Risk Management Guide

November 2019

ndis.gov.au

Objectives

This document is a guide for NDIA staff to use in identifying, assessing, managing and reporting risk across the agency. It provides guidance on the risk management process that each of the divisions are expected to apply as part of their annual business planning processes.

How to use this guide

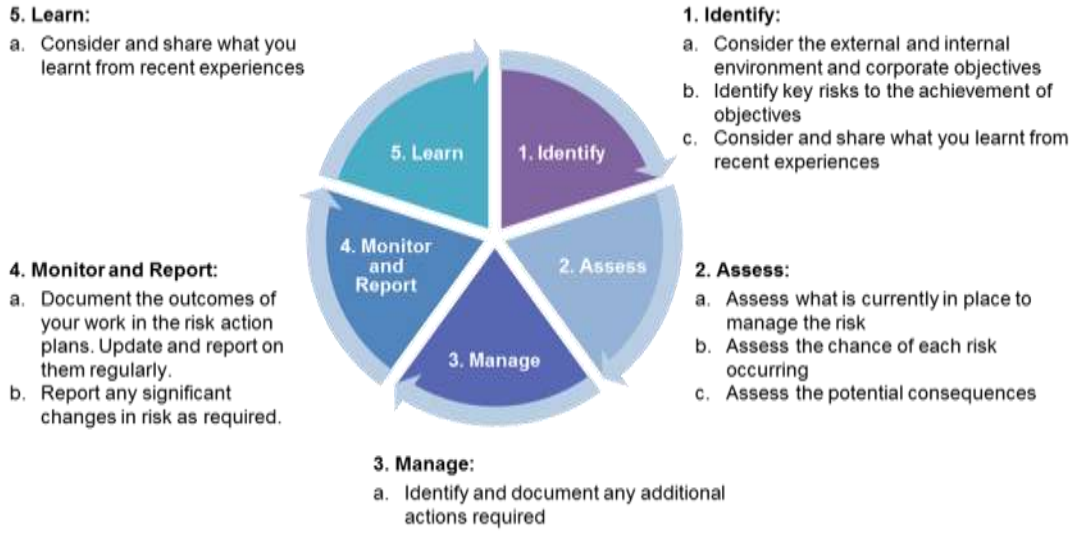
The NDIA has developed criteria, aligned with our corporate plan aspirations and goals, to support a consistent way for us to:

a. Identify risks through the decision making and planning process
b. Consider the relative significance and priority of different risks;
c. Inform decisions on whether actions and resources currently in place are sufficient to manage the risk and what else is required.

These criteria can also be used to inform decisions on the escalation of risk. Separate risk appetite and tolerance guidance has been developed which will be the primary tool used for risk acceptance and escalation. This guide outlines:

- The steps that each Division is required to undertake in relation to the risks that it faces.
- Areas of consideration when carrying out these steps.
- Templates to assist you in carrying out these steps.

The overall process is described in the diagram below:
Diagram 1.



Familiarise yourself with the complete process before using this guide and commencing your annual business planning activities. The outputs of this process should be captured in the Divisional Risk Action Plan or the Regional Risk Snapshot. Further information and guidance on this process can be provided by the Risk Champion in your area or by contacting the Enterprise Risk Branch.

1. Identify

1a. Consider the external and internal environment

The identification of risk should include both external and internal sources of risk as well as the risks that are inherent in the work the Agency is doing. The NDIA has developed a risk taxonomy (Appendix B) that provides sources and examples of risk that can be used to assist the identification process. To ensure appropriate identification of risk it is important that input is sought from a sufficiently broad group of stakeholders and sufficient sources of information.

1b. Identify key risks to the achievement of objectives

Risks should be considered during the Annual Planning Cycle, the Monthly Performance Review, Project Planning and whenever a key decision or change to process is being made. The 6D decision model that is used in key decision making contains a step for the identification of risks.

Risks will be identified and described under three key components:

- **Risks** are uncertainties which, if they occur, would negatively affect achievement of the objectives. What might inhibit the ability to meet objectives?
- **Causes** are events or set of circumstances that give rise to uncertainty (risk). What may cause the risk to occur?
- **Impacts** (effects) are unplanned negative variations from objectives, which would arise as a result of risks occurring. What can happen if the risk occurs?

In generating the description of these three components, it is necessary firstly identify what might happen (the risk name), and then consider the possible causes that lead to the uncertain event or risk, and finally identify the impacts that arise if the risk was to occur. A risk may have one or more causes and, if it occurs, one or more impacts.

1c. Consider and share what you learnt from previous experiences

A source of information that should be considered in reviewing previous experiences to understand how actual performance differed from the expected outcomes and what caused the variance. This information can be used to inform potential risk areas for consideration and highlight any biases that may have prevented appropriate identification of risk previously.

Risks identified should be documented in the Risk Action Plan (insert hyperlink) and assigned a risk owner that will be responsible for the overall management of the risk.

2. Assess

2a. Assess what is currently in place to manage the risk.

Before assessing the likelihood and consequence of each risk it is important to identify and assess what controls or actions are currently in place that will either prevent the risk from occurring or reduce the consequences if it does occur.

Once all current actions have been identified use the table below to assess the effectiveness of current actions.

	Q1 Does the Group of controls address the risk effectively?	Q2 Are all the controls officially documented and communicated?	Q3 Are all the controls in operation and applied consistently?	
Yes	1	1	1	
Partly	3	2	2	
No	6	3	3	
	Total Q1	Total Q2	Total Q3	Total Rating

Rating Score	Control Rating	Description
3	Excellent	No improvements in the control environment (additional actions) can be recommended.
4	Good	Improvements in the control environment (additional actions) can be recommended but are not urgent and could be scheduled within the next 12 months.
5 - 6	Adequate	Improvements in the control environment (additional actions) are recommended and should be scheduled within the next 6 months.
7 - 12	Needs Improvement	The control system is largely ineffective or non-existent. Improvements in the control environment (additional actions) are recommended and should be scheduled within the next 3 months.

2b. Assess the potential consequences.

In determining the potential consequences of a risk if it eventuates, consider the corporate aspirations to form a view of what the risk may impact on and how bad the impact could be.

Using the table below select the most applicable aspiration and metric (e.g. participant satisfaction) and then determine what impact the risk could have on that metric (e.g. significant and sustained underachievement it would be considered 'Five Severe'). For any risk there will typically be more than one aspiration that could be impacted. In this instance, it is important to identify the most material consequence, as this will help in the prioritisation of risk actions.

