National Capital Authority

Risk Management Policy and Framework

June 2023

Table of Contents

1 Introduction

1.1 Purpose

The National Capital Authority (NCA) Risk Management Policy and Framework has been established in accordance with the Commonwealth Risk Management Policy (2023) issued under the *Public Governance, Performance and Accountability Act 2013* (PGPA Act). Section 16 of the PGPA Act provides that:

> *"… accountable authorities of all Commonwealth entities must establish and maintain appropriate systems of risk oversight, management and internal control for the entity".*

The NCA's Risk Management Policy and Framework is aligned with *ISO 31000:2018 Risk Management – Guidelines* and draws on *Implementing the Commonwealth Risk Management Policy – Resource Management Guide 211 (April 2023).* The Policy and Framework is supported by and consistent with the NCA's Accountable Authority Instructions (AAIs – Section 1 – Corporate Governance)

The Policy and Framework outlines the policy and the process for identifying, recording and monitoring risks and provides guidance to NCA staff (including Authority members) on all aspects of risk management. To accomplish this, the policy and framework:

- provides a policy statement about the NCA's approach to the management of risk and the associated responsibilities of the NCA's Authority, Executive and staff at all levels;
- supports risk management practices that advance the objectives of the NCA;
- details the benefits of effective risk management for the NCA;
- supports a systematic approach to managing risk that is endorsed and supported by the Authority and the Executive;
- aims to develop the risk management capability of staff, while concurrently embedding the principles of responsible risk-taking;
- promotes sound governance in the delivery of the NCA's statutory functions and responsibilities under the *Australian Capital Territory (Planning and Land Management) Act 1988*, Government policy and other legislation; and
- enhances stakeholder trust while ensuring due diligence and proper accountability.

1.2 National Capital Authority's approach to managing risk

Through risk management, the NCA is able to minimise the risks associated with successfully performing our functions and maximise its ability to achieve its mission and goals.

The NCA recognises that risk management is an essential element of effective governance, and strategic and business planning that must be incorporated into all relevant processes.

The foundation of the Framework and Policy is the NCA's commitment to having a sound capability in relation to managing risk as part of our 'business as usual' arrangements – whereby sound risk management is central to the NCA's behaviours, processes and practices.

Reflecting the NCA's position as a Commonwealth non-corporate entity with rigorous accountability and oversight arrangements, and with a high degree of public scrutiny and expectations regarding our actions and decisions, the NCA necessarily exercises due care and diligence with respect to our risk appetite and tolerance, based on careful cost-benefit analysis. In short, the NCA has a relatively low risk appetite.

The NCA is open to accepting an appropriate level of risk through balancing the level of risk accepted against potential benefits and opportunities. This approach can promote efficiency and innovation in our work. The implementation of the Policy and Framework ensures the identification and assessment of significant areas of risk to the NCA, and the subsequent application of appropriate measures to mitigate the risk, or where that is not possible, manage the consequences to the best of our ability.

1.3 The NCA's approach to risk culture

The NCA's commitment to managing risk is demonstrated by the Authority and Executive and reflected in the NCA's culture and processes. The NCA's culture of managing risk is a positive one, reflecting recognition of the benefits of managing risk for achieving the NCA's objectives. Understanding, managing and accepting appropriate risk is part of everyday decision-making processes.

The NCA's approach to risk management is consistent with our objectives, and ensures that, as they arise, opportunities for improvement to NCA services are identified and implemented through prudent, informed and structured risk management. This risk management approach is driven through the NCA's governance framework supported by clearly articulated accountabilities and the internal risk structure and reporting frameworks.

Continuous risk management learning

The NCA has a constructive work environment where learning from experience is valued, lessons are shared and improvements are built into management practices. Risk management is an integral and routine part of all planning and related processes (including budgeting). Education, awareness and support will continue to be provided to all business teams.

Driving a culture of managing risk

The NCA is committed to maintaining a positive risk culture where risk is understood and managed by all staff. The development of a positive risk culture is driven by the everyday behaviour of NCA staff. Elements that contribute to the development of a positive risk culture are:

- The Authority, NCA Audit and Risk Committee and Executive support and drive the adoption of the Risk Management Policy and Framework;
- all staff promote and implement the Risk Management Policy and Framework;
- sound risk management is embedded in NCA business processes, from strategic planning and reporting, to day-to-day operations and discussions;
- the benefits of risk management are well communicated;
- those who excel in managing risk in their day-to-day responsibilities are recognised;
- analysis and innovation in the management of risk is encouraged in order to understand the benefits and risks of new activities; and
- risk management is integrated with other key processes and systems, ensuring that risk management is part of everyday decision-making.

