



National Health  
Funding Body

# Risk Management Policy and Framework

DECEMBER 2025

## Document information

<b>Document name</b>	NHFB Risk Management Policy and Framework
<b>Document filename</b>	
<b>Trim reference</b>	D21-1324

## Change history

<b>Author</b>	<b>Date</b>	<b>Description</b>	<b>Version</b>
<b>Sab Bonelli</b>	April 2021	New template and reviewed following 2021 risk review	1.0
<b>Sab Bonelli</b>	May 2021	Addition of 3 lines model and associated references	1.1
<b>Emma Griffin</b> <b>Sab Bonelli</b>	November 2023	New template and review	2.0
Sab Bonelli	Jun-Aug 2025	Review, minor edits not impacting on policy intent and purpose	2.1

## Approval

<b>Title</b>	Chief Executive Officer
<b>Name</b>	Shannon White
<b>Signature</b>	
<b>Date</b>	10 December 2025

## Contents

<b>Introduction .....</b>	<b>3</b>
<b>Risk Management Policy.....</b>	<b>4</b>
Overview of the NHFB's approach to risk management .....	4
Defining responsibilities for managing risk.....	6
<b>Risk Management Framework .....</b>	<b>10</b>
Key elements of managing risk .....	11
The NHFB's risk culture .....	12
Communicating and consulting on risk.....	13
The NHFB's risk management capabilities.....	14
Identifying and managing shared risk.....	14
Embedding risk management into business processes .....	15
Risk performance reporting .....	17
Reviewing and improving risk management.....	18
Use of Artificial Intelligence (AI) risks .....	18
Supporting information .....	19
<b>NHFB risk management elements on a page .....</b>	<b>20</b>
<b>Risk approach overview.....</b>	<b>21</b>

# Introduction

The National Health Funding Body (NHFB) is a non-corporate Commonwealth entity under the *Public Governance Performance and Accountability Act 2013* (Act). Under Section 16 of the Act, the Accountable Authority of a Commonwealth entity must establish and maintain an appropriate system for risk oversight, management, and internal control.

The NHFB is committed to the effective management of risks and promoting a positive risk culture throughout the organisation. Our approach to risk management is consistent with the Commonwealth Risk Management Policy.

The Commonwealth Risk Management Policy sets out the expectations for managing all risks associated with undertaking Government business through nine elements which are to be incorporated in an appropriate system of risk oversight:

1. Establishing a risk management policy
2. Establishing a risk management framework
3. Defining responsibility for managing risk
4. Embedding systematic risk management into business processes
5. Developing a positive risk culture
6. Communicating and consulting about risk
7. Understanding and managing shared risk
8. Maintaining risk management capability
9. Reviewing and continuously improving the management of risk.

These elements are addressed within the NHFB's Risk Management Policy and Framework, detailing our commitment to managing our business operations in a professional and efficient manner, supporting the achievement of NHFB's strategic objectives, statutory obligations, and ethical standards.

# Risk Management Policy

## Overview of the NHFB's approach to risk management

Our Vision is to *'improve transparency of public hospital funding in Australia'* and our Purpose is to support the obligations of the Administrator of the National Health Funding Pool (the Pool) through best practice administration of public hospital funding.

Our approach in managing risk<sup>1</sup> is therefore defined around identifying and managing the risks that would prevent us from successfully achieving our strategic objectives and fulfilling our Vision and Purpose.

Risk management is principles-based and is particularly effective when there is an integration of risk-based decision making into an organisation's governance, planning, policies, reporting, values, and culture (ISO 31000:2018 Risk Management – Guidelines).

Effective risk management is an important component of the NHFB's governance arrangements and an integral part of the NHFB's processes, including strategic planning, business planning and project and change management processes. The NHFB identifies and manages risk to its objectives and works with the Administrator to assess and monitor broader risks to the successful operation of the Pool.

Effective risk management within the NHFB has the following features:

- The NHFB Executive leads the strategic risk conversations with emphasis on providing leadership, defining accountability and responsibilities, and promoting ethical conduct and professional risk competence throughout the NHFB.
- Clear alignment between the NHFB's strategic risks, business objectives, risk controls and treatments with the NHFB's Risk Tolerance Statement.
- All staff understand risk and their roles and responsibilities in managing risk within the NHFB, including shared risks with other entities.
- A systematic reviewing, monitoring, and reporting regime as part of our ongoing management of identified risks and risk controls to ensure we have a holistic and up to date view of our risk environment.
- Effective communication strategies and stakeholder engagement that supports a positive risk aware culture that allows the NHFB to identify and manage new and emerging risks, including shared risks.

