



# Risk management guide & health check – A guide for not-for- profits and social enterprises

MinterEllison Risk &  
Regulatory Consulting

May 2024

Prepared by:

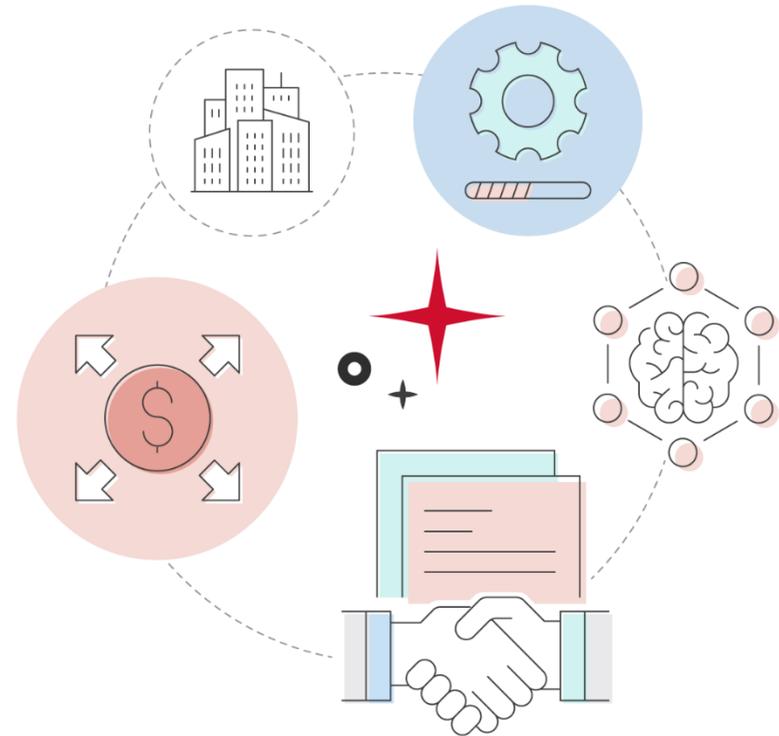
MinterEllison Consulting – Risk & Regulatory Team

This guide is intended only to provide a summary and general overview of risk management considerations for not-for-profits and social enterprises. While reasonable care has been taken in its preparation, it is not intended to be comprehensive, nor constitute legal or professional advice. Due to the evolving nature of risk management practices, this guide may become out-of-date or inaccurate. Persons using this guide should obtain legal or other professional advice, appropriate to their own circumstances, before acting on any of the information provided. To the extent permitted by law, we do not make any express or implied representations, warranties or guarantees in relation to the completeness, reliability or accuracy of the material in this guide. We exclude all liability for any direct, indirect and consequential liabilities, losses, damages, costs and expenses whether arising in contract, tort (including negligence) or otherwise, suffered or incurred by any person in connection with or relating to this guide and associated materials (including third party website content). MinterEllison and MinterEllison Consulting own the copyright and other intellectual property rights in this guide and you must obtain our prior written permission if you wish to copy or reproduce any part of it or use it for any other purposes. Version 2.0 (August 2022).

MinterEllison.

# Contents

<b>Foreword</b>	<b>3</b>
<b>Introduction</b>	<b>3</b>
Objectives of this guide	3
How to use this guide	4
<b>Risk Concepts Explained</b>	<b>5</b>
Risk Management Framework	5
Risk Strategy and Planning	7
Risk Governance	9
Risk Culture and Conduct	12
Risk Appetite	14
Policies, Procedures and Systems	16
Risk Assessment	18
Monitoring and Reporting	22
Risk Assurance	24
Engagement and Consultation	25
<b>Useful resources for managing risk in your organisation</b>	<b>26</b>
<b>Risk Readiness Health Check</b>	<b>28</b>
How to use this Health Check	28
Health Check	28
<b>Glossary</b>	<b>31</b>



## Foreword

▮ *The purpose of risk management is the creation and protection of value. It improves performance, encourages innovation and supports the achievement of objectives.*

*AS ISO 31000:2018 Risk management - Guidelines*

When your risk foundations are strong and integrated into your operational practices and culture, you can position your organisation to meet its purpose through a clear understanding of its key risks and how they are managed.

For many, managing risk, and even knowing where to start, can be overwhelming. The objective of this document is to provide a reference point for not-for-profit and social enterprise organisations. It includes an introduction to risk management concepts, useful external references, and questions to prompt discussion within organisations about risks and how to manage these.

Whether organisations are just getting started or seeking to review existing practice, this guide may help identify priority areas for building or enhancing risk management practices. It is based on our experience working both as consultants, and as in-house risk and governance professionals, within the profit and not-for-profit sectors.

We welcome feedback on the usefulness of this guide in establishing appropriate risk management frameworks to support the achievement of your mission.



**Keith Rovers**

Partner – Social Impact & Sustainable Finance



**Sharon Tumber**

Director - Risk & Regulatory Consulting

## Introduction

Risk is the effect of uncertainty on objectives. The consequences of a risk materialising can have a negative or positive impact on the achievement of your strategy, therefore the management of risk is inextricably linked to your organisation fulfilling its purpose. For not-for-profits and social enterprises, the ability to focus limited resources on what really matters is essential; strong risk foundations can help to provide that focus.

### Objectives of this guide

MinterEllison Risk & Regulatory Consulting has prepared this guide to assist you to:

- understand key concepts relevant to managing risk within the context of your organisation;
- identify resources to help you manage your risks; and
- plan practical steps that support you to integrate risk management practices within your organisation in a meaningful way.

This guide draws upon our experience as legal and risk practitioners, as well as current governance and risk management frameworks, standards and resources including:

- the Australian Charities and Not-for-profits Commission (**ACNC**) Governance Standards; and
- *ISO 31000:2018 Risk management* and *ISO 37301:2021 Compliance management* systems which provides best practice risk management and compliance frameworks that can be applied to all organisations regardless of size.