2 Risk Management Policy

2.1 Objective

The key objective in managing risk within the NCA is to ensure delivery of our objectives in a timely, cost-efficient and effective manner. The measurable outcomes for the policy are to:

- maintain a consistent understanding of risk management (including use of a common risk language);
- provide the methodology and tools to enable effective management of risk;
- implement an effective risk management framework that is tailored to meet our structure, functions and activities, and the challenges of the NCA's internal and external environment;
- foster an environment where all staff assume responsibility for, and exercise judgement in, managing risk and where risk is considered part of business planning and related processes;
- ensure that significant risks facing the NCA are identified, understood, documented and actively managed;
- maintain the highest possible integrity for the services provided by the NCA; and
- demonstrate transparent and responsible risk management processes that align with better practice.

2.2 What is Risk?

Risk is the effect of uncertainty on objectives.[1]

2.3 What is Risk Management?

Risk management is defined as co-ordinated activities to direct and control an organisation with regard to risk.[2] Additional guidance on the implementation of risk management is provided on the Comcover website.[3] A key publication is *Resource Management Guide 211 – Implementing the Commonwealth Risk Management Policy (April 2023*).

Risk can be measured as a combination of two components: the likelihood of an event occurring and the consequences arising from that occurrence. Risk exists in everything we do including dealing with stakeholders, managing projects, purchasing new equipment and setting work priorities.

Risk management is a process which provides assurance that objectives are more likely to be achieved and threats are less likely to be realised.

Risk management supports strategic and business planning, and is a key process for being able to demonstrate the 'efficient, effective, economical and ethical use or management of public resources' required by the PGPA Act.

The benefits of managing risk include:

- improved strategic planning;
- reduction of unexpected events;

[1] IS*O 31000:2018 Risk Management – Guidelines* International Organization for Standardization, February 2018

[2] Ibid. p1.

[3] Risk Management Services | Department of Finance

- improved financial management;
- improved results from projects;
- clearly defined insurance needs;
- improved compliance outcomes; and
- reduction in the potential for litigation.

A risk assessment is the overall process of risk identification, risk analysis and risk evaluation.

Risk assessments are a fundamental component of the risk management process. They involve the measurement of risk to determine priorities and to enable identification of an appropriate level of risk treatment.

2.4 Our risk types

2.4.1 Strategic Risks and Controls

Strategic Risks have the potential to significantly impact NCA's operations and compromise the agency's ability to achieve our purposes and deliverables. The broad nature of many of these risks means they need to be considered and assessed from a cross organisational perspective.

The NCA's Strategic Risks and Controls (including emerging risks) are monitored and updated on a continual basis by the NCA's Executive and Senior Leadership Team. They are also reviewed and updated on at least a quarterly basis by the Authority and the NCA Audit and Risk Committee. The Strategic Risk Register and Treatment Plan includes actions to address risks where indicated.

2.4.2 Management Risks and Controls

The NCA's Management Risks and Controls (including emerging risks) are those that relate to the effective operation and success of the NCA's business units. Management risks and controls are identified and considered in NCA Business Plans and are part of business planning as natural adjuncts to business objectives and resourcing decisions. Business team managers – the NCA's Executive and Senior Leadership Team – are the key officers for oversighting and managing management-level risks and controls.

2.4.3 Operational Risks and Controls

The NCA's Operational Risks and Controls (including emerging risks) relate to the delivery of ongoing, business-as-usual responsibilities and activities. These will mostly be identified in NCA Business Plans. Operational risks and controls are identified, treated, monitored and reviewed by the relevant Executive Level (EL) 1s or EL2s with oversight by the responsible Executive Director or Director. These risks are regularly reviewed and captured in the NCA's WHS Monitor system.

Both management and operational risks may also be strategic risks, as identified by their risk ratings.

2.4.4 Specialist Risk Categories

The NCA also uses specific risk management arrangements for several functions including project management, business continuity/disaster recovery, fraud control, work health and safety, and protective security. These specialist areas align to the extent possible with this overarching policy and framework.

