SISTERS OF THE GOOD SAMARITAN FOUNDATION

RISK MANAGEMENT POLICY

October 2023

Policy Governance

Approver	Board of Directors
Mandatory Reviewer	Finance, Risk and Audit Committee; Governance Committee
Owner	Executive Director
Review frequency	Every two years
Next review	August 2026

Related documents

- Constitution
- Strategic Plan
- Risk Appetite Statement
- Risk Matrix (that is the living document that is regularly updated with risks and treatments)

Relevant legislation

- Fair Work Act 2009 (Cth)
- Privacy and Personal Information Protection Act 1998 (Cth)
- Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth)
- Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth)
- Workers Compensation Act 1987 (NSW)
- Work Health and Safety Act 2011 (Cth)
- Work Health and Safety Regulation 2011 (NSW)
- National Employment Standards

Material policy revisions

Version	Approval date	Effective date	Details
July 2020		July 2020	AFRC changes
March 2023	TBC	TBC	Strategy day risk workshop updates
July 2024	TBC	1 August 2024	Review and update by FRAC and GC

1. BACKGROUND

The Sisters of the Good Samaritan Foundation (the "**Foundation"**) recognises that the Foundation is exposed to certain risks due to the nature of its activities and the environment in which it operates. The key to the Foundation's success is the effective management of risk to ensure its organisational objectives are met. Risks arise due to the Foundation's operational undertakings and from external sources. Risks occur in numerous ways and have the potential to impact financial performance, reputation, health and safety, community, and the overall performance of the Foundation.

Risk management is a central tenet of board governance. Oversight for risk management is the responsibility of the Foundation Board, the Finance, Audit and Risk committee, and the Governance committee.

2. PURPOSE

In order to fully understand such risks, the Foundation has established a Risk Management Policy (the "**Policy**") which provides the framework for how risk will be managed within the organisation. The Policy is based on the Australian Standard, AS/NZS ISO 31000:2018 Risk Management – Principles and guidelines, and forms part of the governance framework of the Foundation. It also integrates with the strategic planning process. The Policy addresses both strategic and operational risks.

The Policy and associated procedures have been developed to ensure compliance with regulatory obligations to the Australian Charities and Not-for-profits Commission, Australian Taxation Office, state-based regulators, Catholic Professional Standards Ltd, and others and in accordance with the Foundation's constitution, philosophy, and strategic objectives.

The purpose of the Policy is to ensure that:

- risk management is an integral part of the operating model, culture, planning, and decision-making to support a sound and sustainable Foundation;
- risks are managed in a consistent, structured, and systematic manner across all areas of the Foundation;
- clear roles, responsibilities, and accountabilities are defined, including monitoring and reporting;
- everyone with risk management roles and responsibilities are provided with the necessary authority, skills, and resourcing to undertake allocated responsibilities; and

- communication within the Foundation in relation to identification and management of risk is promoted and encouraged.

This Policy applies to all employees, contractors and third party suppliers of the Foundation.

Material risk categories within this Policy include:

1. strategic/sustainability risk;
2. reputational risk;
3. funding/donor engagement risk;
4. compliance risk;
5. operational risk including information technology and cyber risk; and
6. other risks that, singly or in combination with different risks, may have a material impact on the institution.

These material risk categories are subject to strategic and environmental changes and do not replace the overarching strategic risks. Specific policies have been developed to align with each of these risk categories.

3. SCOPE

This Policy applies across all areas of the Foundation's operations and activities.

4. RISK MANAGEMENT PRINCIPLES, FRAMEWORK AND PROCESS

The following diagram illustrates the approach to identifying, evaluating, and managing risks by the Foundation, consistent with the guidelines contained in AS/NZS ISO 31000:2018. These components need to be adapted or improved so that managing risk is efficient, effective, and consistent.

