NSW GOVERNMENT
Family & Community Services
Ageing, Disability & Home Care

Disability Resource Hub Disclaimer

The material on the Disability Resource Hub is for reference only. No claim or representation is made or warranty given, express or implied, in relation to any of the material. You use the material entirely at your own risk.

The material is provided as point-in-time reference documents. FACS does not maintain the material and does not undertake to ensure that it is accurate, current, suitable or complete.

Where conditions and warranties implied by law cannot be excluded, FACS limits its liability where it is entitled to do so. Otherwise, FACS is not liable for any loss or damage (including consequential loss or damage) to any person, however caused (including for negligence), which may arise directly or indirectly from the material or the use of such material.

Contents

Glossary

Disclaimer: The Department of Family and Community Services (FACS) does not warrant that these definitions are legally correct. Directors should seek professional legal advice relevant to their issues.

action plan – the details of the activities (what will be done, the timeframes, responsibilities and resource needs) to be carried out during the period of the strategic business plan.

board – the governing body of a non-government organisation, made up of

directors – *Note: some organisations refer to the board as management committee and to the directors as management committee members. The term 'board' is used in this manual to include management committee.*

consequence – the outcome of an event affecting objectives. It can be expressed qualitatively or quantitatively, it can be certain or uncertain and it can have positive or negative effects on objectives.

constitution – the name given to the memorandum and rules of an organisation.

contingency – an additional or alternative action to manage situations when they do not go according to plan. A contingency plan takes account of the impact of uncertain, but possible, events on the achievement of planned objectives.

director – a person formally elected and/or appointed under law to a board, in accordance with the organisation's constitution. *Note: some organisations refer to the members of their governing body as management committee members. The term 'director' is used in this manual to include management committee members.*

dignity of risk – each individual's human right to his/her autonomy and self-determination to make choices for himself or herself regardless of the risk that decision carries.

diligence – the degree of care and caution required by the circumstances of a person.

duty of care – the obligation to take reasonable care to avoid causing harm to another person.

environment analysis – an examination of the context in which an organisation works and the identification of the key factors which impact the organisation.

fiduciary duty – the legal duty to act solely in another party's interests.

governance – the framework of rules, relationships, systems and processes within and by which authority is exercised and controlled in corporations.

hazard – anything in the workplace that has the potential to harm people.

incident database – a register or electronic record of incidents that have potential negative consequences for an organisation.

intellectual property – a product of the intellect that has commercial value, including copyrighted property such as literary or artistic works, and ideational property, such as patents, appellations of origin, business methods and industrial processes.

key performance indicators (KPIs) – the benchmarks or targets that have been chosen to measure how successfully an organisation has achieved objectives.

liability – subject to a legal obligation; or the obligation itself. A person who commits a wrong or breaks a contract or trust is said to be liable or responsible for it.

likelihood – the chance of something happening.

monitor – regularly checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected.

negligence – failure to exercise proper care.

objectives – what an organisation wants to achieve as a result of its planned activities. Sometimes the term 'objective' is used interchangeably with the terms 'goals' or 'aims'.

work health and safety (WHS) – concerned with providing a safe and healthy workplace for all employees, volunteers, the employer, as well as visitors, contractors and suppliers.

organisation – a company, firm, enterprise or association, or other legal entity, whether incorporated or not, public or private, that has its own function(s) and administration.

organisation culture – collection of values, beliefs, customs and practices that are shared by an organisation's people and guide the way they interact with one another and with stakeholders outside the organisation.

outcomes – the results of actions and plans.

outsourcing – contracting activities or work to be carried out by someone outside the organisation.

policy – a general statement of a principle that guides decision making.

procedures – specific statements that detail what steps or actions are to be taken in a particular situation.

purpose statement – an organisation's written summary of its values and core business. Also referred to as mission statement.

residual risk – The risk that remains after risk treatment (also referred to as "retained risk").

risk – the effect of uncertainty on objectives. The effect can be positive and/or negative, it is often characterized by reference to potential events and consequences and the associated likelihood.

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

risk elimination – action taken to remove the root cause of a potential risk.

risk identification – process of finding, recognizing and describing risks by identifying risk sources, events, their causes and their potential consequences.

risk management – coordinated activities to direct and control an organisation with regard to risk.

risk reduction – a potential risk treatment that deals with negative consequences. It can also be referred to as risk mitigation, risk elimination or risk prevention.

risk treatment – process to modify risk. Risk treatment can involve avoiding the risk, taking increasing risk, removing the risk source, changing the likelihood, changing the consequences, sharing the risk with another party or retaining the risk by informed decision. Risk treatments can sometimes create new risks or modify existing risks.

root cause – the underlying needs, beliefs or circumstances that give rise to risks.

stakeholders – within a risk management context, a stakeholder is a person or organisation who may affect, be affected by, or perceive themselves to be affected by a decision or activity.

SWOT (Strengths, Weaknesses, Opportunities and Threats) analysis – a snapshot assessment of an organisation's environment and capacity.

system – a set of principles governing the way something is done.

vision – where an organisation wants to be. Its ultimate objective.

volunteer – an individual who willingly gives time for the common good and without financial gain (based on Volunteering Australia's definition).

About this chapter

This chapter explores what risk management is and how it can be applied to organisations to improve activities, make them safer and increase their sustainability.

The approach adopted in this chapter is based on the Australian Standard on Risk Management AS/NZS ISO 31000:2009.

Policy checklists and resources are included at the end of this chapter. They can be copied and worked through by your entire board on an annual basis, or as required.

6.1 About risk management

6.1.1 What is risk?

The Australian Standard AS/NZS ISO 31000:2009 defines risk as the *effect of uncertainty on objectives* whereby an effect is a positive and/or negative deviation from the expected. Risk is often expressed in terms of a combination of the consequences of an event and the associated likelihood of occurrence.

6.1.2 What is risk management?

Risk management is increasingly important for boards, volunteers, paid staff and stakeholders of all services and is an essential component of good governance. It is part of an organisation's culture, its philosophy, practices and business processes. It should not be viewed as a separate activity.

Risk management refers to the coordinated activities to direct and control an organisation with regard to the effect of uncertainty, or risk. Risk management:

- is a procedure aiming to avoid or minimise any negative consequences and reduce potential legal liability
- seeks to address potential problem areas before they occur
- is a process to test the effectiveness of measures to prevent events happening that may result in negative outcomes or an inability to take advantage of positive outcomes.

6.1.3 The Australian Standard AS/NZS ISO 31000:2009

The Australian Standard AS/NZS ISO 31000:2009 sets a number of principles that need to be satisfied to make risk management effective and provides a framework that integrates the process for managing risk into the organisation's overall governance, strategy and planning, management, reporting processes, policies, values and culture.

Risks will vary from organisation to organisation depending upon the circumstances and the way the organisation operates. Risk management plans should be tailored to specific risks and operational practices, and should be reviewed regularly.

6.1.4 Who is responsible for risk management?

Risk management, in general, is a shared responsibility of all stakeholders but ultimately it is the responsibility of directors and management. Risk management is not a stand-alone activity and it should be seen as an integral part of all organisational processes, including strategic planning.

Management of risk should be integrated into the management philosophy of an organisation.

Directors are required to understand the needs of the organisation and their legal responsibilities. Directors have a fiduciary duty in every aspect of the organisation and to every transaction that the organisation enters into.

Directors must demonstrate that they are duly diligent and that they have taken all reasonable steps to prevent a reasonably foreseeable loss or injury occurring.

Due diligence is a legal requirement for directors to act with care and in the best interests of the organisation when carrying out their governance role.

> **TIP:** Your organisation should have a robust risk management framework that has been approved by the board and is linked to the organisational plan and strategy. There may even be some benefits to communicate your approach to risk management as means of providing assurances to stakeholders.

6.1.5 Why is risk management important for an organisation?

Risk management creates and protects value and it contributes to the demonstrable achievement of objectives and improvement of performance in a wide range of areas, including health and safety, compliance, environmental protection, efficiency of operations, governance and reputation.

Risk is an integral part of doing business and risk management addresses uncertainty and helps decision makers make informed choices and prioritise.

Risk management is not limited to health and safety and should be considered as an essential element of running an organisation.

Non-government organisations may be exposed to risk when:

- they do not have a well-functioning governance structure
- management plans, policies and processes are inadequate
- staff and volunteer roles and responsibilities are unclear
- they do not require service users to sign service agreements, consent forms or waivers
- equipment and facilities are not safe for intended use
- they have not implemented a comprehensive WHS plan
- insurance is inadequate or inappropriate
- operations are not regularly evaluated.

> **TIP:** Your organisation's risk management framework should be embedded into the organisation's daily processes and activities; it should contain a risk strategy and a risk appetite statement.