2.5 Risk Appetite

As noted above, the NCA is a non-corporate Commonwealth entity with rigorous accountability and oversight arrangements. The NCA also has a high degree of public scrutiny and expectations regarding our resources, actions and decisions. In this context, the NCA necessarily exercises a high level of care and diligence with respect to our risk appetite and tolerance. We aim to have as low a level of risk as is prudent, based on careful cost-benefit analysis of risk exposure and controls. The following diagram sets out the approach the NCA has to managing risk.

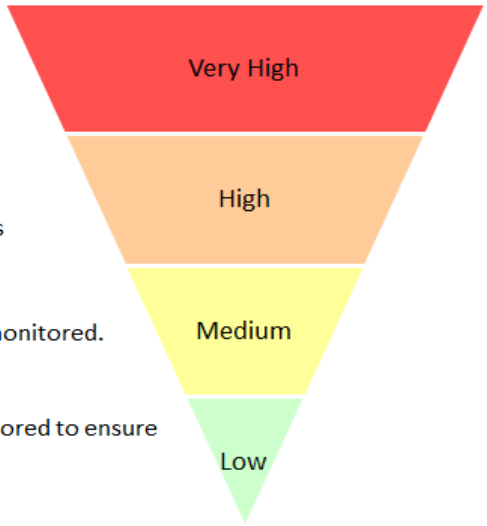
Figure1: Risk management arrangements

Very High Risks may be acceptable to the NCA if the possible benefits outweigh the consequences. Quality control measures must be implemented. Regular review and reporting needs as determined by the Executive to be implemented.

High Risks may be acceptable to the NCA if the possible benefits outweigh the consequences. Regular review and reporting needs to be implemented.

Medium Risks are generally acceptable to the NCA but must be monitored.

Low Risks are generally acceptable to the NCA but must be monitored to ensure that the risk rating does not change.



2.6 Risk Reporting

Risks and treatment options should be monitored and reported on regularly at a project level.

In addition to this progress reports will be produced as follows:

Frequency	Level	Report
Quarterly	Authority	Strategic and other high-level risks will be reported to the Authority at least quarterly through the Strategic Risk Register and Treatment Plan.
Quarterly	NCA Audit and Risk Committee	Strategic and other high-level risks will be reviewed by the NCA Audit and Risk Committee at its quarterly meetings.
Weekly, or as required in response to a Very High risk that requires urgent attention	Executive/ Senior Leadership Team	The Executive will receive a report which will include the following: • details of **Very High and High** level risks including their status • overall progress of risk management actions • effectiveness of implemented actions • anticipated emerging or aggregated risks that will require specific management attention

2.7 Risk Registers and Reporting

The NCA maintains risk registers and/or reporting as follows:

- The NCA Strategic Risk Register and Treatment Plan is monitored and updated at Authority, Audit and Risk Committee and/or Executive and Senior Leadership Team meetings;
- NCA Management Risk is set out in Branch/Team Business Plans – these are monitored over the course of the business planning cycle; and
- NCA Operational and Specialist Risk are maintained in the relevant project or specialist risk registers, including the NCA's WHS Monitor system.

These documents are dynamic – they are populated, monitored and reviewed throughout the life of the activity using the risk assessment and evaluation process. This process enables all risks to be analysed, communicated, quantified and ranked, and provides a structure for collecting information about risks that will:

- support the analysis of risk;
- support decisions about whether or how these risks could be mitigated and monitored;
- provide a framework for scrutiny and prioritisation of actions; and
- support strategic analysis and organisational decision making.

Project and Operational risks rated 'High' or above must be appropriately recorded and reported by the relevant Director or project manager to the Senior Leadership Team, the Executive, the Audit and Risk Committee or the Authority.

2.8 Risk Roles and Responsibilities

The table below describes the roles and responsibilities for managing risks. In general, responsibility for managing specific risks are to those entities or individuals who are best placed to manage the risk.

Role	Responsibilities
Authority	• provides strategic leadership and direction on the application and importance of risk management across the NCA • endorses the Risk Management Policy and Framework, including with respect to risk appetite and tolerance • considers the risk of matters brought before the Authority • reviews the NCA's strategic risks on at least a quarterly basis
Chief Executive	• is responsible for escalating risks to the Authority as required and ensuring risks are dealt with at an appropriately senior level • is responsible for the implementation of the Risk Management Policy and Framework, and operational matters that arise.
Executive/Senior Leadership Team	• provides support and input to assist the Authority and Chief Executive in the oversight and management of risk management in the NCA.
NCA Audit and Risk Committee	• provides independent advice of the effectiveness of the NCA's risk management framework • assist the Authority and Chief Executive with oversight of the NCA's strategic risks, assurance arrangements and control framework

