Risk management

Last edited: 26 Mar 2025, 10:15 AM

Introduction

Risk management involves identifying and managing risks. This includes a wide range of risks including risks to the organisation's operation, to workers and to participants. Risks are inevitable but risk management aims to reduce the chance of a particular event from happening. If it does happen, risk management helps to reduce its impact. Benefits of risk management can include:

- reduced business downtime
- reduced loss of cash flow
- reduced injuries or illness to participants and workers
- increased health and well-being of participants and workers
- increased innovation, quality and efficiency through continuous improvement.

Risk management areas

All of our supports and services will be provided in a way that is consistent with our risk management system. Our risk management system will cover:

- incident management
- complaints management and resolution
- financial management
- governance and operational management
- human resource management
- information management
- work health and safety
- emergency and disaster management
- infection prevention and control.

Identifying risks

Risk is the combination of the likelihood (chance) of an event occurring and the consequences (impact) if it does. Risk management aims to increase the likelihood and impact of a desirable outcome as much as possible. Risk identification is the process of finding, recognising and describing risks.

Unmanaged risks

Unmanaged risk is the level of risk before any action has been taken to manage it. Managed risk is the risk remaining after taking into account the effectiveness of current controls (e.g. training, management plans or using personal protective equipment). In other words, it is the level of risk remaining after plans have been put in place and are being followed.

Risk tolerance

Risk tolerance is an informed decision to accept a particular risk, with or without risk treatment, in order to achieve a goal.

Risk analysis

Risk analysis is the process to understand the nature, sources and causes of risks to determine the degree of risk. The degree and consequences of risk together inform risk evaluation and decisions about risk treatment.

Risk assessment

Risk assessment is the overall process of risk identification, risk analysis, and risk evaluation.

Risk evaluation

Risk evaluation is the process of determining whether the risk is tolerable or whether it requires risk treatment.

Risk treatment

Risk treatment are the measures taken to change the level of risk. Possible treatment responses include:

- avoiding the risk
- removing the risk source
- making decisions or taking actions which change the likelihood and/or the consequences
- sharing the risk with another party
- tolerating the risk by informed decision.

Applicability

When
• applies to all parts of the service.

Who
• applies to all representatives including key management personnel, directors, full time workers, part time workers, casual workers, contractors and volunteers.

Governing regulations for this policy

- NDIS (Provider Registration and Practice Standards) Rules 2018 (Cth)
- NDIS—Risk Management Rules 2013 (Cth)

Applicable processes for this policy

- Manage risks to participants

Documents relevant to this policy

- Home visit safety checklist
- Participant risk assessment
- Risk management plan
- Risks register

Risk matrix

A risk matrix is used during risk assessment to define the level of risk by considering the category of likelihood against the category of consequences. A risk matrix aids to increase visibility of risks and assist management decision making.

		Consequence				
		Insignificant	Minor	Moderate	Major	Extreme
Likelihood	**Almost certain** More than 90% likelihood of occurring	Medium	Medium	High	High	High
	Likely Between 50% and 90% likelihood of occurring	Low	Medium	High	High	High
	Possible Between 20% and 50% likelihood of occurring	Low	Medium	Medium	High	High
	Unlikely Between 10% and 20% likelihood of occurring	Low	Low	Medium	Medium	High
	Rare Less than 10% likelihood of occurring	Low	Low	Low	Medium	High

Participant risk management

Identifying risks to participants is an important part of providing supports and services. Identifying risks to participants and regular reviews of those risks is an ongoing process. Regular reviews help to ensure risk management strategies in place are effective and that they adequately address identified risks. With this in mind:

- risk assessments for new participants must be conducted during the on-board process
- risk assessments for existing participants must be conducted every 12 months or more often if there are changes in the participant's needs
- risk management plans for participants should be reviewed quarterly or more often if there are changes in the participant's needs.

