Organisational Risk Management Framework

December 2023

Framework Statement

The purpose of the organisational Risk Management Framework ("RMF") is to provide a comprehensive approach to managing risks within the context of Good Neighbours Australia's ("GNAU") current and future operating environments.

In managing its risks, GNAU recognises that adopting the ISO 31000:2018[1] principles and ACFID's Good Practice Framework (Quality Principle 4.2)[2] provides all stakeholders with confidence that risks are not only understood and well-managed by the leadership at GNAU; they are also consciously prioritised, mitigated, and linked to strategy from a day-to-day operational perspective by all its employees.

In developing GNAU's RMF, consideration has been given to the important relationship between Vision, Mission, Strategic Objectives, and the interplay and impact of vulnerabilities and opportunities that the concept of "Risk" represents, as follows:

Vision: "*Empowering People, Transforming Communities*".

Mission: *"We exist to make the world a place without hunger, where people live together in harmony. We respect the human rights of our neighbours suffering from poverty, disasters, oppression, and help them to achieve self-reliance and enable them to rebuild hope".*

Strategic Objectives: To accomplish GNAU's mission, GNAU has adopted the following four Strategic Objectives: [3]

- Objective 1: Programs
  Help those suffering from poverty, disasters and oppression, to rebuild hope and achieve self-reliance.
- Objective 2: Sustainability
  Manage and grow resources through financially, environmentally and socially responsible practices, to achieve organisational goals.
- Objective 3: Operations
  Work smartly and efficiently, to achieve the most for the people and communities we serve.
- Objective 4: Governance
  Ensure our governance, policies and planning is in place, to safely and effectively drive the mission, vision, values and commitments of the organisation.

[1] ISO 31000:2018 - Risk management — Guidelines
[2] https://acfid.asn.au/good-practice-toolkit/quality-principle-4/commitment-4-2/
[3] GNAU 2025 to 2030 - Organisational Strategy.pptx

Risk: In pursuing its mission, vision, and strategic objectives, GNAU acknowledges the reality of the possible occurrence of "sudden and unexpected events", and how they might impact the achievement of GNAU's strategic objectives. The RMF is therefore designed to support and enhance GNAU's capabilities to proactively and effectively manage these risks.

Purpose

GNAU's RMF is designed to:

- support and enhance GNAU's capabilities and approaches to manage known risks and unknown risks.
- provide context and guidance to all operations and decision-making where risk prevails.
- assist GNAU's leadership, management, and staff in determining which risks are significant and which ones are not, so that limited time, energy, and resources can be invested most effectively and efficiently.

Obligations and Standards

Legislations

GNAU will comply with relevant state and federal legislations relating to risk management.

Australian NGO ("ANGO") Sectoral Standards

GNAU will also comply with the Code of Conduct of the Australian Council for International Development ("ACFID"). ACFID is the ANGO sector's peak body that continuously promotes sectoral good standards and practices on risk management, and at the same time, regulates the activities of its members to ensure they comply with the said standards and practices. ACFID collaborates closely with the Department of Foreign Affairs and Trade ("DFAT") to enable the accreditation of ANGOs, and their access to DFAT's foreign aid grants.[4]

International Standards

ISO31000:2018 defines risk as the "*effect of uncertainty on objectives*".[5] GNAU's approaches to risk align with the ISO31000:2018 risk management processes – risk identification, assessment, treatment, reporting, monitoring, and learning.