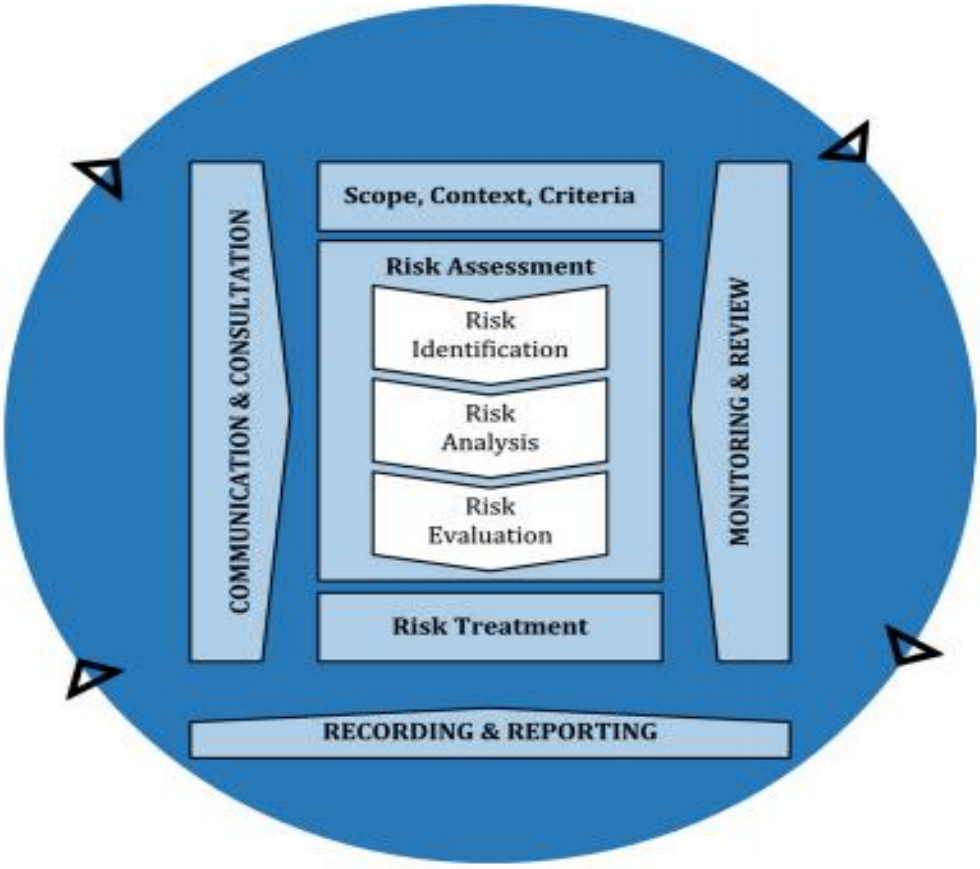
Role	Responsibilities
Executive (SES officers, including CE)	• is the risk owner for strategic risks in their area of responsibility • re-assesses strategic risks at least quarterly • is responsible for ensuring strategic risks are managed in accordance with the NCA's risk management process and that risk reporting is up to date • intervenes to control risks that affect projects and operations with strategic objectives • keeps the Chief Executive appraised of the status of any risks with an overall risk rating 'High' or 'Very High' including advice on how the risk will be treated, monitored and reviewed • responsible for notifying the Chief Executive of relevant strategic risks that could impact Projects or Operations • making decisions on Managers' recommendations regarding the management of risk • determining a balance between the level of risk and the potential benefits that the project or initiative may achieve • ensures risks when realised are captured as Project or Operational issues and managed accordingly • include Business Unit level risks, capturing relevant strategic, project and operational risks in the unit's annual Business Plan
Chief Operating Officer, Governance and Legal Services Section, Manager, WHS and Risk	• is responsible for oversight and facilitation of risk management, including reporting • is responsible for maintaining the Risk Management Policy and Framework, and associated strategies for monitoring risks • provides support and advice on risk management • provides or facilitates internal training and promotes the importance of relevant staff attending Comcover's suite of risk management training • prepares the NCA's biennial response to Comcover's risk management benchmarking survey
Directors (EL2s), Senior Managers (EL1s), Project Managers (EL1s, APS6s)	• complete the Risk Assessment and Treatment Template where required • regularly review and effectively manage risks • modify plans to include agreed actions to avoid or reduce the impact of risks • escalate risks to the relevant Executive for resolution as required in a timely manner • evaluate the potential impact on benefits should risks relating to time, cost or quality be realised
All staff (included contracted personnel)	• adhere to the Risk Management Policy and Framework • assist in the identification and management of strategic, management and other relevant risks