## How to use this guide

This guide has been designed as a quick reference point, where readers can go directly to areas/components of interest within a risk management framework. It can also be read in its entirety if the reader is new to risk management concepts and would like to understand the components of a framework and how they fit together.

Each section of this guide contains:

		
<b>An overview of risk concepts/components of a risk framework</b>	<b>References to other websites that provide tools or examples<sup>1</sup> that can bring the concept to life</b>	<b>Questions that can be used as a discussion point within your organisation to identify areas of focus</b>

The questions provided for discussion purposes have been broken up into each component of a risk framework. We have also provided a consolidated list of the questions on page 22 "Risk Readiness Health Check".

---

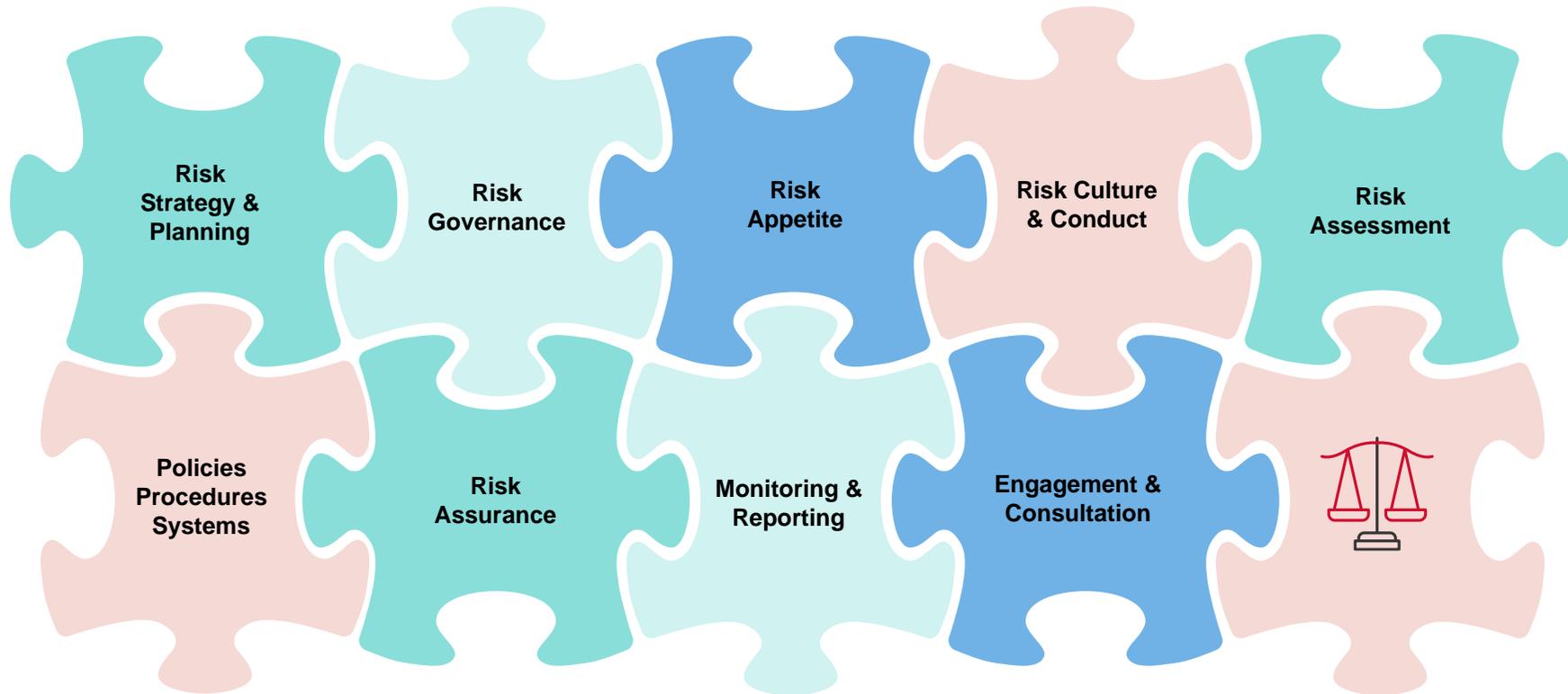
<sup>1</sup> Please note: any links to third party websites are provided for your convenience only. We have no control over these other sites and we are not responsible for their use, effect or content. By accessing these third party sites, you agree to any terms of access or use imposed by those sites. We do not endorse any material on third party sites and do not provide any warranty, or assume any responsibility regarding the quality, accuracy, source, merchantability, fitness for purpose or any other aspect of the material on those sites, nor do we warrant that material on other sites does not infringe the intellectual property rights of any other person.

## Risk Concepts Explained

The management of risk is not linear or a standalone piece. It is a journey that will be unique for your organisation. It is likely that you are already managing risks and, as your organisation matures, so too should your approach to risk management.

### Risk Management Framework

A framework for risk management comprises many interconnected parts. When integrated into your existing governance structures and processes, they work together to deliver a robust approach to decision-making and activity that supports your strategic objectives.