Table 3. Risk consequences on NDIA aspirations

	Participant outcomes	Scheme sustainability[1]	Market[2]	Agency Staff and Partners in the Community	Public confidence & trust[3]
E	***Significantly below*** target levels across ***most regions*** for: • Participant intake levels for > ***Two quarters*** • Participant satisfaction levels for > ***Three quarters*** • Participant outcomes for > ***One year***	• ***Scheme*** support ***costs > 20 per cent over target*** • Agency costs > 20 per cent over budget • Divisional underspend > 60 per cent	• ***Significant shortages*** in availability of critical ***service supply*** across ***most regions*** for > ***Two quarters***, requiring significant NDIA intervention • Significant and sustained impact on provider sentiment across most regions for > ***Two quarters***	• ***Significant deficiencies*** in **workforce** capacity, quality and engagement across most of the agency for > Two quarters • ***Single or multiple fatalities*** or serious sustained health impacts for a large number of people	***Complete loss of public confidence and trust for the agency's management of the scheme*** leading to significant Government intervention and/or inquiry. Board and/or CEO removed.
D	***Significantly below*** target levels across ***multiple regions*** for: • Participant intake levels for > ***One quarter*** • Participant satisfaction levels for > ***Two quarters*** • Participant outcomes for ***6 - 12 months***	• ***Scheme*** support ***costs 10 – 20 per cent over target*** • Agency costs 10 – 20 per cent over budget • Divisional operating costs > 25 per cent over budget • Divisional underspend 40 - 60 per cent	• ***Significant shortages*** in availability of ***some critical service supply*** across ***multiple regions*** for > ***One quarter*** requiring some NDIA intervention • Significant and lengthy impact on provider sentiment across multiple regions for > ***One quarter***	• ***Significant deficiencies*** in ***workforce*** capacity, quality and engagement across most of the agency for > ***One quarters*** • ***Potentially serious or life threatening*** consequences for a person or with systemic health effects across large parts of the workforce	***Significant loss of public confidence and trust relating to multiple aspirations over > One quarter.*** Increased scrutiny at ministerial level.
C	***Moderately below*** target levels across ***One or more regions*** for: • Participant intake levels for > ***One month*** • Participant satisfaction levels for > ***One quarter*** • Participant outcomes for Three - ***Six months***	• ***Scheme*** support ***costs 5 – 10 per cent over target*** • Agency costs 5 - 10 per cent over budget • Divisional operating costs 20 – 30 per cent over budget • Divisional underspend 25 – 40 per cent	• ***Moderate shortages*** in availability of ***some service supply*** across ***One or more regions*** for > ***One month*** • ***Moderate impact*** on provider sentiment across ***One or more regions*** for > ***One month***	• ***Moderate deficiencies*** in ***workforce*** capacity, quality and engagement across ***One or more divisions and/or multiple regions for > One month*** • ***Significant injury*** or ***health effects*** to a person or cohort	***Moderate loss of public confidence and trust on One or more issues for > One month***
B	***Slightly below*** target levels across ***One or more regions*** for: • Participant intake levels for < ***One month*** • Participant satisfaction levels for < ***One quarter*** • Participant outcomes for < ***Three months***	• ***Scheme*** support ***costs 2 – 5 per cent over target*** • Divisional operating costs 10 – 20 per cent over budget • Divisional underspend 10 – 25 per cent	• ***Delay*** in availability of ***few non-critical services*** across ***One or more regions*** for < ***One month*** • Minor impact on provider sentiment across ***One or more regions*** for < ***One month***	• ***Minor deficiencies*** in ***workforce*** capacity, quality and engagement within ***One division*** for < ***One month*** • ***Minor impact on a person's health***	***Some loss of public confidence and trust on a single issue for < One month***
A	***Below target*** levels within ***One region*** for: • Participant intake levels for < ***One week*** • Participant satisfaction levels for < ***One month*** • Participant outcomes for < ***One month***	• ***Scheme*** support ***costs < 2 per cent over target*** • Divisional operating costs 5 – 10 per cent over budget • Divisional underspend < 10 per cent	• ***Minor delay*** for < ***One week*** in availability of ***non-critical services within One region*** • Minor impact for < ***One week*** on provider sentiment ***within One region***	• ***Temporary minor shortfall*** in ***workforce*** capacity, quality and engagement ***within One region***	***Minor and isolated damage to public confidence and trust within 1 region or issue.***

Notes:

1. As measured by performance against the 6 cost drivers set by the Quality and Sustainability team
2. Note, availability of services will be driven by the number of providers, provider satisfaction, prices of services and level of demand relative to expectations
3. Impact on public confidence and trust is measured by impact on media attention (including social media), ministerial complaints and market research

2c. Assess the chances of the risk occurring.

For each risk that is identified in step 1 an assessment should be made as to the chances of that risk occurring, with the selected consequences (2b), within the next year using the guidance table below outlines the different probabilities to assess the chances of the risk occurring.

Table 2. Likelihood ratings

Likelihood rating	Likelihood of the risk occurring in the next year
Five	> 80 percent likelihood of the risk occurring in the next year
Four	50 percent – 80 percent likelihood of the risk occurring in the next year
Three	20 percent – 50 percent likelihood of the risk occurring in the next year
Two	5 percent – 20 percent likelihood of the risk occurring in the next year
One	< 5 percent likelihood of the risk occurring in the next year

Risk Heat Map

The likelihood and consequence rating are used to assess the overall rating of the risk based on the risk heat map outlined below.

Table 4. Consequences per risk rating category

	Likelihood				
Consequence	**One**	**Two**	**Three**	**Four**	**Five**
E	**M**	**H**	**H**	**C**	**C**
D	**M**	**M**	**H**	**H**	**C**
C	**M**	**M**	**M**	**H**	**H**
B	**L**	**L**	**M**	**M**	**M**
A	**L**	**L**	**L**	**L**	**L**

Risk Level	Low (L)	Medium (M)	High (H)	Critical (C)

Risk escalation and acceptance guidance

Based on the risk rating determined for each risk the following risk acceptance and escalation guidance will be used. This is not prescriptive and is meant to be used as a guide only. This table should help guide the level of manage effort that should be given to managing the risk and what level of monitoring and reporting is required.

Table 5. Risk escalation criteria

Risk Rating	Risk acceptance and escalation guidance	Escalation to ERC	Escalation to Board
Critical	**Risks with this rating are unacceptable and urgent action should be taken to avoid or reduce the risk as soon as possible**. Avoiding a risk may mean deciding not to start or continue with the activity where this is practicable. **In relation to health and safety risk, the activities that give rise to the risk must NOT be performed.** The CEO and Chairman must review the risk and the CEO must provide direct oversight of the response.	**Yes**	**Yes**
High	**Risks with this rating are typically undesirable.** Cost/benefit analysis required to assess extent to which risk should be treated – monitor to help ensure risk does not adversely change over time. **In relation to health and safety risk**, the task must NOT be performed or substantial revision to activities must be	**Yes**	**As determined by ERC**
Medium	**Risks with this rating may or may not require further mitigation and require ongoing monitoring.** Constant/regular monitoring to ensure that exposure to the risk is managed effectively, disruptions are minimised and outcomes monitored. **In relation to health and safety risk**, activities must NOT be performed without the approval from the Regional/Branch Manager and General Manager; who will verify that all reasonably practicable treatments have been implemented	**Yes**	**Typically no**
Low	**Risks with this rating are typically acceptable.** Treatment measures should be subject to monitoring by the General Manager. Effectively manage through routine procedures and appropriate internal controls. In relation to safety risk, control measures should be effective and reliable and subject to appropriate monitoring.	**Typically no**	**No**

3. Manage

3a. Identify and document and additional actions that are required.

If step 2a has identified that the current actions in place to manage the risk are not sufficient, or if the risk rating is still too high against the risk appetite if the agency then consideration should be given to what else can be done to better manage the risk on a cost effective basis.

When thinking through additional actions things to consider include whether the action will:

- Reduce the chances of the risk occurring (preventative)
- Reduce the consequences if the risk does occur (post-event management)
- Limiting the variability around a certain outcome

Consideration should also be given to the:

- Resources required to implement
- Ongoing resources required to operate
- Time required to implement (i.e. Certain risks may be more time sensitive than others)
- Capacity for the Agency to accept the change and alignment with any other initiatives underway

Any additional actions that are agreed should be documented in the Risk Action Plan with assignment of clear deadlines and accountabilities.

4. Monitor and Report

Monitor and review of Risk Action Plans is an essential ongoing component of the risk cycle as it will:

- detect any changes to the internal and external context
- identify emerging risks
- measure performance of risk actions in place
- provide oversight and governance of risks and treatments
- assess if the risk has changed and requires escalation, or is no longer valid and can be archived from the risk action plan.

Consistent reporting of risk will:

- support stakeholder engagement and accountability in the process
- include the right people to help to reduce uncertainty
- provide information and reports to relevant stakeholders
- create opportunities to collaborate, advise and provide expertise to assist the process
- increase awareness of risk management and its value
- improve the decision-making process.

4a. Document the outcomes of your work in the risk action plans. Update and report on them regularly.

The ongoing monitoring of risk exposures and the effectiveness of current actions in place is an important component of the risk management process, providing the opportunity to refine activities as circumstances change.

The process of monitoring is through the review and update of the Risk Action Plan on a Quarterly Basis. In addition to this there should be continuous and regular discussions on the progress of risk management actions and the levels/ratings of risk.

The review of the Risk Action Plans will be facilitated by the Risk Champions but the Risk Owners should drive the review, assessment and update of the Risk Action Plan. When a significant change occurs within the division or region or a critical decision is being made a review of the Risk Action Plans should also occur.

4b. Report any significant changes in risk as required

The Risk Action Plan is reviewed and updated on a quarterly basis and reported through to the Enterprise Risk Committee for review.

In addition, any incidents and significant risks should be escalated as and when they happen.