6.1.6 Risk management principles

The AS/NZS ISO 31000:2009 identifies 11 principles for effective risk management:

1. Risk management creates and protects value
2. Risk management is an integral part of all organisational processes
3. Risk management is part of decision making
4. Risk management explicitly addresses uncertainty
5. Risk management is systematic, structured and timely
6. Risk management is based on the best available information
7. Risk management is tailored
8. Risk management takes human and cultural factors into account
9. Risk management is transparent and inclusive
10. Risk management is dynamic, iterative and responsive to change
11. Risk management facilitates continual improvement of the organisation.

Organisations should develop a risk management policy and a plan for how the risk management process will be managed. An organisation's risk management policy should incorporate the above principles.

A risk management policy and a risk management plan should describe the:

- commitment and leadership from management
- delegation of defined tasks to ensure accountability
- reporting system – including progress reports, reports on extraordinary incidents and perceived risks
- operating procedures
- education and training programs for employees and volunteers
- risk control monitoring process
- risk reduction process
- emergency response procedures
- complaints handling procedures.

Board members are responsible for ensuring the risk management plan is implemented in the organisation.

Operating procedures designed to minimise and manage risks

Organisations need to develop and review documented policies and procedures and ensure all relevant staff and volunteers receive appropriate and ongoing training, to support an effective risk management program.

Education and training programs for employees and volunteers should cover:

- risk management monitoring process
- reporting and rectification process
- procedures to deal with emergencies
- procedures to deal with complaints, in a fair, appropriate and timely manner.

When developing or reviewing risk management plans, organisations should consider the:

- effectiveness of existing business and risk management systems
- existing risk management culture
- integration and consistency of risk management processes
- processes and systems requiring modification
- constraints
- compliance or legislative requirements
- resource availability and constraints.

To maintain effectiveness, risk management plans must be reviewed and evaluated regularly.

6.1.7 Risk management policy

Risk management policies should be brief, high-level documents that can be easily understood.

The risk management policy should be communicated appropriately and clearly state the organisation’s objectives for and commitment to risk management and state:

- the rationale for managing risk
- links between the organisation’s objectives and risk management
- accountabilities and responsibilities
- the way in which conflicting interests are dealt with
- commitment to allocating appropriate resources
- measuring and reporting
- commitment to periodical review and improvement

External requirements and the public interest should also guide the policy and the following factors should be considered:

- the policy should be developed to clearly reflect the law and relevant standards
- where the system for the formulation, interpretation and enforcement of the policy works properly and effectively, that policy is essentially in the public interest
- a clearly expressed and well-defined policy which provides for appeals and procedural fairness, procedural fairness, strengthens arguments that the organisation is operating in the public interest.

6.1.8 Conclusion

Risk management policies and plans are important. They document the steps an organisation plans to take to manage actual and potential risks. The board is responsible for approving the documents and ensuring the plans are implemented within the organisation.

> **TIP:** Reporting on key issues should occur at both management and board level on a regular basis. Regular review of risks is particularly important during a time of change and/or transition.

6.2 The risk management process

6.2.1 Key Elements of the risk management process

The AS/NZS ISO 31000:2009 sets out the following key elements to establish a risk management process:

- communicate and consult
- establish the context
- identify the risk
- analyse risk
- evaluate the risk
- treat the risk
- monitor and review.

6.2.2 Communicate and consult

Effective communication and consultation with key stakeholders about risk helps an organisation to establish trust and a positive attitude to risk management and should take place during all stages of the risk management process.

Early discussion should focus on the potential implications of new initiatives and suggest improvements or alternatives.

Organisations should adopt a collaborative role in developing the risk management process. This enables organisations to achieve early consensus and agreement.

6.2.3 Establish the context

There are three areas to consider when establishing the context. These are:

External context

The external context is the external environment in which the organisation operates. The external context may include social, cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment as well as the relationships with, and perceptions and values of, external stakeholders.

Internal context

The internal context is the internal environment and may include:

- structure, roles and accountabilities
- capabilities
- relationships with and perceptions and values of internal stakeholders
- culture
- information systems and decision-making processes
- standards adopted by the organisation
- contractual relationships.

Risk management context

The risk management context defines where and how an organisation can apply the risk management process and it will vary according to the needs of the organisation.

Organisations will vary in their risk management processes depending on the:

- size of the organisation
- organisational structure and location
- governance structure
- composition of the workforce
- management expertise
- organisational planning
- range of activities the organisation is involved in
- available resources
- assets.

Establishing the risk management context may involve defining:

- goals and objectives of the risk management activities
- responsibilities
- scope, depth and breadth
- time and location
- relationships between projects, processes or activities
- methodologies
- evaluation of performance and effectiveness.

6.2.4 Identify the risks

Organisations should identify actual and potential risks associated with the services they provide. It is important that people with appropriate knowledge of the business are involved in identifying risks. Employees, drawing on their experience, can identify the:

- areas where they are exposed to risk
- extent and severity of the risk
- frequency of the occurrence which gives rise to the risk.

Risks can also be identified through:

Informal processes

- stakeholder feedback including suggestions, concerns and complaints.

Formal processes

- consultation
- monitoring of regulatory requirements
- strengths, weaknesses, opportunities and threats (SWOT) analysis
- a review of systems and processes
- results from monitoring processes including completion of audits and inspections
- surveys and questionnaires
- hazard reporting processes
- identification of organisational trends e.g. analysis of incident databases and injury history (including type of injury and cause)
- insurance claims reports.

It is important that information used to identify risks is reliable.

6.2.5 Analyse the Risk

After identifying the general areas of risk, an analysis of the risks should be undertaken to develop an understanding of the risk, which will then inform risk evaluation.

In analysing the risk organisations should consider:

- the causes and sources of the risk
- whether the risk has positive and/or negative consequences
- the likelihood of those consequences
- existing controls
- possible interdependencies of risks.

Analysis could be qualitative, quantitative or a combination of the two, depending on the risk.

6.2.6 Evaluate the risk

The risk evaluation phase requires estimating the potential and actual consequences, which might arise from identified risks and will involve determining whether an activity should cease because the consequences of continuing the activity would create unnecessary risks, or too high a risk.

Once risks have been assessed, the severity and frequency of occurrence of risk should be examined – for example, the number of risks, potential consequence and frequency. This will enable prioritisation of the risks, and also prioritisation of remediation of the risks.

In conducting the evaluation, the level of risk identified during the analysis phase should be compared with the risk criteria established when the context was considered and the organisation’s risk attitude tolerance.

6.2.7 Treat the risk

Risk treatment involves identifying the range of options for treating (or managing) risks, assessing these options and preparing and implementing treatment plans. The development of effective treatment plans requires an understanding of the immediate causes of the risk and the underlying factors that might influence the effectiveness of proposed treatments. These factors are sometimes referred to as 'root causes'.

When treating risks a cyclical process should be applied that involves:

- assessing the risk treatment
- deciding if the residual risk level is tolerable
- if the residual risk level is not tolerable, identify a new risk treatment
- assessing the effectiveness of the new treatment.

Treatments will depend on the risk and may include:

- avoiding the risk
- taking increasing risk
- removing the risk source
- changing the likelihood
- changing the consequences
- sharing the risk with another party
- retaining the risk by informed decision.

The choice of treatment will depend on a number of factors including balancing the costs and efforts against the potential benefits derived.

Any residual risk after treatment should be documented, monitored and reviewed on a regular basis.

Dignity of risk and duty of care

The 'principles of dignity' of risk and 'duty of care' are important considerations when making risk treatment decisions.

Dignity of risk refers to the service user's right to make an informed choice to experience life and take advantage of opportunities for learning, developing competencies and independence and, in doing so, taking a calculated risk. However, the welfare of the client outweighs dignity of risk.

Duty of care is the obligation to take reasonable care to avoid causing harm to another person.

6.2.8 Monitor and review

Risk management systems and treatment plans should be monitored and reviewed on an ongoing basis as circumstances change that may affect the risk management plan.

> **TIP:** Your organisation's risk management framework should be regularly reviewed for relevance along with defined risk mitigation strategies and plans for any risks identified. A robust risk management framework will be particularly important for disability service providers as they transition to the National Disability Insurance Scheme. As indicated earlier in this chapter, it will help them to identify potential risks and address areas of uncertainty which will help inform decision making and prioritising. And in a new market, it will also act as a means of providing assurances to stakeholders.

6.2.9 Documentation

It is important to document each step of the risk management process:

- to record the process of risk identification and analysis
- to demonstrate accountability – including a compliance and due diligence statement
- to provide information for decisions or processes to be reviewed
- to provide a record of risks on a risk register
- to provide information to relevant stakeholders
- to support continuing monitoring and review
- to provide an audit trail
- to maintain an incident database.