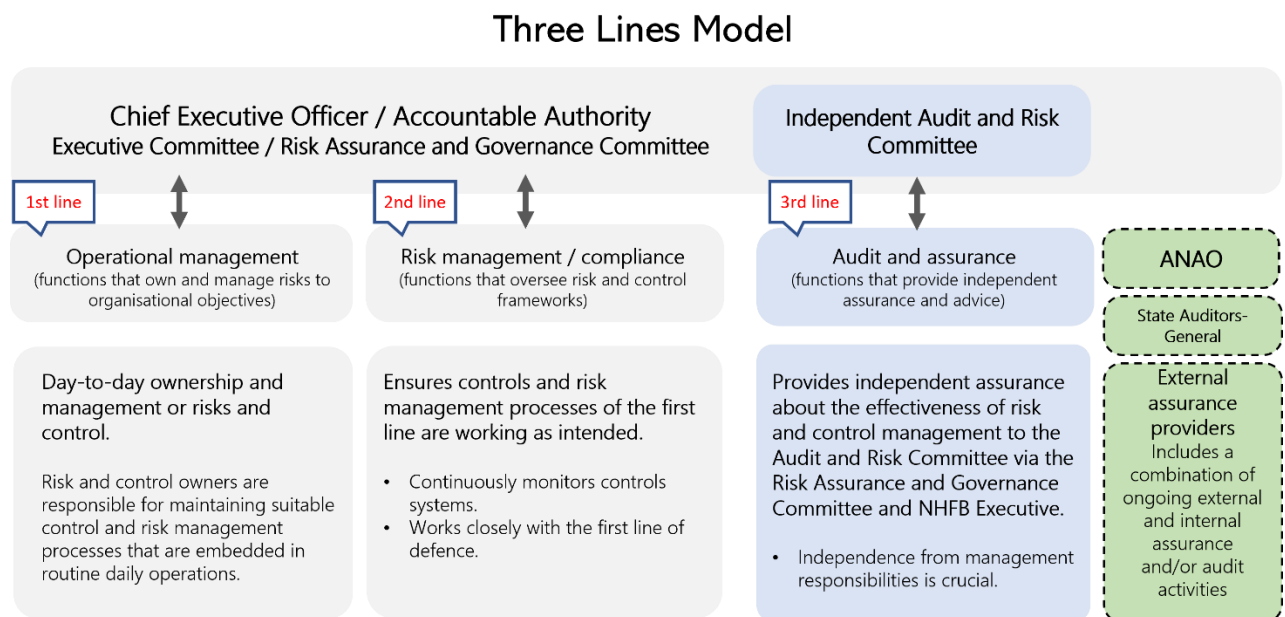
---

<sup>1</sup> The NHFB recognises risk as the possibility of a future event or factors that could adversely impact on achieving planned outcomes or stated objectives.

Additional mechanisms that support our risk management practices:

- A revised Three Lines Model (revised March 2021) which details the structured interactions between the key areas in the NHFB responsible for maintaining effective alignment, collaboration, and accountability to achieve our strategic objectives. It confirms the roles of the Executive leadership team, the supporting internal Risk Assurance and Governance Committee (RAGC) as well as the oversight by the independent Audit and Risk Committee. Independent assurance is maintained (Third line) through audit and external providers, including the ANAO.
- The NHFB Risk Register documents our current identified risks and provides the platform for managing those risks via controls and new treatment strategies. The Risk Register identifies the Risk Owners and the current controls and proposed treatments for each risk and where necessary, any recovery strategies required. The Risk Register also includes the NHFB's Near Miss log, which captures near misses that occurred, and may have impacted on one or more of our strategic risks.
- The NHFB Risk Tolerance Statement sets out the amount of risk the NHFB is prepared to accept to meet our objectives. Some identified risks may have a higher tolerance level, signifying our confidence in managing those risks because the impacts do not represent an immediate threat to the achievement of our objectives. Other risks, such as those relating to incorrect calculations and payments or illegal activity such as fraud, carry a lower tolerance because the consequences of those risks are too high for us to accept.

**Figure 1 Three Lines Model**



## Defining responsibilities for managing risk

The NHFB Chief Executive Officer (CEO) champions a culture of active risk management within the NHFB, and the Executive leadership team supports the adoption of a structured and consistent approach to risk management.

It is the Executive's responsibility to provide leadership in promoting and disseminating a positive risk culture by leading strategic risk discussions, pursuing, and addressing shared risks with internal stakeholders and external entities. The Executive and staff manage risk in accordance with the NHFB's Risk Management Instructions.

For each risk, risk control and risk treatment there is a responsible and accountable owner who assesses, monitors, and reports on all relevant developments with the controls and treatments, which are recorded in the NHFB Risk Register.