At least once a year each Divisional General Manager is required to report to the Enterprise Risk Committee to give a more detailed overview of the risks to their area and key actions that are being taken to manage the risks.

The main risk reporting activities and outputs are outlined below.

Table 6.

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 ERC 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 EMG. The report will be accompanied by a reporting view of the material divisional and/or project risks.	Monthly	EMG	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	EMG	Initiative Owners	Board
2) Divisional Plans	**Divisional Risks** Quarterly review of the risk impacting on the ability of the divisions to achieve their divisional plans and informs Strategic Risk Reporting. Co-discussion with Risk Champions and reporting provided to the ERC (phased handover approach from ES&R branch to Risk Champions).	Quarterly	GMs	BMs	ERC
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 Risk Champions and reporting provided to the Divisional GM's.	Monthly	GMs	RMs	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	PMC

5. Learn

5a. Consider and share what you learnt from previous experiences.

A key component of a risk management cycle and one of the key risk behaviours at NDIA is that staff share and learn from the NDIA's mistakes and successes. Whenever the risk management cycle is used or whenever the Risk Action Plans are reviewed and updated there should be an element of looking back to understand what happened previously and how that differed from expectations.

This information can be used to inform potential risk areas and mitigation strategies for consideration. Insights gained from the exercise should be shared with the rest of the Agency on a regular basis.

The Risk Champion network is in place to facilitate this process but Divisional and Regional Managers should also look to share risk learnings at meetings and forums that they attend.

Appendix A – Risk Action Plan

Add Risk

Risk Action Plan

Identify				Assess							Manage			
ID	Risk Description	Cause(s)	Impact(s)	What is currently in place to manage the risk	Effectiveness of current actions	Likelihood	Consequence	Highest Consequence Category	Overall Impact		What additional actions are required	Accountabilities	Due Date	Comments
1		1	1	1							1			
		2	2	2							2			
		3	3	3							3			
		4	4	4							4			
		5	5	5							5			
		6	6	6							6			
		7	7	7							7			
		8	8	8							8			
		9	9	9							9			
		10	10	10							10			
2		1	1	1							1			
		2	2	2							2			
		3	3	3							3			
		4	4	4							4			
		5	5	5							5			
		6	6	6							6			
		7	7	7							7			
		8	8	8							8			
		9	9	9							9			
		10	10	10							10			
3		1	1	1							1			
		2	2	2							2			
		3	3	3							3			
		4	4	4							4			
		5	5	5							5			
		6	6	6							6			
		7	7	7							7			
		8	8	8							8			
		9	9	9							9			
		10	10	10							10			
4		1	1	1							1			
		2	2	2							2			
		3	3	3							3			
		4	4	4							4			
		5	5	5							5			
		6	6	6							6			
		7	7	7							7			
		8	8	8							8			
		9	9	9							9			
		10	10	10							10			

Appendix B – Risk Taxonomy

NDIA Risks	Risk Types	Examples
Macro environment	Economic	Economic downturn, changing socio-economic circumstances,
	Social	Changing demographics, social trends, community expectations
	Market	Changing market structure, market expectations, market participants' quality
	Political	New or changing legislation/regulation, more active enforcement/ monitoring, change in government
	Environmental	Natural disasters, climate change (e.g. heatwaves impacting participants)
	Human threat	Terrorist attack, vandalism, theft, malicious software attacks, computer viruses, external fraud
Industry environment	Market	New market entrant, industry convergence, technological breakthroughs, changing market structure, market expectations,
	Participants	Changing participant needs, increase in participant complaints, participant numbers over target
	Third Parties	Contract failure, reputational damage, adverse third party strategy/action
Operational/Value Chain	Assessment	Data issues, inadequate guidance, lack of information from state governments
	Planning Process	Workflow issues due to data loading, lack of sufficient policy guidance around planning process, lack of clinical experience for complex decisions, lack of accurate data for bilateral targets, system issues prevent first planning contact, staff knowledge and training is not adequate, ineffective recruitment/on-boarding processes, inconsistent decision making and provision of supports
	Coordination of Services	Lack of or appropriate physical accommodation, inadequate coordination with LACs, Data exchange issues,
	Service Provided	Not enough services available to meet demand, inconsistent decision making and provision of supports,
	Billing	Payment integrity, fraud, data issues, billing errors, system issues impacting on billing
	Review of Plans	Lack of monitoring of plans and achievement of goals, lack of communication/feedback regarding planning decisions made
	Plan Adjustments	Poor response to complaints, changing definitions, lack of policy guidance,
Corporate Support Functions	Business Transformation	Information security, data availability, data integrity, system functionality, system capacity, shared-services arrangements, tiered complaints handling
	People and Culture	Skills shortage, key staff dependency, morale, culture, health & safety, internal fraud
	Finance	Payment integrity, funding arrangements, Agency costs, Buildings and infrastructure, procurement of services
	Governance and Stakeholder Relations	Non-compliance with laws or regulations, communications, external relations

Risk in Change Guide

December 2019

Document Version Control

Version	Author	Date	Comment
1	s22(1)(a)(ii) - irrelevant material	9 Sept 2019	
2	s22(1)(a)(ii) - irrelevant material	13 Sept 2019	
3	s22(1)(a)(ii) - irrelevant material	23 Sept 2019	
7	s22(1)(a)(ii) - irrelevant material	31 Oct 2019	

Reviewers

Version	Author	Date	Comment
1	Tammy Lamperd	10 Sept 2019	
2	Julian Toscano	18 Sept 2019	
7	Tammy Lamperd	31 Oct 2019	
8	Julian Toscano	20 Nov 2019	
9	s22(1)(a)(II) - irrelevant materta	22 Nov 2019	

Approvals

Version	Author	Date	Comment
8	Tammy Lamperd	1 Nov 2019	
9	Tammy Lamperd	23 Nov 2019	

Distribution List

Version	Author	Date	Comment

Table of contents

Risk in Change Guide 1
Table of contents 3
1. Introduction 4
1.1 Context of Risk in Change 4
1.2 Purpose of this Guide 5
2. What is Risk in Change? 5
3. Objectives and Benefits 5
4. Scope of Risk in Change Activity 6
5. Risk in Change Process 7
6. Risk in Change Governance 12
7. The Roles and Responsibilities 13
Helpful Links 15
Attachments 16

1. Introduction

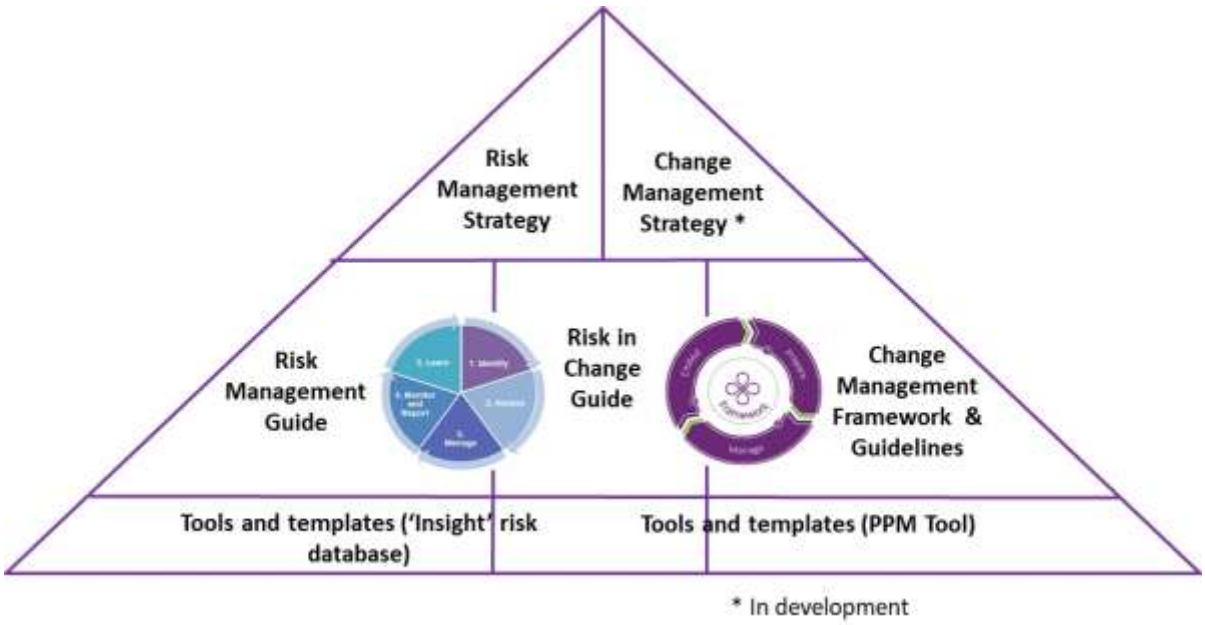
1.1 Context of Risk in Change

The scale, pace and complexity of change required to implement the NDIS brings with it considerable uncertainty. To address this uncertainty the Agency has largely managed risk within business areas and programs/projects.