6.2.10 Conclusion

Risks will vary from organisation to organisation depending upon circumstances and the way an organisation operates. Directors are responsible for ensuring that a risk management plan is developed and implemented.

Resources

Diagram 1: Risk management overview in accordance with the Australian Standard

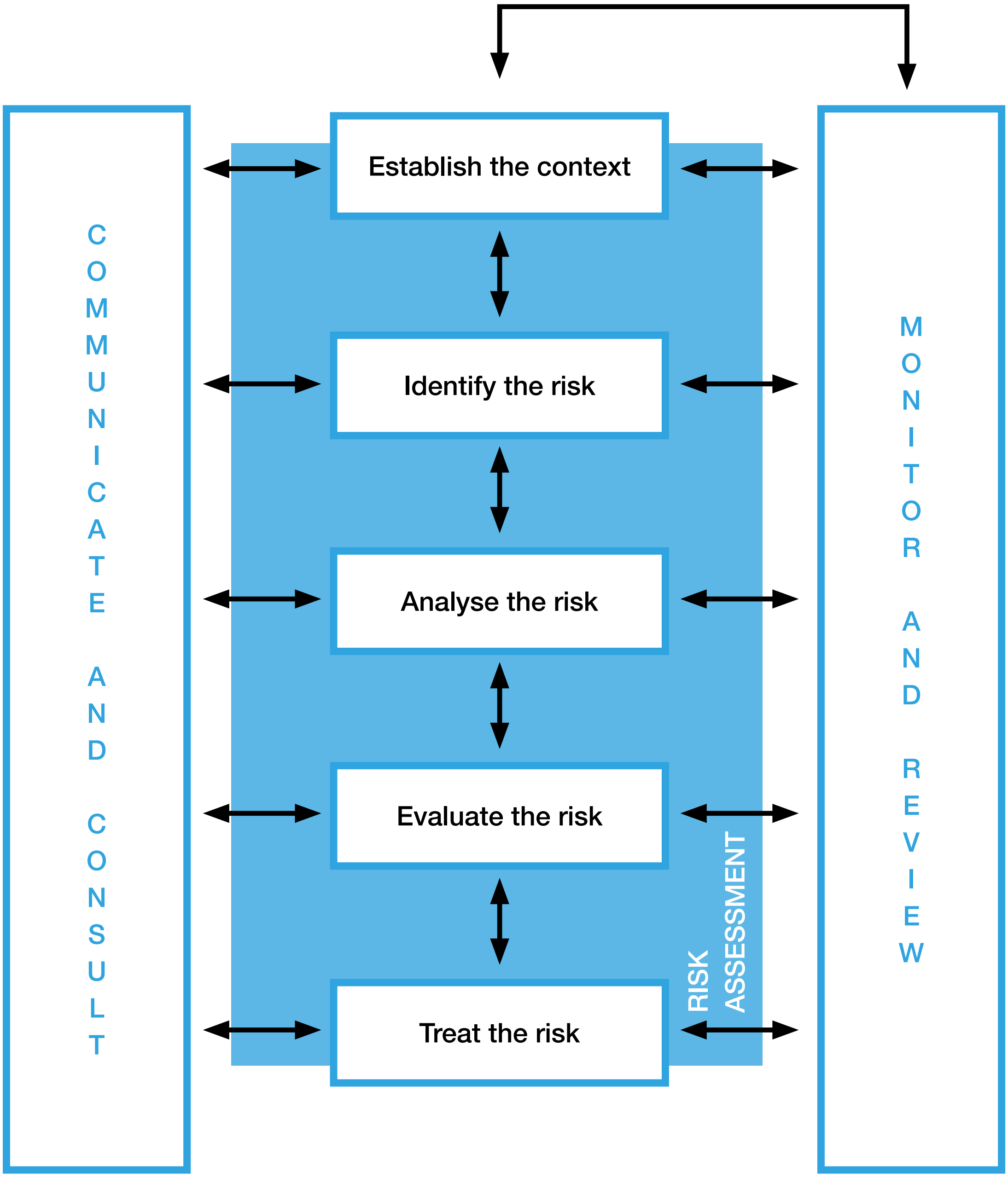
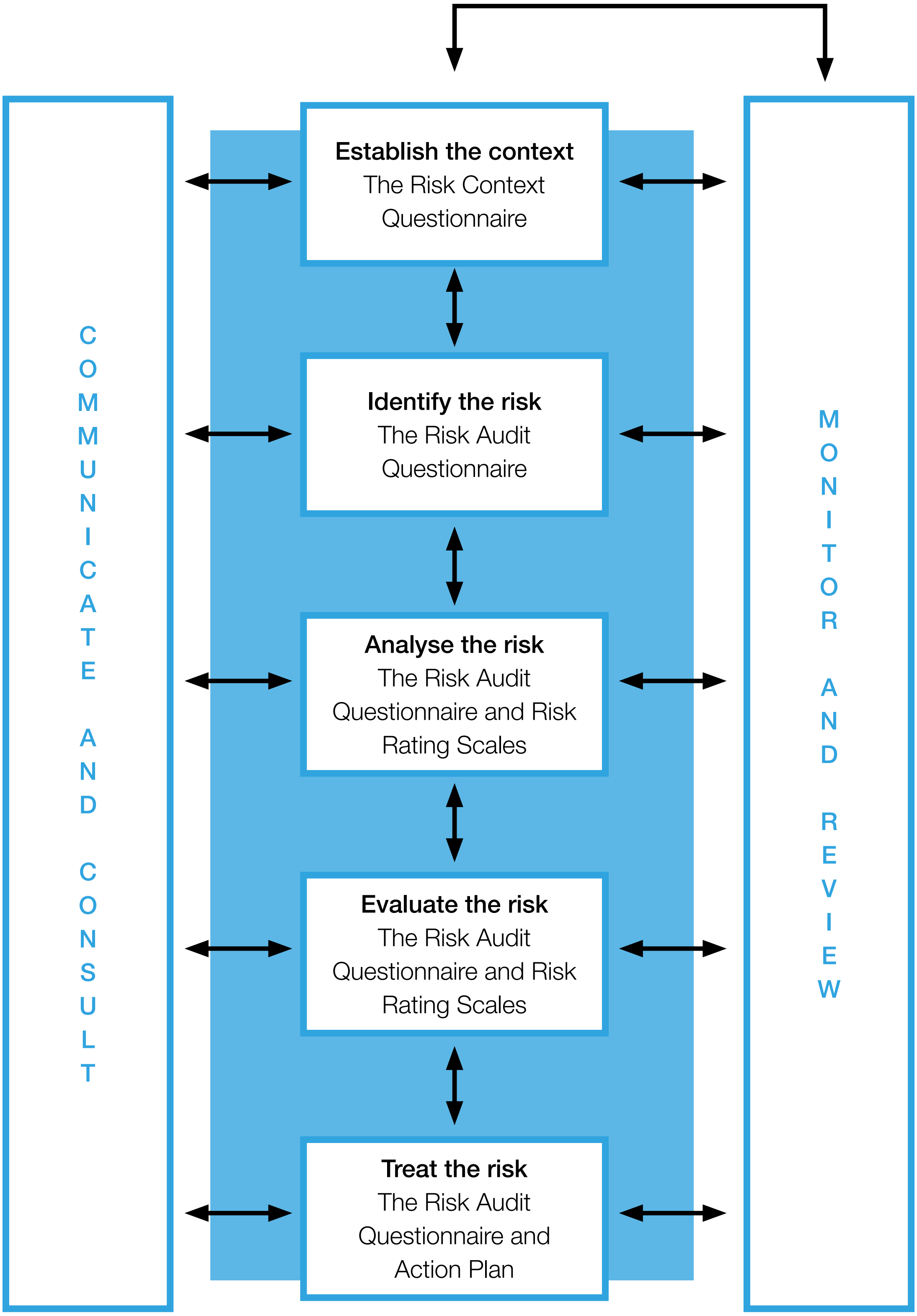


Diagram 2: Applying the risk management process



COMMUNICATE AND CONSULT

Establish the context
The Risk Context Questionnaire

Identify the risk
The Risk Audit Questionnaire

Analyse the risk
The Risk Audit Questionnaire and Risk Rating Scales

Evaluate the risk
The Risk Audit Questionnaire and Risk Rating Scales

Treat the risk
The Risk Audit Questionnaire and Action Plan

MONITOR AND REVIEW

Director: risk management
Points to remember

	Tick to indicate understanding		
Use this checklist to review the information within the introduction section of this chapter.	Yes	No	Limited
I have read and understand each of the following:			
• Corporate governance and risk management			
• What a risk is			
• What risk management is			
• Why risk management is important to your organisation			
• The benefits and opportunities of using a risk management approach			
• Who is responsible for risk management in your organisation			
• Who should be involved in the risk management process			
• Implementing a risk management plan			

If you have ticked the 'No' box please review that section again.

