NDIA Risk Management Strategy

Ministerial Council approved 9 February 2024

ndis.gov.au

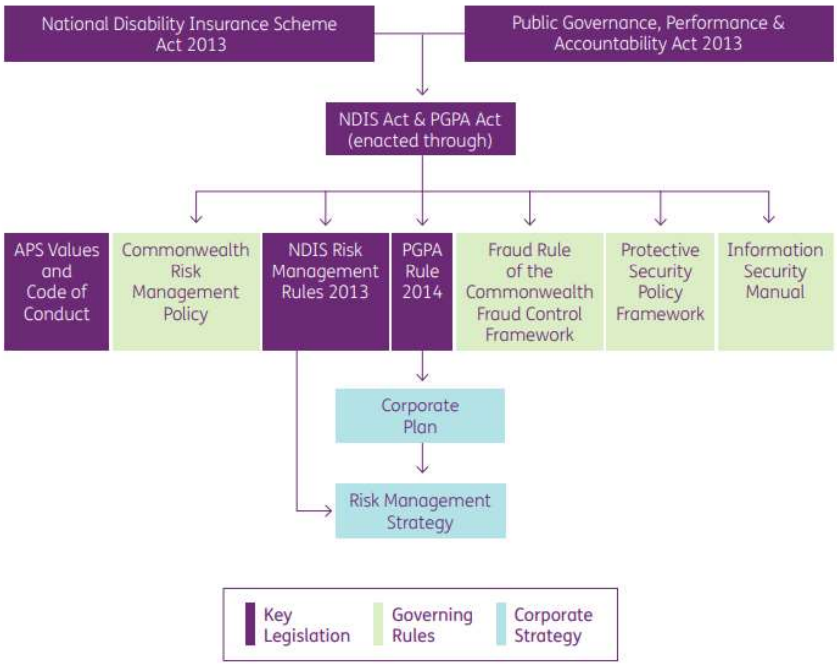
1. Purpose and context

The National Disability Insurance Agency (**NDIA or the Agency**) invests in risk management to support its statutory function of delivery of the Scheme in accordance with the *National Disability Insurance Scheme Act 2013*, Corporate Plan objectives, and delivery of a sustainable Scheme. The Risk Management Strategy (**RMS**) outlines how the Agency will manage the material risks that arise as part of our operations and initiatives.

As a Corporate Commonwealth Entity, the NDIA has a range of legislative obligations that inform our risk management approach. The RMS has been developed to meet the Agency's obligations under Commonwealth law, including the:

- *Public Governance, Performance and Accountability Act 2013*
- *National Disability Insurance Scheme Act 2013*
- *National Disability Insurance Scheme – Risk Management Rules 2013* (the **Rules**).

The legislative and risk governance landscape is summarised below.



The RMS aims to embed the following risk management principles in the Agency's operations:

- early and proactive identification, mitigation, and escalation of risk for awareness/ management, taking account of emerging and shared risks
- systematic consideration of risk in business planning and decision making
- strong risk leadership and designation of operational managers as Risk Owners, supported by independent Risk Specialists
- a control environment that is actively monitored and enhanced
- active consideration of partner performance and third-party risks
- robust processes and systems that support compliance, assurance, and integrity

- a positive risk culture sustained through ongoing maturity and capability uplift.

2. Our risk assessment process

The overall approach is for uncertainty, opportunity, and threats to be identified, assessed, managed, and monitored within the planning and execution levels of the Agency, including at Group, Divisional, Branch (where risks could impact the ability to plan and meet business objectives), and at an individual level.

2.1 Risk management process

The Agency's risk management artefacts include information and tools to provide guidance on the identification, assessment, management, monitoring, and reporting of risks. Key risk assessment tools are accessible on the Agency's intranet, including risk management process guidance and risk assessment criteria.

The Agency's risk management process is a continuous cycle and comprises the following inter-related components:

- identify key risks
- assess current internal controls, likelihood, and consequence of each risk
- manage any additional actions required to mitigate the risk
- monitor and report on the risk profile and performance
- learn and share from experience.

2.2 Risk management declaration

In accordance with the Rules, the Board will provide the Ministerial Council with an annual Risk Management Declaration. The Chief Risk Officer and Chief Executive Officer will support the Board declaration by completing an annual risk maturity self-assessment in accordance with the Board approved Risk Maturity Assessment Methodology.

2.3 Risk classification

The Agency classifies its material risks into the following categories:

- **Strategic risks –** risks that might significantly impact the delivery of the Scheme
- **Enterprise risks –** risks that have the potential to span across the Agency, requiring active management by multiple groups and/ or a whole-of-Agency response
- **Payment risks –** risks associated with Scheme payments, fraud and non-compliance
- **Regulatory risks –** risks associated with legislation / regulatory obligation compliance

- **Operational risks –** risks associated with the delivery of services and the day-to-day business activities of the Agency, including security risks and emergency and business continuity planning and response
- **Project risks –** delivery and delivered risks inherent in, and stemming from, key strategic or business initiatives.