3 Risk Management Framework

3.1 The NCA's Risk Management Process

The steps in the NCA risk management process outlined below in Figure 2 follow the principles of *ISO 31000:2018 Risk Management – Guidelines.*

Figure 2: *Risk Management Process*[4]



3.1.1 Establishing the Context

Establishing the context defines the external and internal parameters to be taken into account when managing risk and sets the scope and risk criteria for the remaining process.[5] This step in the process is required to be conducted to gain an understanding for the risk assessment being conducted, and the internal and external operating environments within which the NCA operates.

[4] Ibid. p9

[5] Ibid. p10

In completing the risk assessment, the relevant NCA manager (SES, EL2, EL1 or APS6) should:

- **Clarify Objectives** — identify the desired outcomes, outputs and objectives that the risk assessment is being conducted for
- **Determine Environment** — identify the external and internal environments in which the objectives are to be pursued
- **Identify Stakeholders** — who are our key internal and external stakeholders and what are our relationships with stakeholders
- **Conduct a SWOT analysis** — what are major strengths, weaknesses, opportunities and threats
- **Identify communication aspects** — identify the communication and consultation processes with internal and external stakeholders for every step and include appropriate strategies in your list of controls as part of the risk management process.

3.1.2 Risk Identification

On an ongoing basis, NCA managers need to identify sources of risk, areas of impacts, events (including changes in circumstances) and their causes and their potential consequences.[6]

The aim of this step is to produce a register of risks based on those events that might prevent, degrade, hasten or delay the achievement of NCA objectives.

To ensure comprehensive identification of potential risk events an analysis of the sources and causes of risks should be undertaken i.e. consideration of how and why a risk event may occur. Risk identification should include risks whether or not their source is under the control of the NCA. Comprehensive identification is critical because a risk that is not identified at this stage will not be included in further risk analysis.

Risk criteria for each potential risk event should be identified and assessed in reference to the NCA's Risk Assessment – Consequence Ratings (at **Appendix B**):

- Safety;
- Assets;
- Environmental / heritage;
- Financial;
- Human Resources
- Information management;
- Reputation;
- Legal / compliance; and
- Stakeholders.

[6] Ibid. p11.

3.1.3 Risk Analysis

Risk analysis is the process to comprehend the nature of the risk and to determine the level of the risk.[7]

Risk analysis involves developing an understanding of the risk. The purpose of this step is for the relevant manager to consider each risk event in terms of its likelihood of occurrence and the consequences of its occurrence. This analysis will provide a risk level. The objective is to establish the significance of each risk as a prelude to making informed decisions about the strategies required to deal with each risk and the resources required.

Current controls

A control is a process, policy, device, treatment, practice or other action which maintains and or modifies risk.[8]

In addition to considering the likelihood and consequence of individual risks, current controls and management strategies should also be reviewed by the relevant manager. Current (also referred to as 'existing') controls for each risk should be identified and assessed for effectiveness. The effectiveness of controls can change so the relevant manager must review the controls on a regular basis.

Consequences and Likelihood

The consequence of a risk occurring refers to the impact to the NCA if the risk occurs. There can be more than one consequence from a risk event. Refer to **Appendix B** of this framework to determine Consequence Rating.

The likelihood of a risk event occurring refers to the possibility of the event occurring and when the risk may occur. **Appendix C** of this framework provides a Likelihood rating scale.

Level of risk

An assessment of the consequence and likelihood of a risk event will determine its level of risk. Relevant managers must refer to the Risk Level Matrix (**Appendix D** of this framework) to combine consequence and likelihood of the risk to produce risk level. For each risk, identify where the consequence level and the likelihood level intersect in the Risk Matrix. Where the levels meet determines the risk level. Any risk rated as High or Very High must be brought to the attention of the Executive as soon as possible. Further details on actions required at each risk level are provided in **Appendix E** of this framework.

3.1.4 Risk Evaluation

The purpose of risk evaluation is to assist in making decisions based on the outcomes of risk analysis about which risks need treatment and the priority for treatment implementation.[9] Risk evaluation is a major decision point in the process with important consequences. The higher the level of risk, the higher the priority and the higher the level of involvement by the Executive.

