Mahboba’s Promise Risk Management Policy and Architecture

1. Purpose

This Risk Management Guidance Note and Framework (RMF) explains how Mahboba’s Promise (MP) identifies and manages risks that may prevent the organisation from achieving its mission and purpose.

2. Why this matters

Effective risk management creates organisational value, as it supports:

- Proactive identification of opportunities and threats reducing the need for reactive management responses.
- Avoidance of unexpected losses.
- Compliance with relevant legal and regulatory requirements.
- Improved risk reporting and corporate governance.
- Reliable decision making and planning.
- Appropriate allocation of resources.
- Enhanced health and safety.
- Incident management and prevention; and
- Operational effectiveness, reliability and resilience.

3. Scope

This RMF addresses how MP is proactive in applying a risk-based approach to the identification, assessment, mitigation, prevention and mitigation of risks that may impact our strategy, reputation, operations or communities and people we serve.

This framework applies to all Management Committee members, directors, management, staff, contractors, consultants and volunteers of MP. This includes where MP has management or regulatory responsibilities for MP International activities or offices.

4. Roles and Responsibilities

Risk management is the responsibility of everyone in MP, from Management Committee members, all management staff and volunteers.

MP Management Committee are the ultimate duty holders when it comes to risk management, with a particular focus on setting, checking and communicating organisational risk appetite and ensuring risk management oversight through the risk management framework implementation and monitoring.

5. Risk Management, Finance and Governance Committee

The Risk, Finance and Governance Committee supports the MC meet financial and strategic risk by conducting a quarterly review of the risk management framework, organisational risk register and mitigation strategies and ensures strategic risks are formally reported to the Management Committee in line with the Risk Appetite Statement.

MP Executive Manager (ExMgr) is responsible for the day-to-day implementation and management of risk, focused on scheduled performance reviews to identify and manage any performance barriers, progress and goals. The ExMgr is also responsible for confirming a risk review after a major event or change in the strategic or operational environment that may represent a new or changed risk profiles to MP, its assets and people.

MP relies on the knowledge and advice from the field. MP proactively identifies and invests in organisational risk champions. MP people are open to learning and applying risk management principles and processes because it keeps the organisation, their teams and communities we serve safe. MP leaders rely on MP risk management champions to provide invaluable feedback on gaps, barriers and performance issues so that our policies, processes and procedures are fit for purpose and have the intended impact.

6. Risk Management Overview and Principles

What is Risk Management?

Risk is defined as the effect of uncertainty on objectives. MP faces many risks as well as opportunities. There is a direct link between risk and opportunity that has both financial and non-financial implications. MP are committed to think holistically about risk, while also ensuring risk relating to country contexts (e.g., Violent conflict rates) or technical (safeguarding) or thematic (cash programming) functions are specifically considered in relation to MP’s Risk Appetite.

Risk management focuses on identifying, assessing and understanding risks and taking appropriate actions to minimise, accept, or avoid the risk. Risk management can also help in identifying opportunities where MP is prepared to consider taking more risk in the pursuit of important objectives.

MP's Commitment to Risk Management

In joining MP, as a partner, volunteer, Management Committee member or service provider, means signing up to a commitment to adopting a risk-based approach consistent with this framework and ISO 31000:2018.

This commitment includes ensuring the internal capacity and capability in people, systems, processes and governance exist to achieve risk management. We embrace a culture of risk awareness, transparency and accountability to compliance. This culture is defined by evidence that our people and partners speak up about their concerns, are heard and risks are proactively managed together.

As MP continues to operate in more challenging and complex environments, MP is committed to engage with risk, within our defined risk appetite, to achieve our mission.

Definitions

- **Consequence:** The outcome of a risk event affecting objectives (if it occurs).
- **Control:** Any measure or action that maintains and/or modifies risk. Any measure taken that either reduces or mitigates the likelihood of a risk occurring or reduces the potential impact arising from that risk.
- **Inherent Risk:** The likelihood and impact of the risk arising before actions or controls have been implemented.
- **Key control:** A control that significantly reduces the impact or likelihood of a risk. Key controls are controls that MP must do and have in place to mitigate key risks from happening or minimise the damage they cause. Key controls must be effective in the management of risks, and therefore they should be treated as priority.
- **Likelihood:** The chance that a particular risk will occur.
- **Residual risk:** The risk remaining after agreed actions and controls have been implemented.

