Risk Management Guide and Health Check

A guide for not-for-profits and social enterprises

MinterEllison Risk & Regulatory Consulting

October 2021

Prepared by

Donna Worthington
Partner, Risk & Regulatory Consulting

T +61 466 504 252
donna.worthington@minterellison.com

MinterEllison.

This document has been provided to Koda Capital to support the work of its Philanthropy & Social Capital Team. This document is intended only to provide a summary and general overview of risk management practices. While reasonable care has been taken in its preparation, it is not intended to be comprehensive, nor constitute legal advice. Due to the evolving nature of risk management practices, this document may become out-of-date or inaccurate. Persons using this document should obtain legal or other professional advice, appropriate to their own circumstances, before using or relying on the contents of it. To the extent permitted by law (i) MinterEllison does not make any express or implied representations, warranties or guarantees in relation to the completeness, reliability or accuracy of the material in this guide; and (ii) MinterEllison excludes all liability for all direct, indirect or 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 in any way relating to this guide and associated materials (including website content). Version 1.1

Contents

Introduction

Risk is the effect of uncertainty on objectives. In this context, risk and the management of risk is inextricably linked to your organisation's purpose and strategy. Risk generally arises from a change in circumstances and the consequences of the risk eventuating can have a negative or positive impact on the achievement of your strategy. For charities, not-for-profits and social enterprises, the ability to focus limited resources on what really matters highlights the value that strong risk foundations can provide.

Objectives of this guide

When it comes to managing risks, today's leaders face more complex operating and regulatory issues than ever before. Engaging the right people to design and adopt a fit-for-purpose approach to risk and compliance is daunting, even for the most seasoned entrepreneurs and leaders. But it doesn't need to be complex.

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 useful resources for managing your risk and compliance obligations; and
- plan practical steps that support you to integrate and operationalise risk management within your organisation in a way that is fit-for-purpose.

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
- *AS ISO 31000:2018 Risk management – Guidelines*, which presents a best practice framework that can be applied to all organisations regardless of size.

How to use this guide

We recommend you:

1. read this guide and explore the useful resources referenced within this document;
2. share this guide with key stakeholders within your organisation; and
3. work through the Risk Management Health Check with key stakeholders to identify practical steps and priorities for your organisation.

Our Health Check is designed to guide discussion and planning for risk management across the following areas:

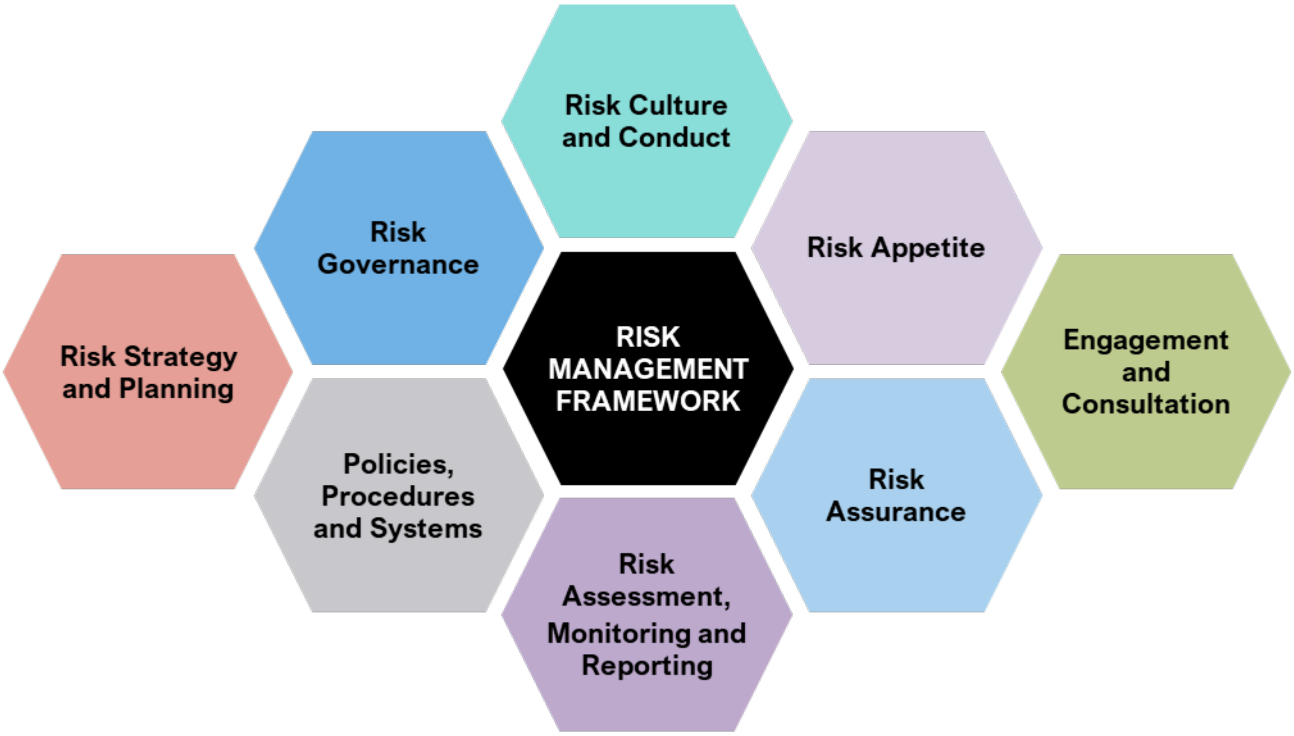
- Business Context and Risk Appetite;
- Risk Management Processes;
- Monitoring and Reporting; and
- Engagement and Communication.