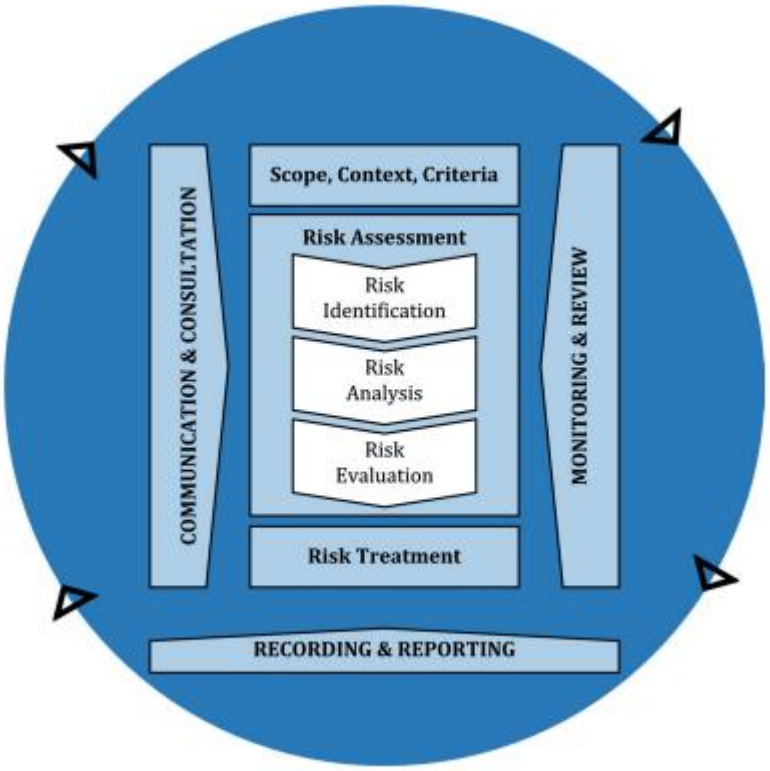

Figure 1 – ISO 31000 Risk Management principles, framework and process

Governance Structure

The Board of directors is responsible for setting the risk appetite of the Foundation and ensuring that the Policy and framework are implemented effectively. Through delegation from the Board, the Finance, Risk and Audit committee is responsible for overseeing the implementation of the Policy ensuring risks are managed effectively. They provide regular reviews of the Risk Management Plan.

Current and emerging risks will be incorporated into the Risk Management Plan as they are identified.

All employees, contractors, and third-party suppliers are responsible for identifying and reporting risks in a timely manner and implementing mitigating measures as required.

Risk management includes communication and reporting on risks that have been identified, as well as continued risk analysis, prioritisation and treatment options.

Policies and procedures

The policies and procedures required for dealing with risk management matters must:

- include processes that identify and assess material risks and controls;
- validate, and approve use of any models to measure components of risk;

- establish, implement, and test mitigation strategies and control mechanisms for material risks;
- monitor, communicate, and report risk issues, including escalation procedures for the reporting of material events and incidents;
- identify, monitor, and manage potential and actual conflicts of interest;
- outline mechanisms in place for monitoring and ensuring ongoing compliance with all prudential requirements;
- ensure consistency across the risk management framework; and
- review the risk management framework.

This information is managed by the Executive Director and stored digitally to be accessed by those authorised to do so. The status of the Policy review programme is scheduled to be reported at each Governance Committee and Board meeting.

Risk identification
Identifying risk sources, areas of impact, events, causes, and possible consequences to form a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate, or delay the achievement of objectives.

Risk analysis
Considering the range of causes, sources of risk, consequences, likelihood, events, scenarios, controls, and their effectiveness to produce a risk rating. The rating can be used to determine further management by the Foundation.

Risk evaluation
Comparing the risk analysis results with the established risk criteria to determine where additional action is required. The level of risk identified during risk analysis can be ranked and prioritised according to a consistent overall ranking and rating system. Risk evaluation supports decisions.

Risk treatment
Selecting one or more options for modifying risks includes balancing the potential benefits derived in relation to achieving the objectives against the costs, effort or disadvantages of implementation.

Monitoring and Review of Risks
The Policy and Risk Management Plan provide mechanisms for monitoring and reviewing risk. Continual monitoring and reviewing of risk profiles is essential to maintain the effectiveness and appropriateness of the Foundation's risk management profiles, including more specifically, risk treatment plans, risk assessments and to identify emerging risks.

Monitoring and reviewing includes planning, gathering and analysing information, recording results, and providing feedback. The results of monitoring and reviewing should be incorporated

throughout the organisation's performance management, measurement and reporting activities.

While risks may never be eradicated, they may be mitigated or controlled.

Risk Mitigation Strategies
The following table is used when identifying and determining risk mitigation strategies:

Strategy	Detail
Avoidance	Not proceeding with a task, project, or activity that is likely to generate the risk.
Acceptance	Accept risk and establish an appropriate management plan.
Reducing Likelihood	Develop processes to reduce the likelihood of risk, e.g. preventative maintenance, audits, inspection and testing.
Reducing Consequence	Develop processes to reduce the consequence of risk. e.g. contractual arrangements, redesign, security measures and contingency planning.
Transfer	Transfer all or part of the risk to a second party through insurance, contractual arrangement and organisational structures.
Retention	Accept all residual risk.