- **Risk:** The effect of uncertainty on objectives i.e. an uncertain event or condition that if it occurs will affect achievement of one or more objectives.
- **Risk Management:** Coordinated activities to direct and control an organisation with regard to risk i.e., the process of taking appropriate decisions and implementing appropriate actions in response to known risks, based on the results of a risk analysis.
- **Risk Treatment:** A risk modification process. Once a treatment has been implemented, it becomes a control, or it modifies existing controls. There may be many treatment options, i.e., can avoid a risk, reduce a risk, remove the source of the risk, modify the consequences, change the probabilities, share the risk, or simply retain the risk, or you can even increase the risk in order to pursue an opportunity.

Principles of Risk Management

Integrated:	Risk management is an integral part of all organisational activities.
Structured and comprehensive:	A structured and comprehensive approach means consistent and comparable results can be achieved regardless of this issue/risk, being assessed. For example, child protection and safeguarding risk can be assessed as a risk in relation to other risk issues. (See Risk Management Process).
Customised:	The risk management framework and process should be customised and proportionate to MP's external and internal context related to its objectives. (See Risk Architecture).
Inclusive:	Appropriate and timely involvement of stakeholders is necessary. (Step 2, Risk Identification).
Dynamic:	Risk management anticipates, detects, acknowledges and responds to changes. This requires regular monitoring. (See Step 5, Monitoring)
Best available information:	Risk management explicitly considers any limitations of available information. (Step 6, Risk Reporting).
Human and cultural factors:	Human and cultural factors influence all aspects of risk management. (See MP's Commitment to Risk Management).

Continual improvement:	Risk management is continually improved through learning and experience.

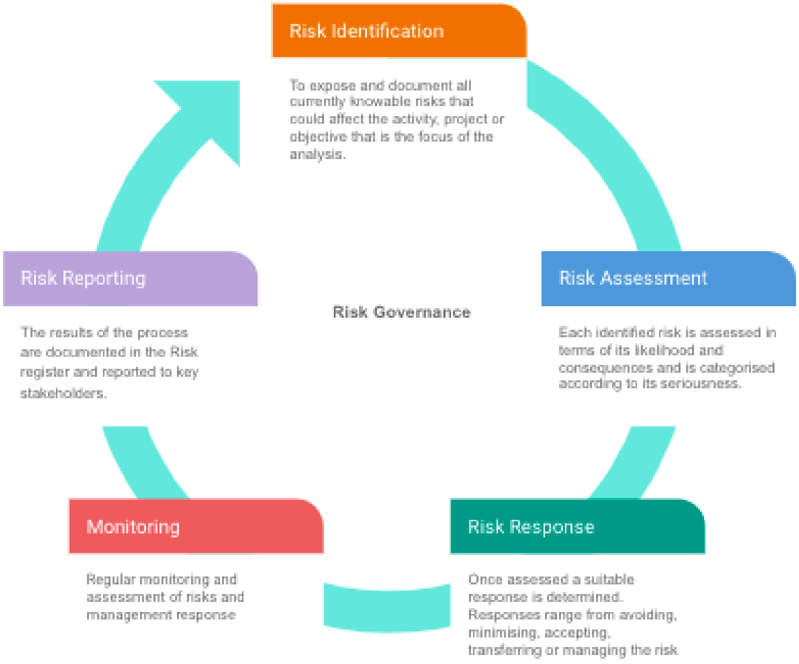
7. Risk Architecture

Just as a building provides us with physical protection and security, so too does our risk management architecture. When we are in the shelter of MP, we take a united approach to identifying, assessing and managing risk management. This united approach allows us to use the same terms, to use the same language and have a shared understanding. While we may need to think about different risks in different places or programs, we use the same language to assess and manage risks so that our leaders understand which ones need our early attention, resources or action.