However, it is also acknowledged that any change driven by a 'project, or a business improvement delivered within a business area', has the potential to impact the activities of other projects or business areas. Our change management approach has always been focused on mitigating risks and impacts to the business as a result of the change delivered from projects to business areas, however, there has not been a framework to capture these risks in any formal way. Risks associated with change were variably reported from projects, and were not often transferred to impacted areas.

To ensure our approach to managing risk within NDIA is comprehensive the Agency is now implementing Risk in Change practices that essentially integrate our existing, well established, Enterprise Risk Management Guide and Change Management Framework (Attachment 1 and Figure 1 below).

Figure 1 Risk in Change Architecture



This Risk in Change Guide supports the NDIA Risk Management Strategy by helping to build a robust, high-performing, professional and systems-based Agency that continues to improve its practices through six areas of focus:

- 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

1.2 Purpose of this Guide

This Guide is built on the Agency's commitment to high quality risk and change management, as described in its Risk Management Strategy and Change Management Strategy respectively.

The purpose of the Guide is to build an understanding of how to successfully implement Risk in Change practices within the NDIA and specifically aims to:

- explain the context of Risk in Change and the scope of its implementation
- explain the objectives of Risk in Change and the benefits to be achieved
- explain how Risk in Change is an integration of NDIAs enterprise risk management and change management frameworks
- describe the Risk in Change management phases and steps
- describe how Risk in Change is incorporated into the Program Execution Framework
- explain the roles and responsibilities for implementing Risk in Change
- provide guidance on available Risk in Change management tools and templates
- provide a common language when communicating about risk in change
- embed consistent Risk in Change methodology throughout the Agency

2. What is Risk in Change?

Let's break it down…a risk is, by definition, the effect of uncertainty on objectives and change is to make something different.

- Risk in Change is the process of identifying and managing risks, resulting from a business improvement, and associated change. implemented within a program/project, or business activity, that can impact on Agency aspirations/goals and delivery of business processes (unintended consequences)
- Delivered Risk is a risk impacting the objectives of the business area, or program/project, who will receive the change (people, process, system).

3. Objectives and Benefits

By implementing a structured approach to identifying and managing delivered risks it is expected that key stakeholders (including business process owners, product owners, project owners, project managers, change managers, and risk partners) will have an understanding of how:

- the change, being implemented by their Project or business activity, *can potentially impact other areas* of the NDIA, and that these impacts will be acknowledged as delivered risks in their risk management activities
- their activities *can potentially be impacted on from changes being implemented in other areas* of the NDIA, and will incorporate associated delivered risks into their risk registers

While project delivery risks and business risks are largely managed internally, it is clear that the successful implementation of a Risk in Change process requires effective engagement and collaboration between business areas and projects.

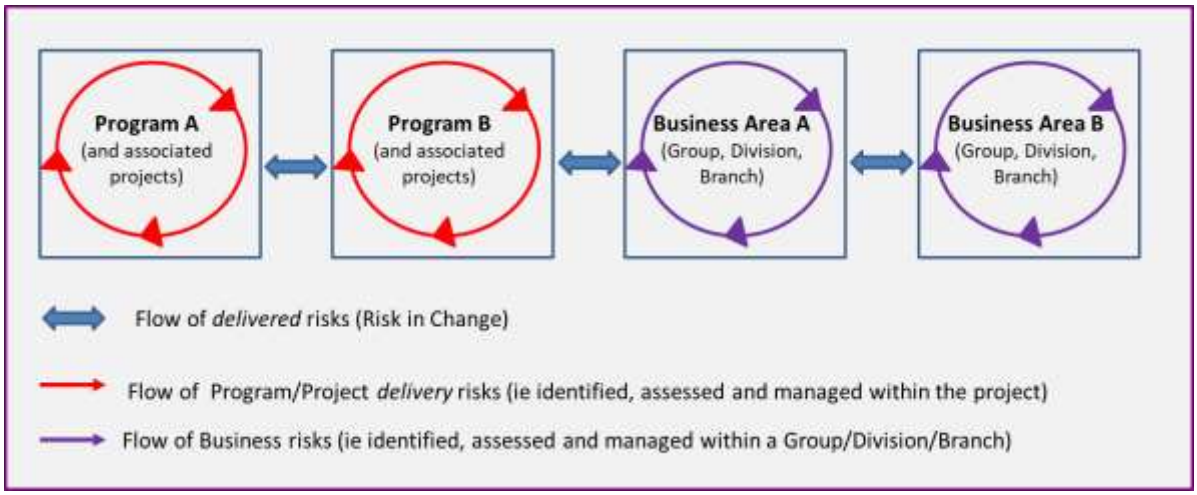
Formal consideration and incorporation of Risk in Change practices, within a project or business area, will lead to:

- a more complete understanding of your entire risk exposure
- clearly identified areas/processes of the Agency impacted and where control/treatment needs to be focused
- more confident and improved decision making
- more effective allocation of resources
- continued maturing of Agency Risk Management Framework

4. Scope of Risk in Change Activity

Risk in Change practices will be implemented in any area of the NDIAs operations where a change driven by a project or business area has the potential to create a risk in another project or business. Figure 2 below highlights that risks can be delivered between programs/projects, programs/projects to business areas and between business areas

Figure 2: Scope of Risk in Change Activities

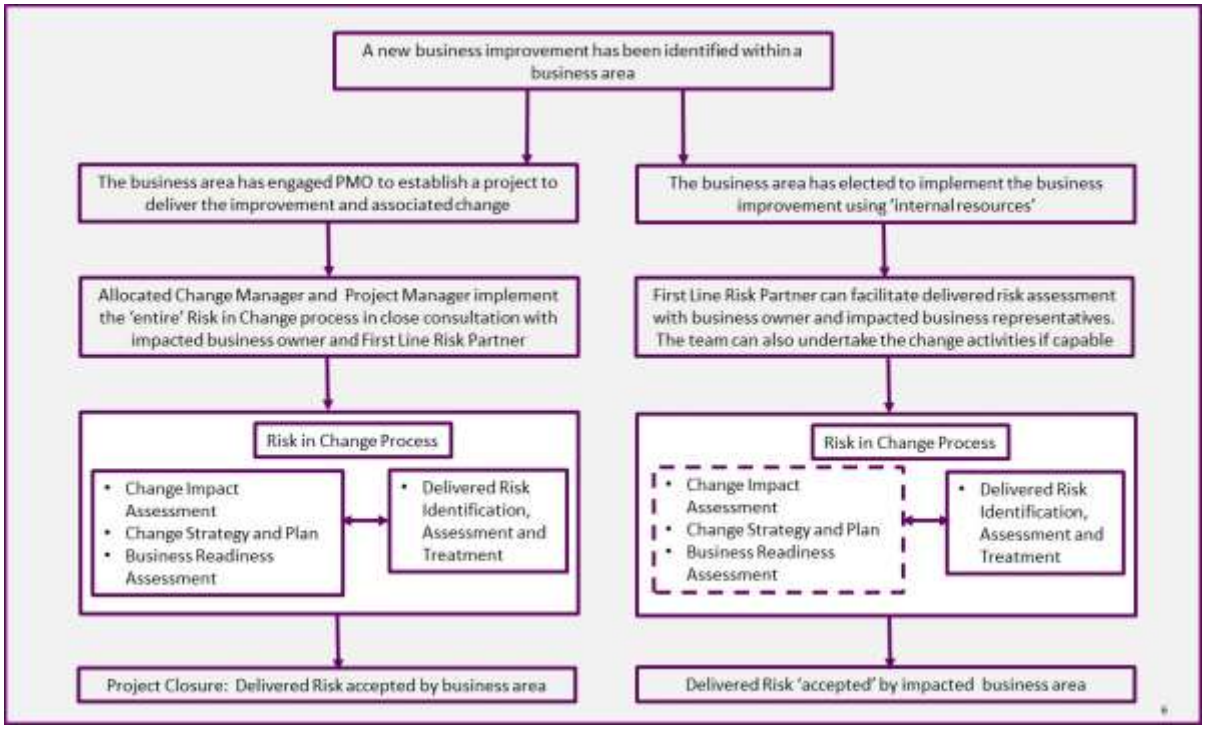


Risk in Change practices can either be formerly implemented through PMO coordinated projects, facilitated by a dedicated Change Manager and Project Manager, or 'less formerly' implemented within a business area using internal resources and facilitated by the relevant

