NDIA

Risk Management Strategy

04 December 2017

Board endorsed for Ministerial Council approval

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 12 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
- 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
- Operating model and risk governance – ensuring the way we work is contemporary and reflects better practice in risk management and governance
- Supporting infrastructure – establishing what's 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.

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.

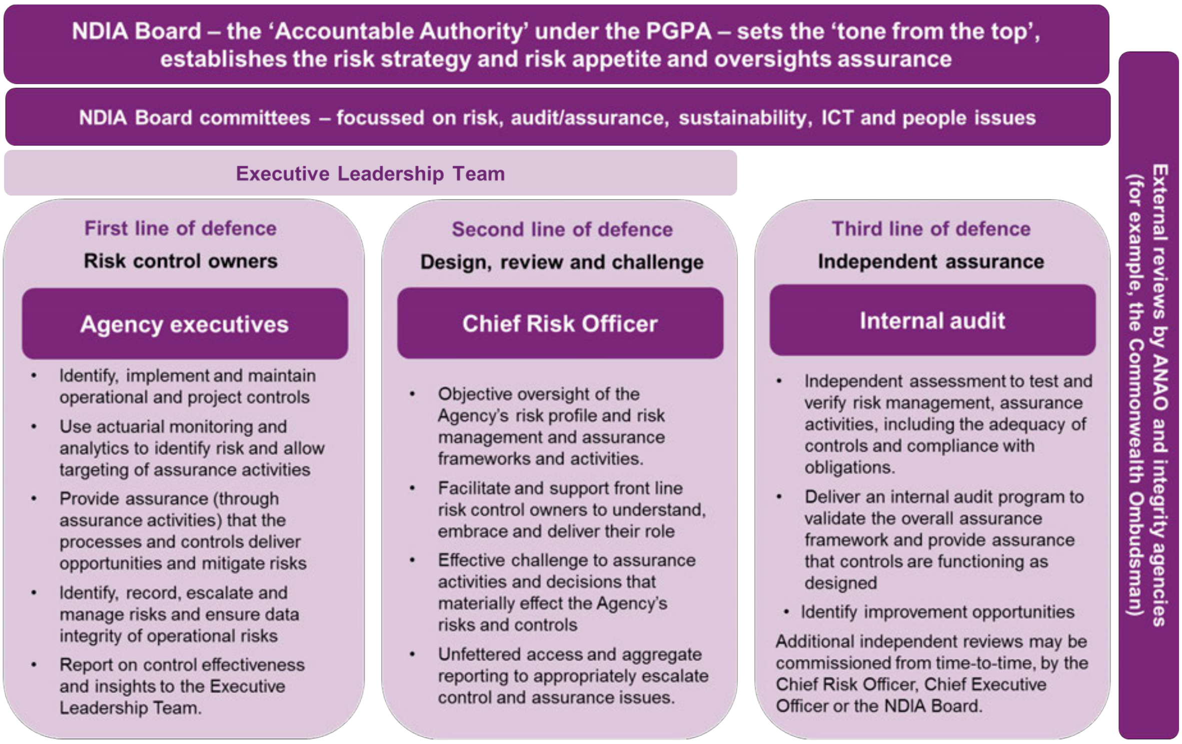
The Agency maintains strong strategic oversight of uncertainty, opportunity and risk through its Executive Leadership Team. Each executive team is supported by the Agency's Chief Risk Officer and the Risk Division.

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



NDIA Board – the 'Accountable Authority' under the PGPA – sets the 'tone from the top', establishes the risk strategy and risk appetite and oversights assurance

NDIA Board committees – focussed on risk, audit/assurance, sustainability, ICT and people issues

Executive Leadership Team

First line of defence

Risk control owners

Agency executives

- Identify, implement and maintain operational and project controls
- Use actuarial monitoring and analytics to identify risk and allow targeting of assurance activities
- Provide assurance (through assurance activities) that the processes and controls deliver opportunities and mitigate risks
- Identify, record, escalate and manage risks and ensure data integrity of operational risks
- Report on control effectiveness and insights to the Executive Leadership Team.