Strategic risk management

Risk management should consider strategic risks. This includes identifying and managing risks related to the service achieving its business objectives. This may include risks to:

- funding—this might include donors, gifts and funding bodies
- mismanagement—risks to the organisation's reputation
- founder risk—where the organisation's original benefactor lacks the required business and financial skills to run the service appropriately.

Strategic risk management strategies involve thorough research and planning.

Compliance risk management

Ensuring the organisation operates within the law carries its own compliance risks. These risks must be identified and assessed under a risk management framework. Examples of compliance risks may include:

- unregistered and/or uninsured company vehicles
- fulfilling reporting requirements to comply with legislation or funding agreements
- fundraising activities or sources which breach legislative requirements
- key management personnel operating outside their authority
- activities that are outside the organisation's constitution.

Compliance risks must be eliminated entirely unlike other types of risks where elimination may not be possible. Strategies to prevent compliance risks include (among others):

- a robust compliance culture
- internal controls in areas of compliance
- regular internal audits in areas of compliance.

Human resources risk management

Risk management should consider risks related to human resources including:

- unplanned exit or retirement of key management personnel
- not having workers with the required knowledge and skills
- industrial action and disputes or absenteeism
- lack of diversity (gender, race, age, ability)
- recruitment of workers and their retention or dismissal.

Strategies to manage or reduce human resources risks include:

- a robust leadership, a positive culture, and a values framework
- succession planning for key roles
- documenting critical information and key processes so others can continue to run the service
- comprehensive training program for new workers
- training workers so that more than one person knows how to perform each task
- a supervision and mentoring program for workers.

Special events risk management

Risk management is a required part of organising or participating in an event. The main risks at events includes anything that could:

- cause harm to another person
- cause damage to equipment, infrastructure or the event site, or
- harm the future of the event organiser.

Risk assessments for events may require, where appropriate:

- a risk assessment of the event site—including existing risks, risks caused by inclement weather, and risks from bodies of water
- a risk assessment of the event including all proposed activities e.g. rides, vehicles and security

- a risk assessment of all external risks such as an evacuation—if so, are there any guests that may have higher risks?

To prevent, minimise or manage identified risks, an event organiser will require appropriate management plans to ensure risks are appropriately managed.

Work health safety risk management

Under WHS laws, key management personnel (or person conducting a business or undertaking) have a duty to eliminate WHS risks as far as reasonably practicable. This means risk management needs to consider work health and safety (WHS) risks. Managing WHS risks is an ongoing process which should begin when:

- starting a new business or purchasing a business
- changing work practices, processes or work equipment
- purchasing new or used equipment or using new substances
- planning to improve productivity or reduce costs
- responding to workplace incidents (even if they have caused no injury)
- responding to concerns raised by workers or others at the workplace
- required by the WHS regulations for specific purposes.

Identifying hazards involves finding things and situations that cause harm to people. This includes workers':

- physical work environment
- equipment, materials and substances used
- work tasks and how they are performed
- work design and management.

Common hazards include:

- manual handling—when lifting or moving objects or people
- gravity—fallen objects, falls, slips and trips of people
- electricity—shock, fire, burns or electrocution
- machinery and equipment—hit by moving vehicle or caught by moving parts of machinery
- hazardous chemicals—chemicals, dusts
- extreme temperatures—heat stroke, burns, fatigue, hypothermia
- noise—permanent hearing loss
- radiation—microwaves, lasers
- biological—infection, allergies
- psychosocial hazards—stress, bullying, violence, fatigue.

Finding hazards involves:

- workplace inspections
- consulting workers
- training workers to report hazards and risks
- reviewing incident reports and complaint registers.

WHS risk assessments should be carried out:

- if there is uncertainty about how a hazard may cause an injury or illness
- the work involves a number of different hazards and it is unclear how these hazards may interact to produce new or greater risks
- changes in the workplace that may impact control measures.