First Line Risk Partner (Figure 3). In this situation the change management tasks are not always undertaken, as indicated by the dashed line box in Figure 3. Change management tasks can, however, be completed by the First Line Risk Partner, or a business area representative(s) assuming they have participated in change management training and are capable in effectively completing the change templates etc located on the intranet. Assistance can be provided by Enterprise Change.

In the future as the change and risk management frameworks are further adopted by business area's it will be expected that the formal application of the risk in change process will be applied to all change initiatives within the Agency.

Figure 3: Implementing Risk in Change



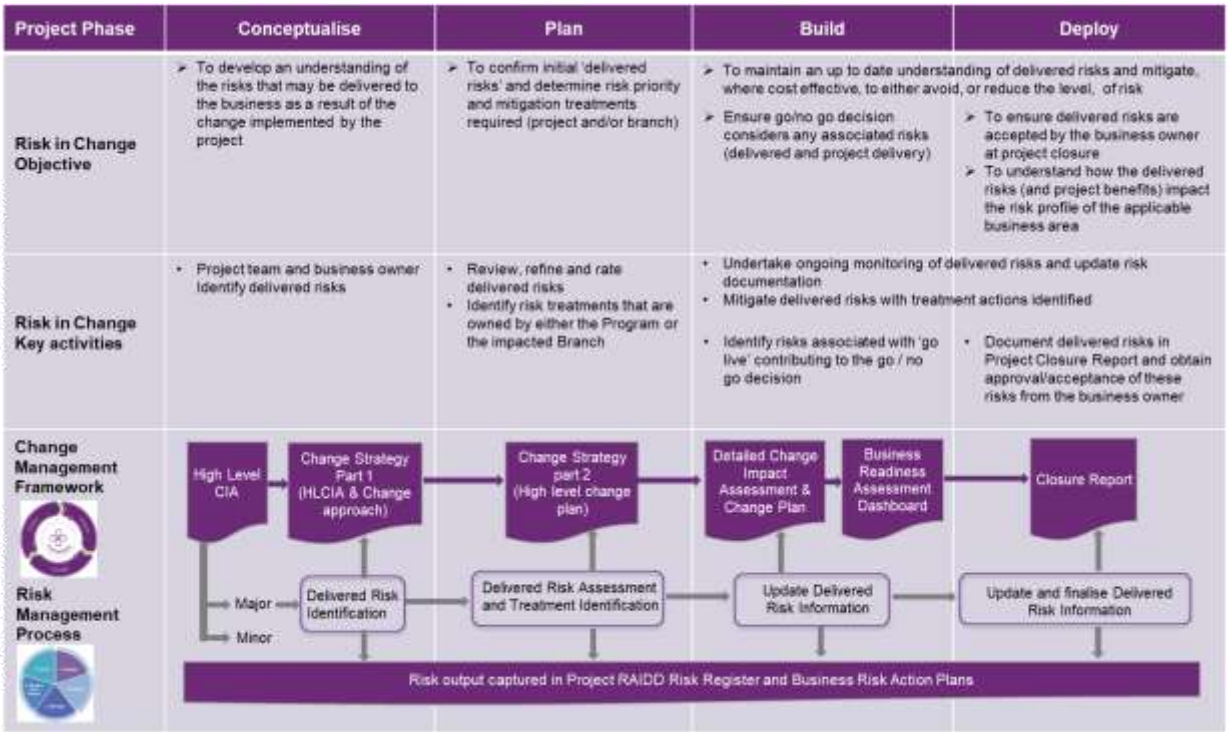
5. Risk in Change Process

The Risk in Change process is effectively the integration of existing enterprise risk and change management frameworks.

It is important to note that the change management process may vary dependent on project size, complexity and time factors. However, the change process indicated in the figure below, is a good indication of the types of change activity as they occur across a typical project lifespan. Aligned with this flexibility the risk process can commence at whatever stage the change management approach commences.

Figure 4 shows the Risk in Change Process (Change and Risk Processes), and how the Risk in Change process is deployed across the key phases of the NDIA Project Execution Framework (PEF).

Figure 4: Risk in Change Process



It is worth highlighting again that for the Risk in Change process to be successful there *must be* engagement between the project team (project owner, change manager, project manager) and the business area receiving the change (business process or product owner, first line risk partner …) *from project commencement to completion*. **This ensures that any delivered risks are well considered, relevant and are agreed to between project and business teams throughout project delivery and therefore, avoiding any 'surprises' at project closure and handover.**

The key stages of the Risk in Change process, highlighted in Figure 4, are summarized below. The NDIA's Risk Management Guide and Change Management Guidelines provide further information on the Risk in Change process stages.

Stage 1 High Level CIA

At the commencement of a change activity ("Conceptualise Phase" in the PEF), a "High Level Change Impact Assessment" (HLCIA) is completed to determine the size and complexity of the change impact to:

- service delivery stakeholders including participants, providers, Partner LAC, service delivery staff, and national access and workflow
- NDIA national office groups and divisions
- size, scope and risk associated with the change

The outcome of the assessment will determine if the proposed change impact is either "Major" or "Minor". A Minor impact is often limited to a specific group or team, whereas a Major impact often affects multiple groups or divisions, internally and/or externally.

Stage 2 Delivered Risk Identification

If the HLCIA determines the change impact to be "Major" this triggers the requirement to undertake a 'delivered' risk assessment, consistent with the approach described in the NDIA Risk Management Framework. A delivered risk review meeting needs to held with appropriate project and business representatives at the 'Conceptualise' Project Phase (see above) to identify the delivered risks associated with the change. To support this risk identification process the NDIAs "Risk Categories" can be referred to for 'prompts' (Attachment 2). These risks are captured in both:

- *"PPM Tool"* by the Project Manager, working closely with the Change Manager, and are referred to as 'Delivered Risks' in the Tool
- *"Risk Module"* in the Insight Tool, by the applicable First Line Risk Partner, and are referred to as 'Operational Risks'

Note that a "Minor" change impact from HLCIA does not preclude the project and business teams from identifying and recording any delivered risks.

Step 3 Change Strategy (Parts 1 & 2)

If delivered risks have been identified high level mitigating actions are identified in the Change Strategy.

The Change Strategy provides an overview of the change characteristics, scope and change vision for an initiative. The strategy also defines at a high level the approach to be taken for elements including but not limited to:

- stakeholder communication requirements and timelines
- training requirements, timeline and approach for the stakeholder group
- activities to be included in the Business Readiness to Go-Live checklist
- support strategy to handover to the Business

The Strategy describes at a high level the sequencing of such activity in order to take impacted stakeholders through the change in such a way that they have the desire, knowledge and ability to adopt the change in a sustainable way.