Compliance with the relevant legislative, ANGO sectoral and international principles and standards are summarised as follows:

[4] Australian Council for International Development (ACFID) partnership | Australian Government Department of Foreign Affairs and Trade (dfat.gov.au)
[5] ISO 37000:2018 - Risk management

Legislation and Standards	*Requirement*
Australian Charities and Not-for-Profits Commission ("ACNC") Act 2012	• Chapter 3 Part 3.1 Div. 45.5.1(c) - registered entities must minimise the risk of mismanagement and misappropriation. • Risks of terrorism, fraud, and other forms of abuse must be reduced through good standards of governance and accountability.
Work Health and Safety Act 2011 (NSW) Work Health and Safety Regulation 2017 (NSW) Work Health and Safety Amendment Act 2023 (NSW)	• Division 2 (Primary Duty of Care) (Part 2) - *"A person conducting a business or undertaking must ensure, so far as is reasonably practicable, that the health and safety of other persons is not put at risk from work carried out as part of the conduct of the business or undertaking"*.
ACFID Quality Principle 4.2[6]	• Establish protocols for the conduct of regular risk reviews. • Share risk assessment, analysis and management strategies with the governing body and periodically review these. • Appoint a staff member or committee to be responsible for ensuring regular risk assessments are carried out. • Use ISO standards to guide our risk assessment processes. • Undertake targeted risk analysis for particular initiatives, for example risks related to child protection, risks related to vulnerable groups, risks related to gender or gender identification. • Communicate our commitment to risk analysis and management amongst our staff, governing body, and partners. • Work with partners to develop their risk management capacity and procedures.

[6] https://acfid.asn.au/good-practice-toolkit/quality-principle-4/commitment-4-2/

Department of Foreign Affairs and Trade ("DFAT") - Child Protection Compliance Standards[7]	• DFAT has minimum child protection standards to ensure that all funded partners (as defined in the DFAT Child Protection Policy 2017) understand and act on their obligations for managing risks to children. • All organisations and individual contractors must immediately report any suspected or alleged case of child exploitation, abuse or policy non-compliance in connection with official duties or business. All reports should be made to childwelfare@dfat.gov.au
ISO 31000:2018 Risk Management[8]	• Internationally-accepted principles and guidelines for risk management • A structured framework for implementing risk processes • Standard criteria for monitoring, reviewing, and improving risk management • Tools for reporting and communicating risks organisation-wide

[7] Child protection compliance standards | Australian Government Department of Foreign Affairs and Trade (dfat.gov.au)
[8] ISO 31000:2018 - Risk management — Guidelines

Definition

In this RMF, Risk is defined by GNAU as:

"An event that may:

1) ***have a positive or negative impact on the accomplishment of GNAU's Mission and the achievement of its Strategic Objectives, and,***
2) ***cause damage to GNAU's people, assets, programs, and reputation".***

Risk may arise from external factors (for e.g., risks from global economic crisis, global pandemic, changing legislations, etc.), or internal sources (for e.g., new large-scale projects, significant infrastructure and capacity challenges, organisational financial performance and health, key person risk, etc.).

It is acknowledged that Risk should not be totally eliminated, rather, GNAU believes that it is a good and prudent practice to adopt **a context-appropriate Risk Appetite, to enable opportunities for better outcomes of the organisation's strategic objectives**.

As such, the Committee's Risk Appetite Statement ("RAS") is proactively reviewed annually by the Committee.

Framework Components

GNAU's RMF components include:

- Framework Statement (Summary)
- Purpose
- Legal Obligations and Sectoral Standards Compliance
- Definition of Risk
- Summary of Risk Assessment, Treatment, Reporting, and Monitoring
- Risk Register
- Risk Appetite Statement
- Prioritisation of Risks
- Risk Identification, Ranking, and Treatment
- Business Continuity Management
- Training
- Roles and Responsibilities
- Review

Summary of Processes:

When to do a risk assessment:	Committee: Ongoing review and governance and management of risks, including quarterly review of organisational risks (Finance, Programs, Regulatory and Compliance)
	Executive Director ("ED"): Quarterly assessment of Top 10 critical risks (from the Risk Register)
	ED and Treasurer: Identify capital project risks (over $10K in value); during planning phase
	ED and Treasurer: Annual assessment of Risk Register