Risk levels are usually acceptable or unacceptable. Acceptable risks usually only require regular monitoring only to ensure the risk does not increase, whereas unacceptable risks should be treated. Acceptable risks are generally risks with Low or Medium risk levels that can often be managed through current controls. Risks rated as high or very high are generally unacceptable and require treatment. High or Very High risks must be brought to the attention of the Executive

[7] Ibid. p12.

[8] Ibid. p2.

[9] Ibid. p12.

as soon as possible. Risks ratings should be discussed with the relevant Executive Leader to determine if controls are adequate and whether the risk will be accepted or if further treatment is required.

Factors to consider when evaluating risk include:

- the importance of the activity you are risk assessing in the context of the NCA's objectives and priorities. (Undertaken when Establishing the Context);
- the suitable degree of control you have over mitigating the risk;
- the potential and actual damage which may arise should the risk eventuate; and
- the benefits and opportunities presented by the risk to your activity.

3.1.5 Risk Treatment

Risk treatment is the process to select and implement an option or options to address (modify and maintain) risk.[10]

Once risks have been analysed, evaluated and prioritised, the relevant manger needs to determine strategies to mitigate or treat each individual risk. Very High and High risks require treatment plans to reduce the risk to an acceptable level within a reasonable timeframe. The management options for treating risks include:

- ***avoid*** the risk—cease (or do not take on) the function or activity that gives rise to the risk.
- ***transfer*** the risk—ensure that risks are borne equitably by transferring risks. Risk can be transferred to another party who may have greater control over the risk, are less susceptible to the risk factors or who stand to gain from the risk. This may be achieved through insurance or contractual arrangements. Responsibility for 'duty of care' cannot be transferred.
- ***sharing*** the risk—ensure that risks are borne by parties for which the risk is more acceptable or appropriate (eg. through contract management and/or insurance).
- ***reduce*** the risk—develop and implement controls to either reduce the likelihood and/or ameliorate the consequences of occurrence. When developing treatment strategies, the relevant manager may identify alternative approaches to achieving objectives which may ultimately reduce the risk.

An important consideration in this step is to identify the cost-benefit relationship between the risk and the treatment options. There will generally be a range of options available, it is important the most cost-effective options are selected.

The relevant manager should document risk treatment options using the Risk Assessment template, including details of the proposed risk treatment, who is responsible for implementing the risk treatment and when the treatments will be implemented.

Risk treatment in itself can create risks. A major risk can be the ineffectiveness or failure of mitigation strategies and treatments introduced to lessen risks. Monitoring is a vital part of risk treatment to ensure that the mitigation strategies and treatments are effective. The relevant manager is responsible for monitoring and reviewing risk treatments.

3.1.6 Communicate and Consult

A fundamental requirement for an effective risk management framework is the development of plans, processes and products through ongoing consultation and communication with

[10] Ibid. p13.

stakeholders (both internal and external). These stakeholders should include all those who may be involved in or affected by an NCA's decisions and actions.

Risk communication involves a range of activities, including issue identification and assessment, analysis of the environment (including stakeholder interests and concerns), development of consultation and communications strategies, message development and working with the media.

Effective communication and consultation is important throughout the risk assessment and management process to:

- identify current risks and possible emerging risks during the activity;
- ensure those responsible for implementing the controls identified in the risk treatment plan understand the basis of how decisions have been made and what particular actions are required by them;
- provide assurance and confidence to stakeholders that the department is suitably identifying and managing risks in our activities; and
- share lessons learnt from the implementation of effective treatment and mitigation strategies.

3.1.7 Monitoring and Review the Risks and Controls

Monitoring and review is an ongoing process designed to ensure the validity of the process and to maintain the currency of the risk assessments and the risk reporting[11]. It is important to also monitor the currency and effectiveness of controls.

Reviewing risk assessments regularly will ensure that they are still relevant while reporting progress provides assurance that our objectives are being achieved. This review process provides a sound basis for making further decisions.

All risk assessments will be reviewed regularly to update the risk level for current risks, and to identify and analyse any new risks that may have emerged. Factors such as change of policy or a requirement to reduce operating costs may impact the likelihood or consequence of risks. This can cause changes to individual risks and the level of impact of such risks. The relevant manager will review and report as required on progress in implementing risk treatments and controls. The process of monitoring and review provides assurance to the relevant manager, the Authority and NCA Executive that there are no surprises from new or emerging risks, and that risk treatment strategies remain effective.

