements for the documentation of risk assessments and risk management plans,
- Requirements for reporting on risks and risk management strategies.

This policy applies to all employees at PCO.

1. Key responsibilities

Parliamentary Counsel	• The Parliamentary Counsel is responsible for the management of risk at PCO through the implementation and maintenance of sound risk management practices at PCO. • Managing PCO's strategic risks (ie those risks that affect PCO as a whole or the achievement of PCO's strategic objectives). • Monitoring and reviewing progress of identified High and Significant risks and emerging risks on a regular basis.
PCO's Leadership Team	• Assisting the Parliamentary Counsel with the management and oversight of strategic risks. • Reviewing and endorsing the formal assessment of identified risks and monitoring the implementation of actions to treat or mitigate those risks. • As leaders, ensuring PCO staff are aware of the relevant PCO policies and approaches to risk management and understand their responsibility to identification and manage risk.
Executive Director	• Establishing, reviewing and maintaining PCO's risk management framework by developing sufficient infrastructure to identify, measure, manage and report risks. • Monitoring and reviewing progress with the management of risks and considering new and emerging risks on a regular basis and drawing them the attention of PCO's leadership. • Updating, reviewing, and reporting about risks on the Risk Register. • Is the designated "Risk Officer" for PCO under TPP 15-03.
Manager, ICT	• The identification, assessment and management of risks relating to PCO's information systems and communicating these to the Executive Director. • The identification, assessment and management of risks relating to any information systems projects including listing risks in project business cases and monitoring them. • Providing information to the Executive Director for updating the Risk Register on risks relating to information systems or ICT project risks, where applicable.
Supervisors	• Identifying, assessing, and managing risks relating to their work area and for communicating identified risks to the Executive Director. • Ensuring that their staff are aware of the relevant PCO policies and approaches to risk management and have the

	necessary skills to manage risks related to their particular area of work. • Providing information to the Executive Director for updating the Risk Register.
Project leaders	• Identifying, assessing and managing risks relating to a project and communicating these to the Executive Director. • Listing risks in project business cases. • Providing information to the Executive Director for updating the Risk Register about any identified risks with a project.
All PCO Staff	• Identifying and managing risks that relate to their particular area of work in a manner consistent with PCO's policy and framework on risk management.
Audit and Risk Committee (ARC)	• Providing advice to PCO on the adequacy of the Risk Management Framework, including policies and processes at PCO.

2. Policy statement

PCO recognises that effective management of risk is integral to good management and business practice. It is important to consider not only adverse consequences but also consider the potential opportunities or benefits that can be achieved by risk management.

Risk management is a critical component of governance arrangements at PCO and is integrated into PCO's governance, planning (including business planning, business continuity and project planning) and reporting framework.

3. Policy and procedure details

3.1 Principles

Risk management at PCO is guided by the following principles:

- The policy applies to all areas of work including all major programs and business processes, with risks rated in accordance with the methodology outlined in PCO's Risk Management Framework.
- The level of response to a risk needs to be proportionate to the level of risk.
- All PCO employees have a responsibility to proactively identify and manage the risks that relate to their particular area of work in a manner consistent with PCO's policy and framework.
- PCO is responsible for ensuring that staff and supervisors have the necessary skills and risk management tools to undertake effective risk management.
- Risk management is used proactively by PCO to identify and be conscious of the risks it faces, make informed decisions about managing those risks and to identify and harness potential opportunities.

3.2 Appetite for risk

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

- 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, pandemic or other incident.

There are no absolute tolerance limits available to assist in making decisions about risk. Identifying, assessing and managing risks requires the exercise of informed, careful and prudent judgement, taking account of the controls that are in place to prevent risks from occurring or preventing or mitigating the consequences if the risk event did occur.

3.3 Risk delegations

Risks rated as High and Significant should be documented and actively monitored by the Executive Director and the Parliamentary Counsel and reported to the ARC on a quarterly basis.

For corporate wide business risks the following delegations apply in relation to the management of those risks:

For risks rated as High – management strategies should be approved by the Parliamentary Counsel.

For risks rated as Significant – management strategies should be approved by the Parliamentary Counsel.

For risks rated as Moderate – management strategies should be approved by the Executive Director.