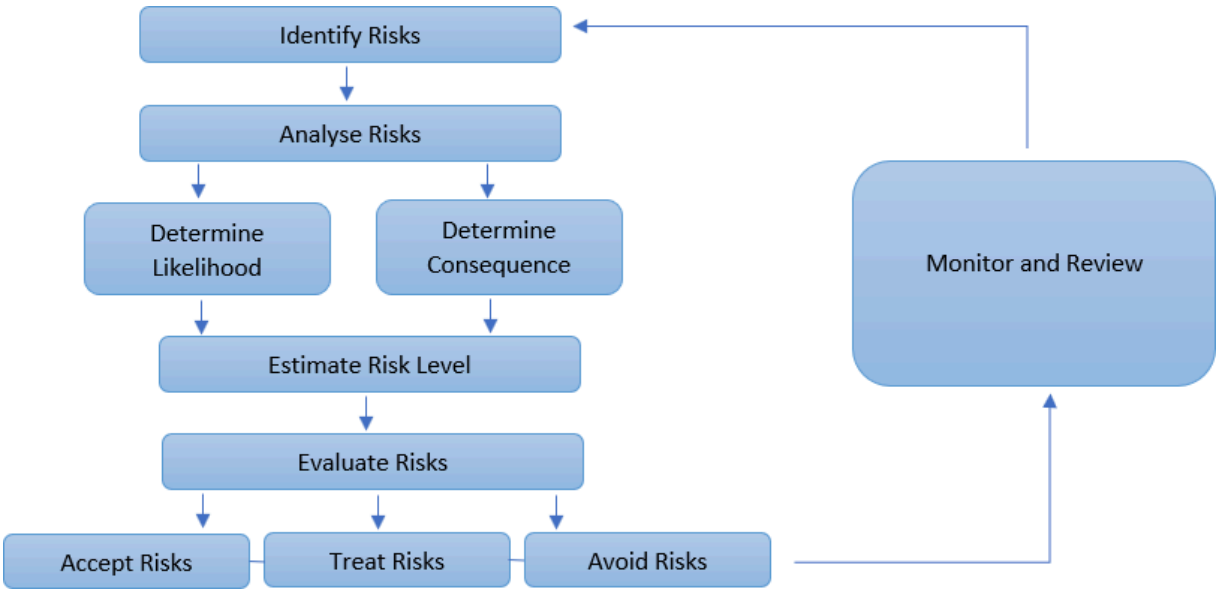
How to assess risks:	Assess risks by considering both probability and impact
	Document all key controls to manage risk
	Assess overall control effectiveness
	Risk decision against risk appetite

How to treat risks:	Develop risk mitigation actions
	Implement risk mitigation plans
	Establish accountability and timeframe
	Develop respective risk management plans in departments that determine priorities, budgeting, and planning requirements to address key risks

How to report, communicate, and train:	Summary of risk assessment is tabled at Quarterly Committee Meetings
	Summary of top 10 critical risks in ED's Committee report, including mitigating strategies, action taken and outcomes
	Annual summary of Risk Register in Committee report
	Annual risk management training (or a refresher course) for Committee, employees, and volunteers

Monitoring and assurance:	Regular review of:
	Adequacy and effectiveness of key controls to manage high risks
	Post-event reviews are undertaken in relation to failures, successes and near misses
	Regular audits of the RMF's effectiveness

GNAU's approach to risk management is consistent with ISO 31000 Risk Management Process:[9]



Risk Register

- **Master Register** - the Risk Register allows GNAU to assess the risk in context with the overall GNAU strategy and activities, and help record the controls and treatments of those risks. Identified risks are collated in a master register, of which primary risks critical to GNAU's operations are continuously monitored, reviewed, treated, and reported to the Committee on a quarterly basis.

- **Managed Risks** – these are identified organisational risks which are actively managed. Any risks identified with a score over 15 are immediately raised with the Risk and Finance Sub Committee.