3.1.8 Risk Assessment and Treatment Template

Risk Assessments and Risk Treatment options should be documented using the Risk Assessment and Treatment Template. A Risk Assessment and Treatment Template is available in Trim (reference – 534798).

[11] Ibid p14.

4 Further information

The Governance and Legal Services Team and Manager, WHS and Risk, are available to provide support to NCA officials in the effective identification, management, monitoring and reporting of risk for your project and/or operational responsibilities. For assistance please contact the Director, Governance and Legal Services, on 6271 2857, the Manager, Governance on 6271 2861 or 0412 515 126, and/or the Manager, WHS and Risk, on 0407 736 010.

Other references:

- International Organisation for Standardisation, *ISO 3100: 2018 Risk Management – Guidelines*, February 2018 https://www.iso.org/standard/65694.html
- Department of Finance, *Commonwealth Risk Management Policy* (1 January 2023) Commonwealth Risk Management Policy | Department of Finance
- Department of Finance, *RMG 211 - Implementing the Commonwealth Risk Management Policy – Guidance* (Resource Management Guide 211, 2023) Implementing the Commonwealth Risk Management Policy (RMG 211) | Department of Finance

Appendix A: Definitions and Glossary of terms

Accountable authority – The person or group of persons who has responsibility for, and control over, a Commonwealth entity's operations. The Authority is the accountable authority for the NCA.

Commonwealth entity – A Commonwealth entity is a:

(a) Department of State; or

(b) Parliamentary Department; or

(c) listed entity; or

(d) body corporate established by a law of the Commonwealth

> ***Corporate Commonwealth entity*** *– A Commonwealth entity that is a body corporate and legally separate from the Commonwealth.*
>
> ***Non-corporate Commonwealth entity*** *– A Commonwealth entity that is not a body corporate and legally part of the Commonwealth.*

Internal control – Any process, policy, device, practice or other actions within the internal environment of an organisation which modifies the likelihood or consequences of a risk.

Risk – The effect of uncertainty on objectives.

> ***An effect is a deviation from the expected*** *— positive and/or negative. Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances or knowledge) and the associated likelihood of occurrence.*

Risk assessment – The process of risk identification, risk analysis and risk evaluation.

Risk appetite – The amount of risk the NCA is willing to accept or retain in order to achieve its objectives. It is a statement or series of statements that describes the entity's attitude toward risk taking.

Risk criteria – Terms of reference against which the significance of a risk is evaluated.

Risk management framework – A set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation.

Risk management – Co-ordinated activities to direct and control an organisation with regard to risk.

Risk oversight – The supervision of the risk management framework and risk management process.

Risk profile – A description of any set of risks. The set of risks can contain those that relate to the whole organisation, part of the organisation or as otherwise defined.

Risk tolerance – The levels of risk taking that are acceptable in order to achieve a specific objective or manage a category of risk.

> *The NCA's risk tolerance is partly defined within the risk assessment matrix (the level of risk attributed to different combinations of likelihood and consequence) and the associated risk responses. Risk tolerance levels at the NCA are assessed on a case-by-case basis as they are dependent on the key issue and situation under consideration.*

Shared risk – A risk with no single owner, where more than one entity is exposed to or can significantly influence the risk.

Appendix B: Risk Assessment – Consequence Rating

Rating	Consequence								
	Safety	**Assets**	**Environment/ Heritage**	**Financial**	**Human Resources**	**Information Management**	**Reputation**	**Legal/compliance**	**Stakeholders**
Severe	Fatalities and/or irreversible disability or impairment of numerous people.	Destruction/loss or permanent impairment of significant NCA assets (Departmental & Administered).	Destruction or serious permanent damage to significant environment, ecosystems or heritage resources.	Net loss impacting the NCA's financial position by greater than $1.0m.	Extreme loss or unavailability of NCA staff or staff in key positions; extreme staff disengagement.	Severe loss or corruption of the majority of critical information systems and resources (including IT-based and other significant records) severely impacting business continuity for a prolonged period.	Widespread public outrage or condemnation and high-level political criticism (eg. resulting in government inquiry). Includes sustained adverse media attention or public outcry, across multiple media channels.	436755	Severe Commonwealth (and/or ACT) government, public/community effects or social issues, resulting in complete loss of confidence and support for the NCA and being unable to deliver its outcomes.
Major	Extensive injuries, irreversible disability or impairment to multiple people.	Destruction/loss of a major NCA's assets (Departmental & Administered).	Major detrimental damage to the environment, ecosystems or heritage resources or long-term effects.	Net loss impacting the NCA's financial position between $0.25m and $1.0m.	Substantial loss or unavailability of NCA staff or staff in key positions; very high staff disengagement	Loss or irrecoverable corruption of critical or significant information systems and resources impacting business continuity for a period.	Substantial public outrage or condemnation and local political criticism (resulting in inquiry). Includes adverse media attention or public outcry, across multiple media channels.	Breaches of legislation or regulatory requirements with major consequences such as litigation, major fines, and/or ANAO inquiry.	Major government, public/community effects or social issues, resulting in significant loss of confidence and support in the NCA.