2.4 Risk appetite and tolerances

The Agency's risk appetite will be reviewed and set by the Board on an annual basis. The Agency Risk Appetite Statement articulates how a risk appetite is applied across the key operational elements of:

- People
- Financial sustainability
- Fraud
- Stakeholder confidence and trust
- Legislative obligations
- Information communication technology.

The Agency sets annual quantitative thresholds (tolerance ranges) through the performance metrics assigned to the above risk classifications (e.g., strategic risk performance metrics, incident and regulatory escalation thresholds, and group key performance indicators).

Performance metrics are monitored on a monthly basis and reported to Senior Executives and/or governing committees on a quarterly basis via the Chief Risk Officer Report. Material non-conformances are escalated to relevant Executives when identified and reported to the Strategic Leadership Team.

3. Our strategic risk management approach

3.1 Governance and accountability arrangements

***Our Objective:* The Agency will maintain comprehensive risk governance, with regular communication and escalation through to the Strategic Leadership Team and Board.**

NDIA Board – The Board is ultimately responsible for overseeing the establishment of an effective Agency risk management approach. The Board fulfils its responsibilities with advice and support from the Risk and Audit Committees.

Strategic Leadership Team – The Agency maintains strong strategic oversight of uncertainty, opportunity and risk through its Strategic Leadership Team led by the Chief Executive Officer.

Chief Risk Officer – The Strategic Leadership Team is supported by the Agency's Chief Risk Officer in the monitoring of strategic, enterprise, operational, regulatory and project risks, and the provision of independent assurance and audit.

Risk and Control Owners – Senior Executive Staff are the risk and control owners and responsible for the identification, management, monitoring, and escalation of risk exposures.

All staff in the Agency have a responsibility to be risk aware, report any identified risks, and take risk mitigation actions as appropriate. Specific roles and responsibilities are detailed in **Appendix A.**

3.2 Risk Management Framework

***Our Objective**: The Agency will support prudent and sound risk management outcomes through a robust risk management framework.*

An annual implementation plan will facilitate the operationalisation of the RMS and ongoing risk maturity, and will include a continuous improvement approach to:

1. strengthening Agency controls
2. enhancing Agency fraud and compliance response
3. further embedding risk management in the operating environment
4. risk management capability and capacity uplift.

The Agency's risk management approach will be further articulated in enterprise-level risk, assurance, fraud and corruption prevention, and security management plans.

The Agency will utilise a centralised risk management system (Insight) to capture, manage, analyse, and report material risk, control, and treatment data.

3.3 Controls and treatments

***Our Objective**: The Agency will continue to strengthen internal control design and assurance.*

The Agency will maintain an effective internal control environment by designing and implementing controls and treatment actions that directly impact identified risks. Risk Owners will be responsible for developing and implementing treatment plans. Completed treatments will be assessed for impact on the control and residual risk environment.

Risk and control owners will undertake reviews of their risk and control profiles and report outcomes on a quarterly basis (or more regularly should the prevailing risk environment warrant).

Assurance activities will facilitate control assessment and review, and the identification of weaknesses and recommendations to increase control effectiveness. Responsibility for implementation of assurance recommendations will reside with the Risk Owner.

3.4 Monitoring and reporting

***Our Objective**: The Agency will continue to support risk-based decision making through proactive risk performance reporting.*

Risk reporting will reflect performance against key risk indicators and threshold tolerances, control effectiveness, and treatment plan activity. Quarterly strategic, operational, fraud and compliance, and regulatory risk performance reports will be presented to the Strategic Leadership Team and Board.

Event-based risk reporting and escalation of issues will occur as appropriate.

3.5 Culture and capability

***Our Objective**: The Agency will continue to mature the risk culture and build capability.*

The Agency will endeavor to build an environment in which risk is openly and honestly discussed. To further enhance risk culture, additional assurance and key insights will come from risk maturity assessments. The Agency will provide regular risk communications and recognise sound risk management practices.

Training and coaching opportunities will be articulated in a risk capability strategy. Accountabilities and performance expectations for risk management will be reflected in position descriptions and the Agency's Performance Framework.

The RMS is published in an accessible format on the Agency's intranet.

3.6 Review

***Our Objective**: The Agency will evolve its risk management strategy consistent with the prevailing risk appetite and strategic settings.*

The RMS will be reviewed annually by the Board. Material amendments will be submitted to the Ministerial Council for approval. As appropriate, the Agency will also commission independent comprehensive reviews of the effectiveness of the risk management framework, including the RMS.