This united whole of organisational approach that allows our leaders to create a safe and professional organisation, is often called the Enterprise Risk model. Enterprise risks are defined as the kinds of risks that could stop or reduce the ability of MP to assist the women and girls of Afghanistan. Defining what these enterprise risks are, is the job of MP’s Management Committee and Executive Team. The management and oversight of these is delegated to the ExMgr and Risk Committee by the Management Committees. When you follow the steps in this document, you are helping the entire organisation and our leaders to achieve the organisation’s important goals.

Risk Management Process

The following diagram outlines the * step process for how MP identifies, assesses and responds to risk together.



Risk Identification

To expose and document all currently knowable risks that could affect the activity, project or objective that is the focus of the analysis.

Risk Assessment

Each identified risk is assessed in terms of its likelihood and consequences and is categorised according to its seriousness.

Risk Response

Once assessed a suitable response is determined. Responses range from avoiding, minimising, accepting, transferring or managing the risk

Monitoring

Regular monitoring and assessment of risks and management response

Risk Reporting

The results of the process are documented in the Risk register and reported to key stakeholders.

Risk Governance

Step One: Risk Appetite Statement

MP works in complex and challenging contexts. The Risk Appetite is the way the Management Committee and executive make sure MP’s provides a safe and legally compliant workplace. This is no small thing, as the Management Committee and some executives not only are professionally responsible but in the event these systems are not adhered to, could be held personally liable for any harm that occurs under Australian law. This means everyone is working to ensure the day-to-day activities are safe as possible, are resourced as best as possible and that the people you serve are too.

The Risk Appetite tells you the maximum levels of risk that MP is prepared to take to achieve its objectives. The Risk Appetite is reviewed annually as part of the Management Committee calendar or in the event of a major strategy change.

Statement of Risk Appetite

No.	Key Risks	Residual Risk Appetite after Mitigation
1	Financial viability and trust – inability to generate enough money to resource the organisation to achieve the mission and strategy.	HIGH. MP understand the inherent risk level of financial viability is moderate due to the volatility of public fundraising, uncertainty of resource mobilisation and required reporting requirements. MP also acknowledges the high-risk operational model (limited banking systems available) required to operate in Afghanistan. MP is committed to reduce this risk to Moderate by improving financial accountability and audit reporting and program monitoring to increase donor investment and fundraising.
2	Governance and Compliance - risks related to non-conformance with laws, regulations and requirements; and internal policies, procedures and practices in place to achieve strategic intent.	HIGH. MP and partnered operations operate in complex and high risk dynamic operating environments. MP business model has increased humanitarian action. MP is committed to take all action to bring this risk appetite down to a moderate risk level, together with MP partners.
3	Reputation - risks related to reputational damage with the Australian public, donors, and communities.	HIGH. MP recognises the high risk of facilitating cross cultural understanding and integration between the Afghan-Australian communities – including through public and private sector donations. Equally, MP has a low-risk appetite for any reduction in trust by Afghan women and children in MP. MP will take proactive steps to balance these

		priorities while also working to reduce this risk appetite to moderate.
4	Programmatic risks - risks related to program implementation, effectiveness and efficiency as well as resource mobilisation challenges.	VERY HIGH. Despite the extreme complexity and uncertainty of the operating environments, program adaptation to meet the increasing humanitarian need has reduced the risk appetite to Very High. Extensive and adaptive local controls maintain this risk backed by Australian program support. MP is committed to reduce this risk appetite to high while not compromising the lives of the women and children of Afghanistan, MP people or minimum Australian compliance and standards.
7	Accountability to Affected Populations (Child Protection, Sexual harassment, exploitation and abuse) and misconduct.	MODERATE. The unmitigated risk level is high due to the inherent risk of incidents occurring in the sector and in Afghanistan. MP is committed to reducing this to a low level of risk through preventative and monitoring controls and a culture of reporting, accountability and transparency.
9	Safety and Security - risks posed by safety and security threats to staff working in complex and challenging environments.	HIGH. The unmitigated risk level is extreme due to MP people and partners located in Taliban-governed locations. MP has reduced the overall risk appetite to high. It is understood that there may be specific activities that are depended on to save lives. Very high-risk activity can only occur with Board level approval.