For risks rated as Low – management strategies should be approved by the Executive Director.

Delegate approval will be required on the level of risk being undertaken on all new significant initiatives, activities and projects.

3.4 Use of risk management at PCO

There are internal controls at PCO to manage the identified risks. Risk management policies are included in many of PCO's corporate policies, including the Business Continuity Plan, Fraud and Corruption Control policies, and Work Health and Safety policies. PCO has a Corporate Governance framework that details these controls.

Risk management is considered in:

- the annual business planning process,
- the development and implementation of new, or changes to, policies, programs and legislation, including new policies and procedures, new strategies and activities, changes to levels of activity and potentially sensitive issues,
- any new activity, change in activity, initiative or project with the potential to cause significant reputational or other damage should they fail.

The principles and basic techniques of risk management are to be applied by staff in their daily work, whether in drafting legislation, technical or editorial support for drafting, service delivery or providing corporate services to PCO or other activities.

PCO has an Internal Audit Charter with a 3-year internal audit plan that focuses on key risk areas.

3.5 Documentation of risks

PCO will maintain and monitor a Risk Register to record all risks. High and significant risks on the Register will be periodically reviewed by senior management and the ARC.

The risk management process undertaken in respect of each identified risk should be recorded appropriately. The Risk Assessment Worksheet records the identified risks, likelihood, consequence, current risk management controls and overall rating of the identified risks. Risk treatment plans and proposed reporting and monitoring arrangements are also detailed. The completed documentation is kept for accountability purposes and is retained by the Executive Director.

3.6 Reviewing and reporting on risks

PCO's risks will be reviewed during business planning or more regularly as required. Project risks will be assessed during project initiation and reviewed during the life of the project.

Risk management and risks are reported as follows:

- Annually to the Parliamentary Counsel as part of the business planning,
- Quarterly reporting in the Risk Register of the status of identified risks,
- Quarterly status reporting to the Parliamentary Counsel on the treatment of Significant and High risks, or as requested,
- Provision of status reports on the treatment of Significant and High risks and other risk management matters to the ARC in accordance with the ARC Management Reporting Plan.

B. RISK MANAGEMENT FRAMEWORK

Introduction

Risk management is a critical component of governance arrangements at PCO. This document establishes the framework that integrates the process of risk management into PCO's overall governance, strategy and planning, management, reporting processes, policies, values and culture.

PCO risk framework is largely based on the Department of Premier and Cabinet's (DPC) framework but has been developed in a manner appropriate to the scale and operations of PCO.

1. Background

PCO is an executive agency under the *Government Sector Employment Act 2013*. PCO has had its own risk management policy and framework since 2014. PCO's risk management framework detailed in this document is based on the DPC's framework and incorporates the findings and analysis about PCO's key risks.

Due to the small size of PCO, there is a formal shared arrangement with the DPC for the ARC to provide independent oversight of PCO's internal audit and risk functions by overseeing and monitoring PCO's governance, risk and control frameworks and its external accountability requirements.

1.1 PCO's Approach to Risk Management

PCO has numerous stakeholders including the Government, Parliament, Ministers and government agencies and the public, all of whom expect PCO to deliver its functions in a thorough, professional, timely and responsive manner. To achieve this, PCO requires an effective Risk Management Policy and Framework to identify and manage risk across its operations. This Risk Management Framework provides a structured and transparent approach to managing risk at PCO.

The methodology detailed in this document provides for a systematic and consistent identification, assessment and management of risk at PCO. The Framework also defines reporting processes to ensure exposures are managed across the organisation. The Risk Management Framework supports PCO's Risk Management Policy.

2. Critical Success Factors

To ensure an effective implementation of a risk management process, it is critical that implementation of the Risk Management Framework is carefully planned and considers the following critical success factors:

1. Risk Management leadership and responsibilities
2. Management commitment and involvement
3. Communication and support
4. Documentation
5. Sustainability and continuous improvement.

PCO's processes and methods for meeting these critical success factors are detailed further in this document.

2.1 Risk Management leadership and responsibilities

The Parliamentary Counsel is responsible for managing risk at PCO and approves the Risk Management Policy and Framework and ensures that both documents are reviewed at least annually. PCO's leadership team considers the outcome of formal risk assessments and proposed mitigation and treatment plans. The Executive Director reports to the Parliamentary Counsel and the ARC and is responsible for ensuring that appropriate risk management responsibilities are carried out within PCO.