Second line of defence

Design, review and challenge

Chief Risk Officer

- Objective oversight of the Agency's risk profile and risk management and assurance frameworks and activities.
- Facilitate and support front line risk control owners to understand, embrace and deliver their role
- Effective challenge to assurance activities and decisions that materially effect the Agency's risks and controls
- Unfettered access and aggregate reporting to appropriately escalate control and assurance issues.

Third line of defence

Independent assurance

Internal audit

- Independent assessment to test and verify risk management, assurance activities, including the adequacy of controls and compliance with obligations.
- Deliver an internal audit program to validate the overall assurance framework and provide assurance that controls are functioning as designed
- Identify improvement opportunities

Additional independent reviews may be commissioned from time-to-time, by the Chief Risk Officer, Chief Executive Officer or the NDIA Board.

External reviews by ANAO and integrity agencies (for example, the Commonwealth Ombudsman)

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 weaknesses in the controls that usually mitigate these risks being realised.

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.

Regional 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 LAC staff complete compulsory training and operational procedures are followed. 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).

These responsibilities are aligned to the Agency’s Leadership Framework and are reinforced within a dedicated risk training program for senior leaders and front line managers.

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 divisional and regional operational risk partners who promote, guide and facilitate local risk management practices. These partners also provide a communication and feedback channel back to the Risk Division
- Appropriately qualified and experienced specialist risk management practitioners within the Agency's Risk Division. The Division 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.

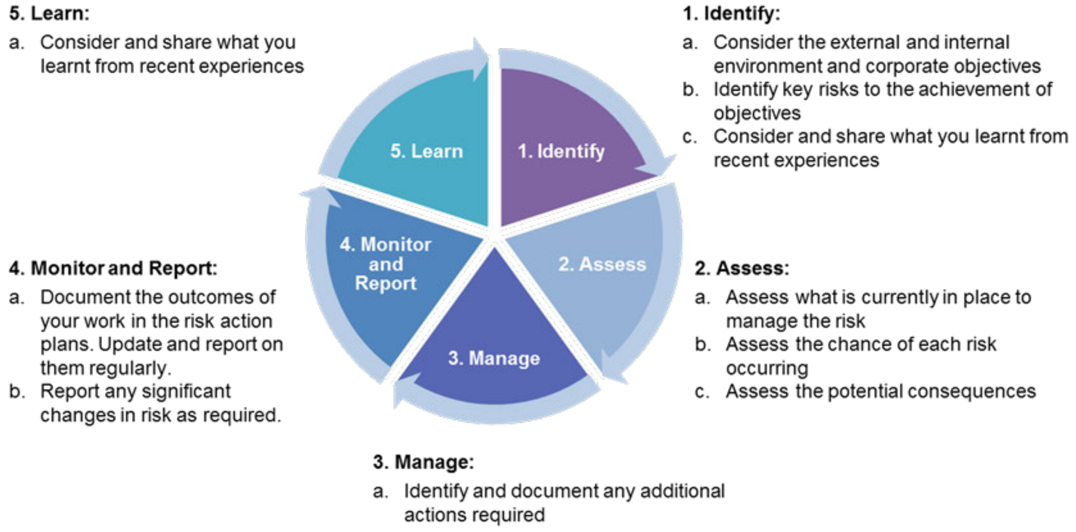
The Agency maintains a comprehensive suite of guidelines and toolkits to enable leaders and team members to understand and carry out their risk responsibilities. These documents and tools detail the Agency's risk management processes and approach.

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 risks.

The Agency’s risk management cycle is set out in Figure 1 below.

Figure 1: NDIA risk management cycle



5. Learn:

a. Consider and share what you learnt from recent experiences

1. Identify:

a. Consider the external and internal environment and corporate objectives
b. Identify key risks to the achievement of objectives
c. Consider and share what you learnt from recent experiences

4. Monitor and Report:

a. Document the outcomes of your work in the risk action plans. Update and report on them regularly.
b. Report any significant changes in risk as required.

