RISK MANAGEMENT

Introduction:

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

- Reduced business downtime

- Reduced loss of cashflow

- Reduced injuries or illness to clients and employees

- Increased health and wellbeing of clients and employees

- Increased innovation, quality and efficiency through continuous improvement

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 employees, part time employees, casual employees, contractors and volunteers

Risk matrix

A risk matrix is used during risk assessment to define the level of risk by considering 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	Critical	Critical

		Consequence				
		Insignificant	**Minor**	**Moderate**	**Major**	**Extreme**
Likelihood	**Likely** **Between 50% and 90 % likelihood of occurring**	**Low**	**Medium**	**High**	**High**	**Critical**
	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**

Client risk management

Identifying risks to clients is an important part of providing supports and services. Identifying risks to clients 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 clients must be conducted during the on-board process
- Risk assessments for existing clients must be conducted every 12 months or more often if there are changes in the client's needs
- Risk management plans for clients should be reviewed quarterly or more often if there are changes in the client'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 organisations reputation
- Founder risk – where the organisations 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 employees with the required knowledge and skills
- Industrial action and disputes or absenteeism
- Lack of diversity (gender, race, age, ability)
- Recruitment of employees 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 employees
- Training employees so that more than one person knows how to perform each task
- A supervision and mentoring program for employees

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)
- Required by the WHS regulations for specific purposes

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

- 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, dust
- Extreme temperatures – heat stroke, burns, fatigue, hypothermia
- Noise – permanent hearing loss
- Radiation – microwaves, lasers
- Biological – infection, allergies
- Psychological hazards – stress, bullying, violence, fatigue

Finding hazards involves:

- Workplace inspections
- Consulting employees
- Training employees 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 employees 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 "employee" means any representative of the organisation including key management personnel, directors, 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 employees:

  - Steal money or assets that belong to the organisation
  - Steal cash donations that belong to the organisation
  - Claim non-existent, excessive or purchase order 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 employees
- Effective supervisory processes
- Due diligence checks on suppliers and contractors
- Employee training to increase awareness of ethics and on risk management strategies
- 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 whistle-blower
- Unannounced financial and asset audits
- Fraud testing

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 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 clients

The steps to manage risks for clients are:

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

Risks for clients must be managed:

- With a risk assessment as part of a periodically revied 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	Extreme	Major	Moderate	Minor	Insignificant
Financial Impact	>$1m	$500K - $999K	$250K - $499K	$10k-$249k	<$10k
Effect on employees	One or more fatalities or severe permanent disability to one or more people	Extensive injury or impairment to one or more persons	Injuries to one or more persons	Significant medical treatment Loss injury time <2 weeks	First aid treatment
Reputation	Wide spread negative media coverage Significant impact on funding for several years long term loss of clients	Negative media coverage Loss of key management personnel Loss of clients for many months	Media coverage Loss of clients	Complaint to key management personnel	Complaint to employee

Service outputs	Multiple services ended for many months	Disruption of multiple services for several months	Disruption to a service for several months	Some service disruptions	Minimal disruption
Legal and compliance	Major investigation on costs of >$1m Investigation by regulating body resulting in long term interruption of operations	Major breach of regulation Fines or litigation costs of<$1m	Breach of Regulations Fines or Litigation costs of <$400k	Breach of Regulations Fines or legal costs	Minor legal issues Minor breach of regulations
Management impact	Restructuring of the organisation with loss of senior manage ment	Significant disruption requiring considerable time from key management personnel	Disruption requiring time from key management personnel	Requires some time of key management personnel over many days	Requires some attention of key management personnel
Privacy and information	Major data breach of sensitive personal information affecting many thousands of records, high risk of harm to those affected, widespread negative media	Data breach of personal information of hundreds of records, risk of harm to those affected, negative media coverage	Breach of privacy and Confidentiality or data breach, some risk of harm to those affected, some media coverag e	Breach of privacy and confidentiality to a few persons but little risk of harm to those affected	Minor breach of privacy and confidentiality to an employee or client, no risk of harm to those affected

- Financial impact consequence ratings, litigation costs and costs of fines may differ depending on an organisations size and turnover

Responsibilities of key management personnel

In the context of this policy, key management personnel include 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 employees

All employees should:

- Follow client risk management plans
- Support clients to communicate and self-advocate if the client requests or requires support
- Assist the client, if they request or require support, to maintain a risk management plan as safety needs change
- Inform the team of any changes to a clients 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 or relevant WHS policies

Duty of care

Providing a duty of care to clients involves ensuring adequate care is taken to avoid injury. When assessing activities or situations for possible injury, we should keep in mind:

- What is already known about a person's capacity to carry out similar activities safely
- What is known about a person's awareness of what risks might be involved and how to avoid them
- What is known about the dangers involved in the activity and whether the person can deal with them
- What can be learnt from relevant assessments or reports about the persons abilities or skills

Clients, employees and others important to the client should work cooperatively to develop strategies and to identify solutions for issues that challenge duty of care for employees and dignity of risk to clients. In order to achieve this, we must:

- Take all steps to avoid harm
- Understand the client's capacity for making decisions about the risk they are managing
- Seek advice and assistance from their line manager when they encounter something that is outside their delegation, experience or skill set
- Ensure the relevant legislation, policies and procedures are part of their decision making processes
- Provide information to the client, other employees and family about any risks, duty of care obligations and the clients right to experience and learn from risk taking
- Develop lifestyle plans in consultation with the client, family, friends and support workers, and commence with the least restrictive option for the client
- Facilitate discussion with the client about the consequences of particular choices
- Communicate with the person, family, or guardian at each stage of support and document all actions, communications and decisions
- Document decisions by a person or their representative, to continue behaviour they believe is reckless, and seek further advice from a line manager
- Review how support is provided from a work health and safety perspective if support workers are affected by a decision
- Record the reasoning behind risk management decisions, including background, decisions, issues and solutions why some strategies were adopted and others rejected

<u>Breach of duty of care</u>

- The organisation and all employees must provide appropriate standards of care at all times

- If an employee or the organisation is proven to have not provided the appropriate standard of care, this is a breach of duty of care

- A breach of duty of care is any case where an employee or the organisation has done something they should not have done or failed to do something they should have done – such a breach may potentially result in harm or injury to another person and a finding of negligence

- All suspected incidents of breach of duty of care should be investigated

- Anyone found to be in breach of duty of care will be disciplined including termination of employment