Specific risk management responsibilities are detailed in the Policy section of this document under 'Key Responsibilities'.

2.2 Management commitment and involvement

To be effective, risk management must be part of PCO's culture through dedicated commitment and involvement of management and staff in the risk management process. PCO management must:

- reinforce the importance of risk management and internal control by integrating them with all organisational governance, planning (including business planning, business continuity and project planning) and reporting framework,
- provide opportunities for strategic or business objectives to be discussed with staff so that they understand how they can contribute to them and the importance of identifying and managing risks as an integral part of management activity,

- provide opportunities for management and staff to actively participate in the identification of risks and in the development of appropriate treatment plans to manage those risks,
- promote a clear message for all staff on their role in managing risk.

2.3 Communication and Support

Communication and support are important to ensure that every individual in PCO is aware of the development in risk management and to understand how the process fits within the business operations and activities. Communication and support are the responsibility of the Executive Director.

2.4 Documentation

Risk management documentation is part of PCO's Risk management framework and is in place to:

- demonstrate that the risk management process is conducted properly,
- provide evidence of a systematic approach to risk identification and analysis,
- provide a record of risks to support the development of a register of PCO's risks,
- record current controls and any risk treatment plans for identified risks,
- provide accountability for managing the risks identified,
- facilitate continuous monitoring and review,
- provide an audit trail,
- share and communicate risk management information across PCO.

The responsibility for documenting the implementation of the Risk Management Policy and Framework is the Executive Director.

2.5 Sustainability and Continuous Improvement

Risk management is a continuous improvement process to facilitate effective management of risks. As the system matures, it is being continuously developed and reviewed. PCO recognises that continuous improvement is critical to the achievement of strategic objectives and business plans. The Risk Management Framework will continue to be updated and refined from time to time to ensure key concepts and processes remain relevant. This will be achieved through:

- monitoring and reviewing the implementation process and outputs,
- continuing to develop and review risk assessments for all identified risks,
- regular reporting through this Risk Management Framework,
- embedding this process into other key business systems and management processes such as business planning, policy reviews, internal audit and performance appraisals.

The Executive Director is responsible for the ongoing maintenance of the Risk Management Framework.

3. Methodology

3.1 Definition

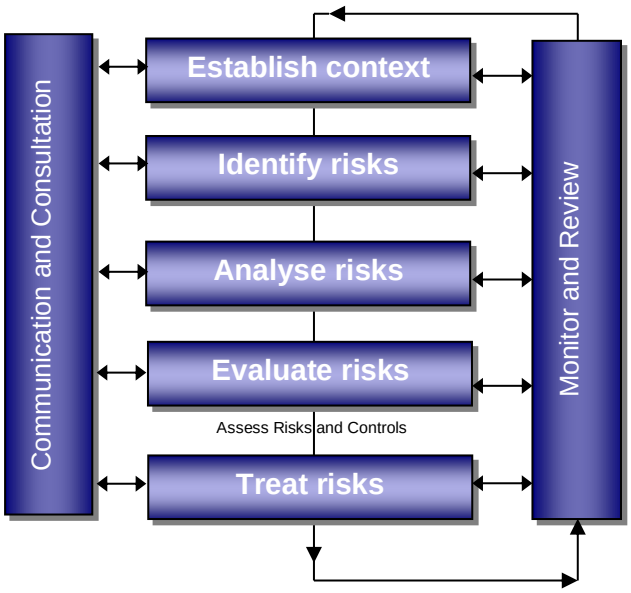
The International Organisation for Standardisation Principles and Guidelines on Risk Management (ISO 31000:2009) defines risk as the effect of uncertainty on objectives. Risk is measured in terms of the likelihood of the event occurring and the consequences that result from an event occurring.

Risk management is "the activities and actions that are taken to ensure an organisation is conscious of the risks it faces, makes informed decisions in managing these risks, and identifies and harnesses potential opportunities".

3.2 Risk Methodology (Basis of Risk Register)

The risk assessment methodology used in the Risk Register is based on DPC's Risk Management Framework which has been adopted by PCO and used in conducting risk management audits.