2. Assess:

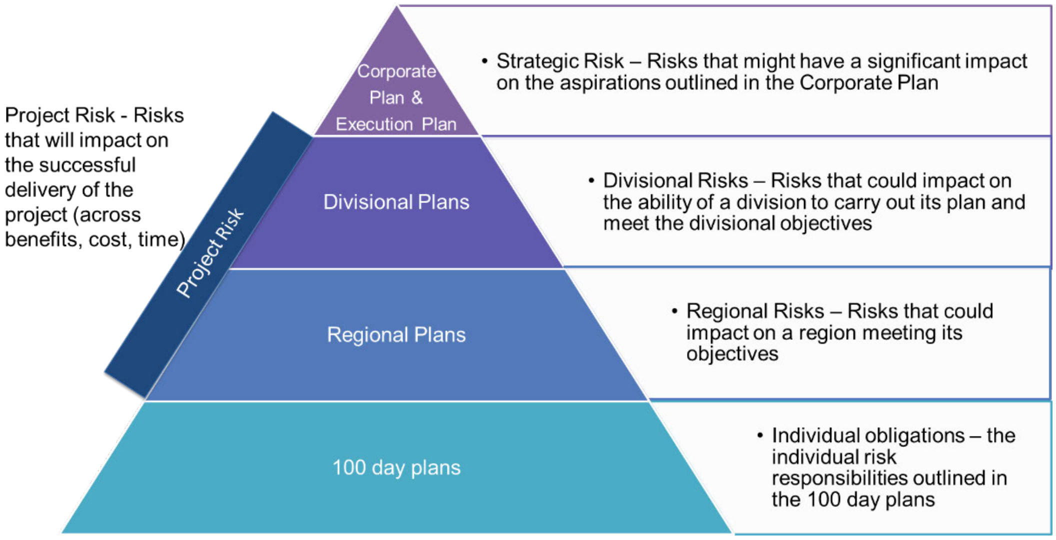
a. Assess what is currently in place to manage the risk
b. Assess the chance of each risk occurring
c. Assess the potential consequences

3. Manage:

a. Identify and document any additional actions required

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



Project Risk - Risks that will impact on the successful delivery of the project (across benefits, cost, time)

- Strategic Risk – Risks that might have a significant impact on the aspirations outlined in the Corporate Plan
- Divisional Risks – Risks that could impact on the ability of a division to carry out its plan and meet the divisional objectives
- Regional Risks – Risks that could impact on a region meeting its objectives
- Individual obligations – the individual risk responsibilities outlined in the 100 day plans

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 locally-based 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.	Monthly	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.	Monthly	ELT	Initiative Owners	Board
2) Group and divisional Plans	**Group and/or Divisional Risks** Quarterly review of the risk impacting on the ability of the Group and/or divisions to achieve their divisional plans and informs Strategic Risk Reporting. Co-discussion with Operational Risk Partners and reporting provided to the ELT (phased handover approach from ES&R branch to Operational Risk Partners).	Quarterly	DCEOs GMs	GMs BMs	ELT
3) Regional Plans	**Regional Risks** Monthly snapshot of the risk impacting on the ability of the regions/branches to achieve their plans/targets. Facilitated by the Operational Risk Partners and reporting provided to the Divisional GM's.	Monthly	GMs	RMs	DCEO
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 Enterprise Portfolio Project Committee.	Monthly	Project Sponsor	Project Manager	EPPC and ELT

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 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.

Position	Roles and Responsibilities
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 risk oversight across the enterprise risk management framework and associated internal 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 EMG approval.

Position	Roles and Responsibilities
Risk Division	• 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.
Regions	• Identify and manage risks that may impact on the divisional objectives • Provide feedback and updates to leadership on risk management in their divisions • Identify and manage risks that may impact on the regional objectives • Provide guidance and direction to regional staff on risk management expectations.
Divisional and regional operational risk partners	• 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.