Once a WHS hazard or risk is identified and assessed, managing the risk may involve:

- elimination—where possible a WHS risk should be eliminated
- substitution—replacement with less hazardous options

- isolation—if elimination or substitution is not possible isolate the hazard so workers cannot come into contact with it
- control—where elimination, substitution or isolation is not possible, controls such as safe work practices and/or personal protective equipment.

Fraud risk management

In this context, "worker" means any representative of the organisation including key management personnel, directors, employees, contractors and volunteers.

Risk management should cover risk of fraud. This includes:

- internal fraud—fraud that is carried out within the organisation such as when workers:
    - steal money or assets that belong to the organisation
    - steal cash donations that belong to the organisation
    - claim non-existent, excessive or purchase orders to obtain payment for goods and services that are not supplied
    - submit false applications for grants or other benefits
    - create non-existent beneficiaries or employees for the purposes of directing unauthorised payments
- external fraud—scams and fraud initiated externally from the organisation, such as when an external actor:
    - submits false invoices to the organisation
    - steals identities in order to obtain credit card or bank account details
    - uses a charity's name to obtain funds fraudulently e.g. a fraudulent fund raising appeal
    - makes phone calls or sends text messages or emails which pose as another organisation in order to obtain funds fraudulently.

The likelihood of fraud can be reduced by:

- having a strong ethical culture with clear commitments to integrity and ethical values
- strategies in place to protect the organisation from fraud rather than just accepting the risk.

There are three accepted ways to mitigate against risk of fraud:

- prevention—controls designed to reduce the risk
- detection—controls designed to uncover risk when it occurs
- response—controls designed to facilitate corrective action and harm minimisation.

Prevention controls can include:

- fraud risk assessments
- conflict of interest policy
- strong internal controls
- screening for new workers
- effective supervisory processes
- due diligence checks on suppliers and contractors
- worker training to increase awareness of ethics and on risk management strategies
- support programs for workers
- independent audits.

Detection controls can include:

- continuous internal monitoring and auditing of processes
- allocation of resources for fraud detection
- fraud detection software to provide real time data monitoring and analysis
- mechanisms to report fraud while protecting the whistleblower
- unannounced financial and asset audits
- fraud testing.

Response controls can include having an internal investigation team and a fraud response plan.

Financial risk management

Risk management should include managing risks to finances such as:

- liquidity risk—not enough funds to pay debts
- interest rates—when there is a dependence on borrowed funds or income generated from interest-bearing deposits
- credit risk—when goods and services are sold on credit
- risks from competitors—competition can impact market share
- risks from the market or economy—changing trends, impacts from economic downturn
- unexpected exit from business owner or partner—in the case of death or incapacitation.

Risk management strategies include:

- having the right insurance
- backup plans if things go wrong
- researching market trends.

Key personnel succession risk management

Risks to the service which relation to key personnel should be considered. A succession plan is one way to minimise the impact of one or more unplanned absences of key personnel.

Consequence ratings for participants

The steps to manage risks for participants are:

- identify risks—identify risks specific to each individual participant
- assess risks—understand how likely it is to happen and how bad it could be
- control risks—implement appropriate lifestyle plans to lessen the likelihood and/or the amount of harm
- review control measures—check and ensure risks are under control and there are no new risks.

Insignificant	Minor	Moderate	Major	Extreme
• Less than first aid injury • Brief emotional disturbance	• First aid injury • Emotional disturbance impacting more than two days - does not require treatment	• Substantial injury resulting in medical treatment • Temporary impairment/ development • Exacerbation of mental illness requiring treatment or some cases of abuse/neglect of the participant	• Significant injury causing permanent impairment • Severe, long lasting or significant exacerbation of mental illness requiring long-term treatment • Significant faults allowing significant abuse/neglect of participants	• Avoidable death of a person • Systemic faults allowing widespread abuse/neglect of participants

Risks for participants must be managed:

- with a risk assessment as part of a periodically-reviewed individual support plan
- during a transition from one service provider to another.