A quarterly Risk Management Performance Report is prepared for the Executive Management Committee, the Risk, Assurance and Governance Committee and independent Audit and Risk Committee highlighting any significant issues, near misses, new and emerging risks and the status of any new or ongoing treatments being implemented.

It is essential that all staff, including contractors, understand their responsibilities to ensure the ongoing effectiveness of the NHFB's risk management process. Staff are provided training<sup>2</sup> as required to assist them in further understanding their obligations and responsibilities.

All contracts must include clauses that ensure that personnel working with the NHFB, and the Administrator, comply with the NHFB Risk Management Policy and Framework.

---

<sup>2</sup> On-boarding process for all staff includes the creation of a SAP profile which initiates mandatory induction and e-learning modules allocated to the staff member to complete.

**Table 1 Outlines the key risk management roles and responsibilities.**

Role	Responsibilities
<b>Administrator</b>	<ul style="list-style-type: none"> <li>Alert the CEO to risks arising from the Administrator's duties in relation to the operation of the National Health Funding Pool (NHFP)</li> <li>Work with the NHFB to assess and mitigate risk to the successful operation of the NHFP</li> </ul>
<b>Audit and Risk Committee (ARC)</b>  (independent external assurance)	<p>In providing advice on the appropriateness of the NHFB's system of risk oversight and management, the Committee is to:</p> <ul style="list-style-type: none"> <li>Review whether NHFB management has in place a current and sound enterprise risk management framework and associated internal controls for effective identification and management of the NHFB's and Administrator's risks</li> <li>Satisfy itself that management has followed a sound approach in managing the NHFB's highest risks including those associated with individual projects</li> <li>Assess the impact of the NHFB's risk management framework on the NHFB's control environment</li> <li>Review the process of developing and implementing the NHFB's fraud and corruption control arrangements and satisfy itself that the NHFB has appropriate processes and systems in place to detect, capture and effectively respond to fraud and corruption risks</li> <li>Review reports on fraud from management that outline any significant or systemic allegations of fraud, the status of any ongoing investigations and any changes to identified fraud risk in the NHFB; and</li> <li>Satisfy itself that the NHFB has appropriate systems and procedures in place to identify the NHFB's key assurance arrangements and that it is reviewed annually.</li> </ul>
<b>NHFB Chief Executive Officer (CEO)</b>	<ul style="list-style-type: none"> <li>Ensure appropriate governance arrangements are in place, including an effective system of risk management.</li> <li>Champion risk management in the organisation.</li> <li>Develop an annual Risk Tolerance Statement and approve the NHFB and NHFP risk tolerance level, the latter in consultation with the Administrator.</li> <li>Promote and ensure an appropriate culture is in place to foster an effective and committed approach to risk management.</li> <li>Review and act in an appropriate way on recommendations from the Risk, Assurance and Governance Committee and the independent Audit and Risk Committee.</li> <li>Approve the Risk Management Policy and Framework and associated instructions, procedures, and tools.</li> </ul>



Role	Responsibilities
<b>Directors</b>	<ul style="list-style-type: none"> <li>▪ Ensure the Risk Management Policy and Framework is embedded effectively as part of day-to-day business activity in their respective Sections.</li> <li>▪ Review the Section's identified risks and where necessary prepare an assessment and evaluation of the existing controls and proposed treatment schedule.</li> <li>▪ Ensure all staff are adopting the NHFB's Risk Management Policy and Framework as intended.</li> <li>▪ Ensure all staff are aware of their obligations and responsibilities as per the Risk Management Instructions.</li> </ul>
<b>Executive Leadership Team</b>	<ul style="list-style-type: none"> <li>▪ Actively foster and support staff awareness and understanding of the NHFB's governance arrangements, including risk management.</li> <li>▪ Lead the organisation by example by promoting and observing best practice corporate governance, including risk management practice (such as the regular identification, monitoring and review of risks).</li> <li>▪ Review and assess the current and planned approach to managing significant and critical risk areas.</li> <li>▪ Lead the discussion on risk management.</li> <li>▪ Coordination and oversight of audit and assurance activities including the review of the effectiveness of risk controls and treatments.</li> </ul>
<b>Risk, Assurance and Governance Committee (RAGC)</b>	<ul style="list-style-type: none"> <li>▪ Ensure that the NHFB has in place a risk management framework with associated policies and procedures.</li> <li>▪ Review and evaluate the effectiveness of the NHFB's Risk Management Policy and Framework, Risk Management Instructions and Risk Tolerance Statement.</li> <li>▪ Monitor, review and evaluate the effectiveness of NHFB's Risk Register including internal controls and proposed new treatments.</li> <li>▪ Monitor and review the NHFB's risk performance reporting.</li> </ul>