Control Effectiveness
The following table is used when determining control effectiveness:

Score	Rating	Description
5	Highly Ineffective	Controls are non-existent or have major deficiencies and do not operate as intended.
4	Ineffective	Limited controls in place and a high level of risk remains.
3	Significant Improvement Required	Key controls in place, with significant opportunities for improvement identified.
2	Limited Improvement Required	Controls properly designed and operating, with opportunities for improvement identified.
1	Effective	Controls properly designed and operating as Intended.

The risk mitigation strategy and control effectiveness ratings relevant to each identified risk are recorded in the Risk Management Plan.

Recording and reporting

The Chair of the Finance, Risk and Audit and sub-committee will report on risk issues to the Board in conjunction with the Executive Director.

Communicate and consult
Effective communication, consultation and education in risk management are necessary to achieve a successful integration of the risk processes into the business.

5. PROCEDURES

All contracts or agreements over $30,000 or those involving children shall have a formal risk assessment by the relevant committee ortExecutive Director before signing.

All staff, volunteers, and Board members must always take reasonable care, and report all significant incidents, complaints, losses and near misses involving the Foundation, incidents, and hazards involving staff and visitors, including, but not limited to, injuries or potential hazards.

Occupational health and safety is to be incorporated into the staff and volunteer induction process and included in Board member induction.

The Policy will be reviewed every two years by the Board.

The Finance, Risk and Audit committee will provide a quarterly risk report to the Board.

Changes to the Policy, risk appetite statement, or the risk management framework must beapproved by the Board.

RISK ASSESSMENT MATRIX

Risk ratings are determined through a combination of the consequences for the Foundation if the risk is not treated, and the likelihood of this happening. The following risk assessment matrix is to be used as a guide:

- Likelihood rating for risk occurring – this is an assessment of the potential frequency of occurrence without reference to known management controls and mitigating processes.
- Consequence rating for risk occurring – this is an assessment of potential people, financial, reputation, compliance, or business process/system impact.

FOUNDATION - RISK MATRIX - JUNE 2020

Likelihood: (vertical axis) *Impact: (horizontal axis)*	1. Insignificant	2. Minor	3. Moderate	4. Major	5. Catastrophic
5. Almost Certain					
4. Likely					
3. Possible					.
2. Unlikely				.	
1. Rare					

TABLE KEY: BLUE = LOW RISK, GREEN = MEDIUM RISK, YELLOW = HIGH RISK, RED = EXTREME RISK (TABLE TEMPLATE SOURCED GOVERNANCE INSITITUTE OF AUSTRALIA 2020)

Sisters of the Good Samaritan Foundation Risk Policy

Appendix A: Risk Appetite Statement

The Board of the Sisters of the Good Samaritan Foundation (the "**Foundation**") takes a long-term view of sustainability and makes decisions accordingly. Relationships with key stakeholders such as the Sisters of the Good Samaritan ("**SGS**") congregation and ministries, donors, and Good Samaritan Education ("**GSE**") schools are central to the Foundation's ongoing success.

The Foundation recognises that taking on risk is an inherent part of achieving our goals and objectives. The Board is committed to managing risk effectively in order to achieve the Foundation's strategic priorities and create value for all stakeholders. The aim of the risk appetite statement is to define the amount of risk that the Foundation is willing to accept and within which management willoperate at all times.

Following is a statement of the Foundation's overall risk appetite. This statement informs the Foundation's risk framework and the specific processes that are conducted within this risk system. The Foundation's risk appetite is guided by the following principles:

- risks taken only if necessary to achieve the Foundation's strategic priorities, follow the philosophy of the Good Samaritan, and creation of value for stakeholders;
- no risks will be taken if they jeopardise the safety or well-being of staff, beneficiaries, or the public;
- risks taken will not compromise the Foundation's integrity or violate the ethical standards in pursuit of the Foundation's objectives;
- a strong risk management framework will be maintained that allows the identification, assessment, and mitigation of risks effectively; and
- regular review and update of the risk appetite statement to ensure that it remains relevant and aligned with the Foundation's strategic priorities.

Terms used in this document.

Risk Appetite

Risk appetite is the amount and type of risk that the Foundation is willing to retain.

Risk Tolerances

Risk tolerance is the amount of uncertainty that the Foundation is prepared to accept in total within certain categories.