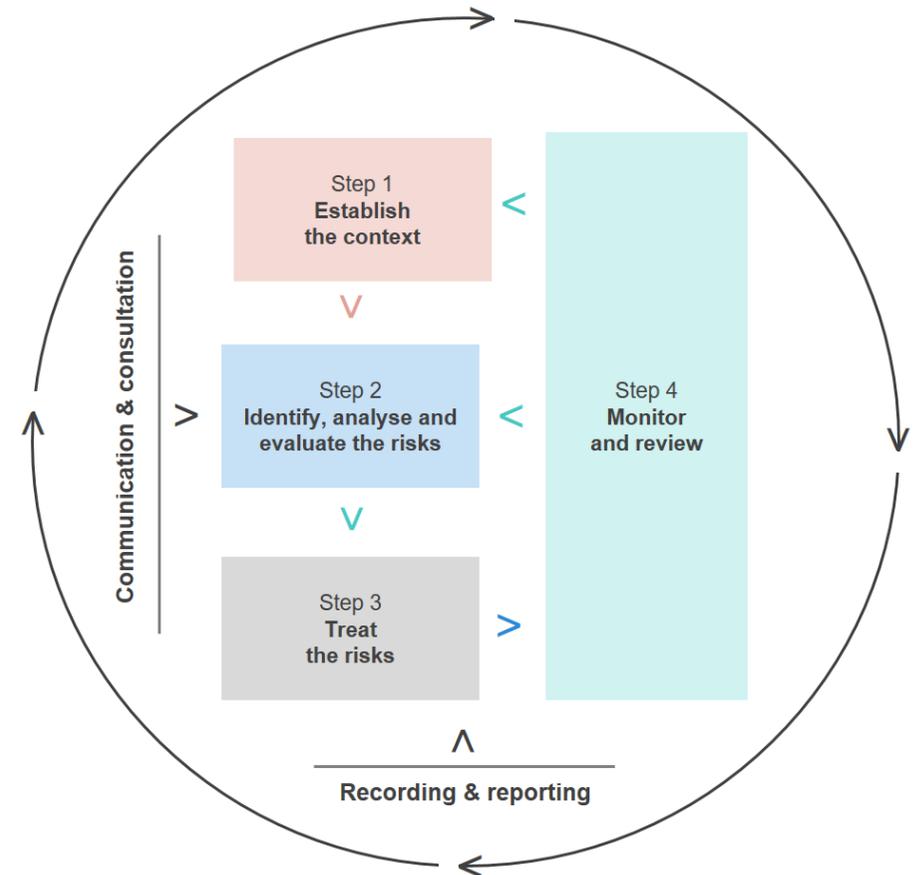
**Components of a risk framework**

## Outline of Risk Management process aligned to ISO 31000

A risk management framework for your organisation provides a structured approach to articulating and embedding:

- a risk strategy, including the principles and culture that will guide your approach;
- risk governance that will provide clear accountability and decision-making structures, which will provide adequate oversight of risk assessment, monitoring and reporting;
- risk management processes, tools and systems required to assess and monitor risks and opportunities;
- regular reviews of the risk management framework for effectiveness and engagement; and
- communication strategies to build risk awareness and understanding with key stakeholders.

AS ISO 31000: 2018 *Risk management - Guidelines* provide a useful framework for establishing and maintaining a risk management process.





## Risk Strategy and Planning

A risk management strategy will help align stakeholders in understanding your organisation's objectives for managing risk, and the principles or values that will drive your target risk behaviours (known as risk culture).

Examples of objectives for managing risk include:

- support informed risk-based decision-making through better identification and assessment of outcomes;
- drive a positive risk culture and a common understanding of how risk is managed with employees, volunteers and partners;
- maintain effective risk governance structures to ensure clear accountability and drive continuous improvement; and
- ensure compliance with regulatory and legal requirements.

An organisation's risk strategy should outline the governance structure and describe how risk is integrated with operational policies and procedures. It should also ensure stakeholders have a consistent understanding of the internal and external business context that defines the scope and approach to risk management in your organisation.

A risk strategy will assist boards and managers when allocating resourcing towards enhancements to their risk management framework.

Risk strategies generally have a medium to long term focus, whereas risk planning is used to identify the short-term needs of the organisation (ie up to 12 months). For example, the risk strategy may have a goal to significantly raise the risk awareness of the organisation. The risk plan may nominate educating the organisations senior leaders as the focus for the first 12 months.

## QUESTIONS TO CONSIDER

- What is your organisation's purpose and objectives? Are they clearly articulated and communicated to stakeholders?
- What is your organisation's strategy for managing risks? What are the key risk priorities and objectives?
- How is risk considered as part of your organisation's strategic planning process?

## OTHER RESOURCES YOU MAY FIND USEFUL

- Risk management for not-for-profit organisations  
[Risk Management Resource FINAL.pdf \(nsw.gov.au\)](#)



## Risk Governance

Risk governance relates to roles and responsibilities, and applies the principles of good governance to the oversight and management of risk. Generally, the board is responsible for oversight of the organisation's risk exposure and the risk management framework. This includes the organisation's resources made available for managing risk and the policies and procedures in place to achieve the risk management objectives. A risk governance structure does not need to be complex, but it should be commensurate to the size and complexity of the organisation and must enable effective management of risks.

Clarity on roles and responsibilities at management and board level is key, particularly in small organisations where board members may be involved in day to day operations. Job descriptions should contain clear responsibilities and the required capabilities for risk management. Behaviours relating to the organisation's risk management should be considered as part of any performance management framework for employees and contractors.

Components of a robust risk governance structure may include:

- Clear board and sub-committee structure. Some boards have created risk sub-committees to enable closer monitoring of the organisation's management of risks;  
*Note:* How this sub-committee is structured will depend on the individual organisations. There may be a dedicated risk committee, or there could be a combined finance, audit and risk committee. Appointing non-directors to the sub-committee is an approach used by some organisations to bring in specialist risk skills that are not present on the existing board.
- Defined roles and responsibilities for managing risks at all levels, including committees and individual managers (example provided on following page);
- Effective and integrated policies, processes, systems and tools for managing risks;
- Insightful reporting that supports the board to challenge management and manage risk effectively;
- Regular reviews of the risk management framework including the adequacy of controls (e.g. policies and procedures); and
- An audit function to provide assurance over adopted controls.

