NDIA

Risk Management Strategy

Board approved February 2019

1.1 Purpose

This Risk Management Strategy (RMS) describes the National Disability Insurance Agency's (NDIA or the Agency) approach to managing risks and opportunities arising from the effects of uncertainty.

1.2 Context and overview

The NDIA's purpose is to increase the ability of individuals with a significant and permanent disability to be more independent, and to engage more socially and economically, at the same time as delivering a financially sustainable National Disability Insurance Scheme (NDIS or Scheme) that inspires community and stakeholder confidence. To do that we need to put people with disability at the centre of everything we do, while recognising and respecting the important role played by carers, providers and disability groups.

To achieve this the Agency's Corporate Plan identifies four aspirations and 10 strategic goals as the key to successful delivery of the Scheme. The scale, pace and complexity of change required to implement this reform and achieve these aspirations and goals brings with it considerable uncertainty. In this context the Agency's ability to harness strategic opportunities, and identify and respond to risks, is critical to delivering on its purpose.

This RMS has been developed to meet the Agency's obligations under federal law, including:

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

It also reflects the expectations of the Scheme's contributors expressed in the Statement of Strategic Guidance for the Board, issued by the Council of Australian Government Disability Reform Council on 15 March 2017 to identify strategic risks early and manage risks well by:

- Taking a structured approach to identifying and managing risks
- Developing a sophisticated understanding of the risk interdependencies that could impact delivery of the NDIS
- During transition, escalate important issues urgently.

This RMS has six areas of focus to help build a robust, high-performing, professional and systems-based Agency that continues to improve its practices through:

- Culture and behaviour – we are risk aware and sensitive to financial sustainability and positive participant outcomes
- Operating model and risk governance – ensuring the way we work is contemporary and reflects better practice in risk management and governance
- Leadership – our leaders setting the 'tone at the top' to reinforce the importance of being prepared for risk
- Capability – building the skills and insights of our staff and community partners
- Processes and approach – ensuring a risk lens informs the way we think and act
- Supporting infrastructure – establishing what is needed to operationalise the RMS.

1.3 Publication

This RMS and supporting information, guidance and tools will be published on the Agency's intranet in a fully accessible format. This will ensure our staff and community partners can easily access, use and contribute to the full suite of risk management resources.

1.4 A positive risk culture

Risk culture is the set of shared attitudes, values and behaviours that characterise how our staff and community partners consider risk in their day-to-day activities and decisions.

A positive risk culture promotes an open and proactive approach to managing risk. It balances both the threats and opportunities that emerge from the uncertainty of this nation-building reform.

Put simply, a positive risk culture sees our people doing the right thing – including when no one is looking. It empowers Agency delegates, their team members and community partners to:

- embrace opportunities when making decisions
- take responsibility for reducing unacceptable levels of potential exposure brought about by risk
- feel confident to be able to speak up to escalate their concerns about significant risks and contribute to practical solutions
- be part of a feedback loop, as part of an open, connected and well communicated approach to risk management.

The NDIA requires staff and community partners to adopt the following principles:

1. Take accountability for managing risks and helping colleagues manage their risks
2. Communicate and escalate risks openly, honestly and quickly
3. Consider risks to quality, participant outcomes and financial sustainability when making decisions and taking actions
4. Openly share and learn from mistakes and successes
5. Understand and apply the Agency's risk management principles, processes and reporting.

The Agency has identified four foundational elements to build a strong, positive risk culture. They are:

- Being clear about the culture and behaviours we expect – ensuring our risk principles and expectations are clearly stated and communicated
- Leaders set the tone and establish the right environment – the Agency Leadership Framework sets out the roles and expectations of leaders to be exemplary risk stewards
- Recognition and reinforcement mechanisms – where Agency and community partner employee recognition programs celebrate a positive risk culture, both formally and informally
- Ongoing monitoring of risk culture – through regular maturity assessments.