The following diagram provides a general overview of the approved risk management methodology for PCO.



A brief explanation of the components of the process is summarised below:

1. Establish context

Establish the strategic, organisational and risk management context in which the rest of the process will take place, the methodology to be utilised, the criteria to evaluate risk and the level of management commitment required will be discussed and defined.

2. Identify risks

Identify what, why and how risks can arise within PCO. This will establish the basis for further detailed analysis of the risks identified.

3. Analyse risks

Identify the existing controls and analyse risks in terms of consequence and likelihood in the context of the controls identified. The analysis considers the range of potential consequences and how

those consequences might occur (i.e. scenarios). Consequence and likelihood are combined to produce an estimate of the level of potential risk to PCO.

4. Evaluate risks

Compare estimated levels of risk against risk criteria to provide a basis for management to identify risk management priorities. If the levels of risk are assessed to be low, then risks may fall into acceptable tolerance levels and no further treatment may be required.

5. Treat risks

Accept and monitor low priority risks. For other risks identified, develop and implement specific management plans including the resources allocated to mitigate the risks to an acceptable level.

6. Monitor and review risks

Monitor and review the performance of the risk management system and changes to business initiatives and other internal processes that may affect it.

7. Communicate and consult

Provide regular reports in accordance with this Framework to the Parliamentary Counsel at each phase of the Risk Management process and also on the effectiveness of the processes as a whole. Report to the ARC as requested.

The process explained above is an interactive process and it will therefore contribute to organisational improvement. Each cycle will provide PCO with opportunities to strengthen the risk criteria and progressively achieve improved risk management.

3.3 Risk Identification, Measurement and Control

Identification

This process incorporates reviews of critical business functions, risk identification, risk analysis, evaluation and effectiveness of controls and mitigation measures and prioritisation and categorisation of risks.

Controls

Management is responsible for implementing and enforcing controls that effectively manage and mitigate identified risks. Controls must be relevant and reflect the likelihood and impact of the risk, if it occurred. An efficient and effective control will have the appropriate balance between the cost of implementing, the likelihood and potential impact of the risk event if it occurred and residual risk.

Measurement

To ensure consistency of application across PCO, risks identified must be assessed and measured in accordance with the **inherent** (likelihood and consequence) and **residual** risk and treatment plan rating tables.

Monitoring/Reporting

Information and communication flows are the key to establishing and maintaining an effective risk management framework. The reporting flows should enable PCO management to monitor the effectiveness of the risk systems. The key risk reporting requirements include the Risk Register and risk status reports. For more detailed reporting information refer to sections 5 and 6 of this document.

3.4 Risk Categories

PCO has adopted the following risk categories. These categories assist risk identification, measurement and provide a basis for organising and reporting outcomes.

Risk Categories	Broad Definitions
Business Continuity	Risks relating to inadequate planning and processes required to maintain the continuity of business activities or recovery response to a disastrous event, which may impact the effectiveness of business operations. This includes internal and external activities and processes (e.g. reliance on key suppliers, system failures, critical staff dependencies, fire, flood, etc).
Contract Management	Risks associated with developing, managing and monitoring contracts as well as compliance with required service levels and cost arrangements as specified within the terms of outsourced and in-house service agreements.
Corporate Governance	Risk of inappropriate governance processes and practices. Compliance/ Regulatory risks relating to non-compliance with legislation, regulations, supervision or internal policies and procedures. This also includes all regulatory issues impacting PCO.
Risk Categories	**Broad Definitions**
Finance	Risks associated with budgeting, management reporting, cost management and asset management.
Information Technology for business operations	Risks arising from the use and reliance on information by the organisation or other external entities, which may impact operations (e.g. internal systems, external service providers systems, internet). Policies, procedures and practices (e.g. people, operational processes and technology) required to provide the appropriate level of protection to corporate information and privacy information.
Information Security	Risks associated with security of PCO's information.
Service Delivery	**Operations:** Business operations and delivery of services is not achieved due to inadequate staffing, systems or policies and procedures being in place and monitored. **Fraudulent Conduct:** Dishonest, deceptive and collusive conduct or other misconduct which results in a financial or other loss or benefit to another staff member/other person or PCO itself (e.g. falsified records and deceptive activities). **Project Management:** Risks associated with projects (system implementations, process re-engineering, establishing, managing and integrating) and the change management issues around these projects.
Strategic	Risks associated with leadership and co-ordination, strategy development, business planning and performance targets. Risks associated with the identification of individuals and organisations with a direct influence on and/or interest in PCO's operations. Ensuring ongoing communication and consultation with key stakeholders e.g. DPC, Treasury.
Work Health and Safety (WH&S)	Risks associated with not complying with WH&S legislation and internal policies concerned with the physical and mental safety of PCO's staff and visitors.