Appendix A – Roles and responsibilities in relation to risk management

Position	Roles and responsibilities for risk management
NDIA Board	• Sets the strategic intent through the corporate plan and determines the strategic risks, risk appetite and risk tolerances • Endorses the Risk Management Strategy • Ensures the Agency maintains an appropriate risk culture • Makes an annual Risk Management Declaration • Regularly monitors performance against risk tolerance settings • Sets commitment to maintaining strong controls and procedures to ensure risk is well managed and obligations are met • Holds the Chief Executive Officer to account for fostering risk management as a strength of the Agency and building a positive risk culture
Audit Committee	• Assists the Board in ensuring there is an appropriate internal control framework for the Agency, the Agency complies with e with legislative obligations and manages interactions with the Australian National Audit Office • Oversees the direction and performance of the Internal Audit Plan
Risk Committee	• Assists the Board in ensuring the Agency has in place systems, policies, and procedures to promote compliance with the National Disability Insurance Scheme – Risk Management Rules 2023 (the Rules) and provides advice to the Board in relation to the Risk Management Declaration • Oversees implementation of the Risk Management Strategy, including regular review of its efficacy • Notifies the Board of any significant breach of, or material deviation from, the risk management strategy or framework
Chief Executive Officer	• Accountable for the Agency's management of uncertainty, opportunity, and risk in the performance and delivery of the Scheme • Champions the focus on risk within the Strategic Leadership Team (SLT) and Senior Executive Staff (SES)
Scheme Actuary	• Assesses the financial sustainability of the Scheme and risks to sustainability, and identifies recommendations to manage and address such risks

Position	Roles and responsibilities for risk management
	• Includes in the annual financial sustainability report commentary on the Agency's risk management arrangements and any recommendations in relation to inadequacies
Strategic Leadership Team (SLT)	• Responsible for implementing an effective risk management approach and culture • Leads risk management by example, drives risk management conversations and communications with staff • Regularly reviews material risks that could impact the Agency and reports risks to the Risk and Audit Committees • Provides feedback to the Agency on risk management strategies, priorities, and incident resolution • Monitors challenges to the Scheme and business integrity and assurance activities • Reviews implementation of risk mitigation and response strategies recommended by internal and external reviews
Chief Risk Officer (CRO)	• Provides an independent and objective review and challenge, oversight, monitoring and reporting of the risk and control environment • Provides advice on risk management framework design • Where necessary, the CRO has independent access to the Risk and Audit Committees to provide risk insight and escalation • Supports Agency executives by monitoring risk, identifying emergent risks, and reporting on management activities
Specialist Risk and Audit Functions	• Supports the CRO in the nominated role under the Rules, with specialist risk management practitioners • Facilitates effective risk, integrity and audit oversight and information for decision making • Provides operational and strategic risk, Scheme integrity and audit advice to the SLT and SES • Sets minimum standards, builds related capability and knowledge, and fosters continuous learning • Provides comfort that expectations and commitments are fulfilled and identify opportunities for improvement • Facilitates and supports front line risk control owners to understand and deliver their responsibilities • Effectively challenges risk activities and decisions that materially affect the Agency's risk and control environment

Position	Roles and responsibilities for risk management
	• Maintains unfettered access to Agency data, staff, and systems to identify and escalate risks, issues and/or control weaknesses • Independently assesses and verifies risk management activities • Delivers the internal audit program to validate and provide assurance that the risk management framework and controls are functioning as designed
Risk Partners	• Supports consistent application of the Agency's risk management framework, processes, and tools • Builds risk management capability through guidance and coaching • Coordinates risk management activities with risk owners • Drives knowledge sharing between risk and business owners
Senior Executive Staff (SES)	• Identifies and manages risks that may impact on Group, Division or Branch objectives • Provides feedback and updates to leadership on risk management in their business area • Provides guidance and direction to staff on risk management expectations
Risk Owners / Control Owners	• Responsible for identifying, assessing, managing, escalating, and recording prevailing and emerging risks and issues, including control and monitoring activities • Provides updates and assurances on actions taken to manage risks, including third-party and shared risks • Develops and executes risk mitigation / control enhancement activities • Uses actuarial monitoring and analytics to identify risks and target assurance activities
All Staff	• Maintains familiarity, and acts in accordance with, the Agency's Risk Management Strategy and framework • Takes accountability for risk management in their day-to-day activities • Facilitates open, honest, and timely escalation of risks and issues • Monitors and responds to risks that may arise in interactions with providers and participants • Uses available training and tools to facilitate the implementation of the risk management strategy • Shares and learns from mistakes and successes