Assurance and key insights will come from an annual risk culture survey, regular pulse surveys and tracking performance results against key performance indicators that include training, application of risk management processes and demonstration of the preferred behaviours.

1.5 Operating model and risk governance

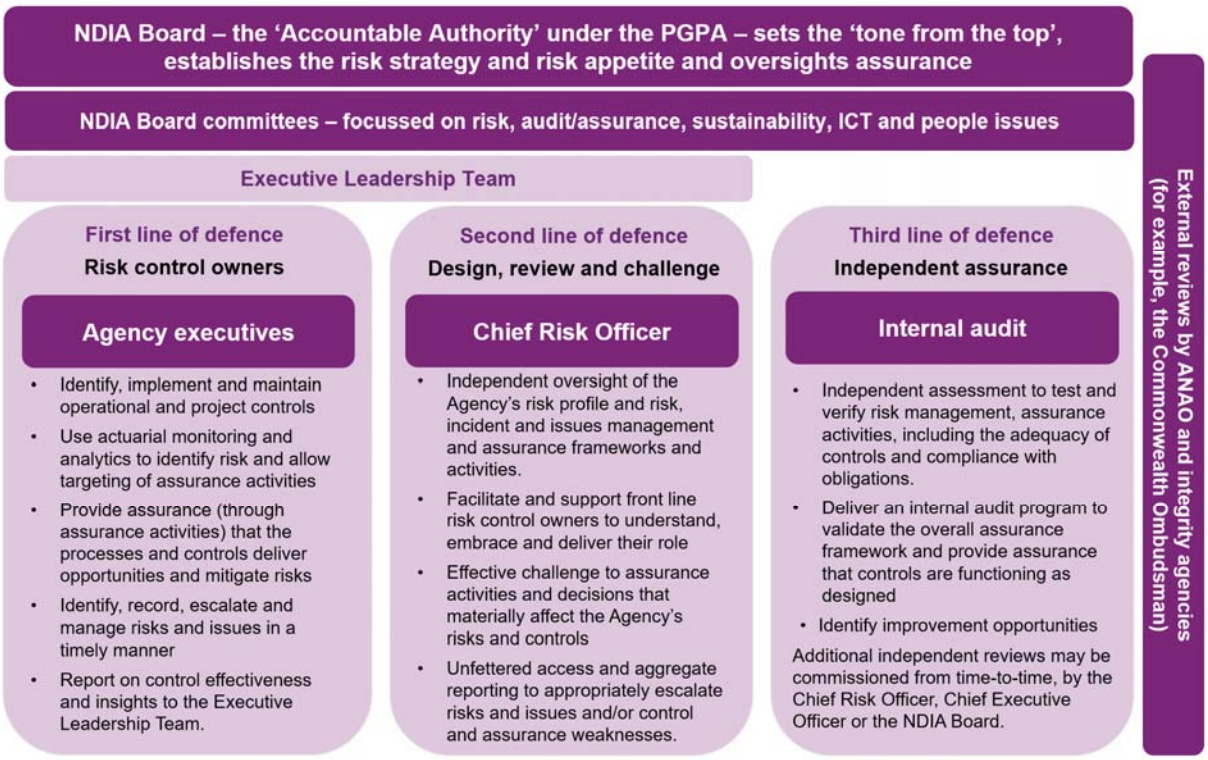
The Board is ultimately responsible for overseeing the establishment of an effective risk management approach at the Agency. The Board fulfils its responsibilities with advice and support from the Board's Risk Committee.

The Agency maintains strong strategic oversight of uncertainty, opportunity and risk through its Executive Leadership Team. The Executive Leadership Team is supported by the Agency's Chief Risk Officer and the Risk Branch.

Clear accountability for the management of key risks is also identified. The Agency has a comprehensive risk governance structure to support the effective management of risk with the Agency and across the NDIS through its community partners.

