Risk Management: An Introduction

Risk management is the practice of identifying potential risks in advance, analysing them and taking precautionary steps to reduce/minimise the risk or potential impacts.

This introduction is a download from the ACOSS Disaster Resilience Web site. It includes some disaster risk management examples.

Risk management, in essence, is a process of:

a) Establishing the context
b) Identifying the risks
c) Analysing the risks
d) Evaluating the risks (for example by considering the likelihood of events and the consequences or impacts of events)
e) Treating the risks (For example by avoiding the risk, controlling the risk, financing the risk, transferring the risk (e.g. insurance) or reducing the risk through changed work practices)
f) Implementing, monitoring and reviewing
g) Communicating with all concerned.

There are many forms of risk management, for example, financial risk management, worker health and safety risk management, disaster risk management. The emphasis and models of risk management can vary with the type of organisation. In community organisations risk management processes are often for:

- worker health and safety
- child protection
- financial security.

Many risk management frameworks in community organisations don't include the risks associated with disasters and emergencies or community organisations' roles in disasters and emergencies.

For community organisations to step up to their role in preparing for and recovering from disasters and emergencies their risk management plans must include risks in relation to disasters and emergencies.

Tools that organisations typically find useful in managing risk are "Rating Tools" and a "Risk Register".

This document provides an introduction to the key elements of the risk management process, followed by examples of risk rating tools and a risk register.

A. Establishing the Context

> **Establishing the context** includes:
>
> - clarifying the vision, mission and goals of your organisation
> - identifying the wider environment within which your organisation operates
> - setting the scope and objectives for the risk management process
> - identifying how risks will be measured
> - identifying what will be involved in the risk assessment process.

Refer to your organisation's mission, values and goals as guiding principles in this process.

Based upon these strategic priorities consider questions like the following:

- Which of your services would be essential or non-essential during and immediately after an emergency?
- Which of your services are dependent upon other organisations or businesses? (for example suppliers of critical items such as food if you provide meals to clients)
- Which services do you provide that no other organisation provides in your community?
- Which personnel are critical in the delivery of your essential services?
- How would your clients or beneficiaries be impacted by your inability to deliver services?
- What laws, rules, regulations or standards apply to your organisation?
- What work is already being undertaken to manage risk?

SWOT Analysis

You may also find it useful to complete a SWOT analysis. As a team identify your organisation's:

- Strengths
- Weaknesses
- Opportunities and
- Threats.

Tip: Strengths and weaknesses are often internal to your organisation, while opportunities and threats generally relate to external factors.

B. Identifying the Risks

The aim is to develop a comprehensive list of the sources of risks (also known as hazards) and their consequences. There is not one right way to do this. Some strategies are:

- brainstorming at a staff meeting
- brainstorming with stakeholders with relevant knowledge and experience
- systematic analysis, e.g. flow charting systems and processes
- development of 'what if' scenarios
- researching relevant data, such as injury rates, insurance claims, death rates, etc.

Risk identification involves a "process of finding, recognising and describing risks." The aim is to create a comprehensive list of risks that may affect your organisation.

Use a risk register to document all of the risks that may affect your organisation's ability to achieve its objectives. There is more detailed information about what a risk register is, how to use one and a template on pages 14 and 15.

Need some inspiration for knowing your disaster and emergency risks?
Some starting points for getting to know your risks are researching:

a) Disasters and emergencies that have occurred in your community/area in the past.

b) The impact of previous disasters and emergencies on your organisation and the clients you serve and the local community

c) Disasters and emergencies that may occur in the future that have not occurred in your community/area in the past (for example risks from climate change).

You might research your risks by:

- Reviewing previous hazards that have impacted your organisation
- Conducting a brainstorming session with staff and volunteers
- Inviting your local emergency service organisations to assess your premises
- Reading your local emergency management plan which will have already identified hazards in your area
- Speaking with your local council emergency management team
- Visiting the CSIRO and Bureau of Meteorology websites which have up to date research and forecasts
- Looking over your insurance claim history and chatting to your insurance company
- Asking other community service organisations what hazards they have identified
- Using the Community Sector Risk Register.

C. Analysing the Risks

Some of the key questions in analysing the risks are:

- What is the likelihood of the risk?
- What is the consequence?
- What is the level of risk (combination of likelihood and consequence)?
- What factors affect the likelihood or consequences?
- What is the level of uncertainty?
- What are the limitations to the analysis?

Similar questions can be asked in relation to opportunities (i.e. risks with positive consequences):

- What is the likelihood of the opportunity?
- What is the consequence?
- What is the level of opportunity/risk (combination of likelihood and consequence)?