Director: risk management process
Points to remember

	Tick to indicate understanding		
Use this checklist to show that you have read and understand the risk management process section.	Yes	No	Limited
• The importance of consultation and communication			
• The risk context			
• The components of the risk context			
• How to establish the risk context			
• How you will consider risks in your organisation			
• The importance of consultation and communication			

If you have ticked the 'No' box please review that section again.

Director: identifying risks

Points to remember

	Tick to indicate understanding		
Use this checklist to show that you have read and understand the information with regard to identifying risks.	Yes	No	Limited
The risk identification process			
The risk audit process			
Completing the risk audit			
The likelihood scale			
The impact scale			
The risk priority scale			
How the risk rating scales are intended to work			
Completing the risk treatment plan			
The identification and treatment of new risks specific to your organisation			
The need for monitoring and review			
The importance of documenting each step of the risk management process			

If you have ticked the 'No' box please review that section again.

Appendix 1: Due diligence

Directors, managers and workers should seek to demonstrate that they used all due diligence or took all reasonable steps to prevent a reasonably foreseeable loss or injury occurring.

The concept of due diligence originates in company law. Section 180 of the *Corporations Act 2001* requires that a director or officer of a corporation exercise a degree of care and diligence in the exercise and discharge of his or her duties. The due diligence concept therefore forms a sound basis for a risk management program.

In quantifying that degree of care and diligence, directors must act in good faith and for a proper purpose, not have a material personal interest, reasonably inform themselves as to the subject matter and consider their decision to be in the best interests of the organisation.

'Practicable' has been defined as having regard to the:

- severity of the hazard or risk in question
- state of knowledge about that hazard or risk and any ways of removing or mitigating that hazard or risk
- availability and suitability of ways to remove or mitigate that hazard or risk
- cost of removing or mitigating that hazard or risk.

In the context of risk management, due diligence has been defined as taking the following measures:

Leadership and management

- strong and visible commitment and leadership
- development and implementation of steps that integrate and prevent risks in all activities
- management of all facilities and activities in a manner that protects the health and safety of employees, volunteers, service users and the public.

Reporting and accountability

- clearly defined accountability and the establishment of clear reporting lines on all aspects of operations which have the potential to create risk
- development and implementation of effective systems to manage and disseminate information on risk management performance and effectiveness
- risk management to be a significant factor in the measurement of staff and volunteer performance.

Education and training

- all relevant personnel should be provided with appropriate training and experience in order to develop the skills and judgement necessary to perform activities in a responsible manner
- maintenance of a high level of awareness of the latest best practice, methods and standards in each worker's or manager's chosen discipline.

Compliance and assessment

- develop a management system to take into account trends in risks in the administration and management of a non-government organisation
- ensure review procedures are put in place.

Response procedures

- recognising and responding quickly to concerns about the impact of activities on employees, volunteers, service users and the public
- development of comprehensive contingency and emergency plans to ensure prompt response to any harmful or dangerous incident or situation.

What constitutes due diligence, and the reasonable steps that should be taken to achieve it, will depend entirely upon the circumstances of the case or the organisation.

Directors and staff of an organisation will be able to establish that they have acted with due diligence and exercised all reasonable care if they can show that a risk management program has been established and provide evidence that reasonable steps were taken to minimise or prevent risks. Other matters that may be taken into account are:

- whether they were aware of particular required levels, standards and methods for risk reduction and increased safety
- whether the risk management program was adequately supervised
- their general degree of authority and specific responsibility
- their previous record in regard to losses, injuries and other incidents
- their responses to problems, incidents and injuries
- whether they were prepared to immediately and personally react when standards had not been met and the system had failed.

Appendix 2: Management principles

The following principles are examples of how organisations can apply good management principles that assist in establishing and maintaining a sound risk management system.

certainty – operating a service with confidence that it will not be threatened by significant unexpected changes to operational standards, and regularly re- evaluating and reviewing requirements as the organisation evolves.

communication – information provided in an accessible format will help stakeholders understand new concepts and the rationale behind them and will contribute to an informed debate.

consultation and collaboration – with key stakeholders will ensure that appropriate policies, procedures and systems are developed.

cost effectiveness – to ensure that maximum value is gained.

efficiency – clearly defined policies and management systems.

flexibility – to encourage the development of alternative approaches that take account of changing circumstances and produce innovative solutions.

integrity – reliability in the development of its policies and procedures.

practicality – objectives are set which are sufficient to achieve the aims of the organisation.

responsibility – the setting of management goals and documenting the accountability of individuals within an organisation.

transparency – openness engenders confidence in the development and application of objectives and leads to acceptance of an organisation's decision.

Conclusion

Boards should seek to adopt better practice in the conduct of their organisation's activities. Services and activities should be provided in accordance with the policies approved by the board and developed in conjunction with service users, staff, volunteers and other key stakeholders.

There will always remain some inherent risks in certain activities. However, unnecessary risks can be reduced or avoided through risk management.

Risk management procedures demonstrate that an organisation is taking steps towards complying with its legal duties, which could be crucial to successfully defending any legal action taken against an organisation and can be used to ensure continued organisational viability.

Management principles summary table

Principle	Poor Practice	Better Practice
Certainty	**Unpredictable**	**Predictable**
	Variable and unclear objectives, practices or standards	Uniform and predictable objectives, practices and standards
	Volunteers unsure of practices which should be adopted	Milestones for review and operation clearly established and set out
Communication	**Ad Hoc**	**Strategic**
	Information difficult to obtain	Forums to provide information, (internal structures)
	Key stakeholders unaware of issues, expectations and requirements	Information regarding policies and processes related to key stakeholders
	Poorly written policies and procedures	Use of plain English
	Rationale for decisions unclear	Proper use of a variety of forms of verbal and written communication
		Regular information dissemination
Consultation	**Selective**	**Integrated**
	Ad hoc and unstructured consultation with key stakeholders	Early discussions
	Reactive consultative processes	Regular forums
	Too many bodies without power and without an interest in the organisation	Guidelines outlining formal consultative process
	Only some stakeholders consulted	Key stakeholders consulted

Principle	Poor Practice	Better Practice
Cost effectiveness	**Irrelevant**	**Relevant**
	Poor promotion and marketing in the entrepreneurial sense	Full assessment of all regulatory measures after consultation with key stakeholders
	Minimal or no cost assessment of proposed policies and procedures	Well defined milestones for implementation
	Unrealistic time lines for implementation of new policies and procedures	Strict financial accountability Finance and administrative staff involved in decision making about operations
Efficiency	**Random**	**Systematic**
	Unclear time lines and late responses in administrative processes	Reduce delays where they exist Minimum number of personnel to be consulted to achieve result
	Documentation unclear	Clearly defined delegation and reporting processes
Flexibility	**Limited**	**Optimal**
	Limited focus	Outcome-oriented
	Unyielding commitment to existing policies and procedures	Recognition of changing standards Innovative application in policy making
Integrity	**Presumed**	**Earned**
	Integrity lacking	Soundly based decisions
	No respect from stakeholders	Sound rationale between regulatory standards and decisions and policy implementation

Principle	Poor Practice	Better Practice
Practicality	Secondary	Primary
	Unachievable targets	Collaborative approaches with key stakeholders to define and achieve outcomes
	Targets exceed objectives	Achievable objectives
	Staff and people at the service delivery level are not consulted about implementation	Interim targets set for long-term objectives Appropriate and measurable performance indicators
Responsibility	Internal	External
	Unaccountability to those most influenced	Clear decision making responsibility
	Volunteers, members and administration staff accountable for matters beyond their influence	Ownership accepted for advice and decisions at appropriate levels Clear lines of delegation and reporting from policy makers through management to direct service staff for implementation
Transparency	Opaque	Clear
	Rationale for decisions unclear and often withheld from key stakeholders	Visible decision making processes Fairness to all parties Rationale clear at point of consultation with stakeholders

Appendix 3: Risk management policy development

The risk management policy statement should be approved by the board and should provide the base on which the risk management plan is built. Procedures should be an implementation of the policy.

Policy statements describe:

- why risk management is important
- the scope of authority and responsibilities of personnel
- where risk management fits into the corporate structure
- the extent and nature of the approaches to be used in managing risk.

Such statements should provide the basis for specific action.

A risk management policy should include:

- the organisation's purpose and vision
- its goals and objectives
- links to strategic business plan
- details of personnel management systems that relate to risk (policy and procedure manuals, competencies and recruitment processes etc)
- financial information.