The Agency has adopted the 'three lines of defence' operating model, as summarised in Figure 1 below:

Figure 1: NDIA risk governance model



All Agency and community partner team members are responsible for the day-to-day management of risk in their work and the timely identification, escalation and communication of risks and issues, upon the identification of weaknesses in the controls that usually mitigate these risks.

Further detail on these roles and responsibilities is included in Appendix A.

1.6 Leadership

Achieving a culture where everybody 'does the right thing' requires an environment where people understand what the 'right thing' is. Leaders at all levels within the Agency are responsible for setting the positive tone, outlook and approach that encourages and rewards risk-based decision making.

Management

Executive staff (defined as anyone within the Agency with oversight of staff or contractors) will both lead and actively participate in risk and control monitoring activities to ensure opportunities are realised and threats are identified and appropriately mitigated.

State executives and managers of front line staff are expected to monitor and respond to risks that may arise in interactions with participants and providers. This will be done by ensuring all Agency and Partner in the Community staff complete compulsory training and follow operational procedures. Risks will be addressed, mitigated and escalated as appropriate in real time.

Senior Executive (defined as CEO, DCEOs and other senior executive level staff) communications will contain direct messages about, and examples of, good risk management and how it is applied to the Agency's work in delivering on the Corporate Plan.

In setting expectations, Agency and community partner executives are responsible for:

- Ensuring systematic consideration of risk is part of business planning and decision making activities
- Maintaining an awareness of their critical controls and actively monitor their effectiveness
- Frequently monitor the risk issues affecting decision quality, participant outcomes and financial sustainability
- Advocating the value of considering risk early and often in business planning and the execution of work tasks by teams
- Encouraging reflections and learnings from successes and failures
- Rewarding team members who demonstrate risk awareness and actively manage risks
- Implementing robust systems and processes to support compliance, control and integrity throughout the Agency and its community partners
- Maintaining regular high quality risk monitoring and reporting (in accordance with section 1.8 of this RMS).

Board

The Board, aided by its Risk Committee, will be diligent in its oversight and will support management in delivering effective risk management by:

- Annually approving the Agency's strategic risks, risk appetite statements, risk

tolerance settings and key risk indicators
- Regularly monitoring performance against risk tolerance settings
- Taking account of shared risks for the NDIS which extend beyond the Agency and require shared oversight
- Being clear in its commitment to maintaining strong controls and procedures to ensure risk is well managed and obligations are met
- Holding the CEO to account for promoting and fostering risk management as a signature strength of the Agency and growing a positive risk culture.

The Board will provide the Ministerial Council with an annual risk management declaration regarding the Agency's compliance with the RMS and the effectiveness of its operation.

1.7 Capability

Successful implementation of this RMS requires the consistent application of the following activities:

- Scanning the environment (internal and external) to identify emerging opportunities and threats and take early action in response
- Universal application of common risk management principles and processes across all business planning, day-to-day team activities and delegate decision-making
- Embedding an effective, consistent approach to how financial and human resources are deployed to manage uncertainty.

The key risk management capabilities to facilitate these activities include:

- All Agency staff having a comprehensive understanding of the NDIA's guiding risk principles and how they apply to their individual accountabilities
- Appropriately trained and supported operational risk partners who promote, guide and facilitate Group risk management practices. These partners also provide a communication and feedback channel back to the Risk Branch
- Appropriately qualified and experienced specialist risk management practitioners within the Agency's Risk Branch. The Risk Branch is responsible for setting the Risk Management Framework, delivery of training and providing support to Agency staff in their risk management activities
- Expert insight and advice to support our internal capability when needed, including through relationships with other commercially-oriented entities in the financial services, insurance and social services sectors.

The Agency's Risk Management Training Strategy identifies the specific capabilities required to understand and manage risk at all levels of the Agency. Training will be undertaken on a regular basis to develop, refine and enhance these skills.