Risk Appetite Statement

Risk appetite is the **amount of risk, at a broad level, that GNAU is willing to accept in pursuit of its mission and strategic objectives**. GNAU has a Risk Appetite Statement ("RAS") that consists of the following risks with impact category scales:

- Program/Partnership risks
- WHS risks
- HR risks
- Reputation/Donor's Trust risks

[9] ISO 31000 Risk management process - Practical Risk Training

- IT Systems risks
- Regulatory / Compliance risks
- Financial risks
- Environmental and Social Safeguards risks

Strategic Priority of Risks

Assessing the critical risks against the RAS enables the leadership team to identify the strategic priorities of organisational risk management and reporting.

Source: https://www.transparency.gov.au/annual-reports/australian-reinsurance-pool-corporation/reporting-year/2019-20-22

Risk Identification

Risks can be identified through:

- Management Team – significant strategic and operational risks will be identified by the leadership team. Mitigating strategies are recommended to the Committee for consideration.
- ED - organisation-wide risks are identified and reviewed by the ED, when escalated from the Finance and Risk Subcommittee, as well as through a quarterly review of critical risks with the Committee.
- Implementing Partners – as an international NGO, GNAU faces significant inherent risks in managing its international programs and/or community projects. These risks will be continuously identified and mitigated by the ED and GNAU's implementing partners.
- GNAU Committee and Finance and Risk Subcommittee - risks and issues arising from daily operations and weekly staff meetings will be reviewed by the Subcommittee. Critical risks are escalated to the Committee for thorough review.

Risk Ranking Matrix

		1	2	3	4	5
	Consequence Likelihood	Insignificant	Minor	Moderate	Major	Catastrophic
5	**Almost certain**	medium	high	extreme	extreme	extreme
4	**Likely**	medium	high	high	extreme	extreme
3	**Possible**	low	medium	high	high	extreme
2	**Unlikely**	low	low	medium	high	high
1	**Rare**	low	low	medium	high	high

Risk Treatment

The following options are available for treating risks and may be applied individually or in combination, with **due consideration of GNAU's risk appetite**:

Avoid the risk	• Not to proceed with the activity or assess the risk choosing an alternative approach to achieve the same outcome
Mitigate the risk	• Reduce the likelihood as far as reasonably practicable - improving management controls and procedures • Reduce the consequence as far as reasonably practicable - putting in place strategies to minimise adverse consequences, e.g., contingency planning, Business Continuity Plan, liability cover in contractsChoose an alternative approach/mitigate the risk to achieve the same outcome
Transfer the risk	• Shifting responsibility for a risk to another party by contract or insurance, can be transferred as a whole or shared
Accept the risk	• Controls are deemed appropriate • These must be monitored and contingency plans developed where appropriate

Business Continuity Management

Insurance Strategy

GNAU's insurances are reviewed on an annual basis, taking into account the organisation's risk profile, the prevailing status of the insurance market, and GNAU's risk appetite at the time.

IT Disaster Recovery Plan (DRP)

An information technology (IT) DRP will be maintained to ensure the continuity of information systems availability and protection of data in the event of a significant event, for e.g., illegal intrusion to the shared drives or the donor/supporter databases. The DRP will include systems that continuously protect GNAU's technical infrastructure, and in the event of a breach, steps for timely restoration and minimal disruption to operations. A Service Level Agreement ("SLA") with external IT vendors will be in place to support the DRP processes. The SLA should:[10]

- include the level of service expected from an IT vendor
- stipulate the metrics by which service is measured
- specify remedies or penalties should service levels not achieved

Business Continuity Plan (BCP)

A Business Continuity Plan will be maintained to ensure that GNAU is able to effectively deal with any issue that may constitute a significant risk to GNAU's operations and/or reputation, for e.g., the sudden departure of key personnel, or a fire (i.e., damage to office premises).[11]

Cyber Risks

The 'Operations Resilience Program' applies to all GNAU functions and representatives. The Program defines a systematic approach to identifying, mitigating and resolving cyber risk and cyber-attacks.

Development Program Risks

Significant risks associated with GNAU development programs (for e.g., child safeguarding, financial wrongdoing, etc.) are managed as part of the programming cycle. On a quarterly basis, they are assessed, treated, monitored, and reported to the Committee.