Risk Concepts Explained

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

Risk Management Framework

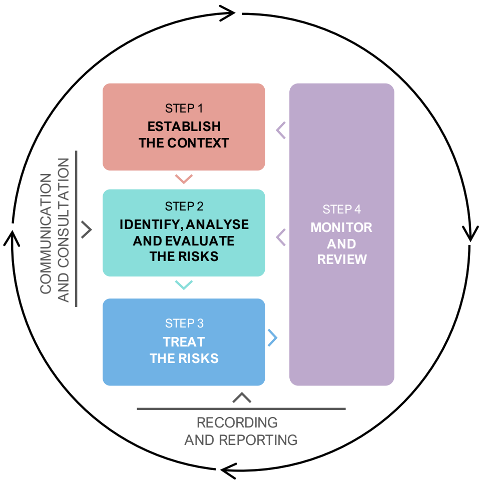
A framework for risk management comprises many interconnected parts. When integrated into your existing governance structures and processes, they work together to deliver a robust approach to decision-making and activity that supports your strategic objectives.


Risk Culture and Conduct
Risk Governance
Risk Appetite
Risk Strategy and Planning
RISK MANAGEMENT FRAMEWORK
Engagement and Consultation
Policies, Procedures and Systems
Risk Assessment
Risk Assessment, Monitoring and Reporting

MinterEllison Risk Framework Model

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

- a risk strategy and 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;
- the 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.



Outline of Risk Management Process aligned to ISO 31000

AS ISO 31000: 2018 Risk management - Guidelines provide a useful framework for establishing and maintaining a risk management process. Key steps in this process align to the MinterEllison Risk Framework Model.

Risk Strategy and Planning

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 (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.

The risk strategy will assist boards and managers allocate resourcing towards enhancements to their risk management framework. Risk strategies generally have a medium-term focus, so risk planning is used to identify the short-term needs of the organisation (ie 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.

Risk Governance

Risk Governance

Risk governance relates to roles and responsibilities in risk management, with a focus on the oversight of risk management. The board is accountable for oversight of the organisation's risk exposure and the risk management framework. This includes the resources made available for managing risk and the policies and processes in place to support the organisation and risk management objectives. Your risk governance structure does not need to be complex, but must work to support the systems and process to manage risks.

Clarity on roles and responsibility at management and board level is key, particularly in small organisations where for valid reasons, board members need to supervise some of the day to day operations. Job descriptions should contain clear responsibilities and the required capabilities for risk ownership and management. Risk behaviours should be considered as part of the performance management framework for employees and contractors/partners.

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;

Role	Example responsibility
Board	Oversight of risk exposure Oversight of the effectiveness of the risk framework Review and approve risk management strategy and framework
Board Risk Sub-Committee	Lead an in-depth review of the risk framework to assist the board in the discharging of its obligations
Management Risk Committee	Oversight of risk exposure Support reviews of the risk management framework Report on risk management to board sub committees Recognise and reward positive risk behaviour
Senior Management	Risk owners are responsible for the identification and management of risks within their areas of accountability Implement the risk management strategy, policies and processes Oversight of risk registers Report significant changes to a management risk committee
Risk Owners (includes Senior Management and key risk roles)	Implement risk assessment procedures and report on risks in their areas of responsibility Manage risk registers

- 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 controls (e.g. policies and procedures) that have been put in place; and
- An audit function to provide assurance over adopted controls.