Example of a risk management policy statement

Policy Statement	**(Insert Organisation Name)** aims to use best practice in risk management to support and enhance our activities in all areas of our organisation. We will ensure risk management is an integral part of all our decision-making processes. We will adopt best practice in assisting our organisation to manage our risk to minimise reasonably foreseeable harm to people, disruption to our operations, damage to the environment and property. We will identify and take advantage of opportunities as well as minimising adverse effects. We will train our people to implement risk management effectively. We will strive to continually improve our risk management practices.
Responsibilities	The risk manager and risk management committee (or other persons delegated with responsibility for overseeing risk management) appointed by the board are accountable to the board for the implementation of the risk management process and ultimately responsible for the management of risks in our organisation. All key personnel are responsible for managing risks in their areas.
Process	A risk management procedure has been established following the Australian Standard AS/NZS ISO 31000:2009. It should be used for guidance by everyone involved with the application of risk management.
Monitoring and review	The risk manager (or other person) will monitor and review the implementation of the risk management plan and report to the board at every meeting. The risk management committee (or person responsible) will facilitate the development of a common risk management approach across areas of our organisation by: • implementing the risk management plan • documenting and communicating information to relevant stakeholders • monitoring and reviewing organisational performance against performance indicators and organisational policy • reporting on the progress of implementing the risk management plan.
Further information	For further information on this policy and the risk management procedures, contact **(Insert the name of the risk manager or person responsible).**
Links	Enter the links between the policy and the organisation's strategic and corporate plans.
Policy review date:	**(Insert date)**

Appendix 4: Strategic and organisational context tool

Context analysis

- What are we here for (our vision and/or philosophy)?
- What are we trying to achieve (our objectives)?
- When and how will we achieve our objectives (our goals)?

Organisational context

- What are we good at (our strengths)?
- What do we need to improve (our weaknesses)?
- What are the main opportunities available to us that we should take advantage of?
- Who are our service users?
- Who are our stakeholders?
- Who are our competitors/potential competitors?
- Who are our partners/potential partners?
- What are the key outcomes for our organisation, against which we could clearly determine how well we are performing?
- How well do we serve our service users, members and stakeholders? What is the environment within which we operate:
    - Financial
    - Community values and attitudes
    - Reliance on fundraising, government funding and grants or independent service user fees
    - Narrow/specialised or broad-based participation
    - Culture of service users, carers and partners
    - Legal
    - Other?
- Is this environment stable or volatile?
- Within this environment, and taking into account our objectives, goals and desired outcomes, how would we determine whether a level of risk was acceptable, given the control measures in place? Are further measures required?
- Do we test:
    - Ourselves against other organisations?
    - Whether our service users and/or other stakeholders are being serviced?

- Do we have and implement a strategic plan?
- Is our strategic plan being achieved?
- What laws and regulations apply to our organisation?
- Do we comply with these laws?
- What contracts and service agreements do we have?
- Do we know what they say and require?
- What intellectual property do we have?
- Is our intellectual property properly protected?
- What premises and facilities do we have? Have they been surveyed to determine whether they comply with all relevant laws, regulations and standards?
- Do we have any actual or potential human relations or workplace issues?
- Is the role of management clearly defined?
- Are there contracts or clear terms of reference for our volunteers?
- Is our insurance cover adequate?
- Do we know our insurance claims history?
- What are our organisation's future claims or liabilities likely to be?
- Have we taken professional advice on the nature and amount of insurance cover needs?
- What were our organisation's financial results for the previous three years? Were they satisfactory?
- Are these results comparable to those of similar organisations?
- Do we have a process for financial auditing?
- What financial controls, reporting systems and accounting policies are in place? Are these complied with?
- Are there any outstanding taxation issues? For example our tax exempt status?
- Are there clearly defined governance and management structures? If yes, what are they?
- What are the physical details of premises occupied by our organisation?
- Are our premises leased? If yes, what are the terms of those leases?
- Have we been involved in any major disputes in the past?
- Are we involved in any existing disputes?
- Do we have any potential disputes?
- Do we know what reporting and compliance requirements apply to our organisation? For example with the NDIA, ASIC, NSW Fair Trading, ACNC, etc.?
- Are we up to date with our reporting and compliance requirements?

Appendix 5: Risk audit and action plan

Potential risk and consequence

The risks in the audit have been expressed as statements, not as questions. When expressed as a statement it is easier to perform a meaningful assessment against the rating scales.

Consider each potential risk area identified in the risk audit tool against the following questions:

- how effective is your organisation's current approach (if any) to controlling or managing the risk?
- what are the weaknesses associated with the current controls?
- what might be the impact on the organisation's objectives if the risk occurred and the controls did not work as intended?

This risk audit is not exhaustive. It is a tool to assist with the risk management process and facilitate your risk treatment and action plan development. It should be adapted to meet your organisation's needs.

Risk rating scale

The risk rating scales will allow you to rate identified risks, analyse and evaluate them, and then identify risk management priorities. As with the context, you should identify a number of new risks that are specific to your organisation and how it operates.

Each identified risk in the risk audit should be rated. These ratings describe:

- the likelihood of the risk event occurring (occurrence)
- the loss or damage impact if the risk event occurred (severity)
- the risk priority scales. The risk priority will be rated according to the potential loss or damage impact, the degree of urgency required to address the risk and the level of importance in the decision to take action to manage the risk.

Likelihood

The likelihood is related to the potential for risk events to arise over an annual evaluation cycle.

Table 1: Likelihood scale

Rating	Likelihood
A	Almost certain: will probably occur, could occur several times per year
B	Likely: high probability, likely to arise once per year
C	Possible: reasonable likelihood that it may arise over a five-year period
D	Unlikely: plausible, could occur over a five to ten year period
E	Rare: very unlikely but not impossible, unlikely over a ten year period

Loss or damage impact (consequence)

The loss or damage impact rating is based on the degree of loss or damage as outlined the table below.

Table 2: Loss or damage impact scale

Rating	Potential impact
A	Catastrophic: most objectives may not be achieved, or several severely affected
B	Major: most objectives threatened or one severely affected
C	Moderate: some objectives affected, considerable effort to rectify
D	Minor: easily remedied, with some effort the objectives can be achieved
E	Negligible: very small impact, rectified by normal processes

Risk priority

The risk priority scale determines the nature of the risk and the action required. It gives indicators to assist in the decision making of what action is warranted for the risks.

Table 3: Risk priority scale

	IMPACT					
		A	B	C	D	E
LIKELIHOOD	A	Extreme (1)	Extreme (1)	Major (2)	Major (2)	Medium (3)
	B	Extreme (1)	Extreme (1)	Major (2)	Medium (3)	Minor (4)
	C	Extreme (1)	Major (2)	Major (2)	Medium (3)	Minor (4)
	D	Major (2)	Major (2)	Medium (3)	Minor (4)	Minor (4)
	E	Medium (3)	Medium (3)	Minor (4)	Minor (4)	Minor (4)

Key

1	Extreme risks that are likely to arise and have potentially serious consequences requiring urgent attention
2	Major risks that are likely to arise and have potentially serious consequences requiring urgent attention or investigation
3	Medium risks that are likely to arise or have serious consequences requiring attention
4	Minor risks and low consequences that may be managed by routine procedures

The risk priority scales have been rated according to:

- the potential loss or damage impact
- the degree or urgency required to treat the risk and/or the type of intervention to treat the risk
- the level of importance in taking action to manage the risk.

Once a risk priority has been determined the board and management should then determine the level of risk treatment and action required for each risk.

Example: How the risk rating works

The response your organisation gives to the question 'Does your organisation fulfil the requirements to maintain incorporation?' would be considered as follows:

Question: Is it likely that our organisation does not fulfil incorporation requirements [likelihood]?

Answer: Yes.

Question: If yes, how likely?

Answer: Likelihood rating would be a C (reasonable likelihood that it may arise over a five-year period).

Question: If yes, what would be the consequences and/or the loss or damage impact of those consequences [severity]?

Answer: Impact rating would be a D (easily remedied, with some effort, objectives can be achieved).

Question: What is the nature of the risk and the action required?

Answer: Given the likelihood rating is a C (possible) and the impact rating is a D (unlikely), the risk rates as a medium (level 3) risk on the risk rating scale. So it is a medium risk that is likely to arise or have serious consequences requiring attention.

Question: How should it be treated?

Answer: Ensure a compliance and regular monitoring regime is in place.

The risk action plan

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

Factors you need to consider when completing the actions on the risk audit and action plan:

- what is needed to treat the risk?
- who has responsibility?
- what is the timeframe?
- how will you know when the risk has been successfully managed?

These elements will comprise your action plan. If your organisation already has a strategy in place to address or manage the risk, insert details of that strategy in the space provided. If not, you will need to devise a strategy.