Role	Example responsibility
<b>Board</b>	<ul style="list-style-type: none"> <li>■ Oversight of risk exposure</li> <li>■ Oversight of the effectiveness of the risk framework</li> <li>■ Review and approve risk management strategy and framework</li> </ul>
<b>Board Risk Sub-Committee</b>	<ul style="list-style-type: none"> <li>■ Lead an in-depth review of the risk framework to assist the board in the discharging of its obligations</li> </ul>
<b>Management Risk Committee</b>	<ul style="list-style-type: none"> <li>■ Oversight of risk exposure</li> <li>■ Support reviews of the risk management framework</li> <li>■ Report on risk management to board sub committees</li> <li>■ Recognise and reward positive risk behaviour</li> </ul>
<b>Senior Management (risk owners)</b>	<ul style="list-style-type: none"> <li>■ Risk owners are responsible for the identification and management of risks within their areas of accountability</li> <li>■ Implement the risk management strategy, policies and procedures</li> <li>■ Oversight of risk registers</li> <li>■ Report significant changes to a management risk committee</li> </ul>
<b>Risk Management Function</b>	<ul style="list-style-type: none"> <li>■ Responsible for day to day management of organisational risk, including managing risk registers, implementing controls and testing effectiveness</li> </ul>

## QUESTIONS TO CONSIDER

- Can you describe your organisation's risk governance structure from the board down?
- Can you describe roles and responsibilities for the ownership and management of risks? Are accountabilities clear and documented?
- Have your organisation's board and committee charters been reviewed, updated and communicated to management, to ensure alignment and clarity on roles and accountabilities?
- Does your board and management embrace the need for risk management and seek to obtain a view of your organisation's major risk exposures and opportunities? Can you provide evidence of this?

## OTHER RESOURCES YOU MAY FIND USEFUL

- ACNC<sup>2\*</sup> Governance Standards  
[ACNC Governance Standards | ACNC](#)
- ACNC Guide for Charity Board Members  
[Governance for good: The ACNC's guide for charity board members | ACNC](#)
- ACNC self-evaluation tool  
[Self-evaluation for charities | ACNC](#)

---

<sup>2</sup> Australian Charities and Not-for-profits Commission (**ACNC**) is the national regulator of charities, helping charities understand and meet their obligations through information, advice and guidance.



## Risk Culture and Conduct

Risk culture refers to the common values, understanding, attitudes and behaviours about risk shared by people in your organisation. A sound risk culture is one where individuals:

- are aware of risks;
- understand how risks are managed; and
- make risk management an intrinsic part of their day-to-day activity, regardless of their level or role.

The risk culture will be influenced by the formal structures in place within an organisation, e.g. the people management processes. The risk culture will also be influenced by informal signals e.g. if a poor risk behaviour is tolerated or not addressed.

Risk culture can be monitored through leadership behaviours, internal messaging, risk outcomes, and performance-based signals such as incentives and consequences.

## QUESTIONS TO CONSIDER

- What is the tone from the top with respect to risk culture?
- Have you sought feedback from stakeholders on your organisation's risk culture?
- How do you monitor and review your organisation's risk culture?

## OTHER RESOURCES YOU MAY FIND USEFUL

- The Institute of Risk Management (IRM) publishes free and subscription based materials on their website, including risk culture information and practical guidance
- How to develop a positive risk culture  
[Risk-Culture.pdf \(finance.gov.au\)](#)



## Risk Appetite

Risk appetite refers to your organisation's willingness to accept risk in the pursuit of its strategic objectives. It is set by the board and is documented in a Risk Appetite Statement (**RAS**). The RAS should identify the key risks to which an organisation is exposed, set out clear tolerance (qualitative or quantitative) for those risks, and outline the process for managing risks outside tolerance. Understanding the tolerance to risk taking should be applied during decision-making processes. The RAS should be reviewed and approved by the board at least annually.

Qualitative tolerances could include:

- We will not operate in countries outside of Australasia;
- We will only accept funds from ethical donors;
- We have no tolerance for bullying, harassment and other workplace misconduct; and
- We have no appetite for fraud. When fraud is identified, it will be immediately addressed and the controls improved.

Quantitative tolerances could include:

- Low appetite for compliance breaches – e.g. two open compliance breaches at any point;
- Low appetite for critical system outages extending beyond 24 hours – e.g. two per year; and
- Moderate appetite for financial impact – e.g. tolerance for funding variation is 20% compared to budget.

## QUESTIONS TO CONSIDER

- Can you describe how the board and management consider risk appetite in decision making?
- Would your organisation benefit from documenting risk tolerance (i.e. a RAS)?
- How well is risk appetite understood by your stakeholders and is there consistency in the way it is applied across your organisation?

## OTHER RESOURCES YOU MAY FIND USEFUL

- Tools to help define your risk appetite  
[Defining your organisation's risk appetite | Victorian Managed Insurance Authority \(vmia.vic.gov.au\)](#)
- RAS examples can be found on some organisation websites. Also, speak to others within your network, as they may be comfortable sharing their RAS (or a redacted version).



## Policies, Procedures and Systems

An organisation's risk appetite should be reflected in policies, procedures and systems. Your organisation will need to document policies and procedures so employees and contractors know what is expected of them. These should be clear and simple and contain the steps that must be followed to manage risks. The policies and procedures should help stakeholders understand the link between the management of risks and the achievement of the organisation's objectives.

Where possible, risk management activities should be integrated into existing (operational) procedures, to demonstrate to stakeholders that managing risks are part of day-to-day operations. Training on the procedures should be provided regularly.

An effective risk management framework may include policies and procedures to cover:

- Risk management
- Compliance management
- Conflict of interest
- Responsible fundraising
- Acceptable use of technology
- Expenditure delegation
- Data handling, storage and privacy
- Equal opportunity employment
- Workplace health and safety
- Whistle-blower
- Business continuity
- Working with children
- Codes of conduct
- Use of social media
- Complaints

The key system/tool within your risk management framework is a **risk register**, which is used to document risks and how they are controlled. It is a repository for identified risks and relevant information including:

- the category and type of risk (refer to section below);
- risk rating;
- risk owner;
- controls in place to mitigate the risk (eg policies and procedures); and
- any remediation/ rectification action needed to further mitigate the risk.

The risk register format will vary depending on the size and needs of your organisation. An effective risk register, will support informed strategy development and decision-making by management and the board.