Role	Responsibilities
<b>Director</b>  <b>Policy, Planning and Performance</b> <i>(with assistance from the Risk and Corporate Services Officer)</i>	<ul style="list-style-type: none"> <li>Supports contributions to the NHFB risk assessment process and risk management plans through regular contact and with input from relevant risk managers, risk control / risk treatment owners.</li> <li>Maintains the NHFB Risk Register and Near Miss Log, which includes providing and maintaining an appropriate information storage system – such as TRIM.</li> <li>Encourage and support of a risk-based culture within the NHFB through regular communication and consultation with stakeholders.</li> <li>Review and maintain the Risk Management Policy and Framework, the Risk Management Instructions, and associated documents on an annual or 'needs' basis (usually following a risk review).</li> <li>Undertake the Comcover Benchmarking Survey to track progress towards suitable and agreed risk maturity for the NHFB.</li> <li>Prepare the Quarterly Risk Performance Report and follow-up on outstanding action items arising from the Audit and Risk Committee.</li> </ul>
<b>Risk Owners</b>  <b>Primary point of contact for the allocated risk(s) associated with their area of responsibility.</b>	<ul style="list-style-type: none"> <li>Responsible for the active monitoring of Strategic Risks, ensuring that they are accurately reflected in the relevant Risk Register and should the risk change significantly, escalate appropriately. Specific responsibilities include identifying changes in the environment impacting on the risk, assessing (with the relevant risk control owners) the ongoing effectiveness of controls, and progressing agreed treatments.</li> <li>Risk owners may also be responsible for managing the 'operational' risks and controls associated with the Strategic Risk(s) or the work of the team.</li> </ul>
<b>Risk control / Risk treatment owners</b>	<ul style="list-style-type: none"> <li>Monitor and arrange regular assessment of effectiveness of risk controls, including verification and assurance of the key critical controls, feeding into the risk review process.</li> <li>Develop suitable treatments and/or strategies to align the residual risk with the defined risk tolerance.</li> <li>Oversee the risk treatment implementation and report on progress</li> </ul>
<b>Project / Procurement Managers</b>	<ul style="list-style-type: none"> <li>Undertake a risk assessment and, if required, prepare a Risk Management Plan prior to the commencement of a project or procurement (over \$80,000), and maintain the currency of the plan for the tenure of the project / procurement.</li> </ul>
<b>All NHFB staff (including employees, contractors, and consultants)</b>	<ul style="list-style-type: none"> <li>Through their actions, promote a positive risk management culture.</li> <li>Undertake appropriate risk awareness training as required.</li> <li>Escalate or report near misses, risks/issues and recommendations to the relevant Director or Executive.</li> <li>Always observe the Australian Public Service (APS) Code of Conduct and all NHFB policies and procedures, including this Risk Management Policy and Framework and the Risk Management Instructions.</li> </ul>

# Risk Management Framework

The NHFB Risk Management Framework was developed consistent with *‘Element Two – Establishing a risk management framework’* under the **Commonwealth Risk Management Policy**. The Framework is designed to provide the NHFB CEO, Administrator and all NHFB staff with the assurance on the integrity of NHFB’s risk management processes and its compliance with Government mandated policies and requirements, as outlined in the Introduction. The Framework also supports the NHFB’s Accountable Authority Instructions (*under 4.1 Risk Management*), by promoting and providing guidance on risk management practices across the organisation.

The Framework outlines the NHFB’s commitment and approach to implementing a positive risk culture and the arrangements for implementing, monitoring, reviewing and continually improving risk management throughout the NHFB.

The range of functions undertaken by the NHFB highlights specific, yet interlinked risk pools:

- Risks to the NHFB as an entity. Each NHFB risk has a Risk Manager who leads the discussion at Executive meetings on the progress of controlling and mitigating the risk and the implementation of proposed treatments.
- Risks to the successful operation of the Pool, whether they might directly or indirectly impact on the NHFB. This would also include risks associated with funding calculations and the determination of funding entitlement.
- Operational and project risks. Operational risks are those which may affect the objectives of one or more business areas. Examples include security, fraud or project risks, the latter being those which could adversely affect the time, cost, scope, or outcomes of a project. Procurement risks are captured at the project level.
- Shared risks are those which require the responsibility for management and control of the risk to be shared with other agencies. Although the management of these risks is by their nature shared, the NHFB has a leading role in identifying, assessing, and supporting their management where it impacts on the Pool. Any assessment of these risks should consider the NHFB’s responsibilities for their management, and the responsibilities of other stakeholders.

The NHFB works with the Administrator to review the overall risk environment to identify shared risks, which involves engagement with relevant key stakeholders. The NHFB monitors these risks through effective strategic management, stakeholder engagement, service level arrangements with providers and seeks legal advice where necessary.