Appendix B - NDIA Risk Management Framework

Framework element	Components
Risk management mandate, commitment and framework design	
Risk Management Policy statement	Commitment Key Principles Roles and Accountabilities
Risk Management Strategy (3 year)	Context Culture and Behaviour Leadership Capability Process and Tools Operating Model and Risk Governance Supporting Infrastructure
Enterprise Risk Management Plan (annual)	Roles and Responsibilities Framework review requirements and schedule Risk register review requirements and schedule Strategic risk assessment requirements and schedule Assurance activity requirements and schedule
Group Risk Management Plans (annual)	Participant and Planning Markets and Supports Governance and Stakeholder relations Office of the CEO and Scheme Actuary
Regional/Site Risk Management Plans (annual)	Victoria New South Wales South Australia Queensland Tasmania Australian Capital Territory Northern Territory Western Australia
Implementing risk management	
Risk Management Procedures and Guidelines	Risk management glossary Tolerance and Appetite *(including Tolerance Matrix and Key Risk Indicators)* Risk management process guidelines (incorporating establishment of context and risk categorisation guidelines) Risk assessment procedure – identification, assessment and evaluation Qualitative assessment Quantitative assessment Control effectiveness evaluation methodology Risk Action Plans Risk management communication strategy and guidelines Risk management training strategy
Risk Registers	Strategic risk register Regional Risk Snapshots Divisional Risk Action Plans Program/Project Risk Snapshots Functional Risk Registers (ie WHS)
Monitoring, review and reporting	
Reporting	Executive Leadership Reporting (monthly and/or as required) Board Risk Committee Reporting Board Reporting Annual Board Risk Declaration
Assurance	First line assurance activities Second line assurance activities Internal audit program External Audits/reviews CPS220 Compliance Audits/reviews
Continual improvement	
Improvement Process	Future State Model Program of planned activities Risk Management Training Delivery Risk Management Maturity Reviews (internal and external) Comparative / Benchmarking Analysis

Item 2.4 Attachment A

NDIA Business Continuity Management Policy

April 2018

Draft for ELT Risk Committee Approval

Version	Author	Date	Comment
1.0	Risk and Assurance	April 2015	Broadfoot/Rogan/Suter
1.1	Craig Rogan	March 2018	Updated to reflect new framework
1.2	Craig Rogan	April 2018	Minor content changes

Reviewers

Version	Reviewer	Date
1.2	Tammy Venturoni	April 2018

Approvals

Version	Name	Position	Signature	Date
1.2	ELT Risk Committee			

Distribution List

Name	Position	Organisation
ART		

Contents

1. Introduction

Business Continuity Management (BCM) encompasses a set of planning, preparatory and related activities that ensure the Agency:

- responds in a timely, coordinated and effective manner to an interruption or declared disaster;
- continue to be operational despite serious incidents or disasters that might otherwise have interrupted them; and
- actively manage and resolve an incident in the shortest possible timeframe to minimise impacts.

Significant business disruption events can result from a wide range of causes including: loss of access to building(s); utility outages; ICT outages; and loss of staff. The National Disability Insurance Agency (NDIA or Agency) BCM arrangements are designed to minimise the impact of a significant business disruption on the Agency's critical business functions and services and aims to ensure uninterrupted availability. Where this is not possible, the BCM activities will guide the rapid restoration of critical business activities and assist in the resumption of business as usual in an appropriately prioritised and orderly manner.

2. Objectives and Guiding Principles

The guiding principles of NDIA's BCM Framework are:

- we ensure access to medical and care supports for impacted staff members at all times and ensure participants are not put at risk; and
- nationally consistent systems are in place to support the business.

These guiding principles drive the key objectives of NDIA's BCM Framework, which are to:

- minimise disruptions to time critical business activities;
- ensure a timely resumption of operations following a disaster or other significant business disruption; and
- preserve stakeholder confidence, credibility and goodwill.