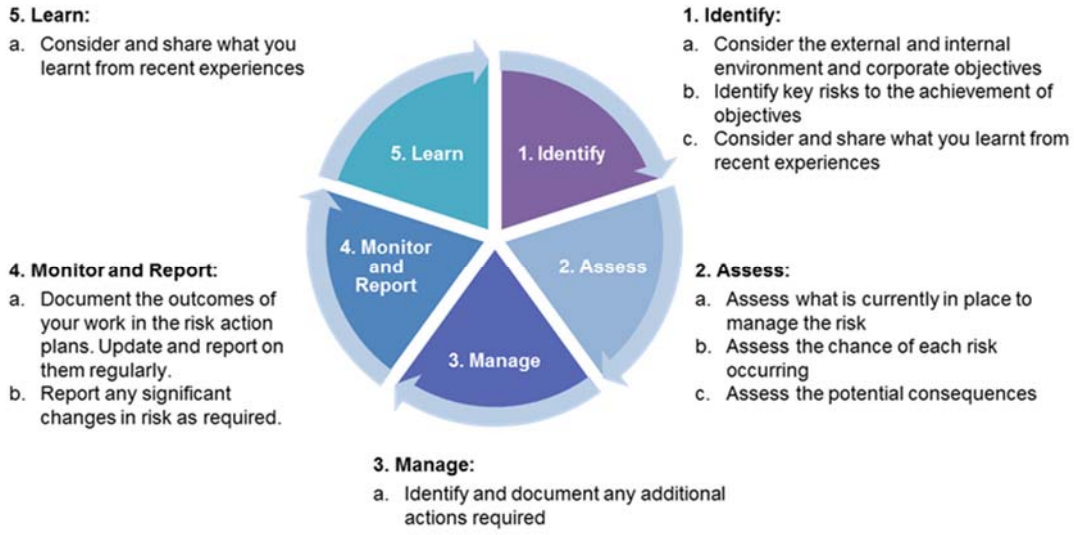
The Agency maintains a comprehensive suite of guidelines and toolkits to enable leaders and team members to understand and carry out their risk responsibilities. These documents and tools detail the Agency's risk management processes and approach.

1.8 Processes and approach

The Agency's risk management process includes information, guidance and supporting tools to provide clear guidance on the identification, assessment, management, monitoring and reporting of both risks and issues.

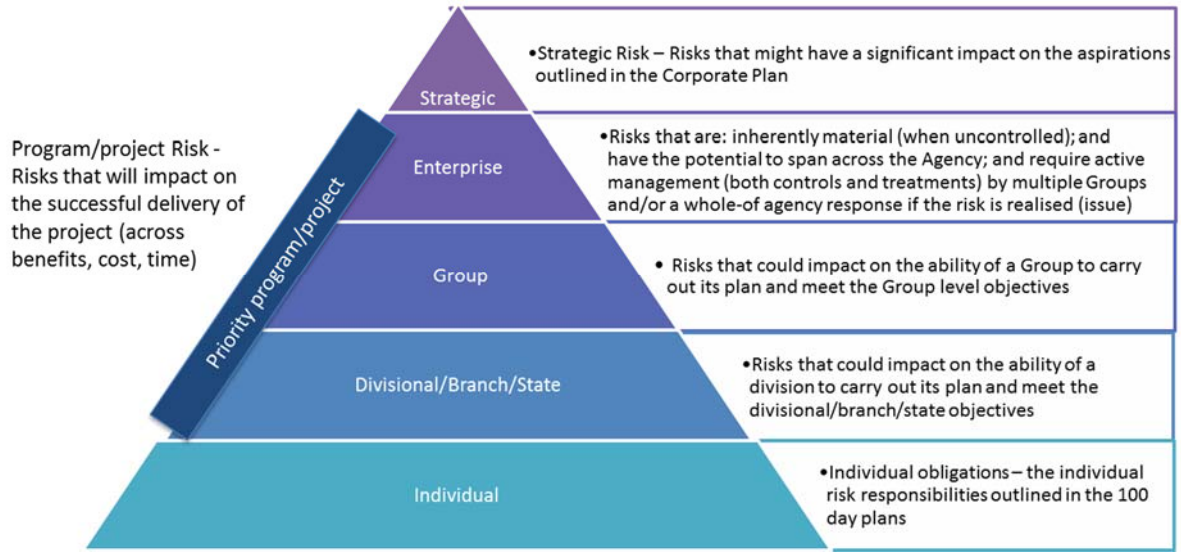
The Agency's risk and issues management cycle is set out in Figure 1 below.