## Key elements of managing risk

The NHFB's approach to risk management is summarised by the following key elements:

- Development and maintenance of a suite of documents for managing risk, including the Risk Management Policy and Framework, the Risk Management Instructions, and the annual Risk Tolerance Statement.
- Identification, assessment, and targeted strategies to control risk within accepted levels of risk tolerance, documented in the Risk Register.
- **Embedding risk management into management processes**, including corporate, business and project planning.
- Identifying suitable persons within NHFB to assume the **responsibility** and accountability for risk stewardship and the ownership of risk controls and risk treatment.
- Continuous improvement in the ability to identify and assess emerging risks, shared risks and environmental factors impacting on risk, respond to near misses and assessing the effectiveness of risk controls and treatments<sup>3</sup>.
- Independent oversight and assessment of risk management, including risk controls and the Risk Management Performance Reports by the independent Audit and Risk Committee
- Development and maintenance of a positive culture that is fully supportive of effective risk management.
- Suitable risk management training for all staff.
- Identifying and implementing best practice, fit-for-purpose risk management for a small agency.

---

<sup>3</sup> The NHFB uses external providers to undertake regular and ongoing audit and assurance activities across the CCM, Payments System and other risk areas such as fraud, payroll, credit card uses, travel and privacy.

## The NHFB's risk culture

Risk culture is the set of shared attitudes, values and behaviours that characterise how an entity considers and addresses risk in its day-to-day activities.

A positive risk culture promotes an open and proactive approach to managing risk that assesses both threats and opportunities and how risk is identified, communicated, and managed across all levels of the entity. The key drivers of the NHFB's risk culture include:

**Awareness:** The NHFB's risk tolerance is widely understood and used in the management and the governance arrangements of the agency. The NHFB Risk Management Policy and Framework is intended to play a key component of every day decision making processes.

**Leadership:** Risk awareness is demonstrated at all levels within the NHFB and in its key business processes. Decision making processes are clear and consistent with risk tolerance and business strategies. Positive risk management is advocated by the CEO and Executive, with decisions made that are consistent and aligned with the NHFB's values.

**Communication and training:** Managing risk forms an important component of the induction process and risk awareness training is conducted on an annual basis. All staff have access to formal risk and awareness training to support and promotes a positive risk culture.

**Responsibility:** NHFB staff at all levels are expected to undertake appropriate risk training and adopt positive risk awareness in their day-to-day activities and inform risk owners and risk control owners of any relevant developments that they may become aware of.

The NHFB encourages a positive risk culture through:

- Reporting realised risk events and near misses and analysing causes through lessons learned
- Incorporating measures of risk management effectiveness in individual's performance agreements
- Leaders and managers at all levels modelling good risk management behaviours
- Routine messaging to all employees on the importance of effectively and actively managing risk and the support mechanisms available
- The availability and utilisation of relevant risk awareness training.

## Communicating and consulting on risk

Effective communication, collaboration, and consultation with relevant internal and external stakeholders about risk is critical to ensure a transparent, complete, and timely flow of information between decision makers.

As part of this important process, the NHFB works to identify all relevant stakeholders, including their objectives, strengths, vulnerabilities, and agendas. Engaging as early as possible with stakeholders ensures that both the NHFB and its stakeholders have clearly defined objectives and a shared understanding of the process, so that they can work successfully towards a mutually beneficial outcome.

The NHFB has and will continue to maintain and update an understanding of the following two areas of risk context as part of the risk assessment process:

- **External** – things outside the NHFB which might create, influence or control risk. For example, business relationships, cultural expectations, commercial pressures or interests, political environments, legislative changes, new policy proposals and priorities and the intentions of external stakeholders
- **Internal** – things inside the NHFB which might create, influence or control risk, such as internal stakeholders, culture, resources, systems and processes, organisational goals, and objectives.

The NHFB's internal and external stakeholder engagement, includes effective communication and consultation on managing risk and is largely achieved through:

- Internal risk workshops with the Executive and staff (held regularly as part of overall risk reviews)
- Executive Committee meetings
- Risk, Assurance and Governance Committee meetings
- Independent Audit and Risk Committee meetings
- Meetings of the Administrator's Jurisdictional Advisory Committee and the IHACPA Jurisdictional Advisory Committee (which involve all jurisdictions)
- Monthly Commonwealth roundtable meetings
- Regular engagement with the Administrator
- Identifying and discussing shared risks with strategic stakeholders – for example Independent Health and Aged Care Pricing Authority (IHACPA), Department of Health, Disability and Ageing (Health), Reserve Bank of Australia (RBA), and the Commonwealth Treasury
- New starter NHFB (Approach to risk management) presentations.