Step 4 Delivered Risk Assessment and Treatment

While the Change Strategy is being updated an assessment of the identified delivered risks is conducted to determine the risk rating (significance of the risk). If a delivered risk is impacting on a business process or product then it is imperative that the enterprise 'consequence' and 'likelihood' criteria, shown in the NDIA Risk Management Guide, are referred to during this assessment. If however, a delivered risk is impacting on the delivery

of another project then the equivalent criteria used for project risk assessment, provided in the "*PPM Tool"*, must be referred to. Key tasks to assess and treat the risk comprise:

- identify the controls that are currently in place, within the impacted business area or project, to manage the delivered risks
- undertake 'current risk assessment' by determining consequence and likelihood levels of the risk occurring *with* the current controls in place
- determine the additional actions (treatments) that could be cost effectively implemented, either during project delivery, or within the impact business area, to further mitigate the risk. Clearly any mitigation that can be implemented during the change activity may eliminate the risk from ultimately being delivered into the impacted business area or project, or at least reduce the significance of the risk when delivered
- undertake 'treated risk assessment' by determining the most probable consequence and likelihood levels *after* additional actions have been applied

Once agreed, the risk assessment ratings, controls and additional actions are included in both *"PPM Tool"* and the risk module in *"Insight"*, and also incorporated into the Change Strategy.

Step 5 Detailed Change Impact Assessment, Change Plan, and Risk Update

The Detailed CIA and Change Plan builds on the output of the HLCIA and Change Strategy for each of the key stakeholders impacted by the change, and documents:

- in detail, what is changing for each stakeholder and the impact of that change
- the change impact rating (high, medium or low)
- the type of change activity required
- the actions necessary to mitigate the change
- a sequence of activity to take the impacted stakeholders through the change

The information compiled in both *"Insight"* and *"PPM Tool"* needs to be regularly reviewed during the project, with impacted business area representatives, to ensure it remains up to date and is an accurate record of delivered risk information. A key consideration during this review is to determine if any 'additional actions' (treatments) identified are being implemented. Once agreed the controls and additional actions are and also incorporated into the Detailed CIA and plan as change impact mitigating actions.

Stage 6 Business Readiness Assessment Dashboard

The purpose of the Business Readiness Assessment is to indicate the readiness status of a change from a business adoption perspective and to ensure stakeholders (participants, providers and staff) considerations are at the centre of our thoughts. It provides business owners with a succinct summary of the readiness status of a change prior to the change 'going live'. This information allows the business owner to make an informed decision to proceed with the change or make alternate plans. The readiness assessment aims to answer the question: Is the business ready to support the change and ensure it is a success at implementation?

The Dashboard has a section indicating the status of delivered risks which must be completed by the project team.

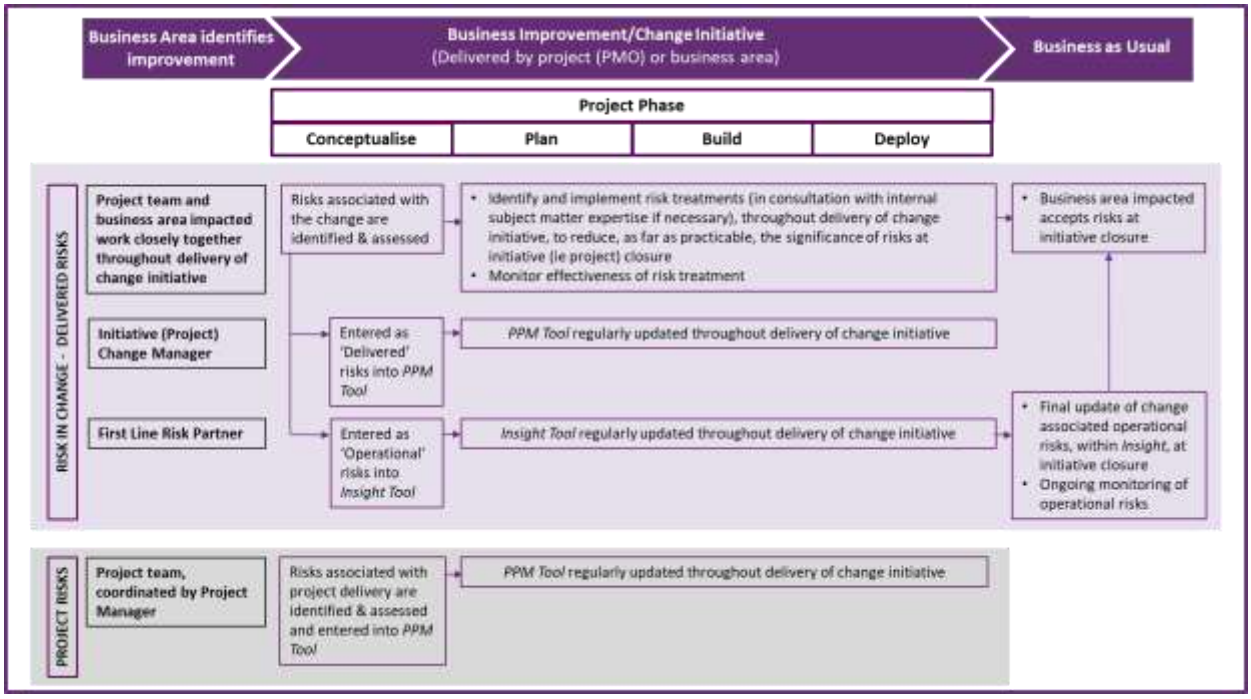
Stage 7 Project Closure (Change and Risk Inputs)

At the completion of a project a closure report is prepared by the Project Delivery Lead in order to complete the business improvement (change activity) transition to business and project closure process. The report includes the requirement for the:

- Project Change Manager to document 'Performance Against Change' (change objectives, change measures and change performance)
- Project Risk Lead or Project Change Manager summarise key risk information (risks being delivered to the impacted business area, impacts if the risk was to occur, risk rating, and the controls/treatments to mitigate the risk by the business area). Assuming the required engagement between project and impacted business area representatives has occurred throughout the project (ie from 'Conceptualise' to 'Deploy'), the delivered risks listed in the Project Closure Report will have been recorded as 'Operational Risks, in *"Insight"*, for the impacted business area. Therefore, their agreement for these risks to be transferred into the business, from the project, will be a 'formality'.

The interaction of the key risk in change activities, responsibilities, and supporting tools, during the delivery of a change initiative, and transition into business as usual, is shown in Figure 5.

Figure 5 Interaction of risk in change activities, responsibilities and supporting tools



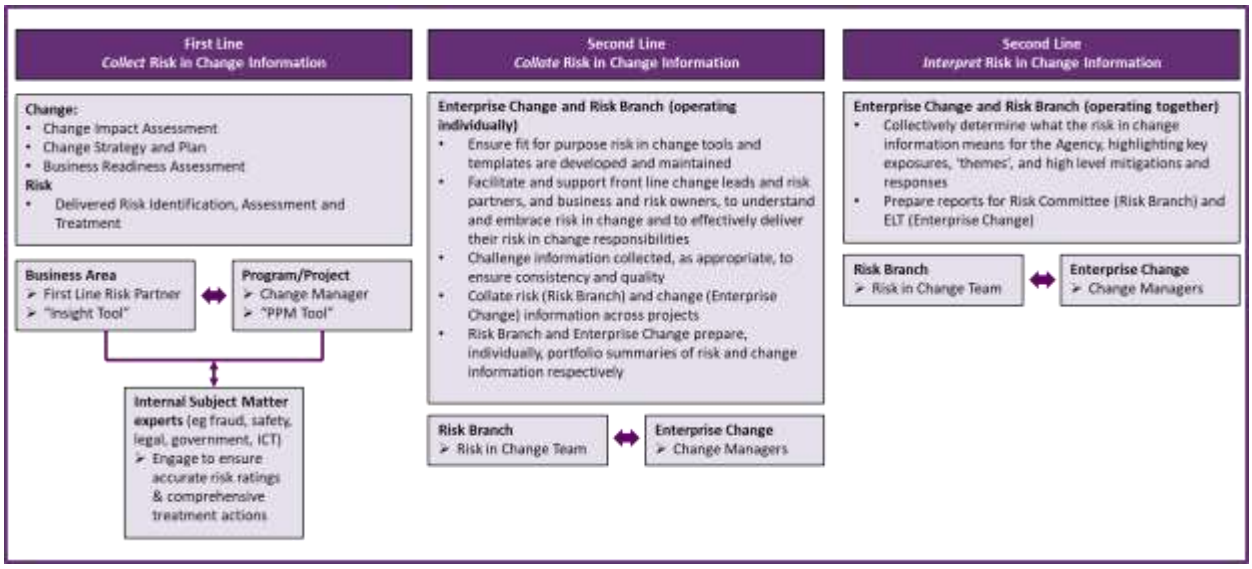
Project Impacts on Business Areas Risk Profile

While not a prescribed stage in Risk in Change process it is highly recommended that the Project Change Lead consults with the applicable First Line Risk Partner, one to two months after project closure, to determine how the project change activity impacted the business area's risk profile (ie have the current risk ratings been increased or reduced as a result of the change and delivered risks?) This is an informal consultation, however, provides further insight into how successful the change activity was.