Figure 1: NDIA risk management cycle



The overall approach is for uncertainty, opportunity and threats to be identified, managed and monitored within the planning and execution levels of the Agency, as described in Figure 2 below.

Figure 2: Alignment of NDIA planning and risk activities



Risk reporting will reflect performance against leading and lagging key risk indicators, monitoring of critical control effectiveness and treatment plan implementation.

Coaching and support for senior leaders and their teams will be provided by the Risk Branch and Group operational risk partners.

The Agency's monitoring and reporting activities are outlined in Table 1 below.

Table 1 – NDIA Risk management monitoring and reporting activity

Planning Level	Activity/ Output	When	Accountable	Responsible	End recipient
1a) Corporate Plan	**Risk Management Declaration** The Board evaluates the operational effectiveness of the risk management framework and makes a qualified or unqualified risk management declaration. In addition an annual review of the risk management process is overseen by the ELT to provide a view to the Board on the operating effectiveness.	Annually	Board	Chair of the Risk Committee	COAG Disability Reform Council
1b) Execution Plan	**Strategic Risks** Strategic risks are risks that could impact on the Agency's ability to execute the Corporate Plan are reported to the Board by the ELT. The report will be accompanied by a reporting view of the material divisional and/or project risks.	Quarterly	ELT	Individual Risk Owners	Board
	Priority Initiative Risk discussion and feedback This is a view of the most significant risks associated with projects and priority initiatives and informs the Strategic Risk Reporting.	Quarterly	ELT	Initiative Owners	Board
2) Business Plans	**Group/Divisional/Branch Risks** Quarterly review of the risk impacting on the ability of the divisions to achieve their group, divisional and/or branch plans and informs Strategic Risk Reporting.	Quarterly	DCEO GM BM	GMs BMs	ELT Risk Committee
3) State Plans	**State Risks** Monthly snapshot of the risk impacting on the ability of the regions/branches to achieve their plans/targets. Facilitated by the Risk Champions and reporting provided to the Divisional GM's.	Monthly	GMs	State Managers	Divisional GM
4) Project Plans	**Project Risks** Monthly review of the key risks impacting on the successful delivery of the projects. Facilitated by the EPMO and reporting provided to the Project Management Committee.	Monthly	Project Sponsor	Project Manager	Strategic Portfolio Committee

1.9 Supporting infrastructure

Successful implementation of this RMS relies on supporting infrastructure, including:

- An Enterprise Risk Management Plan, developed on an annual basis, to guide the effective implementation of the RMS
- Risk and issues management training, designed to build and maintain a strong level of risk management capability
- Performance assessments, designed to reinforce and recognise the demonstration of appropriate risk behaviours
- Risk systems to allow the collection and analysis of appropriate data to enable accurate reporting and guide risk-informed decision making and oversight.

The Agency's Risk Management Framework and supporting infrastructure is documented in the Board-approved Risk Management Framework Architecture at Appendix B.

1.10 Review

This RMS will be reviewed annually. The Board's Risk Committee will undertake an initial assessment and make recommendations for change, or not, to the Board for its consideration and approval.

In addition, the Agency will commission an independent external review of its Risk Management Framework, including the RMS, every three years to assess the adequacy and effectiveness of risk management activities at the Agency.