---

[10] https://www.cio.com/article/274740/outsourcing-sla-definitions-and-solutions.html

[11] https://www.smallbusiness.nsw.gov.au/sites/default/files/2023-11/16370_SBC%20Prepare%20for%20the%20unexpected%20ACCESSIBLE_0.pdf

Roles and Responsibilities

Although the Committee has delegated day-to-day risk management responsibility to the Finance and Risk Subcommittee and ED, ultimately the Committee is responsible for all risks – including assessment of emerging risks.

A Finance and Risk Subcommittee ensures ongoing implementation of an effective RFM. It is acknowledged that successful implementation of the RFM is a leadership responsibility, which also requires the active support of the Committee and the ED, and the participation of all staff within the organisation.

ED

The ED is responsible for ensuring that GNAU takes appropriate measures to identify, assess and manage organisational risks, including:

- A risk-conscious culture is implemented and maintained
- Management's risk appetite aligns with the Committee's RAS which may be amended from time to time
- Management's risk management approach aligns with the Organisational Strategy and Strategic Objectives
- GNAU operates within its legal and regulatory obligations
- GNAU can continue to function in the face to major disruptions
- Develop and maintain a Risk Register
- Ensure regular reporting to the Committee against the master/managed risks

The ED is responsible for the implementation of risk management processes by:

- Facilitating regular risk assessments and risk management activities
- Continuous learning of good risk management practices, and providing ongoing advice and support to all staff in proactive risk management
- Monitoring the application of the risk management process across GNAU and reporting on risk management incidents and/or initiatives

Note: it is not the ED's sole responsibility to manage all risks on behalf of the whole organisation. All managers and staff members are responsible for managing risks and controls for which they are responsible.

Committee/Subcommittee

The Committee appoints a Finance and Risk Subcommittee which is responsible for:

- Oversight of risk management processes, including policy, reporting processes and review of risks from the ED
- Ensure the Committee's regular review of the RMF and the RAS

- Oversight of financial risk, including but not limited to:
    - Budget
    - Income and Expenditure
    - Cash-flow
    - Capital Investments

Training and Communication

GNAU will have clarified roles and responsibilities, accountabilities, and authorities at all levels of its operations. The RFM is embedded in operations through a number of communication, training, and support systems, including:

- Regular training courses in risk management processes will be provided. Specific risk management training sessions will be held on an annual basis, aimed at providing an overview of the RFM
- Instruments providing training on appropriate controls include job descriptions, inductions, policies, procedures, terms of reference, performance planning and review, programs, contracts, and delegations.

Responsibilities

The ED is responsible for the RFM.

Review

The RFM will be reviewed annually to ensure its relevancy, currency, and applicability.

References

This should be read in conjunction with:

- Risk Appetite Statement
- Financial Systems and Key Processes Manual
- Financial Wrongdoing Policy
- Segregation of Duties and Delegation of Authority
- Complaint Handling Policy
- Whistleblowing Policy
- Child Safeguarding Policy
- PSEAH Policy
- WHS Policy

Acknowledgement

GNAU acknowledges the templates of this RFM were sourced from the following organisations on 21/11/2023, they were further modified to suit GNAU's operating

environment:

- Australian Catholic University's enterprise risk management framework template: https://policies.GNAU.edu.au/-/media/policies-site/governance/enterprise-risk-management-framework.pdf?la=en&hash=1E835317710D5DE0FD6C22CF6FCF035D
- Asia Pacific Baptist Federation's risk management framework template

Document Control Information

Organisational Risk Management Framework	
Owner	Committee Chair
Master Copy	Executive Director
Date created	04/12/2023
Date last reviewed	N/A
Approved by the Committee	04/09/2024
Minor Revisions Approved by the Executive Director	10/07/2025
Date next Review	09/07/2026

Date	Version	Revision Description	Reviewed / Updated by
04/12/2023	1	Created	Executive Director
10/07/2025	2	Revised to reflect subcommittee and other minor changes	Executive Director