## QUESTIONS TO CONSIDER

- Do you have policies or procedures in place for all of your key risks (per risk appetite)?
- Has your organisation adequately integrated risk management practices into its operational policies and procedures?
- Does your organisation have an overarching risk management framework which outlines your approach to managing risks?

## OTHER RESOURCES YOU MAY FIND USEFUL

- Toolkit including templates from NSW government risk management framework  
[Risk management toolkit | NSW Treasury](#)
- Guides and templates from the Victorian government risk management frameworks  
[The Victorian Government Risk Management Framework \(vmia.vic.gov.au\)](#)



## Risk Assessment

**Risk Assessment** describes the process and tools used to identify, analyse and evaluate risks.

Risks are often grouped into categories, and should reflect your organisation's objectives and strategy. The board will review, approve and adopt risk types for your organisation as part of the RAS development process. Examples of risk categories and types facing not-for-profits and social enterprises include (but are not limited to):

Risk Categories	Risk Types
<b>Strategic</b>	<ul style="list-style-type: none"> <li>Competitor</li> <li>Political</li> <li>Environmental</li> <li>Climate change</li> </ul>
<b>Impact*</b>	<ul style="list-style-type: none"> <li>Stakeholder participation</li> <li>Efficiency</li> <li>Drop-off</li> <li>Execution</li> <li>Endurance</li> </ul>
<b>Financial</b>	<ul style="list-style-type: none"> <li>Funding</li> <li>Accounting and reporting</li> <li>Fraud (including abuse of organisation's finances)</li> </ul>
<b>Operational</b>	<ul style="list-style-type: none"> <li>Talent retention</li> <li>Process or Event-related</li> <li>Health and safety</li> <li>Partner/Supply chain</li> <li>Service providers</li> </ul>

Risk Categories	Risk Types
<b>Compliance and Regulatory</b>	<ul style="list-style-type: none"> <li>Non-compliance</li> <li>Privacy</li> <li>Conflict of Interest</li> <li>Professional liability</li> <li>Regulatory change</li> </ul>
<b>Reputational</b>	<ul style="list-style-type: none"> <li>Conduct</li> <li>Modern slavery</li> <li>Human rights</li> <li>Political activism</li> </ul>
<b>Technology</b>	<ul style="list-style-type: none"> <li>Information security (including cyber security, data handling and storage)</li> <li>Data loss</li> </ul>

\* The Impact Management Project defines impact risk as "the likelihood that impact will be different than expected, and that the difference will be material from the perspective of people or the planet who experience impact". The Impact Management Project outlines nine types of impact risks - refer to the Other Resources You May Find Useful below for further information.

**Risk identification** procedures should be documented within your risk management framework. A first step to risk identification may be a risk workshop with stakeholders where a simple SWOT (strengths, weaknesses, opportunities, threats) or PESTLE analysis (political, economic, social, technological, legal, and environmental) is completed. The output would be an agreed list of risk categories and types relevant to your organisation.

Risk identification is not a one-off event. Triggers to undertake a risk identification exercise could include new projects and activities, changes to the operational (e.g. change in resource availability) and external context (e.g. a change in partner or regulation). Additionally, near-misses, incidents, issues, regular reviews of the risk register may identify new risks.

A more creative and forward-looking risk assessment tool often employed by boards and management, is scenario analysis, which helps to explore the possible outcomes of different hypothetical events and situations.

**Risk analysis** can be undertaken by comparing potential risk outcomes to your organisation's objectives and measures of success. This can then prioritise risk mitigation responses.

A risk matrix table (e.g. a 5x5 matrix shown here) is a tool for assessing materiality and helps measure and prioritise the risks faced based on their likelihood and impact.

Impact ↑	catastrophic	Low Med	Medium	Med High	High	High
	critical	Low	Low Med	Medium	Med High	High
	moderate	Low	Low Med	Medium	Med High	Med High
	minor	Low	Low Med	Low Med	Medium	Med High
	neglectable	Low	Low	Low Med	Medium	Medium
		rare	unlikely	possible	likely	certain
		Likelihood →				

When assessing the impact of a risk, determine an agreed set of risk outcomes, e.g. financial impact in dollar terms, or impact to reputation. The risk likelihood could be expressed as the probability of the event occurring in the next 12 months, or next 24 months etc.

**Risk evaluation** is the process of determining where additional control measures are required to manage the risk to an acceptable level. This involves comparing the results of the risk analysis with agreed risk limits (or tolerance levels). Some organisations may require all risks rated as 'high' to be 'risk accepted' by the CEO.

**Risk registers** are a key output of the risk assessment process and a key system/tool for risk monitoring and reporting. The risk register logs identified risks and assigned risk ratings and documents any associated controls.

Risks can be assessed on an inherent risk basis and a residual risk basis. The inherent risk rating is the assessment of the risk in an environment where there are no controls. The residual risk rating is the assessment of the risk after you consider the controls in place. For example, were you assessing the risk of fraud on your bank account, the inherent risk would be high if there were no controls in place. However, with controls such as passwords and dual authorisation to transact, the residual risk would be lower.

While organisations will generally assess risk on a residual basis, some organisations assess risk on an inherent **and a** residual basis. Assessing risks on an inherent risk basis (ie absence of controls) may seem counter intuitive, however this helps organisations identify their most important controls (ie the controls reducing their highest inherent risks).