Risk Categories	Broad Definitions
Workforce Management	Risks associated with managing PCO's workforce including recruitment, remuneration, retention, using supporting systems, processes and procedures and skills mix, knowledge management and succession planning and risks associated with performance management and learning and development of PCO staff.

4. Risk Ratings

4.1 Risk Likelihood Rating

Analysing risks requires an assessment of their frequency of occurrence. The ratings used by PCO are shown in the table below:

Rating	Description	Definition
5	Almost Certain	The event is expected to occur in most circumstances (daily/weekly); High level of known incidents (records/experience); Strong likelihood of re-occurring, with high opportunities/means to occur.
4	Likely	The event will probably occur in most circumstances (monthly); Regular incidents known (records/experience); Considerable opportunity and means to occur.
3	Possible	The event could occur at some time over 12 months; Few infrequent, random occurrences recorded/experienced; Some opportunity and means to occur.
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.
1	Rare	The event may occur only in exceptional circumstances (10 years); Unheard of; Almost no opportunity to occur.

4.2 Risk Consequence Rating

The outcomes of a risk event or situation expressed qualitatively or quantitatively, being a loss, injury, disadvantage or potential gain. Consequences can range from "insignificant" to "extreme" and are expressed firstly in terms of reputation/image, financial impact, human impact, operational and regulatory/legal.

The Risk Rating Consequence table for PCO is shown below noting:

- the consequences have been identified as Reputation, Operational, Financial or Work Health and Safety related,
- rating levels have been determined as being Extreme, Major, Moderate, Minor and Insignificant,
- each consequence type has a rating (1 to 5).

It should be noted that these are guidelines only to assist in the selection of a consequence rating for a particular risk event. The areas of impact are a guide only and not exhaustive.

Rating	Description	Consequence Area			
		Reputation	**Operational**	**Financial**	**WH&S**
1	**Insignificant** The consequences can be dealt with by routine operations	Negligible impact on image Minister is not specifically concerned Agency relationships generally stable No measurable impact on the environment	Minimal impact on core business	Little or no financial loss	No injuries or fatalities, little or no personal support required
2	**Minor** A threat to the efficiency or effectiveness of some aspects of PCO's operations, but at a level that can be dealt with internally	Marginal decrease in support by stakeholders Minister's dissatisfaction is minor and conveyed only informally Manageable, low-level tensions in relationships with agencies. Small impact on environment, on-site release contained immediately	Some impact on core business	Some financial loss	Minor injuries, no fatalities, first aid treatment required
3	**Moderate** Functions of PCO could be subject to significant review or changes to operations	Attracts media attention Minister is somewhat dissatisfied with PCO Agency cooperation with PCO is not generally proactive Some environmental impact, short-term, requires external assistance on site	Impact on core business requiring some diversion of resources from normal routines	Major financial loss – some assistance required	Medical treatment required but no fatalities
4	**Major** Would produce a threat to the survival or effective performance of PCO	Media concern Minister is dissatisfied with PCO Lack of cooperation of agencies with PCO Some permanent environmental impact	Impact on core business significantly disrupting normal routines – may need external assistance to continue functioning	Major financial loss – requires substantial financial assistance	Many injuries, hospitalisation, possible fatalities, long-term disabilities
5	**Extreme** The consequence would threaten the survival of PCO	Media outrage Minister expresses extreme dissatisfaction with PCO Loss of confidence of agencies in PCO Heavy environmental impact/permanent damage	Major or total disruption of core business	Huge financial loss – requires substantial and ongoing financial assistance	Extensive injuries, fatalities and widespread medical attention required

4.3 Inherent Risk Rating

The consequence and likelihood ratings are then combined in a matrix to determine the inherent risk rating of an activity or an event if it is untreated, as shown in the table below. The Risk Rating signifies to management the level of risk and action required.