## The NHFB's risk management capabilities

The NHFB has strategies in place that focus on increasing the understanding, capacity, and capability of all staff to effectively manage risk. All new NHFB staff receive face-to-face risk induction to understand the agency's risk environment and how the NHFB expects them to identify, treat and manage risks, including:

- Defined and understood management and planning arrangements that explicitly consider risk
- Reporting and recording near miss events as soon as they are identified
- A defined suite of risk management documents and associated processes which are regularly reviewed and updated
- Up to-date and relevant risk information stored in a Risk Register, and
- Continuous capability improvement through regular review and assessment of risks, best practice benchmarking and risk networking with other organisations through relevant Communities of Practice.

## Identifying and managing shared risk

Shared risks are those risks relating to the responsibilities and objectives of the NHFB and the Administrator that extend beyond the NHFB and the Administrator which require shared oversight and management. The NHFB engages with the Commonwealth, States, and Territories, and the National Health Reform Bodies and other stakeholders through committees, forums, and workshops to identify shared risks to ensure it has a good understanding of the controls and treatments being implemented.

The NHFB has close working relationships with the Independent Health and Aged Care Pricing Authority (IHACPA), the Australian Commission of Safety and Quality in Health Care (ACSQHC) and the Australian Institute of Health and Welfare (AIHW), the Department of Health, Disability and Ageing (Health), the Reserve Bank of Australia (RBA) and Commonwealth Treasury. The NHFB endeavours to ensure that shared risks are identified, assessed, and mitigated accordingly in cooperation with these stakeholders.

Other important relations with a broader range of Commonwealth, State and Territory agencies involve obtaining cross-agency input and assistance particularly to ensure full clarity in the data and information requirements of NHFB and the Administrator.

## Embedding risk management into business processes

The objective of effective risk management is to improve or optimise organisational performance. Identifying, assessing, and managing risk is an integral element of the overall management capability of an entity and must include strategic planning, the establishment of governance arrangements, policy development, program delivery and decision making.

To support effective governance and assurance, all identified risks have controls and treatments which are clearly defined, owned, and aligned across the **Three Lines Model**:

- Operational Management
- Risk Management / Compliance
- Audit (internal and external Assurers)

**Table 2 Identifies the business processes within the NHFB, including where and how risk management principles or elements have been embedded.**

Business Process	Risk Management principles or elements
<b>Strategic Planning (Strategic Direction and Corporate Plan)</b>	<p>During strategic and corporate planning processes, risk is considered:</p> <ul style="list-style-type: none"> <li>▪ NHFB and NHFP environment and risk profile is assessed and updated to provide context to the Strategic Plan.</li> <li>▪ Any new strategic or corporate initiatives are assessed against the impact on existing risks and controls, and in terms of any new risks that are associated with the initiative.</li> </ul>
<b>Business Planning</b>	<p>Risk management is embedded in all business planning including:</p> <ul style="list-style-type: none"> <li>▪ Fraud and Corruption Control Plan</li> <li>▪ Security Risk Management Plan (including information security)</li> <li>▪ Workplace Health and Safety.</li> </ul>
<b>Governance Arrangements</b>	<p>The foundation for our governance arrangements is a Corporate Governance Framework that embodies the APS Values and Code of Conduct – Impartial, Committed (to service), Accountable, Respectful, Ethical and Stewardship – in our management practices, including committees, business planning, risk and fraud management, audit and assurance activities and policies and guidelines.</p>
<b>Procurement</b>	<p>Risk assessment completed on all procurement over \$80,000.</p>
<b>Project Management</b>	<p>Project Risk Plan and Register established for all projects.</p>
<b>Policy Development</b>	<p>New Policy Proposal risk assessment process undertaken.</p>
<b>Decision Making</b>	<p>All staff to comply with the principles of risk management in all decision making.</p>



Business Process	Risk Management principles or elements
<b>Annual reports</b>	The NHFB's approach to risk management included in the NHFB Annual Reports.
<b>Financial</b>	<p>The principles of risk management apply to:</p> <ul style="list-style-type: none"> <li>▪ Financial delegations</li> <li>▪ Financial controls</li> <li>▪ Preparation of Financial Statements and associated reports.</li> </ul>
<b>Human Resources</b>	The principles of risk management apply to Human Resource delegations.
<b>Learning and Development</b>	<p>Formal risk management awareness training accessible through Health's e-learning (Success Factors).</p> <p>Utilisation of the Department of Finance (Comcover) risk management education <b>program</b><sup>4</sup>, including appropriate training in risk management for staff to facilitate the NHFB's risk management arrangements.</p> <p>Ongoing, informal risk management information sessions provided to staff as required.</p>
<b>Internal assurance</b>	<p>Review the alignment of NHFB activities against the requirements of the Risk Management Policy and Framework and Risk Management Instructions as required and review of the risk management process and approach as part of internal assurance processes.</p> <p>Review and assess evidence of the effectiveness of risk controls.</p> <p>Implement relevant risk audit and assurance recommendations arising from the Audit and Risk Committee.</p>
<b>Individual Performance Development Plans</b>	<p>The engagement and participation of all staff in the discussion on risk is an important component in building, supporting, and maintaining an organisational risk management culture.</p> <p>The NHFB conducts risk reviews annually and all staff have access to Health's e-learning for risk-related courses (such as Privacy, Integrity, Fraud and Security).</p> <p>Risk performance is an important part of staff reviews.</p>