Consequence ratings for organisational risks

In the organisation, persons conducting a business or undertaking:

- are required by law to manage WHS risks
- are required by law to minimise the risks of breaches of privacy.

The steps to manage risks in the organisation:

- identify risks—find out what could cause harm
- assess risks—understand the nature of the harm that could be caused by the risk, how serious the harm could be and the likelihood of it happening
- control risks—implement the most effective control measures reasonably practicable in the circumstances
- review control measures—ensuring control measures are working as planned and there are no new risks.

The following table provides example consequence ratings for organisational risks:

Consequence rating	Financial impact*	Effect on workers	Reputation	Service outputs	Legal and compliance*	Management impact	Privacy and information
Extreme	>$1m	• One or more fatalities or severe permanent disability to one or more people	• Widespread negative media coverage • Significant impact on funding for several years • Long term loss of clients	• Multiple services ended for many months	• Major litigation costs of >$1m • Investigation by regulating body resulting in long term interruption of operations	• Restructuring of the organisation with loss of senior managers	• Major data breach of sensitive personal information affecting many thousands of records, high risk of harm to those affected, widespread negative media coverage

Major	$500k-$999k	• Extensive injury or impairment to one or more persons	• Negative media coverage • Loss of key management personnel • Loss of clients for many months	• Disruption of multiple services for several months	• Major breach of regulation • Fines or litigation costs of <$1m	• Significant disruption requiring considerable time from key management personnel	• Data breach of personal information of hundreds of records, risk of harm to those affected, negative media coverage
Moderate	$250-$499k	• Injuries to one or more persons	• Media coverage • Loss of clients	• Disruption to a service for several months	• Breach of regulations • Fines or litigation costs of <$499k	• Disruption requiring time from key management personnel	• Breach of privacy and confidentiality or data breach, some risk of harm to those affected, some media coverage
Minor	$10k-249k	• Significant medical treatment • Lost injury time <2 weeks	• Complaint to key management personnel	• Some service disruptions	• Breach of regulations • Fines or legal costs	• Requires some time of key management personnel over many days	• Breach of privacy and confidentiality to a few persons but little risk of harm to those affected

Insignificant	<$10k	• First aid treatment	• Complaint to worker	• Minimal disruption	• Minor legal issues • Minor breach of regulations	• Requires some attention of key management personnel	• Minor breach of privacy and confidentiality to a worker or client, no risk of harm to those affected

* Financial impact consequence ratings, litigation costs and costs of fines may differ depending on an organisation's size and turnover.

Responsibilities of key management personnel

In the context of this policy, key management personnel includes the organisation's board of directors, management committee or director/owner.

Key management personnel are ultimately responsible for setting all risk management appetite in the organisation. Their responsibilities are to:

- set overall risk management strategy
- understand the scope of risks faced by the organisation
- ensure robust oversight of risk at senior management levels
- promote a risk-focused culture
- promote open communications within the organisation
- assign clear lines of accountability and encourage effective risk management framework.

Key management personnel must also ensure risk management policies and processes are implemented and followed across the organisation.

Responsibilities of risk manager/risk management committee

In the context of this policy, the risk manager may also be the business owner/director.

If appropriate, key management personnel may assign a risk manager or a risk management committee to assume the responsibilities described.

The responsibilities of a risk manager/risk management committee:

- form overall risk management strategy
- identify and prioritise risks across the organisation
- make risk management recommendations to key management personnel/board of directors/management committee.

Responsibilities of workers

All workers should:

- follow participant risk management plans
- support participants to communicate and self-advocate if the participant requests or requires support
- assist the participant, if they request or require support, to maintain a risk management plan as safety needs change
- inform the team of any changes to a participant's safety needs
- seek support from key management personnel to manage a risk, if required
- collaborate with relevant parties when concerns about risk management escalate to key management personnel
- be actively engaged during supervision and team meetings to work through risk management issues
- have a basic understanding of NDIS Quality and Safeguarding Framework
- have a basic understanding of relevant WHS policies.