Analysing the risk means working out how likely it is that a hazard will harm your organisation and how serious the harm could be.

Risk Matrix

A Risk Matrix helps you define and categorise how likely a risk is to occur and how serious the consequences of that risk occurring are. This makes it easier for you to figure out which risks you need to address urgently by using a *Risk Rating.* You can find examples of different risk rating tools from page 8.

What if?

Leading a discussion with your team about all the 'what ifs' can be helpful in identifying the consequences of particular risks. It is often easy to identify a risk but a little trickier to list all the different ways that risk may affect your organisation's objectives.

You could prompt the discussion by presenting a scenario to the group such as what if our building was destroyed by flood? Some possible consequences may include:

- Safety – the safety of your staff, volunteers and clients may be affected
- Financial cost – could you afford to restore or rebuild physical infrastructure?
- Service delivery failure – can you deliver services without your building, IT systems, goods?
- Access – can you deliver services without key personnel who may be unable to reach your premises due to a hazard?
- Reputational damage – what do your external stakeholders expect from you?

Take a look at the 'what if' thinking examples included in Step 3 of the Resilient Community Organisations website to help you get started.

D. Evaluating the Risks

Some of the key questions in risk evaluation are:

- What are acceptable levels of risk?
- What are intolerable levels of risk?
- Does the risk need treatment? (i.e. do you need to take action to minimise or avoid the risk?)
- What are the priorities for treatment of risks? (which risks need to be addressed as a matter of urgency and which are less important?)

"Risk evaluation is a process that is used to compare risk analysis results with risk criteria in order to determine whether or not a specified level of risk is acceptable or tolerable."

Determine your current risk ratings and identify which risks are your priorities to address.

Analysing the current controls

Controls refer to the actions you have taken to reduce the likelihood or consequences of particular risks occurring.

Review the risks in your Risk Register and briefly document what controls you already have in place. You can then update the likelihood and consequence ratings in your Risk Register. Some examples of existing controls may be insurance, staff and volunteer training, existing disaster and emergency policies and procedures. The rating you determine for each risk after considering the current controls in place is referred to as your 'residual' or 'current' risk rating.

Preparing to Act

"Risk Assessment is a process to prioritise activity; it is not a method for forecasting or prediction"

Matthew Hogan, London Community Risk Register [1]

After reflecting upon your risk criteria allocate responsibility for each risk to the most appropriate people in your organisation.

Some risks are more important than others. Through this process you will have identified which risks need the most urgent attention. Prioritise your risks so that your team works on reducing the most serious risks first. It is useful to provide a timeframe in which people need to have implemented controls to maintain momentum.

E. Treating the Risks

To effectively treat risks you need to understand how risks arise. Some of the ways that risks are treated are:

- Contingency planning (i.e. plan in advance for an event that may happen so as to minimise any negative effects should it happen)
- Sharing the risk e.g. when entering into contracts with other service providers specifying they share the risk, use of waivers
- Transfering the risk, e.g., through insurance
- Avoiding the risk, e.g., no longer undertaking the activity or re-locating your offices
- Financing the risk e.g., setting funds aside to pay for the consequences
- Reducing the risk, e.g., through changing work practices

In treating risks there will be trade-offs between costs and benefits. You will have to make a judgment that the cost of reducing the risk is worth the benefit of the reduced risk.

Key question: What is acceptable risk?

There are countless ways you can manage the risks you have identified in your risk assessment.

The activities you identify to manage your risks are referred to as 'risk treatments' and once they are put in place they are called 'controls'.

Controls include any policy, procedure, practice, process, technology, technique, method, or device that modifies or manages risk. They can be used to avoid, reduce or share risks.

In this step identify a range of risk treatment options that meet your organisation's risk management needs and implement them.

In particular, ensure that your organisation is adequately insured, has effective emergency plans and procedures, a business continuity plan and is aware of some of the challenges you may face during the community recovery phase of an emergency.

F. Communicating with all Concerned

Good communication and consultation is essential for risk management and attempts to:

- improve people's understanding of risks and the risk management processes
- ensure all relevant stakeholders are heard
- ensure that everyone is clear on their roles and responsibilities.

G. Implementing, Monitoring and Reviewing

Risk management is an ongoing process:

- the risk management process needs monitoring
- the effects of risk treatments need to be monitored and reviewed to ensure they are adequate and effective
- new risks need to be scanned for.