<sup>4</sup> These courses are now being delivered through the APSC Academy

## Risk performance reporting

The NHFB Risk Performance Report is presented quarterly to the Executive, the Risk Assurance and Governance Committee and at each Audit and Risk Committee meeting, highlighting the NHFB's risk performance across the following:

- Managing risks within tolerance as per the NHFB Risk Tolerance Statement.
- The status of new treatments across all risks, including a brief commentary where risks are outside tolerance.
- Any additional treatments proposed including treatments that enhance the effectiveness of existing controls.
- Risk rating variations arising from risk reviews (using Bow Tie methodology<sup>5</sup>).
- New and emerging risks.
- Near misses, risks realised, and the lessons learned.
- Reviewing, verifying and assurance of the critical controls in place.

The Quarterly Risk Management Performance Report is also discussed and reviewed with all staff in monthly Organisational Performance meetings.

---

<sup>5</sup> An example of the Bow tie methodology (risk assessment worksheets) can be found in the NHFB's Risk Management Instructions.

## Reviewing and improving risk management

Effective management of risk is a process of continuous improvement, requiring regular reviews and evaluation mechanisms.

The NHFB's Risk Register and Risk Management Policy and Framework and associated processes are reviewed regularly so they remain effective and current and are relevant to both its internal and external environment. Regular monitoring and review of risk documentation ensures the NHFB maintains a culture of continuous improvement.

Using the Bow Tie methodology, the NHFB also regularly reviews the current risk environment to ensure risks and risk control are relevant, effective and that tolerance levels are being maintained within agreed tolerances.

The NHFB participates in a **Risk Management Benchmarking Program** to assess the maturity of our risk framework against the nine elements of the Commonwealth Risk Management Policy (**CRM Policy**). These biennial survey findings are used to inform how successfully we have integrated risk management into NHFB core business activities and processes and prioritise strategies to ensure our risk management maturity remains on track, is best practice and fit-for-purpose for a small agency.

Our overall findings in the benchmarking surveys are reported in the Quarterly Risk Management Performance Report when the results are available.

The NHFB utilises the Australian National Audit Office (ANAO) performance audits to gauge common aspects of administration or compliance across relevant themes such as, risk management, fraud and corruption, IT security, credit card (mis)use, grants management, business continuity, etc., Recommendations arising from ANAO performance audits applied across APS agencies, can help determine whether the NHFB's own performance in similar areas is meeting best practices or suitable standards, and provides the agency with opportunities to improve where it can.

## Use of Artificial Intelligence (AI) risks

While the technology behind artificial intelligence (AI) models has been in existence for many years, the rapid development of advanced AI has the potential to support government entities to drive efficiencies and productivity growth, to improve service delivery and to deliver on their objectives more effectively. Poor implementation of AI use, however, could risk eroding trust in the public service or cause harm.

Given the breadth of AI, there is no one-size-fits-all approach<sup>6</sup> to AI governance, therefore, good governance and robust assurance arrangements are critical in supporting the delivery of ethical and lawful AI.

The NHFB seeks to enhance the quality and efficiency of our services through our commitment to innovation and excellence. The NHFB may pursue utilising AI to take advantage of the benefits the technology provides while carefully managing the risks to support our vision of improving the transparency of public hospital funding in Australia.

The NHFB is committed to using AI responsibly and transparently, ensuring that any AI initiatives align with our values and are in the best interests of the public. As the NHFB is reliant on the Department of Health, Disability and Ageing for its ICT infrastructure and associated Cyber security

---

<sup>6</sup> The Organisation for Economic Co-operation and Development (OECD) has highlighted different AI systems bring different benefits and risks. In comparing virtual assistants, self-driving vehicles and video recommendations for children – benefits and risks of each are very different. These specificities require different approaches to policy making and governance.

arrangements, we will continue to work closely with our Shared Services provider and use AI in accordance with applicable legislation, regulations, frameworks, policies and best practice.

At the time of this policy's approval, the NHFB **does not utilise** public facing AI applications that involve direct public interaction or significant public impact. (See our **Transparency Statement** for updates).