AUDIT				ACTION PLAN				
Potential risk and consequence	**Likelihood**	**Loss/ Damage Impact**	**Risk Priority Rating**	**Strategy to Address the Risk** (How will you do this?)	**Resources** (What do you need to do this?)	**Who is Responsible for Action?**	**Timeframe** (Specify a time or date)	**Completion**
PART A: ADMINISTRATION								
1.Your members do not have access to a copy of your constitution Leading to:								
2.Your organisation does not follow your constitution Leading to:								
3.Suitable minutes are not recorded, distributed and properly approved Leading to:								

AUDIT				ACTION PLAN				
Potential risk and consequence	**Likelihood**	**Loss/ Damage Impact**	**Risk Priority Rating**	**Strategy to Address the Risk** (How will you do this?)	**Resources** (What do you need to do this?)	**Who is Responsible for Action?**	**Timeframe** (Specify a time or date)	**Completion**
4. Records are not maintained to the standard required by law Leading to:								
5. Procedures are not in place to ensure security of membership information Leading to:								
6. Your organisation has not recently reviewed its current and future goals Leading to:								

AUDIT				ACTION PLAN				
Potential risk and consequence	**Likelihood**	**Loss/ Damage Impact**	**Risk Priority Rating**	**Strategy to Address the Risk** (How will you do this?)	**Resources** (What do you need to do this?)	**Who is Responsible for Action?**	**Timeframe** (Specify a time or date)	**Completion**
7. Management (operational) does not have sufficient time and resources to fulfil its responsibilities Leading to:								
8. Information is not well presented to the board or membership when relevant Leading to:								
9. Management (operational) does not have direct access to information, e.g. member database Leading to:								

AUDIT				ACTION PLAN				
Potential risk and consequence	**Likelihood**	**Loss/ Damage Impact**	**Risk Priority Rating**	**Strategy to Address the Risk** (How will you do this?)	**Resources** (What do you need to do this?)	**Who is Responsible for Action?**	**Timeframe** (Specify a time or date)	**Completion**
PART B: GOVERNANCE								
10. Minutes do not show the actions and responsibilities agreed to at the meeting Leading to:								
11. There is no follow-up for action items arising from meetings Leading to:								
12. The board is not distinct from management staff Leading to:								

	AUDIT					ACTION PLAN		
Potential risk and consequence	**Likelihood**	**Loss/ Damage Impact**	**Risk Priority Rating**	**Strategy to Address the Risk** (How will you do this?)	**Resources** (What do you need to do this?)	**Who is Responsible for Action?**	**Timeframe** (Specify a time or date)	**Completion**
13. The skills and experience of directors are not adequate Leading to:								
14. There is no induction process for new directors Leading to:								
15. The directors have potential or actual conflicts of interest Leading to:								

	AUDIT			ACTION PLAN				
Potential risk and consequence	**Likelihood**	**Loss/ Damage Impact**	**Risk Priority Rating**	**Strategy to Address the Risk** (How will you do this?)	**Resources** (What do you need to do this?)	**Who is Responsible for Action?**	**Timeframe** (Specify a time or date)	**Completion**
16. Conflicts of interests are not properly declared and not kept in a register of nterests Leading to:								
17. The directors do not know their legal and ethical obligations Leading to:								
18. The board does not meet on a regular and formal basis Leading to:								

	AUDIT			ACTION PLAN				
Potential risk and consequence	**Likelihood**	**Loss/ Damage Impact**	**Risk Priority Rating**	**Strategy to Address the Risk** (How will you do this?)	**Resources** (What do you need to do this?)	**Who is Responsible for Action?**	**Timeframe** (Specify a time or date)	**Completion**
PART C: FINANCE								
19. Formal agendas are not set for the board meetings Leading to:								
20. The board fails to ensure it has information necessary to fulfil its functions Leading to:								
21. Your organisation does not have a financial plan Leading to:								

AUDIT				ACTION PLAN				
Potential risk and consequence	**Likelihood**	**Loss/ Damage Impact**	**Risk Priority Rating**	**Strategy to Address the Risk** (How will you do this?)	**Resources** (What do you need to do this?)	**Who is Responsible for Action?**	**Timeframe** (Specify a time or date)	**Completion**
22. Your organisation does not prepare budgets where appropriate Leading to:								
23. All financial transactions are not accurately recorded Leading to:								
24. An annual audit is not conducted of your organisation's financial records Leading to:								

	AUDIT					ACTION PLAN		
Potential risk and consequence	**Likelihood**	**Loss/ Damage Impact**	**Risk Priority Rating**	**Strategy to Address the Risk** (How will you do this?)	**Resources** (What do you need to do this?)	**Who is Responsible for Action?**	**Timeframe** (Specify a time or date)	**Completion**
25. The audit is not conducted by an appropriate person Leading to:								
26. A financial report is not provided to each board meeting Leading to:								
27. Expenditure is not authorised through an identified process Leading to:								

AUDIT				ACTION PLAN				
Potential risk and consequence	**Likelihood**	**Loss/ Damage Impact**	**Risk Priority Rating**	**Strategy to Address the Risk** (How will you do this?)	**Resources** (What do you need to do this?)	**Who is Responsible for Action?**	**Timeframe** (Specify a time or date)	**Completion**
28. Suitable banking arrangements are not in place for the organisation Leading to:								
29. Multiple signatures are not required for withdrawals and/ or procedure is not complied with Leading to:								
30. Professional advice is not sought on financial matters Leading to:								

AUDIT				ACTION PLAN				
Potential risk and consequence	**Likelihood**	**Loss/ Damage Impact**	**Risk Priority Rating**	**Strategy to Address the Risk** (How will you do this?)	**Resources** (What do you need to do this?)	**Who is Responsible for Action?**	**Timeframe** (Specify a time or date)	**Completion**
31. Management does not monitor the key financial risks faced by your organisation Leading to:								
32. Financial guidelines are not clearly documented and circulated to key personnel Leading to:								
PART D: INSURANCE								
33. The organisation does not have suitable insurance cover Leading to:								

AUDIT				ACTION PLAN				
Potential risk and consequence	**Likelihood**	**Loss/ Damage Impact**	**Risk Priority Rating**	**Strategy to Address the Risk** (How will you do this?)	**Resources** (What do you need to do this?)	**Who is Responsible for Action?**	**Timeframe** (Specify a time or date)	**Completion**
34. Advice was not sought from an insurance broker Leading to:								
35. Insurance is not regularly reviewed, e.g. on an annual basis Leading to:								
36. The person responsible fails to notify your broker/ insurer of claims in accordance with your policy Leading to:								

AUDIT				ACTION PLAN				
Potential risk and consequence	**Likelihood**	**Loss/ Damage Impact**	**Risk Priority Rating**	**Strategy to Address the Risk** (How will you do this?)	**Resources** (What do you need to do this?)	**Who is Responsible for Action?**	**Timeframe** (Specify a time or date)	**Completion**
37. Board members are not aware of your organisation's insurance with respect to:								
• Cover Leading to:								
• Any excess that may be payable Leading to:								

AUDIT				ACTION PLAN				
Potential risk and consequence	**Likelihood**	**Loss/ Damage Impact**	**Risk Priority Rating**	**Strategy to Address the Risk** (How will you do this?)	**Resources** (What do you need to do this?)	**Who is Responsible for Action?**	**Timeframe** (Specify a time or date)	**Completion**
• Limitations and exclusions Leading to:								
• Responsibilities Leading to:								
38. There is a person responsible for claim procedures Leading to:								

	AUDIT					ACTION PLAN		
Potential risk and consequence	**Likelihood**	**Loss/ Damage Impact**	**Risk Priority Rating**	**Strategy to Address the Risk** (How will you do this?)	**Resources** (What do you need to do this?)	**Who is Responsible for Action?**	**Timeframe** (Specify a time or date)	**Completion**
PART E: POLICY (ORGANISATIONAL)								
39. Your organisation has inadequate policies to guide its decisionmaking Leading to:								
40. Policies are not documented in a uniform manner Leading to:								
41. Policies are not clearly communicated to members Leading to:								

AUDIT				ACTION PLAN				
Potential risk and consequence	**Likelihood**	**Loss/ Damage Impact**	**Risk Priority Rating**	**Strategy to Address the Risk** (How will you do this?)	**Resources** (What do you need to do this?)	**Who is Responsible for Action?**	**Timeframe** (Specify a time or date)	**Completion**
42. Policies are improperly implemented Leading to:								
43. Policies are not monitored and periodically reviewed Leading to:								
44. Policies do not reflect the needs and practices of the organisation in respect of:								

	AUDIT					ACTION PLAN		
Potential risk and consequence	**Likelihood**	**Loss/ Damage Impact**	**Risk Priority Rating**	**Strategy to Address the Risk** (How will you do this?)	**Resources** (What do you need to do this?)	**Who is Responsible for Action?**	**Timeframe** (Specify a time or date)	**Completion**
• Access to services Leading to:								
• Governance Leading to:								
• Employment Leading to:								