6. Risk in Change Governance

The key Risk in Change activities, responsibilities, and supporting tools, as described throughout this Guide, are incorporated into the NDIAs First Line and Second Line governance model (Figure 6).

Figure 6 Risk in Change Governance



7. The Roles and Responsibilities

There are a number of key roles and responsibilities in the effective implementation of the Risk in Change process.

Position	Roles and Responsibilities
(Project) Change Manager	• Is the steward for the Delivered Risks associated with the Project • Engage with representatives from the impacted business area (including First Line Risk Partners) from project 'Conceptualise Phase' to: o identify and assess Delivered Risk and work with Project Manager to record output in the *"PPM Tool"* o confirm existing controls that are in place to manage the identified Delivered Risks, and to identify further treatments that be undertaken either by the project team or impacted business area, to further mitigate the risks o depending on the delivered risks identified you should consult with internal subject matter expertise (eg fraud, ICT, property, safety, legal, government, partners, community) to ensure the risks have been rated appropriately, and to confirm existing controls in place to manage the delivered risks, and/or to identify relevant, additional treatments that are necessary to mitigate the risk further. It may be necessary for both project and business teams to work with these subject matter experts to implement the particular controls and treatments o regularly review risk data including monitoring of treatments by agreed time and update *"PPM Tool"* as necessary • Provide regular, verbal update of Delivered Risk status at project meetings • Ensures delivered risks are discussed amongst project team. • Implements the change process • Ensures Delivered Risks are captured in the Project Closure Report
Project Owner and Project Manager	• Participate and contribute to the identification and recording of Delivered Risks, ensures mitigating actions are captured in project schedule, and assists in the management of Delivered Risks
Program/Project Risk Lead (if present)	• With Change Managers increase Project Managers understanding of Risk in Change process and tools • With First Line Risk Resources increase business process owners and product owners understanding of Risk in Change framework and tools • Facilitate completion of Delivered Risk assessment • Review quality of Delivered Risk data and engage Change Managers, Project Managers and business process owners to improve • Provide risk support as required
First Line Risk Partner	• Together with representatives from the impacted business area (incl Product Owner/Business Process Owner), engage with the project team, from project 'Conceptualise Phase' to closure to:

Position	Roles and Responsibilities
	o identify and assess Delivered Risk and record output in the *"Insight Tool"* o confirm existing controls that are in place to manage the identified Delivered Risks, and to identify further treatments that be undertaken either by the project team or impacted business area, to further mitigate the risks o engage internal subject matter expertise to ensure risks are rated appropriately, and to provide further information on existing controls or additional treatments for specific, identified delivered risks • Regularly review risk data including monitoring of treatments by agreed time and update • If a business is undertaking its own change initiative (ie business improvement), independent of the PMO, then First Line Risk Partners will facilitate the completion of the delivered risk assessment, and record/update the information in *"Insight"* • If there is no dedicated change resource for the change activity the First Line Risk Partner, if capable, can also facilitate the change initiative consistent with the Change Management Framework.
General Manager	• If a particular business area within NDIA elects to implement a business improvement/change activity internally (ie not a PMO coordinated project), then the General Manager of the business area must inform the relevant First Line Risk Partner to then initiate and facilitate the Risk in Change process
Product Owner, Business Process Owner, First Line Risk Partner	• Contribute to development of Delivered Risk assessment and ongoing review/update • Where possible identify and implement risk treatments, that can be undertaken during the change initiative (project), to reduce as far as practicable, the level of risk at project closure • At project closure, agree risks to be 'delivered' to the business
Risk in Change Team (Risk Branch)	• Ensure fit for purpose risk in change tools and templates are developed and maintained • Facilitate and support first line change leads and risk partners, and business and risk owners, to understand and embrace risk in change and to effectively deliver their risk in change responsibilities • Challenge information collected, as appropriate, to ensure consistency and quality • In consultation with Enterprise Change collectively determine what the risk in change information means for the Agency, highlighting key exposures, 'themes', and high level mitigations and responses
Internal Audit	• Conduct quality reviews and/or audits to assess the effectiveness of the Risk in Change process implementation. This will include an assessment of the level of engagement between both project team and impacted business team throughout delivery of the improvement initiative.

