myEmpowerPlan
NDIS SUPPORT SPECIALISTS

Risk Management Policy

Version 1.0 | February 2026

Introduction

*my*EmpowerPlan is committed to a proactive, structured and transparent approach to risk management across all service types. As a registered NDIS provider delivering Support Coordination, Specialist Support Coordination and Plan Management, the organisation recognises that effective risk management is fundamental to protecting participants, safeguarding their funds, maintaining regulatory compliance and ensuring the sustainable delivery of quality services.

Risk management is not a reactive process. At *my*EmpowerPlan, risks are identified, assessed, treated and monitored on an ongoing basis as part of everyday operations and governance. All staff share responsibility for contributing to a risk-aware culture where concerns are raised openly and addressed promptly.

This policy establishes the framework, responsibilities, processes and escalation thresholds that govern risk management across the organisation. It is supported by the Risk Register, which is maintained by the Operations Manager and reviewed on a quarterly basis.

Contents

Scope and Purpose

This policy applies to all employees, contractors, volunteers and stakeholders involved in the delivery of NDIS services at myEmpowerPlan, including:

- Support Coordination services — including participant-level risk, referral integrity, capacity building and service implementation
- Specialist Support Coordination services — including complex risk assessment, crisis planning and multi-agency coordination
- Plan Management services — including financial risk, fraud prevention, invoice management and budget monitoring
- Governance and operational activities — including workforce, technology, compliance and reputational risk

This policy applies to all operational contexts including service delivery, financial management, workforce management, information management, emergency response and organisational governance.

Risk Categories

*my*EmpowerPlan recognises the following categories of risk across its operations. This list is indicative and not exhaustive — staff are expected to identify and report any situation that presents potential for harm, loss or non-compliance.

Risk Category	Examples	Applicable Service / Standard
Financial Risk	Mismanagement of participant NDIS funds, fraudulent invoices, payment errors or delays, overspending, incorrect price limits applied.	Plan Management — Module 4
Operational Risk	IT system failure, cybersecurity breach, staff error, inadequate training, process failure, loss of key personnel.	All Services — Core Std 2.3
Compliance Risk	Breach of NDIS Practice Standards, Privacy Act non-compliance, failure to report reportable incidents, inadequate record keeping.	All Services — Core Std 2.3
Participant Safety Risk	Harm, abuse, neglect, exploitation or inadequate safeguarding of participants, including failure to respond to safeguarding concerns.	All Services — Core Std 1.2
Reputational Risk	Negative participant outcomes, complaints, media exposure, regulatory sanction or loss of registration.	All Services — Core Std 2.1
Conflict of Interest Risk	Undisclosed financial interests, biased referrals, related-party transactions, failure to disclose secondary employment.	SC / SSC / PM — Std 2.4
Support Coordination Risk	Failure to implement NDIS plan, inadequate capacity building, support breakdown, transition failure, dignity of risk not respected.	SC — Module 2a
Specialist SC Risk	Failure to manage complex or crisis situations, inadequate multi-agency coordination, insufficient safeguarding documentation.	SSC — Module 2b

Risk Category	Examples	Applicable Service / Standard
Workforce Risk	Lapsed worker screening, inadequate supervision, unqualified staff in specialist roles, high staff turnover.	All Services — Core Std 2.2
Strategic Risk	Loss of NDIS registration, financial insolvency, failure to plan for organisational growth or regulatory change.	Governance — Core Std 2.1

Roles and Responsibilities

Responsibility for risk management is shared across the organisation, with clear accountability assigned to specific roles.

Director	Holds ultimate accountability for the organisation's risk management framework. Approves the Risk Register annually. Must be notified of all High and Critical risks. Responsible for escalating Critical risks to the NDIS Commission where participant safety is at risk.
Operations Manager / Compliance Officer	Responsible for maintaining and updating the Risk Register. Conducts quarterly risk reviews. Coordinates corrective action plans for Medium and above risks. Reports risk trends to the Director.
Support Coordinators & Specialist Support Coordinators	Identify and report risks arising in participant files and service delivery. Document risk-related actions in case notes. Escalate participant safety risks immediately.
Plan Managers / Finance Officers	Identify and report financial and compliance risks. Monitor participant budgets for overspending risk. Escalate payment and fraud concerns to the Operations Manager.

All Staff and Contractors	Responsible for identifying and reporting any risk or potential risk observed during service delivery. Complete risk management training as required. Must not ignore or conceal risks.