Rating Tools

In developing a risk management process some useful rating tools include:

1. Likelihood scale
2. Consequences scale
3. Risk matrix
4. Risk rating
5. Control effectiveness

Below are examples – use them as a guide remembering each organisation is different.

1. Likelihood Scale

"Likelihood is the chance that something might happen. Likelihood can be defined, determined, or measured objectively or subjectively and can be expressed either qualitatively or quantitatively (using mathematics)."

ISO 31000:2009 Risk management – Principles and guidelines

Determine how likely it is that a risk will occur. Rate each of your identified risks in your Risk Register. At this stage, assess the risk on the assumption that your organisation has not done anything to reduce the likelihood of the risk occurring.

It can be challenging to identify how likely a risk is to occur. Some events may happen regularly, such as every wet season flooding cuts off access to particular areas in your community. However, it is more difficult to determine how likely an emergency such as an industrial accident is to occur. Review the research you undertook when identifying risks. You may find that some hazards occur more regularly than you first thought. You could also ask for advice from experts such as government agencies, insurance companies, emergency service organisations or other community service organisations.

Assessment of the Likelihood of a Risk Occurring

Rating	Description	Definition	Indicative Frequency
5	Almost Certain	Is expected to occur in most circumstances	Once or more per year
4	Likely	Will probably occur	Every three years
3	Possible	Might occur at some time in the future	Every ten years
2	Unlikely	Could occur but doubtful	Every thirty years
1	Rare	May occur in exceptional circumstances	Every hundred years

2. Consequences scale

"A consequence is the outcome of an event and has an effect on objectives. A single event can generate a range of consequences which can have both positive and negative effects on objectives. Initial consequences can also escalate through knock-on effects."

ISO 31000:2009 Risk management – Principles and guidelines

Assessment of the Consequences of a Risk Occurring

Rating	Description	People Impact	Financial Impact	Operational Impact	Reputational Impact	Compliance Impact	Governance Impact
5	Catastrophic	Death or multiple life threatening injuries	More than 50% of total organisation budget	Total cessation of multiple services for many months	National media coverage; Significant impact on funding for several years; long-term loss of clients	Major litigation costing $>3m; Investigation by regulatory body resulting in long term interruption of operations	Restructuring of organisation with loss of many senior managers
4	Major	Life threatening injury or impairment to one or more persons	Between 10% - 50% of total organisation budget	Disruption of multiple services for several months	State media coverage affecting funding or causing loss of clients for many months	Major breach of regulation with punitive fine, and significant litigation involving many weeks of senior management time and up to $3m legal costs	Significant disruption that will require considerable senior management time over several weeks
3	Moderate	Serious Injury causing hospitalisation or multiple medical treatments	Between 5%-10% of total organisation budget	Total cessation of one service for a few months	Local media coverage over several days noticeable loss of clients for many months	Breach of regulation with investigation by authority and possible moderate fine, and litigation and legal costs up to $999k	Disruption that will require senior management time over several weeks
2	Minor	Significant medical treatment	Between 1%-5% of total organisation budget	Some service disruption in the area	Local media coverage, and complaint to management	Breach of regulations; major fine or legal costs; minor litigation	Will require some senior management time over many days
1	Insignificant	First aid or minor medical treatment	Less than 1% of total organisation budget	Minimal disruption	No media coverage; complaint to employee	Minor legal issues or breach of regulations	Will require some management attention over several days

3. Risk matrix – the relationship between likelihood and consequences

The level of risk is the combination of the likelihood and consequences of a specific risk.

Examples of low risks include:

- An event that is likely to occur but has minimal consequences
- An event that is extraordinarily unlikely to occur but has moderately severe consequences.

Examples of high risks include:

- An event that is likely to occur and has moderately severe consequences
- An event that is extraordinarily unlikely to occur but has catastrophic consequences.

The following table is a risk matrix and shows the relationship between *Likelihood*, *Consequence* and *Level of risk*.

In the table:

- A1 is certain to happen but has small consequences so is a low risk.
- A7 is certain to happen and has very large consequences so is a very high risk
- G1 is very rare and has small consequences so is a negligible risk
- G7 is very rare but has large consequences so is a medium risk.

Consequence (small to large)	**Likelihood** (Certain to very rare)						
	A (certain)	B	C	D	E	F	G (very rare)
1 (small)	Low	Low	Low	Low	Low	Very Low	Negligible
2	Medium	Medium	Medium	Low	Low	Very Low	Very Low
3	High	Medium	Medium	Medium	Low	Low	Very Low
4	High	High	Medium	Medium	Medium	Low	Very Low
5	Very high	High	High	Medium	Medium	Medium	Low
6	Very high	Very high	High	High	Medium	Medium	Medium
7 (large)	Very high	Very high	Very high	High	High	Medium	Medium

Specific risks can be located on the matrix. Risks can be compared with each other so they can be prioritised for treatment.