Helpful Links

Change Management

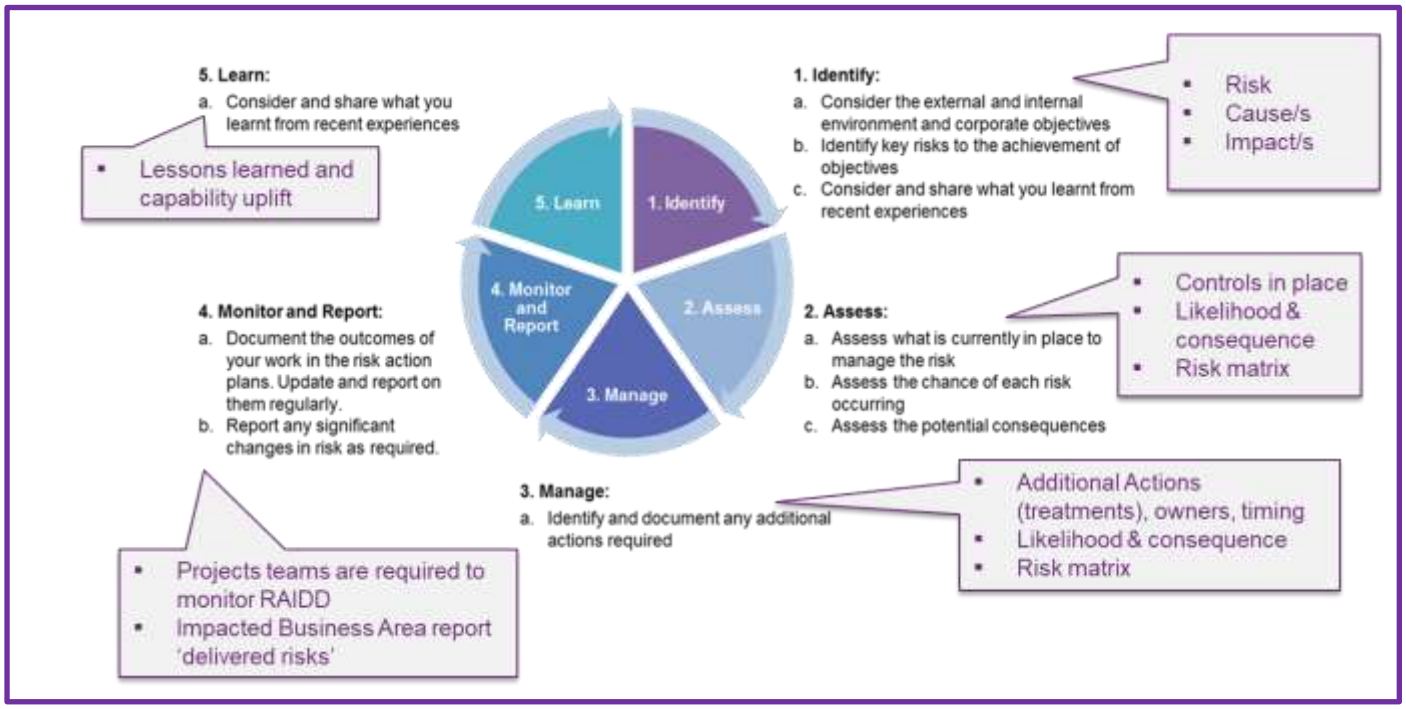
Program / Project Management

Risk Management

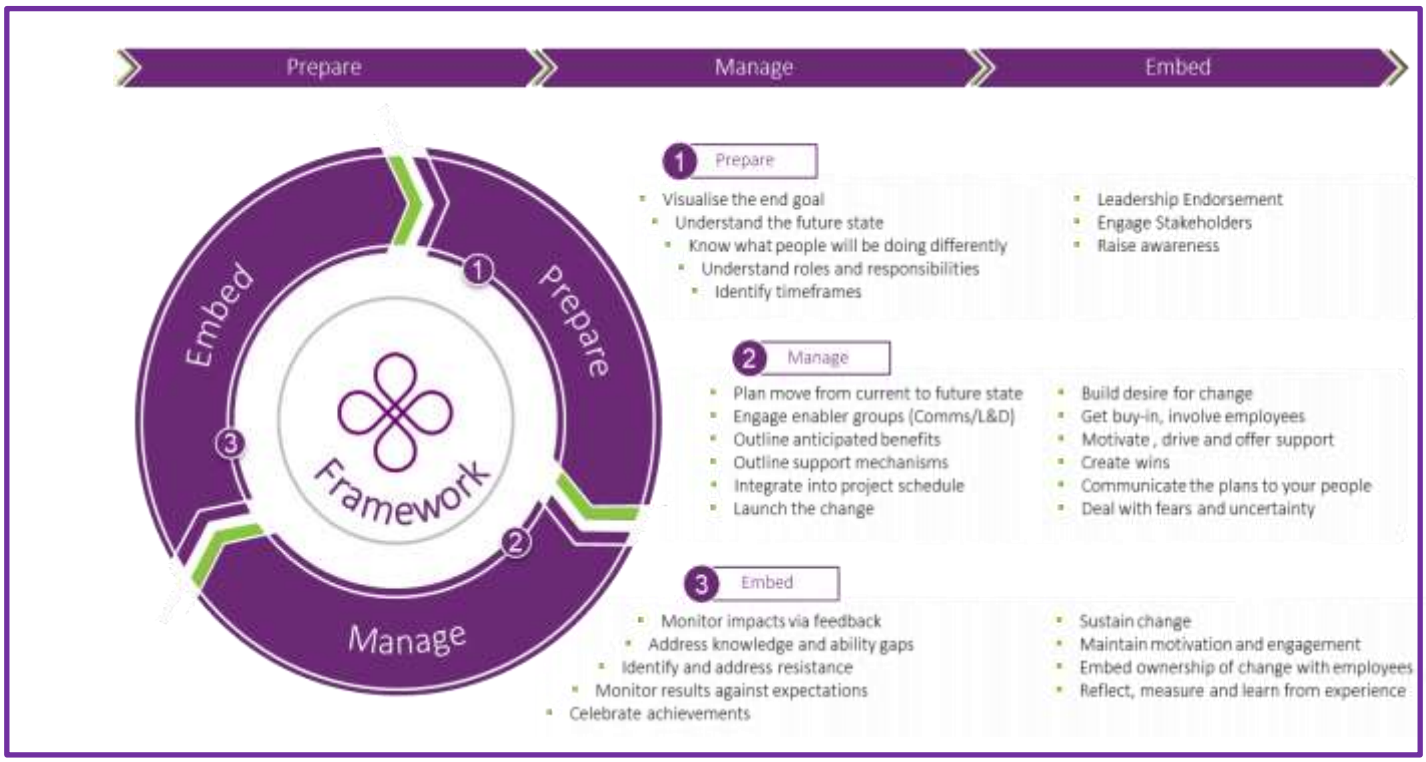
Attachments

Attachment 1

NDIA Risk Management Guide/Process



NDIA Change Management Process



Attachment 2

NDIA Risk Categories

Level 1 Risk Category	Level 2 Risk Category
Participant - Individuals that have applied for access to the NDIS and / or entered into the NDIS	Access
	Planning
	Workload management
	Service Delivery
	Rural & Remote
	Quality
	State
	Complex support needs
	Early Childhood Intervention
Delivery of a Service - The activities undertaken by the Scheme to provide services to participants	Bilateral
	Participants
	Planners / LAC
	Contract management
	Workload management
	Performance
	Strategy
	Complaints
	Escalations
	Mainstream
	Funding
Provider - The people and /or organisations that provide services to the NDIS and NDIS participants	Provider payments
	Market setting
	Markey enablement
	Market relations
	Provider relations
	Quality
	Contract management
	Revocation
	NDIS Quality & Safeguards Commission
Business Resilience - The activities undertaken that have a potential to impact the operations of the NDIA	Business Continuity
	Issues and Incident Management
	Crisis Management

Level 1 Risk Category	Level 2 Risk Category
	IT Loss
	Facility Loss
	Reputation
	Agency wide
	Disruption related event
Financial - The financing, financial management, transfer activities undertaken, and reporting thereof, for the NDIA.	Business Partnering
	Reporting
	Internal Audit
	Compensation Recoveries
	Applications & Decisions
	Triage & Early Resolution
	ANAO
	Insurance
	External Audit
	Budget
Fraud - Dishonestly gaining a benefit, or causing a loss, by deception or other means. There must be intent, not as a result of an honest mistake or poor training'	Fraud on the scheme
	Manipulation, misuse or disclosure of sensitive information
NOTE – these are the Commonwealth Fraud Categories	Manipulation or misuse of identity information
	Manipulation of financial systems
	Manipulation of procurement or contract management
	Administrative fraud on entitlements or recruitment
Legal - The activities of the Agency that support the provision of legal advice	Data Privacy
	Administrative Appeals Tribunal
	Legal Services
	Privacy
	Contracts
	Reviews

Level 1 Risk Category	Level 2 Risk Category
People & Culture - The activities that the Agency undertakes to ensure that it has the most appropriate people and programs in place to ensure the continuing operations of the Agency	Workplace relations
	Organisational capabilities
	Learning & development
	Enterprise bargaining
	Recruitment
	On-boarding
Government Relations - The activities that the NDIA undertakes with Governments to ensure the ongoing activities of the Agency.	Ministerial
	State & Territory
	Briefings/ Reporting/ Information
	Disability Reform Council
	Mainstream Interfaces
Procurement - The activities undertaken to provide procurement services to the NDIA	Contract management
	Vendor management
	Terms and conditions
	External Stakeholder engagement (DHS)
Property - The properties that the NDIA utilises to undertake its activities	Leased
	Sub leased
	Maintenance
	Insurance
	Rural & Remote locations
Project / Program / EPMO - The enabling activities that support the definition, execution and delivery of programs and projects for the Agency.	Time
	Schedule
	Quality
	Cost
	Change
	Budget
	Resourcing

Level 1 Risk Category	Level 2 Risk Category
	System Tools
Protective Security - The enabling activities undertaken to ensure the security of the Agency's people, locations and information.	Physical security
	Personnel security
	Information security
	Security related incidents
Regulatory - The activities undertaken by the NDIA to ensure it complies with legislation and regulations.	Strategy
	Requirements
	Changes
	Obligations
Stakeholder Management - the activities undertaken to ensure strategies, plans or designated relationship owners are in operation for material stakeholders.	Strategy
	Stakeholder Relationship e.g. no formal contact point for a key inter government agency relationship
	Relationship failure
	Community and Mainstream
Strategy - The activities undertaken that support the formulation, execution and monitoring of the Agency's strategy and Corporate Plan	Formulation
	Execution
	Monitoring
	Governance Reporting
Technology - The technology enablers that supports the operation and activities of the Agency and the Scheme.	Disaster Recovery Planning
	Cyber management
	Contract management
	Infrastructure
	Network
Scheme Sustainability - The activities undertaken to support the assessment, analysis, evaluation and dissemination of information relating to the operation of the Scheme.	Modelling
	Business Intelligence

Level 1 Risk Category	Level 2 Risk Category
	Reporting
	Technology
Workplace Health and Safety - The activities undertaken to ensure the health, safety and wellbeing of Agency people.	Hazard analysis
	Risk assessment
	Incident management
	Rural & Remote Travel
Information - The enabling activities to ensure the appropriate access, collation, recording and management of information.	Records management
	Storage
	Destruction
	Disposal
	Access
	Security
Communication – the activities undertaken to ensure that stakeholders are engaged with, in respect of agency deliverables and actions	Internal
	Media
	State & Territories
	Government Agencies
	Participants