Risk Culture and Conduct

Risk Culture and Conduct

Risk culture refers to the common values, understanding, attitudes and behaviours about risk that are 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. Additionally, the risk culture will 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, completion of training, internal messaging, leading risk indicators, risk outcomes, and performance-based signals such as incentives and consequences.

Risk Appetite

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 your organisation's Risk Appetite Statement (**RAS**), which identifies the key risks to which the organisation is exposed. It also sets out clear boundaries (qualitative or quantitative) for those risks that should be applied during decision-making. The RAS should be reviewed and approved by the board at least annually.

Boundaries set by the RAS may be qualitative or quantitative.

Qualitative boundaries 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 boundaries could include:

- Low appetite for compliance breaches – e.g. two open compliance breaches at any point in time;
- 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.

The Useful Resources in Section 2 provides hyperlinks to two examples of not-for-profit organisations' RAS. These have been included for illustrative purposes – MinterEllison Risk & Regulatory Consulting was not involved in their development and do not endorse the documents.

Policies,
Procedures
and Systems

Policies, Procedures and Systems

The RAS should be reflected in policies, procedures and systems. Your organisation will need to document risk policies and procedures so employees and contractors know what is expected of them. These should be clear and simple and contain the steps stakeholders must follow 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 policies and procedures 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 the following policies to cover:

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

Your **risk register** is the key system/tool within your risk management framework used to document your risks and how they are controlled. It is a repository for identified risks and relevant information including the risk type, rating, evaluation criteria, owner, controls and remediation action. Its format will vary depending on the size and needs of your organisation. An effective risk register (also known as a risk profile), will support informed strategy development and decision-making by management and the board.

The Useful Resources in Section 2 provides hyperlinks to the NSW and Victorian governments' risk management frameworks websites (which contain risk register templates).

Risk Assessment

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

Risk types 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 process. Examples of risk categories and types facing charities, not-for-profits and social enterprises can include:

Risk Categories	Risk Types
Strategic	Competitor Political Environmental Climate change
Impact*	Stakeholder participation Efficiency Drop-off Execution Endurance
Financial	Funding Accounting and reporting Fraud (including abuse of organisation's finances)
Operational	Talent retention Process Event-related Health and safety Partner/Supply chain

Risk Categories	Risk Types
Compliance and Regulatory	Non-compliance Privacy Conflict of Interest Professional liability Regulatory change
Reputational	Conduct Modern slavery Human rights Political activism
Technology	Information security (including cyber security, data handling and storage) Data loss

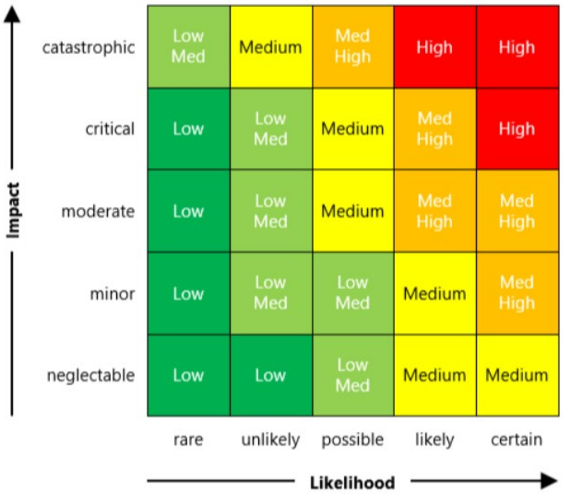
* The Impact Management Project defines impact risk as "the likelihood that impact will be different than expected, and that the difference will be material from the perspective of people or the planet who experience impact". The Impact Management Project outlines nine types of impact risks - refer to the Useful Resources in section 2 for the complete listing and further information.

Risk identification procedures should be documented within your risk management framework documents. A first step of your establishing organisation or a project may be a risk identification workshop with stakeholders. The output would be an agreed list of risk categories and types relevant to your organisation. 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.

As part of the risk identification process, organisations could identify some of its risks using an Environmental, Social, and Governance (**ESG)** framework.

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

A risk matrix table (e.g. a 5x5 matrix shown here) is a tool for assessing materiality.



Impact	rare	unlikely	possible	likely	certain
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

Impact
Likelihood

When assessing the impact of a risk, you should 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.

Refer to the Useful Resources in section 2 for examples on how to assess risks in an organisation.

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 (for both inherent and residual risk), and documents any associated controls. 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, if you were 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.