LIKELIHOOD		CONSEQUENCE				
		Extreme 5	Major 4	Moderate 3	Minor 2	Insignificant 1
Almost Certain	5	High	High	High	Significant	Moderate
Likely	4	High	High	Significant	Moderate	Low
Possible	3	High	Significant	Moderate	Low	Low
Unlikely	2	Significant	Moderate	Low	Low	Low
Rare	1	Significant	Low	Low	Low	Low

- For example, as shown in the matrix all risks where likelihood is considered to be rare and consequence considered to be extreme shall be significant risks.
- The controls existing to mitigate the risk are then considered for existence and effectiveness using the criteria shown in the next section.

4.4 Identification and assessment of mitigating practices and controls

Once risks have been assessed, a second stage of the process assesses the adequacy of existing mitigating practices and controls designed to manage these risks. These practices and controls include all the policies, procedures, practices and processes that are in place to provide reasonable assurance of the management of PCO's risks.

Where mitigating practices/controls exist but are not being followed and monitored, then adequate control does not exist as, in order for mitigating practices/controls to be effective, they also must be communicated, actioned and monitored.

Control Ratings

		Rating *	
ADEQUATE	Excellent	1 or 2	Systems and processes exist to manage the risk and management accountability is assigned. The systems are well documented and regular monitoring/management review indicates high compliance to the process and that the system is effective in mitigating the risk.
	Good	3 or 4	Systems and processes exist which manage the risk. Minor improvement opportunities have been identified but not yet actioned.
INADEQUATE	Fair	5 or 6	Some systems and processes exist to manage the risk.
	Poor	7 or 8	Systems and processes for managing the risk have been subject to major change or are in the process of being implemented and its effectiveness cannot be confirmed.
	Unsatisfactory	9 or 10	No systems and processes exist to manage the risk.

* Range of rating allows for strength of the statement to be varied.

4.5 Residual Risk Assessment

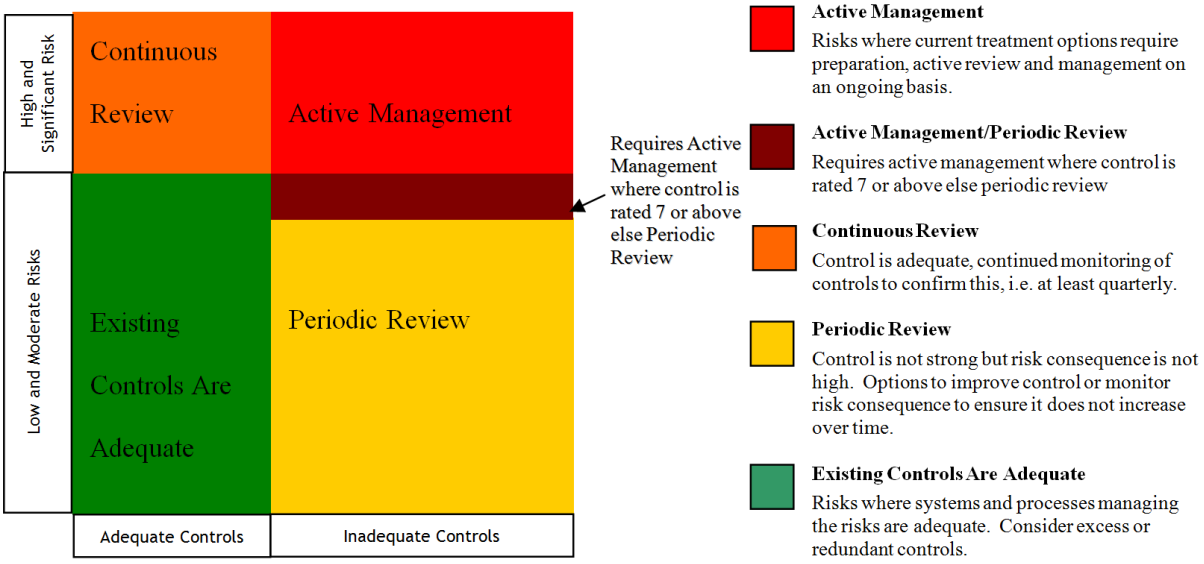
Residual risk is defined as the level of risk that remains after consideration of all existing mitigating practices and controls.