These objectives are achieved by:

- maintaining a set of plans to ensure that NDIA can manage and recover from emergencies, disasters and other business disruptive events;
- fostering a culture and awareness of BCM within NDIA and promoting the practice of its planning as a routine part of business management;
- the ongoing development, exercising and review of BCM plans and procedures; and
- ensuring linkages with NDIA's Risk Management Framework and Emergency Management procedures.

3. Scope

3.1 Scope inclusions

There are a number of scenarios that could seriously impact the ongoing functions and activities of NDIA, as such it is not possible to predict every possible scenario or cause of disruption. Whilst the BCM Framework provides direction, the unique nature of incidents requires that staff exercise judgment and tailor the response to their circumstances.

The NDIA BCM Framework is designed to address the following business disruption scenarios:

- an event that creates a loss of physical access to the NDIA National Office buildings, Regional Office sites and the assets located at those sites;
- loss of core utility services such as electricity, water and air-conditioning to the sites;
- unavailability of personnel;
- unavailability of ICT services including telephony, internet, intranet and email;
- other scenarios specific for an individual critical business activity.

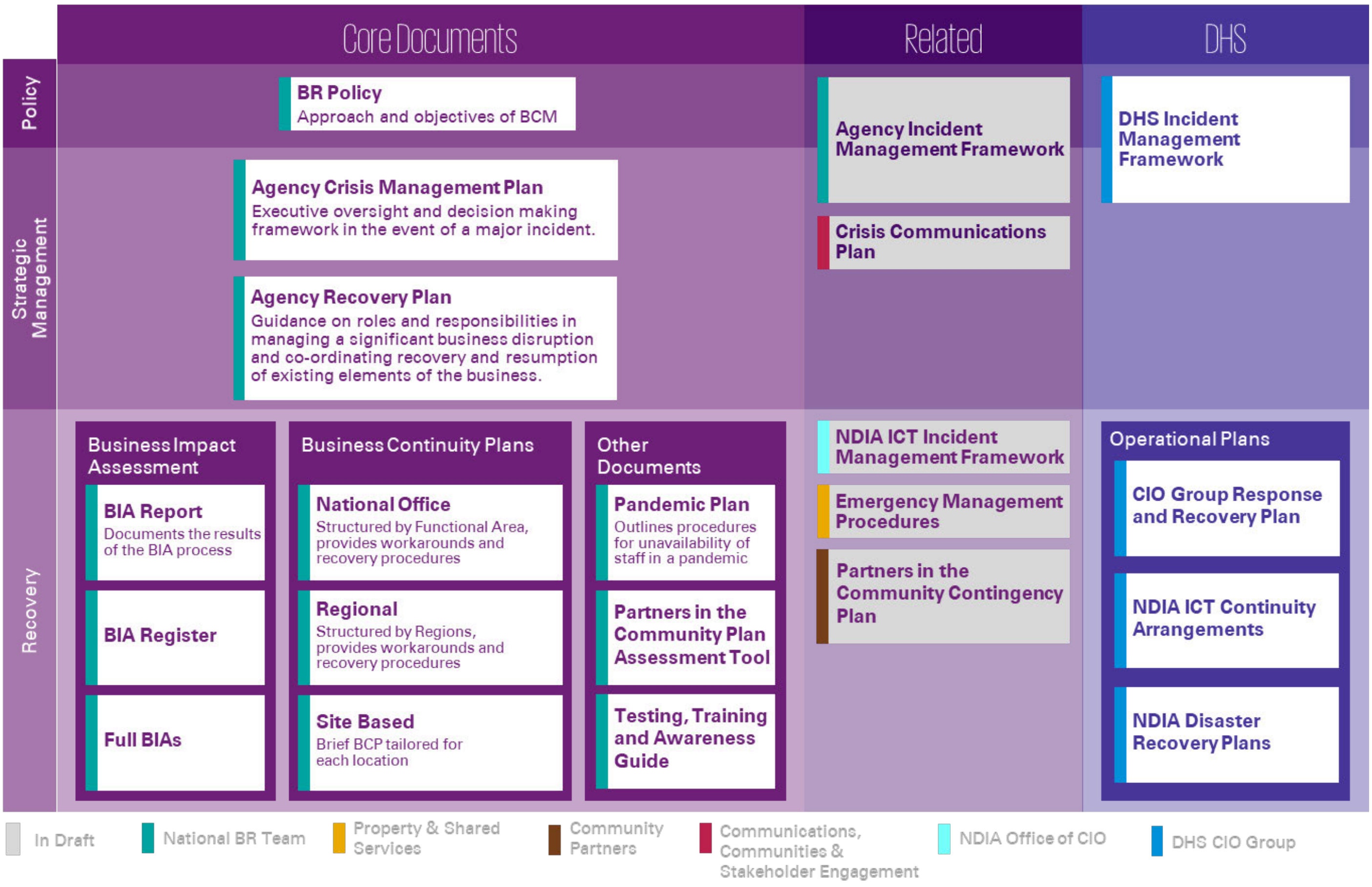
3.2 Scope Exclusions

The scope of the NDIA BCM Framework excludes detailed Information and Communications Technology (ICT) disaster recovery procedures, which are managed by the Department of Human Services (DHS). NDIA's BCPs provide workarounds only, which allow the Agency to continue the identified critical business functions while ICT applications are recovered by DHS.

4. Framework architecture