		There must remain a high-risk appetite to achieve our mission within the current context. This high tolerance comes with the expectation that all MP people will work together to proactively identify, report and mitigate risk quickly, professionally and together.
12	Partnerships	Very High. MP maintains a high-risk tolerance for approved partnerships. MP relies on quality partnerships for access, service delivery, information and flexibility. MP acknowledges the high resource cost of partnerships but is committed to reduce this risk to Moderate through knowledge exchange, systems and processes improvements.

Step Two: Risk Identification

Now you know what the risk appetite is of MP, we need to understand the risks that relate to you, your teams and partners activities. Risks are the things that might affect achieving the goal for MP.

To help you think about what these are, the following 7 categories of possible risk have been developed. These also help in using the same language and reporting process to speak about risks.

Category	**Summary**
Strategic	Things (events/trends/activities/behaviours) that could result in MP unable to achieve the goals that allow the organisation to exist. These

	can include legal, regulatory standards that insurances and operations rely on, budget and environmental or contextual requirements.
Operational	Things that could stop MP from achieving the core mission and core business. This might include an event that means the program or partnership has to stop or our IT systems stop working.
Financial	Things that might reduce or stop funding, result in inefficient or inaccurate financial management, reporting and/or budgeting.
Reputational	Anything, that if made public might damage the brand, our name and logo and reduce the trust or credibility needed for MP to operate.
People	Things that might change the quantity, quality or capacity of our people. This might include how safe and healthy our workplaces are, or how our people feel about their workplace health and safety. Anything that impacts MP's ability to provide healthy and safe workplaces.
Legal	Something that could stop MP meeting its legal obligations and/or anything which could be the subject of legal action involving the organisation.
Governance	Anything relating to damaging or poor action, or inaction by the Board or senior management that impact how MP can achieve its mission.

Within these categories are mandatory thematic issues that need to be assessed. To ensure MP is able to meet Australian legal obligations it is essential that we regularly assess and treat any risk of terrorism financing. With the Taliban registered as a terrorist organisation but also the government of the day in Afghanistan, we are committed to assessing the risk of when our funds may be used to enable terrorist activity versus when it is part of normal government administration and services. This risk must be addressed in all program designs, monitoring and reporting for work in Afghanistan.

Likewise, to help us manage the risks to women and children, we have a mandatory safeguarding risk register that ensures we consider all the relevant categories of risk to the people we are here to serve.

You may find the below ways to identify risk to be useful:

- Bringing the team together to discuss all the possible risks for each category that relates to your activities. Thinking about situations that you expect to happen or that might happen and consider how that might impact your activities. This can also be done with partners so that the problems but also the possible solutions can be shared.
- Think about the incidents that have happened. Think about what you learnt about that incident. Read any reporting that provided recommendations. Consider how you might be able to stop the incident from happening again or reducing the harm that was caused.
- You can get some external advice, to work together as a team or think outside your day-to-day focus.

Note, a risk assessment may not be required for all risks. If a risk is considered rare and to have low consequences, the risk can be ignored in the assessment data. Management of identified risks and the need to manage the risk is at the discretion of management.

Step Three: Risk Assessment

So now you have a list of your risks. The next step is to rate how likely the risk will happen. And, if it did happen, how bad it might be for MP. Thinking about risks like this, is what is called conducing a risk assessment.

To conduct a risk assessment you assess the likelihood, the consequence (or impact) and rate the risk. One by one, consider how likely each risk is of occurring. The table below will help you decide what likelihood rating best fits.

Table One: Event Likelihood

Level	Scale	Description	Probability*
1	Rare	The event is likely to occur only in highly rare or exceptional circumstances. There is no known occurrence. There is an extremely remote chance of occurrence between July to June year. A once in a lifetime event.	<2%

2	Unlikely	The event could occur at some time and has occurred sometime. It would not be considered as a common occurrence and would only occur in isolated circumstances.	2-16%
3	Probable	The event might occur at some time. It has occurred in the past. It has occurred in MP or in by others in the same context on a regular basis and frequency enough to be possible.	17-50%
4	Likely	The event will probably occur in most years and has occurred in MP history. Knowledge or evidence in MP or by others in the same context suggests this event occurs at regular intervals.	51-84%
5	Almost Certain	This event is expected to occur in most circumstances. Has occurred in MP in the past year. The event is common and expected.	>85%

Table Two: Event Consequence

Severity		Operational	Medical /Wellbeing	Financial	Reputational
1	Insignificant	No or very limited disruption to field/work day.	Very minor medical/wellbeing incident self-managed or attended to by medical specialist or health provider.	Net impact of less than 1% of turnover (organisational) or self-funded (individual).	No significant direct reputational impact.