Risk Rating Framework

All identified risks must be assessed using the 5x5 risk matrix below. The Overall Risk Rating is determined by multiplying the Likelihood score by the Impact score.

Likelihood Definitions

Rating	Score	Definition
Almost Certain	5	Expected to occur in most circumstances — highly probable.
Likely	4	Will probably occur — more likely than not.
Possible	3	Could occur at some time — roughly equal chance.
Unlikely	2	Not expected to occur but has happened previously.
Rare	1	May occur only in exceptional circumstances.

Impact Definitions

Rating	Score	Definition
Severe	5	Catastrophic impact — participant serious harm, death, criminal matter, or loss of NDIS registration.
Major	4	Significant impact — reportable incident, major financial loss, formal NDIS Commission investigation.
Moderate	3	Moderate impact — formal complaint, audit finding, service disruption, participant distress.
Minor	2	Minor impact — internal process issue, single participant inconvenience, easily remediated.

Rating	Score	Definition
Insignificant	1	Negligible impact — no harm, no service disruption, resolved at first contact.

Risk Matrix (Overall Rating = Likelihood x Impact

Likelihood \ Impact	Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Severe (5)
Almost Certain (5)	5 Medium	10 High	15 High	20 Critical	25 Critical
Likely (4)	4 Low	8 Medium	12 High	16 High	20 Critical
Possible (3)	3 Low	6 Medium	9 Medium	12 High	15 High
Unlikely (2)	2 Low	4 Low	6 Medium	8 Medium	10 High
Rare (1)	1 Low	2 Low	3 Low	4 Low	5 Medium

Risk Rating Definitions and Escalation Thresholds

Low (1–4)	Monitor and record. Review at next scheduled audit. No immediate escalation required.
Medium (5–9)	Assign owner and remediation timeframe. Escalate if unresolved within 30 days. Include in quarterly review.
High (10–16)	Senior management review required. Corrective action plan must be initiated within 5 business days.

Critical (17–25)	Immediate escalation to Director. Notify NDIS Commission if participant safety is at risk. Suspend activity if necessary.

Risk Management Process

myEmpowerPlan follows a four-step risk management process. This process is dynamic and continuous — risks must be revisited as circumstances change.

Step 1 — Identify

Risks are identified through multiple channels, including:

- Staff observation and reporting during service delivery
- Participant and stakeholder feedback and complaints
- Incident reporting and near miss reports
- Internal audits and file reviews
- External audits and NDIS Commission correspondence
- Financial monitoring and reconciliation processes
- Changes in legislation, NDIS pricing or regulatory guidance

All staff are encouraged and expected to report identified risks to their manager or directly to the Compliance Officer. Risks must not be ignored or managed informally without documentation.

Step 2 — Analyse and Evaluate

Each identified risk must be assessed using the 5x5 Risk Matrix in Section 5. The assessing staff member or manager must determine:

- Likelihood — how probable is this risk occurring?
- Impact — what is the potential consequence if it occurs?
- Overall Risk Rating — Likelihood × Impact score, mapped to Low / Medium / High / Critical
- Existing controls — what controls already exist to reduce this risk?
- Residual risk — what is the remaining risk level after existing controls are applied?

Step 3 — Treat

Risk treatment must be proportionate to the risk rating. Treatment options, in order of preference, are:

- Eliminate — remove the source of the risk entirely where possible
- Reduce — implement controls or process changes to lower the likelihood or impact
- Transfer — transfer the risk to a third party (e.g. through insurance or contractual obligations)
- Accept — accept low-level residual risk with ongoing monitoring where elimination or reduction is not practicable

For Medium, High and Critical risks, a documented treatment plan with an assigned owner and due date must be recorded in the Risk Register. Treatment plans must be reviewed for completion at the next scheduled quarterly review.

Step 4 — Monitor and Review

Risk management is an ongoing process. All risks recorded in the Risk Register must be reviewed regularly. Review triggers and frequencies are set out in Section 7 of this policy. At each review, the Operations Manager must assess whether:

- The risk still exists or has been resolved
- The risk rating has changed
- Treatment actions have been completed effectively
- New related risks have emerged
- Any escalation is required

Risk Register

*my*EmpowerPlan maintains a Risk Register as the central document for recording and tracking all identified risks. The Risk Register is owned by the Operations Manager and is a live document updated whenever a new risk is identified or an existing risk changes.