Figure 1 below illustrates the core documents within the NDIA BCM Framework and identifies accountabilities for BCM and related documents.

Figure 1 – NDIA Business Continuity Management and related frameworks


Core Documents
Related
DHS
Policy
Strategic Management
Recovery
BR Policy
Approach and objectives of BCM
Agency Crisis Management Plan
Executive oversight and decision making framework in the event of a major incident.
Agency Recovery Plan
Guidance on roles and responsibilities in managing a significant business disruption and co-ordinating recovery and resumption of existing elements of the business.
Agency Incident Management Framework
Crisis Communications Plan
DHS Incident Management Framework
Business Impact Assessment
BIA Report
Documents the results of the BIA process
BIA Register
Full BIAs
Business Continuity Plans
National Office
Structured by Functional Area, provides workarounds and recovery procedures
Regional
Structured by Regions, provides workarounds and recovery procedures
Site Based
Brief BCP tailored for each location
Other Documents
Pandemic Plan
Outlines procedures for unavailability of staff in a pandemic
Partners in the Community Plan Assessment Tool
Testing, Training and Awareness Guide
NDIA ICT Incident Management Framework
Emergency Management Procedures
Partners in the Community Contingency Plan
Operational Plans
CIO Group Response and Recovery Plan
NDIA ICT Continuity Arrangements
NDIA Disaster Recovery Plans
In Draft
National BR Team
Property & Shared Services
Community Partners
Communications, Communities & Stakeholder Engagement
NDIA Office of CIO
DHS CIO Group

5. Roles and responsibilities

All staff play a key role in assisting the resumption of critical business activities in the time of a significant disruptive event. Table 1 below outlines key BCM roles and responsibilities.