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

Risk	Preventative Controls (reduce both likelihood and impact)	Detective Controls (identify incident post-event)	Responsive Controls (reduce impact)
Poor customer experience leading to reputational damage	Staff training Communications strategy Contractual obligations	Monitoring of customer complaints Reconciliation or exception reporting	Crisis communications plan
Poor talent retention leading to unnecessary recruitment and onboarding costs	Human resources policies Staff management training	Monitoring employee complaints including anonymous feedback Staff engagement surveys	Remuneration and incentives
Fraud risk leading to loss of financial resources	Online payment system for fundraising Dual signing for payments Daily transaction limits Approval thresholds	Process for monitoring payments and receipts	Forensic accounting investigation

Risk Assessment, **Monitoring and Reporting**

Monitoring and Reporting

Monitoring and reporting on the effectiveness of controls and the overall risk management framework is key to ensuring continual improvement. As such, monitoring and reporting should be incorporated into all steps of the risk management process.

Examples for monitoring and reporting of risk include:

MONITORING

- Incident and issues tracking
- Training participation rates
- Customer research/feedback
- Audits (Internal/External)
- Media monitoring
- Management reviews

REPORTING

- Board papers
- Management attestations
- Process or project outcomes
- Regulatory or finance reporting

Regular and integrated 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 would facilitate early identification of key risk issues. The risk management framework should document the protocols for escalating risk matters to the board.

Both forward and backward-looking data will provide 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 indicators and 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.

Risk
Assurance

Risk Assurance

Risk Assurance activities assess the effectiveness of the risk management framework. This review will identify gaps where controls may be non-existent, not performing, or excessive (ie unnecessary activities that do not reduce risks). Risk assurance can be undertaken by staff, an appointed committee or external auditors.

Engagement
and
Consultation

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.

Useful resources for managing risks and compliance in your organisation

There are many practical resources and guides on managing risks in the context of charities, 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, 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
GOVERNANCE STANDARDS AND REQUIREMENTS FOR CHARITIES, NOT-FOR-PROFITS AND SOCIAL ENTERPRISES OPERATING IN AUSTRALIA		
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 and providing a free searchable database. Resources include: ▪ list of other regulators, and your obligations to them ▪ guidance on financial and other reporting to the ACNC ▪ fundraising information ▪ governance guides for charity board directors	https://www.acnc.gov.au/
Australian Securities and Investments Commission	Your charity may have other obligations to manage its finances or make financial reports to other government agencies such as ASIC. Find resources and information on reporting obligations to ASIC for charities.	https://asic.gov.au/for-business/running-a-company/charities-registered-with-the-acnc/ https://asic.gov.au/for-business/registering-a-company/steps-to-register-a-company/registering-not-for-profit-or-charitable-organisations/#registeringassociation
Office of the Registrar of Indigenous Corporations	Administering the Corporations (Aboriginal and Torres Strait Islander) Act 2006 (CATSI Act), ORIC supports Indigenous groups that want to incorporate or to transfer their registration to operate under the CATSI Act.	https://www.oric.gov.au/
RISK MANAGEMENT AND COMPLIANCE STANDARDS		
AS ISO 31000:2018	'Risk management – Guidelines' covers risk management principles.	Licensed product - https://www.iso.org/store.html
ISO 19600:2014	'Compliance management – Guidelines' provides guidance for establishing and maintaining a compliance management system.	Licensed product – https://www.iso.org/store.html

Resource	Description	Source
GOVERNANCE AND RISK INDUSTRY ASSOCIATIONS		
Governance Institute of Australia	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.	https://www.governanceinstitute.com.au/
Australian Institute of Company Directors	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.	https://aicd.companydirectors.com.au/resources/not-for-profit-resources
Risk Management Institute of Australasia	Professional institution and industry association for Risk Managers in the Asia Pacific region, offering membership and events for professional development.	https://www.rmia.org.au/
Institute of Risk Management (IRM)	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.	https://www.theirm.org/ 'Sound Practice Guides': https://www.theirm.org/what-we-say/thought-leadership/sound-practice-guides/
OTHER USEFUL RESOURCES		
ASX Corporate Governance Principles and Recommendations 4th Edition	Eight principles and detailed recommendations to help achieve good governance outcomes and meet the reasonable expectations of most investors in most situations. A useful benchmark reference and checklist – including the 'if not, why not' approach to their application.	https://www.asx.com.au/documents/regulation/cgc-principles-and-recommendations-fourth-edn.pdf
Australian Prudential Regulatory Authority	APRA's Prudential Standard CPS 220 Risk Management (effective July 2019) applies as an obligation to APRA-regulated entities but provides a useful resource for risk management for all organisations.	https://www.apra.gov.au/sites/default/files/Prudential-Standard-CPS-220-Risk-Management-%28July-2017%29.pdf
Department of Finance, Business Procurement and Asset Management	Commonwealth Risk Management Policy, July 2014.	https://www.finance.gov.au/government/comcover/commonwealth-risk-management-policy
State Government Risk Management Frameworks	NSW and Victorian governments' risk management frameworks.	https://www.treasury.nsw.gov.au/information-public-entities/governance-risk-and-assurance/internal-audit-and-risk-management/risk https://www.vmia.vic.gov.au/tools-and-insights/tools-guides-and-kits/victorian-government-risk-management-framework
Developing Risk Appetite Statements	The links provided outline approaches to designing and implementing risk appetite statements. A supplementary guide for charities is provided.	https://www.theirm.org/media/4666/0926-irm-risk-appetite-12-10-17-v2.pdf Risk Management for Charities: Setting your risk appetite https://www.theirm.org/media/4519/irm-charities-sig-setting-risk-appetite-final-updated-051016.pdf