The Risk Register must capture, at minimum:

- Risk ID and date identified
- Risk category (refer to Section 3)
- Risk description
- Applicable service type (Support Coordination / SSC / Plan Management / All)
- Likelihood score, Impact score and Overall Risk Rating
- Existing controls
- Residual risk rating

- Treatment plan and actions required
- Owner (responsible person)
- Due date for treatment
- Status (Open / In Progress / Closed)
- Date of last review

The Risk Register is a confidential internal document. Access is restricted to the Director, Operations Manager and Compliance Officer unless specific disclosure is required for audit or regulatory purposes.

Escalation Thresholds

The following escalation requirements apply to all identified risks based on their Overall Risk Rating. Escalation obligations are in addition to, and do not replace, any mandatory reporting requirements under the NDIS (Incident Management and Reportable Incidents) Rules 2018.

Rating	Timeframe for Action	Escalation To	Required Actions
Low	Next quarterly review	Compliance Officer	Log in Risk Register. Monitor. No immediate action required.
Medium	Within 30 days	Operations Manager	Assign owner. Document treatment plan. Review at next quarterly meeting.
High	Within 5 business days	Senior Management	Initiate Corrective Action Plan. Senior management sign-off required. Report to Director.
Critical	Immediately	Director	Immediate Director notification. Suspend associated activity if required. Notify NDIS Commission if participant safety at risk.

Review Frequency

The Risk Register and this policy are subject to regular scheduled reviews and must also be reviewed in response to specific triggers.

Trigger	Frequency / Timing	Responsible
Scheduled Risk Register Review	Quarterly	Operations Manager / Compliance Officer
Full Risk Assessment	Annual (or after significant incident)	Director + Operations Manager
Post-Incident Review	Within 5 business days of incident	Operations Manager
Post-Audit Review	Within 10 business days of audit completion	Compliance Officer
Regulatory Change	Within 30 days of change taking effect	Director

Trigger	Frequency / Timing	Responsible
New Service or Registration	Prior to commencing new service type	Director + Operations Manager

This policy will be reviewed annually at a minimum. The Director is responsible for approving any material changes to this policy.

Documentation and Record Keeping

The following records must be maintained in accordance with this policy and retained for a minimum of 7 years in accordance with NDIS record keeping requirements:

- The current Risk Register and all previous versions
- Risk assessment records and treatment plans
- Records of quarterly and annual risk reviews, including attendance and outcomes
- Corrective action records and evidence of completion
- Staff risk management training records
- Incident reports where risk treatment was triggered

All records must be stored securely in accordance with the myEmpowerPlan Privacy Policy and Cybersecurity Policy. The Compliance Officer is responsible for ensuring records are accessible for audit purposes.

Staff Training

All staff must complete risk management training as part of their induction and on an ongoing basis. Training must cover:

- The purpose and application of this policy
- How to identify and report a risk
- How to use the 5x5 risk rating matrix

- Escalation obligations by risk rating
- Service-specific risk requirements for their role (SC, SSC or Plan Management)

Training completion must be recorded in the staff member's training record. The Operations Manager is responsible for ensuring training is current and documented.

Legal and Regulatory Requirements

NDIS (Incident Management and Reportable Incidents) Rules 2018	Requires all registered NDIS providers to have risk management systems that address participant safety and respond to reportable incidents.
NDIS Practice Standards — Core Module, Standard 2.3	Requires registered providers to have a documented risk management framework that identifies, assesses, mitigates and reviews risks across all service types.
NDIS Practice Standards — Module 2a (Support Coordination)	Requires risk identification and management in the context of support coordination, including participant-level risk and referral integrity.
NDIS Practice Standards — Module 2b (Specialist Support Coordination)	Requires documented risk assessments, crisis planning and multi-agency risk management for complex participants.
NDIS Practice Standards — Module 4 (Plan Management)	Requires financial risk controls including separation of duties, fraud prevention, and budget monitoring to protect participant funds.
NDIS Act 2013	Establishes provider obligations to act in the best interests of participants and maintain safe, quality supports.
Privacy Act 1988 (Cth) & Australian Privacy Principles	Requires protection of participant personal information and management of data breach risk.

Work Health and Safety Act 2011 (Cth)	Requires identification and management of workplace health and safety risks affecting staff and participants.

This policy will be reviewed annually to ensure its continued compliance with all applicable legislation and NDIS Practice Standards. Any breach of this policy will be addressed in accordance with the organisation's disciplinary procedures. The Director holds ultimate accountability for ensuring this policy is implemented effectively.

Date: **15 February 2026**

Date for Review: **15 February 2027**

Written By: **Erin Hall**