To determine residual risk, the likelihood factors and consequences previously identified at sections 5.3 and 5.4 respectively are reassessed considering existing mitigating practices and controls (section 5.6) to determine if the ratings have changed. New ratings for residual likelihood and residual consequence are combined in the matrix at section 5.5 to determine the Residual Risk.

Based on that residual risk rating, and PCO's "risk appetite" as defined in the Risk Management Policy, residual risks above acceptable levels receive further consideration in the next stage of the process. This stage outlines what additional options should be considered to manage each risk.

4.6 Determining Management Response to Residual Risk

Residual risk at an unacceptable level may require further strategies to manage that risk in addition to existing practices and controls.



The graph is split into sections that indicate the risk management response needed for residual risks. Low and moderate risks with adequate controls are classified as Existing Controls Are Adequate, meaning no further treatment plans are required.

During the formal risk assessment process, the management response as determined is recorded on the Risk Register. Any necessary additional risk management strategies or controls are also recorded.

5. Risk Register and risk treatment plans

A Risk Register is maintained by PCO and records all risks that have been identified at PCO across the risk categories. Current controls are in place and recorded for all risks on the Register and there are also treatment plans for some risks.

The risks for PCO have been identified and a risk assessment has taken place for each risk using the methodology outlined in this Framework. The risk assessment process has been documented on a Risk Assessment Worksheet and is detailed below.

The Risk Assessment Worksheet is used to document the assessment of:

- the risk,
- its likelihood and consequence rating, hence its inherent risk rating,
- operating environment and context,
- key stakeholders,
- the existing controls and a rating for the adequacy of those controls, leaving a residual risk rating.

Based on that residual risk rating, and PCO's "risk appetite" as defined in the Risk Management Policy, residual risks above acceptable levels will receive further consideration and a risk treatment plan developed and recorded on the Risk Assessment Worksheet. It will record:

- the proposed risk treatment strategies or plans,
- responsibility for considering/acting upon these strategies and a timetable for doing so.

There are close links at this stage between the risk treatment planning process and the business planning process and improvement processes.

The Risk Register is the means of recording progress on implementation of risk treatment plans and monitoring its impact in terms of risk.

6. Risk Reporting and Tools

Risk Management Reporting

Report Recipient	Report	Responsibility	Frequency	Content / Purpose
Parliamentary Counsel ARC	Register of active Risk Issues including status report on any treatments for High and Significant risks.	Executive Director	Quarterly	Report gives a status report on all outstanding risk issues and action items.
ARC	Risk/Compliance Summary	Executive Director	Quarterly	The reports include confirmation that controls are operating and report on any current risk/compliance matters.
Parliamentary Counsel Leadership team	Risk Register Review	Executive Director	Annually	Review of Register as part of the Business Planning process.

Risk Tools

Tool	Purpose	Explanation
Risk Register	Identifies and records all risks facing PCO, including project risks.	To be updated at least annually in conjunction with the Business Planning cycle or as risks / processes arise. To be updated quarterly on progress on implementation of agreed risk management strategies.
Risk Assessment Worksheet	Documents the formal risk assessment process undertaken for	Records detailed assessment of the operating environment and context, the identified risks, likelihood, consequence and overall rating of identified risks, agreed risk treatment

	each risk on PCO's Risk Register.	strategies and proposed reporting and monitoring arrangements.
Risk Assessment Update	Annual status review of key risks	Provides an annual re-assessment and overview of the key risks, their risk ratings, management response and treatment plans and includes a summary of the key risks, their risk ratings and management response. Refer sample table at Appendix 1.

PCO also consults a range of publicly available tools to assist in risk management activities, as required. For example:

- the practical tools provided in *How to manage work health and safety risks – Code of Practice* published by SafeWork Australia,
- the *Risk Management Toolkit for the NSW Public Sector* published by NSW Treasury,
- the *Corporate Governance Lighthouse Model* published and promoted by the NSW Audit Office.