Table 1 – Key BCM roles and responsibilities

Position / Role	BCM Responsibilities
Chief Executive Officer	• Maintain communications with Government and Board in the event of a significant BCM incident.
Crisis Management Team	• Manages strategic issues, decisions and associated risks during a declared crisis event.
Agency Recovery Team	• Senior team responsible for coordinating the NDIA's recovery from a major disruption. The team will focus on prioritising and coordinating restoration of core supporting functions required for NDIA to continue operations. • Agency Recovery Team (ART) will be stood up by the Incident Leader to formulate and coordinate of action for 'severe' and 'major' incidents.
Incident Leader	• Chair of the ART.
National Business Resilience Team	• Develop and maintain the overall BCM Framework. • Monitor, test and exercise the NDIA's overall preparedness. • Provide support to the ART as required. • Foster a culture and awareness of BCM within NDIA and promote the practice of BCM as a routine part of business/operations management. • Ensure best practice BCM in NDIA. • Provide annual reports to the NDIA Board on the BCM Framework.
National Office Site Business Continuity Manager	• Sign-off relevant BCP(s) for the National Office site • Responsibility to confirm plans are fit for purpose for continuity of activities deemed time critical. • Lead Site recovery efforts • National Office Site Business Continuity Teams (NO BCT) will be stood up for 'major' incidents impacting a National Office Site.
Regional Managers	• Sign-off relevant BCP(s) for the Region and each site within the Region • Responsibility to confirm plans are fit for purpose for continuity of activities deemed time critical. • Lead Regional Business Continuity Teams and regional recovery efforts.
Regional Business Continuity Team (Regional BCT)	• Regional Business Continuity Team will be stood up for 'major' incidents by the Regional Manager.
Site Contacts	• Sign-off relevant BCP(s) for areas of responsibility to confirm plans are fit for purpose for continuity of activities deemed time critical. • Lead local Business Continuity Teams and local recovery efforts.

	• Maintain communications with the Regional manager in the event of an incident.
Local Business Continuity Teams (Local BCTs)	• Ensure that the local BCP is reviewed, exercised and updated. • Maintain BCP kits which are accessible including in the event that local sites are closed. • Ensure all local staff are aware of their role or likely stand-down should a business continuity event occur. • Maintain an effective communication system to facilitate contact with local staff during a business continuity event (e.g. contact list).
All staff	• Be familiar with emergency evacuation procedures for the building/facility. • Know the members of their local BCT. • Adhere to relevant business continuity procedures outlined in applicable BCPs.
Secretariat Support – National Business Resilience Team	• Secretariat Support will provide administrative support as required. • Secretariat Support will provide the necessary tools, techniques and guidance material to Local BCTs to develop and exercise BCPs. Local BCTs will utilise the templates provided by the Secretariat. • Secretariat Support will report every twelve months to the Audit and Risk Committee on BCM activity and maturity.

6. Framework review requirements

The Agency's BCM Framework and supporting documentation will be reviewed annually. The Business Impact Assessment will be reviewed following the introduction of any significant changes to business processes, structure or personnel.

Changes in policies and procedures will be endorsed by the Branch Manager – Risk, and approved, as necessary, by the Executive Leadership Team.

6.1 Document maintenance responsibilities and approvals

Ownership, maintenance responsibility and approval requirements for key BCM Framework documents are outlined in Table 2 on the following page.

Table 2: Document Maintenance Responsibilities and Review

Business Continuity Management Documents	Document Owner	Maintenance Responsibility	Formal Review Frequency	Approval
Contact Lists	Site BC Contact	Site BC Contact	Monthly	Local BC Contact
Business Continuity Management Policy	BM Risk	National Business Resilience Team	Annual	ELT Risk Committee
Training, and Exercise Guide	Director – Business Resilience	National Business Resilience Team	Annually	Chief Risk Officer
Business Impact Assessment	Functional GM	Functional BM or GM	Annually	Accountable General Manager
Agency Disaster Recovery Plan	Chief Information Officer	National Business Resilience Team	Annually	Chief Information Officer
Agency Recovery Plan	DCEO Strategy Development and CRO	National Business Resilience Team	Annually	Chief Risk Officer
National Office Business Continuity Plans	Functional General Manager	Function BM or GM	Annually	Accountable General Manager
Regional Business Continuity Plans	Regional Manager	Regional Business Continuity Teams	Annually	Regional Manager
Site Business Continuity Plans	Site BC Contact	Site BC Contact	Annually	Regional Manager
Pandemic Plan	Director – Business Resilience	National Business Resilience Team	Annually	Chief Risk Officer
Content on intranet including templates, exercise schedules, contact lists and exercise scenarios	Director – Business Resilience	National Business Resilience Team	As required	BM Risk

7. Business continuity planning

Each function of the Agency will undertake/ review an annual Business Impact Assessment (BIA) to identify critical business activities. Each critical activity identified in the BIA will be captured in a Business Continuity Plan (BCP).