**Control measures** are the systems or processes implemented to reduce risk exposures. The controls may reduce the likelihood or the impact of a risk (or both). Controls should be reviewed as part of the risk assessment process (to assess the residual risk). Examples of controls include:

Risk	Preventative Controls (reduce likelihood and/or impact)	Detective Controls (identify incident post-event)	Responsive Controls (reduce impact post-event)
<b>Poor customer experience leading to reputational damage</b>	<ul style="list-style-type: none"> <li>■ Staff training</li> <li>■ Communications strategy</li> <li>■ Contractual obligations</li> </ul>	<ul style="list-style-type: none"> <li>■ Monitoring of customer complaints</li> <li>■ Reconciliation or exception reporting</li> </ul>	<ul style="list-style-type: none"> <li>■ Crisis communications plan</li> </ul>
<b>Poor talent retention leading to unnecessary recruitment and onboarding costs</b>	<ul style="list-style-type: none"> <li>■ Human resources policies</li> <li>■ Staff management training</li> </ul>	<ul style="list-style-type: none"> <li>■ Monitoring employee complaints including anonymous feedback</li> <li>■ Staff engagement surveys</li> </ul>	<ul style="list-style-type: none"> <li>■ Compensation or remediation</li> </ul>
<b>Fraud risk leading to loss of financial resources</b>	<ul style="list-style-type: none"> <li>■ Online payment system for fundraising</li> <li>■ Dual signing for payments</li> <li>■ Daily transaction limits</li> <li>■ Approval thresholds</li> </ul>	<ul style="list-style-type: none"> <li>■ Process for monitoring payments and receipts</li> </ul>	<ul style="list-style-type: none"> <li>■ Forensic accounting investigation</li> </ul>

## QUESTIONS TO CONSIDER

- Has your board and management considered what must go right for the strategy to be achieved (ie the inverse of risk)?
- Has your board and management considered what is the worst thing(s) that could go wrong?
- What risk categories have been identified for your organisation? (target up to 10 material risk types)
- What are the triggers for risk identification in your organisation?
- Have you agreed the best methods for analysing identified risks based on the availability of data and capability of your team?
- Have you established processes for evaluating risks and are they recorded in a risk register along with controls and owners?

## OTHER RESOURCES YOU MAY FIND USEFUL

- The Institute of Risk Management (IRM) publishes free and subscription based materials on their website, including a specific section on Charities and voluntary organisations; and Risk management for charities: getting started guide and supplementary guidance.
- The Committee of Sponsoring Organizations of the Treadway Commission (COSO) has published a guide on applying enterprise risk management to Environmental, Social and Governance (ESG) related risks.
- Risk register template and risk categories  
[Risk Management Resource\\_FINAL.pdf \(nsw.gov.au\)](#)



## Monitoring and Reporting

	Monitoring	Reporting
<p>Monitoring and reporting on the organisation's key risks and the effectiveness of controls is key to ensuring continual improvement. As such, monitoring and reporting should be incorporated into all steps of the risk management process.</p> <p>Examples for monitoring and reporting of risk include:</p>	<ul style="list-style-type: none"><li>▪ Incident and issues tracking</li><li>▪ Training participation rates</li><li>▪ Customer research/feedback</li><li>▪ Audits (Internal/External)</li><li>▪ Media monitoring</li><li>▪ Management reviews</li></ul>	<ul style="list-style-type: none"><li>▪ Board papers</li><li>▪ Management attestations</li><li>▪ Process or project outcomes</li><li>▪ Regulatory or finance reporting (to funding bodies)</li></ul>

Regular reporting will enable you to leverage existing reporting processes and ensure risks are considered in decision-making.

Regular reporting is important to support the board in their oversight of risk management. Using dashboards and graphics can help the early identification of key risk issues. The risk management framework should document the protocols for escalating risks to the board.

Both forward and backward-looking data will provide risk insights that inform decision-making and prompt the organisation to take precautionary actions when needed.

Access to reliable data is critical to making informed risk-based decisions. If data quality is an issue, or there are known inaccuracies with the data, this should be disclosed in risk reporting.

It is the role of the board to challenge and question the reporting provided by management. The board should understand the limitations of data presented to them when considering the risk reporting.

The quality of risk reporting should be regularly reviewed to ensure that it is adequate, efficient, and reflects any operational changes within the organisation.

## QUESTIONS TO CONSIDER

- Has accountability for risk monitoring activities been defined and effectively communicated to stakeholders?
- What processes (eg reviews and audits) are in place to ensure your organisation's management can provide assurance on the effectiveness of controls?
- Does your organisation make use of internal or independent external auditing of risk management processes? Is there a plan and resources to support such an activity?
- Is risk data centrally stored and able to be aggregated efficiently for reporting at an enterprise level?
- Is your board clear on the inherent limitations of your risk data which they rely upon?

## OTHER RESOURCES YOU MAY FIND USEFUL

- The Institute of Risk Management (IRM) publishes free and subscription based materials on their website, including Practical guidance for charities; Risk management for charities: getting started guide and supplementary guidance.
- Monitoring and reporting templates  
[Risk management toolkit | NSW Treasury](#)



## Risk Assurance

Risk assurance assesses the effectiveness of a risk management framework; a key element of which is a focus on controls implemented to manage risk exposure.

Assurance reviews will identify gaps where controls may be non-existent, not performing, or excessive (i.e. unnecessary activities that do not reduce risks). Risk assurance can be undertaken by staff, an appointed committee or external auditors.

### QUESTIONS TO CONSIDER

- Have your key controls been captured in the risk register?
- Do treatments for each risk consider preventative, detective and responsive controls?
- Are controls reviewed periodically by management for effectiveness?
- What reporting does your organisation's management and board receive on the effectiveness of controls?

### OTHER RESOURCES YOU MAY FIND USEFUL

- Risk management for not-for-profit organisations  
[Risk\\_Management\\_Resource\\_FINAL.pdf \(nsw.gov.au\)](#)
- Guide to determine if controls are effective  
[Control Effectiveness Guide \(vmia.vic.gov.au\)](#)



## Engagement and Consultation

Engagement and consultation with internal and external stakeholders should be embedded in risk management activities. It will enhance awareness and understanding of your organisation's risks and how they are managed. Engagement and consultation can be conducted through messaging, reporting, workshops and invitation for feedback.

### QUESTIONS TO CONSIDER

- Have you communicated to your stakeholders (including all employees, volunteers and partners) the key risks that could prevent your organisation from achieving its purpose?
- Have you identified appropriate stakeholders, internal and external, that will need to be engaged in discussions about risks in your organisation to ensure you have a variety of views and perspectives?
- Are stakeholders engaged in workshops to improve their understanding and awareness of risks in your organisation and how they are managed?