Risk Culture

Risk culture consists of the norms and behaviours of individuals and groups within the Foundation that determine the way in which they identify, understand, discuss, and act on the risk the Foundation confronts and takes.

Our Risk Tolerances.

The Foundation Board has developed the following standards in regard to specific risk tolerances.

Strategic/ Sustainability Risks – Low-risk appetite.

- We will always have a current constitution and strategic plan.
- We will always have an appropriately skilled Board with a diverse range of financial, operation, management, and governance skills.
- We will always be aware of current government policies that relate to our entity, ministries, and other stakeholders.
- We are committed to our long-term sustainability and building on our capital reserves in accordance with the sustainability plan. We will ensure there is a memorandum of understanding with the Congregation so there is a clear understanding of the Foundation's needs and how these will be met on a long-term basis.
- We will always have an updated allocation of roles and responsibilities relating to the Foundation's activities.

Reputational Risk – Low risk appetite.

- We will always have a framework for Board member selection including background checks and induction training.
- We will always have an appropriately skilled Board with a diverse range of financial, operation, management, and governance skills.
- We will always have an assessment of the reputational damage from cultural differences performed at each program. We will explore having a programme management committee with increased engagement with locals.
- We will have all policies and procedures written, reviewed and available in a central location.
- We will have a framework for governance of communication internally and externally.
- We will have all ongoing research performed before funding or visiting a project in each jurisdiction.
- We will have regular visits by the Executive Director to review the projects and engagement with locals.
- We will always encourage transparency in communication at Board level.

Funding and Donor Engagement Risks – Defensive risk appetite.

- We will have a fundraising committee set up with established terms of reference.
- We will have an annual budget and reforecast it at least every 6 months, with monthly actual reports monitored via distribution to the Finance, Audit and Risk committee.
- We will always be solvent and able to meet short-term liabilities as and when they are due.
- We will maintain diverse revenue sources, with no one source of funds being more than 40% of operating revenue (without Board approval).
- We will always have a current fundraising plan.
- We will have Finance, Audit, and Risk committee members with adequate knowledge of investments.
- We will maintain a register of current and target donors with engagement by members of the fundraising committee or the Board at least on an annual basis.
- We will look to explore the possibility of broadening the responsibilities of meeting the fundraising targets.
- We will continue to explore new sources of funding and grow the reserves with these initially discussed at the Finance, Audit, and Risk committee.

Compliance Risk – Low risk appetite.

- We will always be aware of current government policies that relate to our entity, ministries, and other stakeholders.
- We will ensure statutory compliance requirements are always up to date.
- We will have appropriate policies and guidelines that allow us to meet our legal, business, and community obligations.
- We will ensure all policies and procedures are up to date, stored in a central location, and reviewed regularly.
- We will have all ongoing research performed before funding or visiting a project in each jurisdiction.
- We will have all projects assessed for compliance with relevant laws in each jurisdiction on initial onset and on an ongoing basis.

Operational Risk including IT and Cyber risk – Low risk appetite.

- We will always have signed agreements with third party service providers and ensure monitoring in line with agreed service level agreements.
- We will always have an adequate understanding of the IT support from the Congregation and use of their systems.
- We will always have appropriate insurances including directors and officers,

professional indemnity, public liability.

- We will ensure no new projects put at risk the financial viability of the Foundation.
- The wellbeing and safety of our staff, volunteers, Sisters, and ministry partners is a central priority.
- We will ensure our IT and data systems are properly resourced and secure in accordance with the SGS IT Plan.
- We will ensure all control recommendations raised by external or internal audit are resolved within three months.
- We will ensure adequate training is provided to staff and the Board including information security training.
- We will ensure business continuity and disaster recovery plans are in place with alternative backup communication in place. We will ensure one Board member has access and visibility to all Foundation information in addition to the Executive Director

Totally Unacceptable Risk:

- Serious workplace injuries to employees, volunteers, contractors, and guests are totally unacceptable.
- Deliberate violation of any Australian law is totally unacceptable.
- Any serious breach of the SGS Code of Conduct is totally unacceptable.
- Any violation of the Foundation's Safeguarding Policy is totally unacceptable.
- Any serious breach of the Foundation's policies is totally unacceptableunacceptable.
- Fraud is totally unacceptable.

Procedures

- The risk framework will be monitored by the Finance, Audit & Risk committee.
- The risk appetite statement will be monitored annually and risks reviewed quarterly by the Board.
- Changes to the risk appetite statement must be approved by the Foundation Board.