7.1 BCP minimum requirements

The NDIA operates in a widely dispersed and complex operating environment. To ensure its BCM framework is fit for purpose, the Agency maintains a number of business continuity plans, as outlined in Figure 1 on the previous page.

At a minimum, all BCPs must specify:

a) critical business activities;
b) maximum tolerable period of disruptions for each activity;
c) alternative work locations;
d) minimum staffing requirements;
e) critical equipment requirements and alternative storage arrangements (including emergency kits, computers and motor vehicles);
f) local BCT responsibilities;
g) manual workarounds where available;
h) communication approach with staff and stakeholders;
i) interdependencies with other areas of NDIA;
j) any external stakeholders, including references to, or attachments of, formal agreements with external stakeholders; and
k) recovery checklists.

7.2 BCP maintenance and testing requirements

BCPs will be fully reviewed at least every 12 months to ensure they are fit for purpose. In addition to the annual assessment, a review of business continuity documents will occur following:

a) a business disruption or exercise to capture and address any gaps or lessons learnt;
b) significant organisational restructure;
c) relocation of NDIA or its Offices;
d) significant staff movements; or
e) a shift in the strategic direction of NDIA.

When updating business continuity documents, maintenance teams must ensure:

a) any new activities or services that need to be included in the document are identified;
b) the document is effective, up-to-date, fit-for-purpose, and appropriate to the level of risk faced;
c) the document is clear, simple and concise; and
d) any lessons learned and/or process improvements from exercises or actual business continuity events have been incorporated into the plan.

Copies of all BCPs must be stored:

a) At NDIA sites in hard copy with the Site Manager;
b) Electronically and hard copy with the National Business Resilience Team;
c) Electronically with the Incident Manager; and
d) With delegates as required.

Following an update to a BCP, all hardcopies are to be destroyed and replaced with the revised plans to maintain currency and consistency.

7.3 Post incident review

Where a BCP is invoked, a Post Incident Review (PIR) will be undertaken. Details of the requirements of a PIR are to form part of each BCP.

8. Glossary of Terms

Key term	Definition
Business Continuity Management	Deals with maintaining key business processes and outputs despite disruption
Emergency Management	Deals with time critical threats to lives, livelihoods, assets and the environment
Incident	An event that impacts or threatens to impact the operations of the Agency by exceeding existing processes and risk controls
Non-Business Disruption Event	An event which causes, or could cause, adverse media attention, a legal or reputation impact to the Agency.
Business Disruption Event	An event which causes, or could cause, an outage, stoppage, or failure of a process or system, which impacts the ability of the Agency to deliver services.
Recovery Time Objective	The amount of time required for staff to return processes / infrastructure to normal
Maximum Tolerable Disruption Period	The maximum disruption period before a business suffers significant and/or irreversible loss
Business Impact Analysis	A systematic process to determine and evaluate the potential effects of an interruption to critical business operations as a result of a disaster, accident or emergency
IT Service Continuity	Deals with maintaining / restoring IT services, despite disruption, failure and / or outage
Workaround Strategy	The alternative processes in place to support the business while primary services are disrupted
Recovery Strategy	Procedures of returning business capability back to normal functioning levels (e.g. repairs)
Resumption Strategy	The strategy for returning business processes back to normal following a disruption or outage (e.g. backlog)
Business Continuity Plan	A documented set of procedures and information intended to deliver continuity of critical business processes in the event of a disruption to business as usual operations.
Post Incident Review	An assessment undertaken at the conclusion of a disruption event, which captures areas for improvement and areas of strength from the Agency's response.