### OTHER RESOURCES YOU MAY FIND USEFUL

The Institute of Risk Management (IRM) publishes free and subscription based materials on their website, including Practical guidance for charities; Stakeholder mapping; Risk management for charities: getting started guide and supplementary guidance.

## Useful resources for managing risk in your organisation

There are many practical resources and guides on managing risks in not-for-profits and social enterprises. This section provides some key resources that will assist you in tailoring your organisation's approach to risk management.

Please note: any links to third party websites are provided for your convenience only. We have no control over these other sites and we are not responsible for their use, effect or content. By accessing these third party sites, you agree to any terms of access or use imposed by those sites. We do not endorse any material on third party sites and do not provide any warranty, or assume any responsibility regarding the quality, accuracy, source, merchantability, fitness for purpose or any other aspect of the material on those sites, nor do we warrant that material on other sites does not infringe the intellectual property rights of any other person.

Resource	Description	Source
<b>GOVERNANCE STANDARDS AND REQUIREMENTS FOR NOT-FOR-PROFITS AND SOCIAL ENTERPRISES OPERATING IN AUSTRALIA</b>		
<b>Australian Charities and Not-for-profits Commission</b>	<p>ACNC is the national regulator of charities, helping charities understand and meet their obligations through information, advice and guidance and providing a free searchable database. Resources include:</p> <ul style="list-style-type: none"> <li>▪ list of other regulators, and your obligations to them;</li> <li>▪ guidance on financial and other reporting to the ACNC;</li> <li>▪ fundraising information; and</li> <li>▪ governance guides for charity board directors.</li> </ul>	<a href="https://www.acnc.gov.au/">https://www.acnc.gov.au/</a>
<b>Australian Securities and Investments Commission</b>	<p>Your charity may have other obligations to manage its finances or make financial reports to other government agencies such as ASIC.</p> <p>Find resources and information on reporting obligations to ASIC for charities.</p>	<p><a href="https://asic.gov.au/for-business/running-a-company/charities-registered-with-the-acnc/">https://asic.gov.au/for-business/running-a-company/charities-registered-with-the-acnc/</a></p> <p><a href="https://asic.gov.au/for-business/registering-a-company/steps-to-register-a-company/registering-not-for-profit-or-charitable-organisations/#registeringassociation">https://asic.gov.au/for-business/registering-a-company/steps-to-register-a-company/registering-not-for-profit-or-charitable-organisations/#registeringassociation</a></p>
<b>Office of the Registrar of Indigenous Corporations</b>	<p>Administering the Corporations (Aboriginal and Torres Strait Islander) Act 2006 (<b>CATSI Act</b>), ORIC supports Indigenous groups that want to incorporate or to transfer their registration to operate under the CATSI Act.</p>	<a href="https://www.oric.gov.au/">https://www.oric.gov.au/</a>

Resource	Description	Source
<b>GOVERNANCE STANDARDS AND REQUIREMENTS FOR NOT-FOR-PROFITS AND SOCIAL ENTERPRISES OPERATING IN AUSTRALIA</b>		
<b>Department of Foreign Affairs and Trade (DFAT)</b>	DFAT accreditation acts as a front-end risk management and due diligence process. To gain accreditation, Australian NGOs must undergo a thorough and independent assessment of their organisational structure, philosophies, policies and practices against an agreed set of accreditation.	<a href="https://www.dfat.gov.au/aid/who-we-work-with/ngos/ancp/accreditation">https://www.dfat.gov.au/aid/who-we-work-with/ngos/ancp/accreditation</a>
<b>Council for International Development (CID)</b>	The CID Code of Conduct is a voluntary, self-regulatory sector code of good practice that aims to improve international development outcomes and increase stakeholder trust by enhancing the transparency and accountability of signatory organisations. It serves both as a guide to good practice and a risk management document.	<a href="https://www.cid.org.nz/code-of-conduct/about/">https://www.cid.org.nz/code-of-conduct/about/</a>
<b>The Australian Council for International Development (ACFID)</b>	Good practice toolkit from ACFID provides guidance to support organisations to meet compliance requirements, to promote learning and development and to strengthen organisational policies, practices and operations.	<a href="https://acfid.asn.au/good-practice-toolkit/overview">https://acfid.asn.au/good-practice-toolkit/overview</a>
<b>Governance Institute of Australia</b>	A national membership association, for governance and risk management professionals from the listed, unlisted and not-for-profit sectors. It offers a range of short courses, certificates and postgraduate study, events and resources, including those designed for not-for-profits and non-members.	<a href="https://www.governanceinstitute.com.au/">https://www.governanceinstitute.com.au/</a>
<b>Australian Institute of Company Directors</b>	A national membership association for directors from private, public and not-for-profit sectors. It offers a range of course, events and resources, including a not-for-profit resource centre and articles related to governance of social enterprise.	<a href="https://aicd.companydirectors.com.au/resources/not-for-profit-resources">https://aicd.companydirectors.com.au/resources/not-for-profit-resources</a>
<b>Risk Management Institute of Australasia</b>	Professional institution and industry association for Risk Managers in the Asia Pacific region, offering membership and events for professional development.	<a href="https://www.rmia.org.au/">https://www.rmia.org.au/</a>
<b>Institute of Risk Management (IRM)</b>	IRM is an independent, not-for-profit organisation that champions excellence in managing risks to improve organisational performance. IRM offers internationally recognised qualifications and training, and publishes research and guidance on risk management.	(The terms of use of the IRM website does not allow us to provide links to their webpages in this Guide.)

# Risk Readiness Health Check

## How to use this Health Check

The following Health Check is provided in the format of a questionnaire and has been designed to address the governance standards that are generally expected of charities, not-for-profits and social enterprises operating in Australia. AS ISO 31000: 2018 *Risk management - Guidelines* has also been used to inform the Health Check with the questionnaire structured in alignment with the risk management process outlined in the standard. It is designed to be a standalone checklist.