Appendix A – Risk management roles and responsibilities

Position	Roles and Responsibilities[1]
NDIA Board	• Sets the strategic intent through the Corporate Plan and determines the Agency's strategic risks • Approves the Agency's risk appetite statements • Approves the risk management strategy • Ensures the Agency is building an appropriate risk culture • Provides a risk management declaration
Audit Committee	• Establishes a system of oversight across effectiveness of key risk controls • Assurance of the Agency's internal control environment.
Risk Committee	• Oversees the risk management strategy, its implementation and the regular review of its efficiency and effectiveness • Formulates draft risk appetite statements and tolerances for Board approval • Notifies the Board of any significant breach of, or material deviation from, the risk management strategy or framework.
Chief Executive Officer (CEO)	• Accountability for the Agency's performance and delivery of the Corporate Plan including the accountability for management of uncertainty, opportunity and risk in the delivery of the scheme's outcomes • Champion the focus on risk within the Executive and senior leadership team
Scheme Actuary	• Assess the financial sustainability of the scheme and risks to that sustainability and identify recommendations to manage or address these risks • Include in an annual financial sustainability report a discussion of the Agency's risk management arrangements and any recommendations in relation to inadequacies.
Reviewing actuary	Report significant concerns about the risk management processes of the Agency to the Board as soon as reasonably practicable
Executive Leadership Group (ELT)	• Responsible, for implementing an effective risk management approach across the Agency and with community partners • Lead risk management by example and drives risk management conversations • On a regular basis reviews the strategic and other material risks that could impact the Agency and report to the Board Risk Committee • Provides feedback to the Agency on risk management strategies, priorities and incident resolution • Monitors challenges to Scheme and business integrity and assurance activities • Reviews implementation of mitigation and response strategies recommended in external reviews, including by the ANAO.
Chief Risk Officer (CRO)	• Provides an independent and objective review and challenge, oversight, monitoring and reporting as a direct report to the CEO • Provides advice on design of the risk management framework • Has independent access to the Risk Committee and Audit Committee to provide challenge where necessary • Supports the Executive by monitoring risk, identifying emergent risks and reporting on management responses to risk, in line with the enterprise risk management framework • Recommends updates to the Enterprise Risk Management Framework for ELT approval.

[1] The term risk incorporates an issue – under the definition of a risk that has been realised.

Appendix A – Risk management roles and responsibilities

Position	Roles and Responsibilities[1]
Risk Branch	• Supports the CRO in the performance of the nominated role under the Risk Management Rules • Provides strategic risk advice to the ELT and senior executives • Sets minimum standards and builds capability and knowledge in the application of these standards • Fosters continuous learning • Facilitates effective risk oversight and information for decision making • Provides comfort that expectations and commitments are fulfilled.
Groups	• Identify and manage risks that may impact on Group objectives
Divisions	• Identify and manage risks that may impact on the divisional objectives • Provide feedback and updates to leadership on risk management in their divisions • Provide guidance and direction to divisional staff on risk management expectations.
States	• Identify and manage risks that may impact on objectives • Provide feedback and updates to leadership on risk management in their state • Provide guidance and direction to staff on risk management expectations.
Group operational risk partners (1st line risk advisors)	• Provide input and support on risk management processes and tools developed for the organisation • Build risk management capability through supporting and facilitating risk management training and reinforcement activities outlined in the risk training strategy • Coordinate and facilitate regional and divisional risk management activities, in conjunction with the Risk Branch • Have two-way communications to provide guidance and support to local teams and provide feedback to the Risk Branch • Share good ideas, successes and issues with other champions and senior leaders, helping 'connect the dots' throughout the Agency.
Risk owners	• Are responsible for the assessment and management of risks allocated to them including the development and operation of the control and monitoring activities • Be able to provide updates on actions taken to manage the risks where necessary • Manage third-party risk, including for partners in the community and shared service providers.
All staff and partners in the community	• Conduct themselves in line with the risk management principles outlined in the risk management policy and RMS • Take accountability for management of risks and assist others to manage their risks • Use training, tools and templates available to them to facilitate the implementation of the risk management strategy • Escalate risks and issues openly, honestly and timely • Share and learn from mistakes and successes.