Resource	Description	Source
Sample Risk Appetite Statements	Sources: ▪ Oxfam ▪ Banksia Community Gardens	https://www.oxfam.org.au/wp-content/uploads/2011/10/OAU-Risk-Appetite-Statement-December-2016-Final-green.pdf http://banksiagardens.org.au/wp-content/uploads/2018/03/1.3.1-BGCS-Risk-Appetite-Statement-ENDORSED.pdf
Risk Assessment	Risk and Control Self-Assessment Guide from the Institute of Operational Risk and IRM *Note: free resource, however you need to register with IRM to access*	https://www.theirm.org/account/sound-practice-guidance/risk-and-control-self-assessment/
Impact Risk	The Impact Management Project explains what impact risk is, and the nine types of impact risks that organisations face.	https://impactmanagementproject.com/impact-management/impact-management-norms/risk/#anchor2

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 consider first and foremost the minimum requirements of governance standards that apply to 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.

The Health Check can be used to guide discussion with internal stakeholders and as a benchmark to develop a practical plan for ensuring your organisation is risk-ready with a risk management approach that is effective, efficient and fit for 'your' purpose.

Health Check

Questions for Discussion	
Risk Strategy and Planning	What is your organisation's purpose and business objectives? Are they clearly articulated and communicated to stakeholders?
	What is your strategy for managing risks? What are your key priorities and objectives?
	How is risk considered as part of the organisation's strategic planning process, and vice versa?
Risk Governance	Can you describe your risk governance structure clearly, from your board down?
	Can you describe roles and responsibilities for the ownership and management of risks? Are accountabilities clear and documented?
	Have your board and committee charters been reviewed, updated and communicated to management to ensure alignment and clarity on roles and accountabilities?
	Do 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?
Risk Culture	What is the tone from the top with respect to risk culture?
	Have you sought feedback from stakeholders on your risk culture?
	How do you monitor and review risk culture?
Risk Appetite	Does your organisation have a risk appetite statement?
	How well is risk appetite understood by your stakeholders and is there consistency in the way it is applied across your organisation?
	Can you describe how the board and management consider risk appetite in decision-making?
Risk Policies and Procedures	Do you have documented risk management policies and procedures?
	How is the management of risks integrated into operational procedures? Can you list all your key risk types?
Risk Assessment – Identify, Analyse, Evaluate	Has your board and management considered what must go right for the strategy to be achieved?
	Has your board and management considered what is the worst thing that could go wrong?

Questions for Discussion

	What risk categories have been identified (target up to 10 material risk types relevant to your organisation)?
	What are the triggers for risk identification in your organisation?
	Have you determined an agreed set of risk parameters linked to your objectives to assess risk impact and likelihood?
	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 the evaluation of risks and are they recorded?
Risk Controls	Have risk 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?
Risk Monitoring and Reporting	Has accountability for risk monitoring activities been defined, and effectively communicated to stakeholders?
	Has your management established a process to regularly review your business context and the impact on your strategies and processes for managing risks?
	What processes are in place to ensure your management can provide assurance on the effectiveness of chosen treatments and controls?
	Is your organisation open to internal or independent external auditing of risk management processes and performance? Is there a plan and resources to support such an activity?
	Do you have a consistent and integrated approach to reporting on risks across your organisation?
	Are risk data centrally stored and able to be aggregated efficiently for reporting at an enterprise level?
	Is there evidence of regular reporting to the your board on material risks facing your organisation?
	Does your board receive both forward and backward-looking risk indicators?
	Is your board clear on the inherent limitations of your risk data which they rely upon? Are they asking the right questions of management?
	Is the content and process for risk reporting reviewed periodically for effectiveness and improvement?
Engagement and Consultation	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?

MinterEllison.