The Health Check can be used to guide discussion with internal stakeholders to develop a practical plan to assist your organisation to become risk-ready with a risk management approach that is effective, efficient and fit for 'your' purpose. Each organisation's approach to managing risk will be unique to its needs and contexts.

## Health Check

Questions for Discussion		
<b>Risk Strategy and Planning</b>		<ul style="list-style-type: none"> <li>What is your organisation's purpose and objectives? Are they clearly articulated and communicated to stakeholders?</li> </ul>
		<ul style="list-style-type: none"> <li>What is your organisation's strategy for managing risks? What are the key risk priorities and objectives?</li> </ul>
		<ul style="list-style-type: none"> <li>How is risk considered as part of your organisation's strategic planning process?</li> </ul>
<b>Risk Governance</b>		<ul style="list-style-type: none"> <li>Can you describe your organisation's risk governance structure from the board down?</li> </ul>
		<ul style="list-style-type: none"> <li>Can you describe roles and responsibilities for the ownership and management of risks? Are accountabilities clear and documented?</li> </ul>
		<ul style="list-style-type: none"> <li>Have your organisation's board and committee charters been reviewed, updated and communicated to management, to ensure alignment and clarity on roles and accountabilities?</li> </ul>
<b>Risk Culture</b>		<ul style="list-style-type: none"> <li>What is the tone from the top with respect to risk culture?</li> </ul>
		<ul style="list-style-type: none"> <li>Have you sought feedback from stakeholders on your organisation's risk culture?</li> </ul>
		<ul style="list-style-type: none"> <li>How do you monitor and review your organisation's risk culture?</li> </ul>

## Questions for Discussion

<b>Risk Appetite</b>		<ul style="list-style-type: none"> <li>■ Can you describe how the board and management consider risk appetite in decision making?</li> <li>■ Would your organisation benefit from documenting risk tolerance (i.e. a RAS)?</li> <li>■ How well is risk appetite understood by your stakeholders and is there consistency in the way it is applied across your organisation?</li> </ul>
<b>Risk Policies and Procedures</b>		<ul style="list-style-type: none"> <li>■ Do you have policies or procedures in place for all of your key risks (per risk appetite) ?</li> <li>■ Has your organisation adequately integrated risk management practices into its operational policies and procedures?</li> <li>■ Does your organisation have an overarching risk management framework which outlines your approach to managing risks?</li> </ul>
<b>Risk Assessment – Identify, Analyse, Evaluate</b>		<ul style="list-style-type: none"> <li>■ Has your board and management considered what must go right for the strategy to be achieved (ie the inverse of risk)?</li> <li>■ Has your board and management considered what is the worst thing(s) that could go wrong?</li> <li>■ What risk categories have been identified for your organisation? (target up to 10 material risk types)</li> <li>■ What are the triggers for risk identification in your organisation?</li> <li>■ Have you agreed the best methods for analysing identified risks based on the availability of data and capability of your team?</li> <li>■ Have you established processes for evaluating risks and are they recorded in a risk register along with controls and owners?</li> </ul>
<b>Risk Monitoring and Reporting</b>		<ul style="list-style-type: none"> <li>■ Has accountability for risk monitoring activities been defined and effectively communicated to stakeholders?</li> <li>■ What processes (e.g. reviews and audits) are in place to ensure your organisation's management can provide assurance on the effectiveness of controls?</li> <li>■ Does your organisation make use of internal or independent external auditing of risk management processes? Is there a plan and resources to support such an activity?</li> <li>■ Is risk data centrally stored and able to be aggregated efficiently for reporting at an enterprise level?</li> <li>■ Is your board clear on the inherent limitations of your risk data which they rely upon? Are they asking the right questions of management?</li> </ul>

## Questions for Discussion

<p><b>Risk Assurance</b></p>		<ul style="list-style-type: none"> <li>■ Have your key controls been captured in the risk register?</li> <li>■ Do treatments for each risk consider preventative, detective and responsive controls?</li> <li>■ Are controls reviewed periodically by management for effectiveness?</li> <li>■ What reporting does your organisation's management and board receive on the effectiveness of controls?</li> </ul>
<p><b>Engagement and Consultation</b></p>		<ul style="list-style-type: none"> <li>■ Have you communicated to your stakeholders (including all employees, volunteers and partners) the key risks that could prevent your organisation from achieving its purpose?</li> <li>■ Have you identified stakeholders, internal and external, that will need to be engaged in discussions about risks in your organisation to ensure you have a variety of views and perspectives?</li> <li>■ Are stakeholders engaged in workshops to improve their understanding and awareness of risks in your organisation and how they are managed?</li> </ul>

## Glossary

Term	Definition
<b>Control</b>	Measure that maintains and/or modifies risk
<b>Inherent risk</b>	The level of risk that exists prior to efforts to eliminate or modify the risk (controls)
<b>Residual risk</b>	The level of risk that remains after efforts to eliminate or modify the risk (controls)
<b>Risk</b>	The effect of uncertainty on objectives
<b>Risk appetite</b>	The willingness to accept risk in the pursuit of its strategic objectives
<b>Risk assessment</b>	Describes the process and tools used to identify, analyse and evaluate risks
<b>Risk culture</b>	The common values, understanding, attitudes and behaviours about risk shared by people in your organisation
<b>Risk likelihood</b>	The probability of a risk materialising
<b>Risk management</b>	Coordinated activities to direct and control and organisation with regard to risk
<b>Risk owner</b>	An individual or collective with responsibility for managing a risk
<b>Risk registers</b>	A system used to document risks and information associated to those risks, such as risk owners, controls and risk ratings
<b>Risk tolerance</b>	The level of acceptable risk to achieve a specific objective or to manage a category of risk (qualitative or quantitative)
<b>Stakeholder</b>	Person or organisation that can affect, or be affected by, or perceive themselves to be affected by a decision or activity

