

Risk Incidents and Complaints Management



Risk Management Plan

Instructions:



Risks can be prevented by having a planned way to identify, and collect and analyse data that addresses/manages potential and actual risks for your organisation and the supports you provide. A plan for how you might think about and put into action ways to eliminate or manage risks can guide your approach.

This checklist shows what the NDIS Commission identifies should be included in a Risk Management Plan to guide your risk management. This is for both providers being certified and verified.

✓ Tick when your Risk Management Plan includes the following elements.



Risk Management Plan

The following strategies are used to inform and support how you manage risk.

1. Identification of risks

Areas of risk your business might face are identified and prioritised according to the impact they have. You may:

- Evaluate each function in your business and identify anything that could have a negative impact on it
- Review your records such as safety incidents or complaints and feedback to identify previous issues and any common themes
- Consider any external risks that could impact on your business
- Brainstorm with your staff.

You include the following areas:

- Strategic decisions concerning your business's objectives
- Compliance – the need to comply with laws, regulations, standards, and codes of practice
- Financial – financial transactions, systems, and structure of your business
- Operational – your operational and administrative procedures
- Environmental – external events that your business has little control over such unfavourable weather, pandemic or workforce conditions, storage and handling of waste disposal and infectious or hazardous substances including PPE
- Reputational – the character or goodwill of your business
- Health and safety
- Security to premises
- Administration and information technology records management
- Service delivery
- Emergency and disaster management

Consider risks in each of the above area as they relate to participants, staff, and the business and ask yourself:

- How effective is the business's current approach (if any) to controlling or managing the risk? (For example, what if your computer crashed because of a power surge. Is your electronic information protected?)
- What are the weaknesses with the current controls? (How would you plan to continue working in the above circumstance?)



- What might be the impact on the business objectives if the risk occurred and the controls did not work as intended? (Assess the impact of having no computer access to your business).
- In the event of an emergency or disaster, do you consider and mitigate impacts on participants to ensure continuity of support to the health, safety and well being of participants?

Examples of questions include what if:

- You lost power?
- Your premises were damaged or not accessible?
- There was a natural disaster such as fire or flood in your area?
- One of your key staff members resigned or was injured at work?
- Your computer system was hacked/destroyed?
- You had to move premises?
- You had an infection outbreak?

2. Assessing risk

You assess the likelihood (frequency) of each of these risks occurring and the consequence (impact) on the organisation if this risk did occur to determine how they should be treated. Consider actions to take before, during and after the event.

This calculates the level of risk
 $\text{Level of risk} = \text{likelihood} \times \text{consequence}$

You consider using a risk analysis matrix to assist you to determine the level of risk for each area.

The Risk Matrix allows you to prioritise which actions to take.

Compliance checks are seen as an important part of reducing risk. (See Compliance register).

3. Manage/treat the risk

Once risks have been prioritised you identify actions to respond to and oversee the response to each risk along with timeframes and who is responsible.

You manage risk by developing cost effective options to deal with them including:

- Avoiding - change your process, equipment delivery mechanism to achieve a similar outcome but with less risk
- Reducing - if a risk cannot be avoided, reduce its likelihood and consequence. This could include staff training, documenting policies and procedures, complying with legislation, maintaining equipment, practicing emergency procedures, keeping records safely secured, and contingency planning



- Test your planned response for particular kinds of emergency or disaster that may be relevant to your circumstances
- Transfer the risk - transfer some or all the risk to another party through contracting, insurance, partnerships, joint ventures
- Accepting - this may be your only option.

For each identified risk, the organisation has identified ways to avoid the risk occurring and manage any adverse impacts if they do.

This involves understanding the immediate causes of the risk and the underlying factors that might influence the effectiveness of the proposed treatment.

TIP: a plan need not be sophisticated or complex but should be carefully prepared. It will be specific to each organisation and its own risks.

4. Risk management strategies

You use a range of ways to manage risks. Some examples are below:

- For participants:
 - Individual risk assessment (see below)
 - Feedback mechanisms
 - Advocacy.
- Staff:
 - WHS assessments
 - Training and development in the implementation of the Risk Management Plan
 - P&P/Code of conduct
 - Performance reviews
 - Feedback mechanisms
 - You identify staff that have capabilities to assist in responding to an emergency or disaster.
 - You have a plan for identifying sourcing and induction staff in the event of workforce disruptions in the event of an emergency or disaster
 - Infection prevention and control training (including refresher) is undertaken by all staff involved in providing supports.
- Business:
 - Worker screening
 - Board review and development
 - P&P
 - Strategic, financial, and operational risk assessment
 - Insurances
 - Business continuity and emergency response plans.



5. Individual participant risk assessments

Individual risk assessments are regularly undertaken and documented in their support plans:

- Strategies are planned and implemented to treat known risks eg chronic health risk
- You consider the degree to which each participant relies on your supports to meet their daily living needs and the extent to which the health and safety of participants would be affected if those supports were disrupted
- You ensure you develop and maintain links with other relevant providers (with the participant's consent) to share information, manage risks and meet their needs
- Risk associated with transition of participants to or from your organisation are identified, documented and responded to.

6. Emergency and disaster response plan

You have plans that are straight forward and everyone understands their responsibilities and what they need to do in the event of an emergency. It might include:

- An evacuation strategy
- Access to emergency supplies - PPE/first aid
- Developing a specific security plan
- Regularly practice, refine and review
- Communication plan - who communicates with emergency/NDIS Commission/ participants etc. in the event of an emergency
- Checklists help get the plan into action.

Unexpected events such as emergencies, natural disasters or loss of key staff can impact your ability to run your business. As your business is critical to your financial wellbeing, it is important to plan for these events so you can respond and recover quickly. You also have a responsibility to ensure continuity of support of participants in an emergency or disaster.

An emergency and disaster plan includes:

- You have plans in place to ensure each participant has access to timely and appropriate support without interruption that is critical to their safety, health and wellbeing, during and after an emergency or disaster.
- Your plan includes each of the following:
 - preparing for, and responding to, the emergency or disaster
 - making changes to participant supports
 - adapting, and rapidly responding, to changes to participant supports and to other interruptions
 - communicating changes to participant supports to workers and to participants and their support networks.
- You consult with participants and their support networks about the emergency and disaster management plans



- The plans explain and guide how the board will respond to, and oversee the response to, an emergency or disaster
- Plans are in place for the board to actively test the plans, and adjust them, in the context of a particular kind of emergency or disaster
- The plans have periodic review points to enable the board to respond to the changing nature of an emergency or disaster
- Your board regularly reviews the plans, and consults with participants and their support networks about the reviews of the plans
- Each worker is trained in the implementation of the plans.

A business continuity plan includes:

- A detailed list identifying risks that could disrupt your business
- Actions to be taken if the unexpected event occurs
- A list of key staff and stakeholders and their specific roles in relation to the plan.
- Plans for a relocation strategy if your premises should be inaccessible or for a pandemic outbreak how can supports occur in a safe way
- Emergency contact telephone numbers
- Details of where first aid and key documents are stored
- A list of key documents such as insurance policies and financial records that need to be retrieved if the plan is activated
- A communication plan to broadcast key message about the disruption
- A guide as to when the plan is to be activated.

7. **Monitoring and review**

Your risk management plan is monitored and reviewed on a regular basis to ensure the controls you have put in place are effective.

You use outcomes from audits, complaints, feedback and incident management to feed into this.

You ensure your control measures and insurance cover is adequate.