AUDIT				ACTION PLAN				
Potential risk and consequence	**Likelihood**	**Loss/ Damage Impact**	**Risk Priority Rating**	**Strategy to Address the Risk** (How will you do this?)	**Resources** (What do you need to do this?)	**Who is Responsible for Action?**	**Timeframe** (Specify a time or date)	**Completion**
• Service provision Leading to:								
• Discrimination/ harassment Leading to:								
PART F: PLANNING AND STRATEGY								
• Privacy Leading to:								

	AUDIT			ACTION PLAN				
Potential risk and consequence	**Likelihood**	**Loss/ Damage Impact**	**Risk Priority Rating**	**Strategy to Address the Risk** (How will you do this?)	**Resources** (What do you need to do this?)	**Who is Responsible for Action?**	**Timeframe** (Specify a time or date)	**Completion**
• Personal/child protection Leading to:								
45. Your organisation does not have a clear, documented strategic plan Leading to:								
46. Board members are unaware of and/or not in agreement with the plan								

AUDIT				ACTION PLAN				
Potential risk and consequence	**Likelihood**	**Loss/ Damage Impact**	**Risk Priority Rating**	**Strategy to Address the Risk** (How will you do this?)	**Resources** (What do you need to do this?)	**Who is Responsible for Action?**	**Timeframe** (Specify a time or date)	**Completion**
47. Your organisation has no clearly defined purpose with goals stated in writing Leading to:								
48. The purpose and goals are not developed in consultation with stakeholders Leading to:								
49. The board does not review your strategic direction regularly Leading to:								

AUDIT				ACTION PLAN				
Potential risk and consequence	**Likelihood**	**Loss/ Damage Impact**	**Risk Priority Rating**	**Strategy to Address the Risk** (How will you do this?)	**Resources** (What do you need to do this?)	**Who is Responsible for Action?**	**Timeframe** (Specify a time or date)	**Completion**
50. Your organisation does not consult on the needs and expectations of stakeholders Leading to:								
51. The strategic plan is not properly implemented and monitored Leading to:								
52. Responsibilities are not clearly defined in all plans Leading to:								

	AUDIT			ACTION PLAN				
Potential risk and consequence	**Likelihood**	**Loss/ Damage Impact**	**Risk Priority Rating**	**Strategy to Address the Risk** (How will you do this?)	**Resources** (What do you need to do this?)	**Who is Responsible for Action?**	**Timeframe** (Specify a time or date)	**Completion**
53. Time frames are not set and met in all plans Leading to:								
54. Adequate resources are not allocated to implement all plans Leading to:								
55. Appropriate emergency response procedures are not in place Leading to:								

	AUDIT					ACTION PLAN		
Potential risk and consequence	**Likelihood**	**Loss/ Damage Impact**	**Risk Priority Rating**	**Strategy to Address the Risk** (How will you do this?)	**Resources** (What do you need to do this?)	**Who is Responsible for Action?**	**Timeframe** (Specify a time or date)	**Completion**
56. You do not periodically review your plans Leading to:								
57. Planning is not seen as a key aspect of management responsibility Leading to:								
58. The planning process does not have the full support of management and the board Leading to:								

AUDIT				ACTION PLAN				
Potential risk and consequence	**Likelihood**	**Loss/ Damage Impact**	**Risk Priority Rating**	**Strategy to Address the Risk** (How will you do this?)	**Resources** (What do you need to do this?)	**Who is Responsible for Action?**	**Timeframe** (Specify a time or date)	**Completion**
59. You are unable to identify priorities and react to events that may significantly affect your organisation Leading to:								
PART G: PERSONNEL MANAGEMENT								
60. Your organisation fails to monitor trends in the industry Leading to:								
61. Your organisation does not review itself against other organisations Leading to:								

AUDIT				ACTION PLAN				
Potential risk and consequence	**Likelihood**	**Loss/ Damage Impact**	**Risk Priority Rating**	**Strategy to Address the Risk** (How will you do this?)	**Resources** (What do you need to do this?)	**Who is Responsible for Action?**	**Timeframe** (Specify a time or date)	**Completion**
62. There are no formal personnel strategies, written policies or procedure manuals for personnel, (including volunteers) Leading to:								
63. There is an unreasonable workload imposed on staff and key volunteers Leading to:								
64. Roles and responsibilities are not clearly defined and understood Leading to:								

AUDIT				ACTION PLAN				
Potential risk and consequence	**Likelihood**	**Loss/ Damage Impact**	**Risk Priority Rating**	**Strategy to Address the Risk** (How will you do this?)	**Resources** (What do you need to do this?)	**Who is Responsible for Action?**	**Timeframe** (Specify a time or date)	**Completion**
65. Position descriptions (including volunteer positions) do not clearly detail responsibilities Leading to:								
66. Suitable induction processes are not in place to ensure a smooth transition when key positions change Leading to:								
67. Key volunteers do not have clear terms of reference and contracts Leading to:								

	AUDIT					ACTION PLAN		
Potential risk and consequence	**Likelihood**	**Loss/ Damage Impact**	**Risk Priority Rating**	**Strategy to Address the Risk** (How will you do this?)	**Resources** (What do you need to do this?)	**Who is Responsible for Action?**	**Timeframe** (Specify a time or date)	**Completion**
68. The organisation has not adopted appropriate codes of behaviour Leading to:								
69. The following legislative requirements are not met for paid employees:								
• Workers compensation Leading to:								

	AUDIT			ACTION PLAN				
Potential risk and consequence	**Likelihood**	**Loss/ Damage Impact**	**Risk Priority Rating**	**Strategy to Address the Risk** (How will you do this?)	**Resources** (What do you need to do this?)	**Who is Responsible for Action?**	**Timeframe** (Specify a time or date)	**Completion**
• Taxation requirements Leading to:								
• Superannuation requirements Leading to:								
• Staff salary and conditions Leading to:								

AUDIT				ACTION PLAN				
Potential risk and consequence	**Likelihood**	**Loss/ Damage Impact**	**Risk Priority Rating**	**Strategy to Address the Risk** (How will you do this?)	**Resources** (What do you need to do this?)	**Who is Responsible for Action?**	**Timeframe** (Specify a time or date)	**Completion**
• Workplace, health and safety requirements Leading to:								
• Rehabilitation requirements Leading to:								
70. There is no clear procedure to handle disputes/complaints within your organisation Leading to:								

	AUDIT			ACTION PLAN				
Potential risk and consequence	**Likelihood**	**Loss/ Damage Impact**	**Risk Priority Rating**	**Strategy to Address the Risk** (How will you do this?)	**Resources** (What do you need to do this?)	**Who is Responsible for Action?**	**Timeframe** (Specify a time or date)	**Completion**
71. There is no procedure for handling complaints from outside your organisation Leading to:								
72. Certain key functions are performed by one or few persons Leading to:								
73. There are ineffective lines of communication throughout your organisation Leading to:								

AUDIT				ACTION PLAN				
Potential risk and consequence	**Likelihood**	**Loss/ Damage Impact**	**Risk Priority Rating**	**Strategy to Address the Risk** (How will you do this?)	**Resources** (What do you need to do this?)	**Who is Responsible for Action?**	**Timeframe** (Specify a time or date)	**Completion**
74. There is no succession plan (for staff, key volunteers or directors) Leading to:								
75. Standards are not set for each task to define acceptable performance Leading to:								
76. Your organisation has no personnel policy (including for volunteers) which relates to its purpose and goals Leading to:								

AUDIT				ACTION PLAN				
Potential risk and consequence	**Likelihood**	**Loss/ Damage Impact**	**Risk Priority Rating**	**Strategy to Address the Risk** (How will you do this?)	**Resources** (What do you need to do this?)	**Who is Responsible for Action?**	**Timeframe** (Specify a time or date)	**Completion**
PART H – EDUCATION, TRAINING AND ACCREDITATION								
77. Staff (and volunteers) are not trained in providing the appropriate level of client service Leading to:								
78. Staff (paid and volunteer) have inappropriate or no training or work experience Leading to:								
79. Staff fail to maintain their skills and update their qualifications Leading to:								

	AUDIT			ACTION PLAN				
Potential risk and consequence	**Likelihood**	**Loss/ Damage Impact**	**Risk Priority Rating**	**Strategy to Address the Risk** (How will you do this?)	**Resources** (What do you need to do this?)	**Who is Responsible for Action?**	**Timeframe** (Specify a time or date)	**Completion**
PART I – CONTRACTS, SERVICE AGREEMENTS AND FUNDING AGREEMENTS								
80. Opportunities for training and education (initial or ongoing) are not sought or provided Leading to:								
81. Suitable records are not kept indicating the training and qualifications of staff and volunteers Leading to:								
82. Directors are unaware whether your organisation has any contractual arrangements or if so, the terms and nature of them Leading to:								