For example:

- Risk of fire burning a building down could be located at E7 (rare but very significant consequences and so a high risk).
- Violence during home visits could be located at B4 (likely with serious consequences and so a high risk).

Here is another example of a Risk Matrix:

Risk Matrix	Consequence				
	Insignificant	Minor	Moderate	Major	Catastrophic
Almost Certain	M	H	H	E	E
Likely	M	M	H	H	E
Possible	L	L	M	H	E
Unlikely	VL	L	M	H	H
Rare	VL	VL	M	M	H

In the Risk Matrix table above:

> E = Extreme
> H = High
> M = Moderate
> L = Low
> VL = Very low

The second *Risk Rating scale* below describes the level of action required for each of the risk ratings used in this Risk Matrix.

4. Risk rating

When evaluating the level of risk, i.e. deciding whether it is an acceptable risk or not it is useful to have a scale on which to base judgments, for example:

Risk Level	Risk rating	Description
A	Broadly acceptable level of risk	The situation is not of concern
B	Best achievable level of risk	Achieved with best practice
C	As low as reasonably practicable(ALARP)	Must be achieved (minimum standard)
D	Generally intolerable level of risk	Not tolerated

For any given risk you will need to make a judgment about where the cut off points are for levels A to D in the table. When is an occupational health and safety risk broadly acceptable? When is it intolerable? What is the level or risk the organisation wants to achieve? As low as reasonably practicable? Best achievable?

Here is another example of a Risk Rating scale:

Risk Rating

Risk Level	Description	Action
E	Extreme	Requires ongoing executive level oversight. The level of risk warrants that all possible mitigation measures be analysed in order to bring about a reduction in exposure
H	High	Action plans and resources required. The level of risk is likely to endanger capability and should be reduced through mitigation strategies where possible.
M	Medium	This level of risk should not automatically be accepted for risk mitigation but rather a cost-benefit analysis is required to determine if treatment is necessary.
L	Low	Treatment when resources are available. The risk should be able to be managed via existing controls and normal operating procedures.
V	Very Low	Accept Risk

5. Control effectiveness

Here is an example of a control effectiveness scale:

Control Effectiveness

Rating	Description	Definition
4	Absent	Risk mitigation or control absent or ineffective - almost certain risk of failure in prevention, detection, risk mitigation and/or control response.
3	Improvement Needed	Risk mitigation or control expected to fail in most circumstances - high risk of failure in risk mitigation and control with a definite need and justification to improve risk mitigation and control.
2	Adequate	Compliant (adequate in the circumstances) - low risk of failure in risk mitigation and control and little scope or justification to improve risk mitigation and control.
1	Strong	Strong (more than adequate) - rare risk of failure in risk mitigation and control and no scope and/or justification to improve risk mitigation and control.

Risk Register

Summary

A Risk Register is a document you use to record all of your organisation's identified risks. It is during the risk assessment that you will complete the Risk Register. As you move through the risk management process you will add further information such as the likelihood and consequences of a risk occurring, the actions you are undertaking to reduce those risks and who is responsible for managing them.

Creating a Risk Register

There are a range of risk templates available on line. One example is provided on the following page.

A Risk Register is useful as it enables you to store all of your risk information in one, easily accessible location. It's simple, consistent format makes it easier for people to understand the information presented and to provide feedback. Importantly, a Risk Register specifies the ways your team commits to manage the identified risks and who is responsible for doing so.

The risk register below includes:

> Risk #
> Date
> Description of Risk
> Risk Source
> Risk Consequences
> Consequence Rating - see *Consequence scale* above
> Likelihood Rating – see *Likelihood scale* above
> Inherent Risk Rating   - see *Risk rating scale* above
> Existing Controls
> Residual Risk Rating – see *Risk rating scale* above
> Planned Treatments
> Risk Owner
> Treatment Due Date
> Risk Review Date

A useful way to start a risk register is to get your whole team involved. Remember to include people with unique and diverse roles within your organisation as they will be able to identify risks and consequences that may never have occurred to you.

Risk Register

Organisation	
Date	

Risk #	Date	Description of Risk	Risk Source	Risk Consequences	Consequence Rating	Likelihood Rating	Inherent Risk Rating	Existing Controls	Residual Risk Rating	Planned Treatments	Risk Owner	Treatment Due Date	Risk Review Date