While the use of AI can bring many benefits and opportunities, the NHFB recognises there are a broad range of risks when using AI to provide insights through analytics and enhancing workplace productivity to enable efficiency across our service delivery and particularly our data analysis activities under the NHR Act. These include:

- There is a risk that the NHFB (or those the NHFB shares data or analysis with) does not lawfully or appropriately use its data and analysis
- Privacy concerns due to the sensitivity of the data being manipulated or transformed by the (AI) system
- Security concerns due to the sensitivity or classification of the data being manipulated or transformed by the (AI) system
- Intellectual property concerns due to the (AI) system manipulating, transforming or reproducing material for which a 3<sup>rd</sup> party owns copyright.

When considering using AI for NHFB business activity, it is important that a risk assessment is undertaken that is specific to the use case – that is, the outcomes expected for using AI tools are consistent with the NHFB's Vision and Objectives.

Other use of AI related information:

- **Policy for the responsible use of AI in government**
- **Interim Guidance on government use of public generative AI tools**

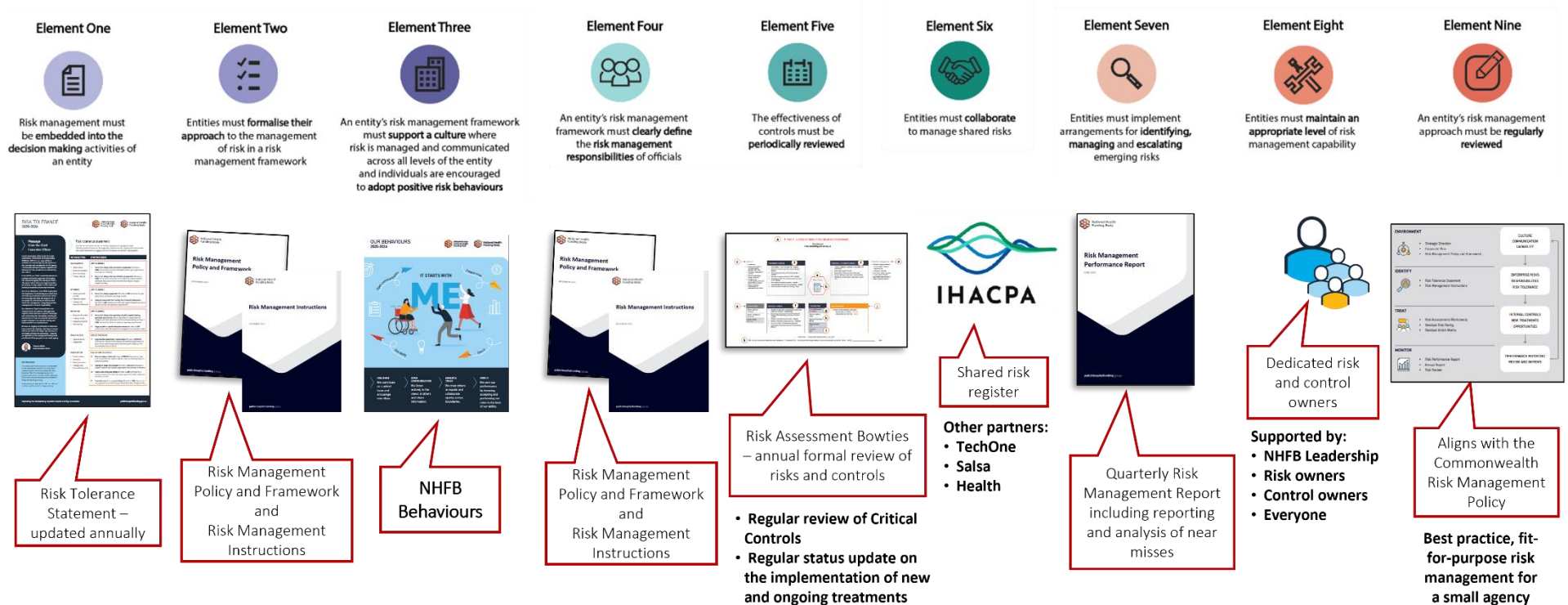
## Supporting information

The NHFB Risk Management Policy and Framework complements and/ or supports:

- The NHFB's Risk Management Instructions
- The NHFB Risk Tolerance Statement
- The Fraud and Corruption Control Plan
- The NHFB Security Risk Management Plan
- The Privacy Policy
- The Privacy Management Plan
- Public Interest Disclosure Policy

# NHFB risk management elements on a page

**Figure 2** Shows how the NHFB aligns its approach to risk management with the nine elements in the Commonwealth Risk Management Policy.



# Risk approach overview