AUDIT				ACTION PLAN				
Potential risk and consequence	**Likelihood**	**Loss/ Damage Impact**	**Risk Priority Rating**	**Strategy to Address the Risk** (How will you do this?)	**Resources** (What do you need to do this?)	**Who is Responsible for Action?**	**Timeframe** (Specify a time or date)	**Completion**
83. There is no register kept containing key details of all Contracts service agreement and funding agreements Leading to:								
84. Your organisation fails to comply with its contracts, service agreements and funding agreements Leading to:								
PART J: THE PHYSICAL ENVIRONMENT								
85. Contracts, service agreements and funding agreements are not subject to an appropriate review before execution or renewal Leading to:								

AUDIT				ACTION PLAN				
Potential risk and consequence	**Likelihood**	**Loss/ Damage Impact**	**Risk Priority Rating**	**Strategy to Address the Risk** (How will you do this?)	**Resources** (What do you need to do this?)	**Who is Responsible for Action?**	**Timeframe** (Specify a time or date)	**Completion**
86. Appropriate risk/safety/hazard assessments are not made:								
• Of all procedures/ programs Leading to:								
• Of buildings/grounds Leading to:								

AUDIT				ACTION PLAN				
Potential risk and consequence	**Likelihood**	**Loss/ Damage Impact**	**Risk Priority Rating**	**Strategy to Address the Risk** (How will you do this?)	**Resources** (What do you need to do this?)	**Who is Responsible for Action?**	**Timeframe** (Specify a time or date)	**Completion**
• Of vehicles/ equipment Leading to:								
• At all or on a regular basis Leading to:								
87. There is no procedure/checklist documented for such assessments Leading to:								

AUDIT				ACTION PLAN				
Potential risk and consequence	**Likelihood**	**Loss/ Damage Impact**	**Risk Priority Rating**	**Strategy to Address the Risk** (How will you do this?)	**Resources** (What do you need to do this?)	**Who is Responsible for Action?**	**Timeframe** (Specify a time or date)	**Completion**
88. Results of assessments are not recorded, filed and/or actioned Leading to:								
89. Assessments are made by unqualified or inexperienced personnel Leading to:								
90. Suitable procedures are not put in place to manage known hazards Leading to:								

AUDIT				ACTION PLAN				
Potential risk and consequence	**Likelihood**	**Loss/ Damage Impact**	**Risk Priority Rating**	**Strategy to Address the Risk** (How will you do this?)	**Resources** (What do you need to do this?)	**Who is Responsible for Action?**	**Timeframe** (Specify a time or date)	**Completion**
91. Risk assessments are not documented Leading to:								
• Employing anyone Leading to:								
• Operating and maintaining premises or facilities Leading to:								

	AUDIT					ACTION PLAN		
Potential risk and consequence	**Likelihood**	**Loss/ Damage Impact**	**Risk Priority Rating**	**Strategy to Address the Risk** (How will you do this?)	**Resources** (What do you need to do this?)	**Who is Responsible for Action?**	**Timeframe** (Specify a time or date)	**Completion**
• Selling products, services or merchandise Leading to:								
• Organising events in public places Leading to:								
95. Legal and/or financial advice is not sought when necessary Leading to:								

AUDIT				ACTION PLAN				
Potential risk and consequence	**Likelihood**	**Loss/ Damage Impact**	**Risk Priority Rating**	**Strategy to Address the Risk** (How will you do this?)	**Resources** (What do you need to do this?)	**Who is Responsible for Action?**	**Timeframe** (Specify a time or date)	**Completion**
96. Staff and directors do not understand their duty of care Leading to:								
97. Changes to standards and law are not communicated across your organisation Leading to:								
98. Your organisation has no compliance review program Leading to:								

AUDIT				ACTION PLAN				
Potential risk and consequence	**Likelihood**	**Loss/ Damage Impact**	**Risk Priority Rating**	**Strategy to Address the Risk** (How will you do this?)	**Resources** (What do you need to do this?)	**Who is Responsible for Action?**	**Timeframe** (Specify a time or date)	**Completion**
99. A detailed budget for each program is not prepared Leading to:								
100. Organisational responsibilities for each program are not clearly defined and allocated Leading to:								
101. A plan for media relations is not prepared Leading to:								

AUDIT				ACTION PLAN				
Potential risk and consequence	**Likelihood**	**Loss/ Damage Impact**	**Risk Priority Rating**	**Strategy to Address the Risk** (How will you do this?)	**Resources** (What do you need to do this?)	**Who is Responsible for Action?**	**Timeframe** (Specify a time or date)	**Completion**
PART L: EVENT MANAGMENT								
102. Appropriate insurance cover is not purchased for each program Leading to:								
103. Risk management is not considered when planning an event Leading to:								
104. All significant risks/hazards in an event are not identified Leading to:								

AUDIT				ACTION PLAN				
Potential risk and consequence	**Likelihood**	**Loss/ Damage Impact**	**Risk Priority Rating**	**Strategy to Address the Risk** (How will you do this?)	**Resources** (What do you need to do this?)	**Who is Responsible for Action?**	**Timeframe** (Specify a time or date)	**Completion**
105. Reasonable steps are not taken to reduce risks to acceptable levels Leading to:								
106. Risk management strategies for events are not documented Leading to:								
107. Procedures have not been developed to respond to foreseeable emergencies Leading to:								

AUDIT				ACTION PLAN				
Potential risk and consequence	**Likelihood**	**Loss/ Damage Impact**	**Risk Priority Rating**	**Strategy to Address the Risk** (How will you do this?)	**Resources** (What do you need to do this?)	**Who is Responsible for Action?**	**Timeframe** (Specify a time or date)	**Completion**
PART M: MANAGEMENT								
108. Appropriate permits to hold the event are not sought and obtained Leading to:								
109. Your organisation is not client and stakeholder orientated Leading to:								
110. There is no formal policy relating to client and stakeholder satisfaction Leading to:								

AUDIT				ACTION PLAN				
Potential risk and consequence	**Likelihood**	**Loss/ Damage Impact**	**Risk Priority Rating**	**Strategy to Address the Risk** (How will you do this?)	**Resources** (What do you need to do this?)	**Who is Responsible for Action?**	**Timeframe** (Specify a time or date)	**Completion**
111. Clients/ stakeholders are not regularly surveyed to obtain feedback on the organisation and its performance Leading to:								
112. Liaison with key stakeholders is an insignificant part of management's role Leading to:								
113. Your organisation does not provide information to clients/ stakeholders Leading to:								

AUDIT				ACTION PLAN				
Potential risk and consequence	**Likelihood**	**Loss/ Damage Impact**	**Risk Priority Rating**	**Strategy to Address the Risk** (How will you do this?)	**Resources** (What do you need to do this?)	**Who is Responsible for Action?**	**Timeframe** (Specify a time or date)	**Completion**
114. Your organisation does not use plain English or simple language that can be understood by relevant stakeholders Leading to:								
115. Your organisation does not provide information in other languages to relevant stakeholders Leading to:								
116. Your organisation does not properly use media and information bulletins Leading to:								

	AUDIT			ACTION PLAN				
Potential risk and consequence	**Likelihood**	**Loss/ Damage Impact**	**Risk Priority Rating**	**Strategy to Address the Risk** (How will you do this?)	**Resources** (What do you need to do this?)	**Who is Responsible for Action?**	**Timeframe** (Specify a time or date)	**Completion**
PART N: RISK MANAGEMENT								
117. Your organisation does not adopt strict financial accountability Leading to:								
118. Your organisation does not have clearly defined delegation and reporting processes Leading to:								
119. Your organisation's board has not demonstrated a commitment to risk management Leading to:								

	AUDIT			ACTION PLAN				
Potential risk and consequence	**Likelihood**	**Loss/ Damage Impact**	**Risk Priority Rating**	**Strategy to Address the Risk** (How will you do this?)	**Resources** (What do you need to do this?)	**Who is Responsible for Action?**	**Timeframe** (Specify a time or date)	**Completion**
120. Your organisation fails to manage all facilities and activities in a manner that protects the health and safety of employees, volunteers, clients, their families and the public Leading to:								
121. Risk management is not a significant factor in the measurement of your organisation's performance Leading to:								
122. Incidents are not reported Leading to:								

AUDIT				ACTION PLAN				
Potential risk and consequence	**Likelihood**	**Loss/ Damage Impact**	**Risk Priority Rating**	**Strategy to Address the Risk** (How will you do this?)	**Resources** (What do you need to do this?)	**Who is Responsible for Action?**	**Timeframe** (Specify a time or date)	**Completion**
123. You do not have an adequate risk management program which is adequately supervised Leading to:								