Rating	Consequence								
	Safety	**Assets**	**Environment/ Heritage**	**Financial**	**Human Resources**	**Information Management**	**Reputation**	**Legal/compliance**	**Stakeholders**
Moderate	Medium term, largely reversible disability to one or more persons. Medical treatment required for one or more persons.	Damage to, or other impairment of, a significant proportion of assets.	On-site environmental releases contained with outside assistance, medium-term environmental effects. Moderate damage to Authority heritage resources.	Net loss impacting the NCA's financial position between $100,000 and $250,000.	Moderate loss or unavailability of NCA staff or staff in key positions; moderate staff disengagement	Corruption of key information systems and resources impacting NCA operations.	Adverse local media attention or criticism from a recognised segment of the community.	Breaches of legislation or regulatory requirements with moderate consequences such as investigations, threat of litigation, moderate fines, additional reporting or ANAO attention.	Moderate adverse government, public/community effects or social issues, resulting in concerns around specific actions or NCA outcomes.
Minor	Minor injuries or ailments. First aid treatment required.	Damage to, or other impairment of, a small proportion of assets.	Minor ecosystem effects, any environmental on-site releases or heritage resources damages are contained.	Net loss impacting the NCA's financial position between $25,000 and $100,000.	Minor loss or unavailability of NCA staff; minor staff disengagement	Disruptions or corruption of routine 'administrative' information resources.	Local media enquiries and minor reporting.	Breaches of legislation or regulatory requirements with minor consequences such as minor legal issues and/or fine imposed.	Local concern or criticism from government, public/community or social matters with minor impact.
Insignificant	Insignificant injury or ailment, no treatment required.	Loss or reparable damage to small number of assets.	Insignificant effects on environment or heritage assets.	Insignificant effect on the NCA's net financial position involving less than $25,000.	Insignificant loss or unavailability of NCA staff; insignificant staff disengagement	Insignificant disruptions, loss or impairment of small amount of administrative information.	Insignificant public or media attention.	Breaches of legislation or regulatory requirements with insignificant consequences and/or breaches of regulations.	Insignificant government, public/community or social impacts.

Appendix C: Risk Assessment – Likelihood Rating Scale

Rating	Likelihood of the risk occurring in the next 3 years	
	Description	Estimated probability
Almost Certain	Almost certainly will occur.	>90 per cent
Likely	Is likely to occur in the current operational environment.	70 – 90 per cent
Possible	Will possibly occur in the current operational environment.	30 – 70 per cent
Unlikely	Is unlikely to occur in the current operational environment.	10 – 30 per cent
Rare	May occur in rare circumstances only.	<10 per cent

Appendix D: Risk Level Matrix for Determining the Level of Risk

Likelihood	Consequence				
	Insignificant	Minor	Moderate	Major	Severe
Almost Certain	Low	Medium	High	Very High	Very High
Likely	Low	Medium	High	High	Very High
Possible	Low	Medium	Medium	High	High
Unlikely	Low	Low	Medium	Medium	High
Rare	Low	Low	Low	Medium	Medium

Appendix E: Management Action Required

Rating	Required Response
Very High	Prompt corrective action by the NCA Executive is required. The Authority, Chief Executive and Audit and Risk Committee must be kept informed of actions and progress until the exposure is at an acceptable level. Further controls are needed unless unrealistic or not financially viable.
High	Chief Executive, Executives and Senior Management must be involved in systematic and regular monitoring. Additional controls may be required to protect the NCA's interests, reputation and operations.
Medium	Manage by specific monitoring or response procedures, with NCA management responsibility specified.
Low	Managed by existing routine procedures and work practices in the NCA.