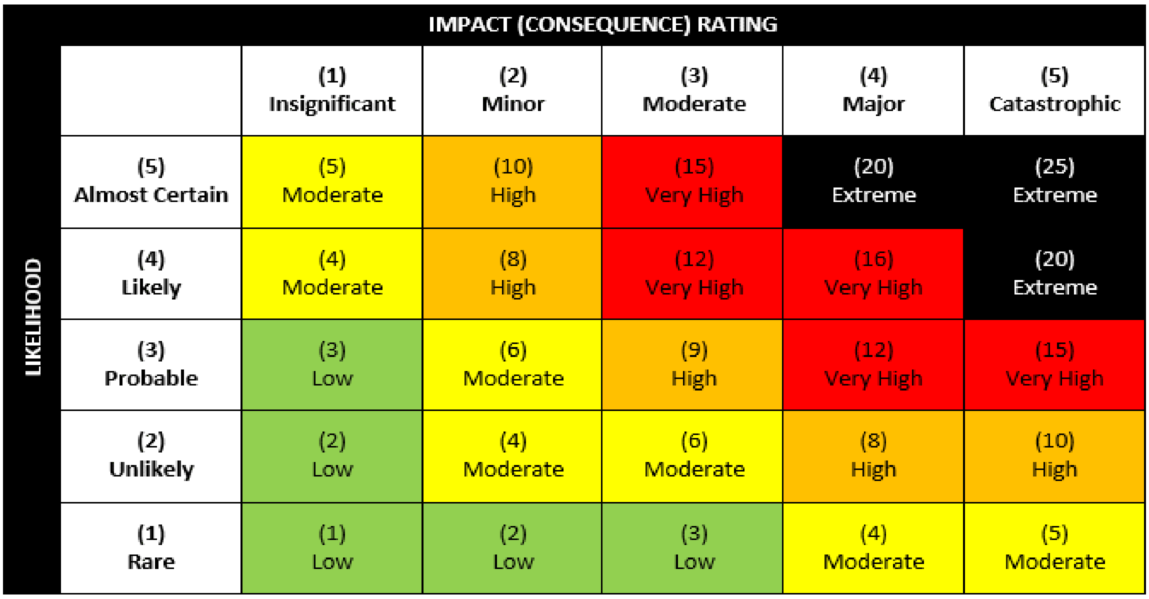
2	Minor	Field day(s) disrupted as a result of administrative and/or bureaucratic issues.	Medical/wellbeing incident requiring brief attention by medical/wellbeing specialist.	Net impact of 1-2% of turnover.	Potential for adverse reputational impact internally or within sector.
3	Moderate	Multiple field days disrupted as a result of minor to moderate administrative issues.	Medical/wellbeing incident requiring out-patient admission (e.g. insect-borne disease, compassionate repat).	Net impact of 3-5% of turnover.	Adverse reputational impact at state/national level.
4	Major	Multiple field days disrupted as a result of a serious (e.g. missing staff, illegal detention, relocation/ evacuation from conflict/disaster) event.	Life-altering (non-life threatening medical/wellbeing incident or event.	Net impact of 6-20% of turnover.	Major adverse reputational impact at international level.

5	Catastrophic	Proximate threat to organsational integrity. Forced suspension or cessation of operations, and/or loss of a substantial part of the organisation.	One or more fatalities. Kidnapping or abduction. Proximate threat to life/long-term wellbeing.	Net impact of greater than 20% of annual turnover, or any time MP's financial obligations threaten to exceed its capacity to fulfil them.	Potential for irreparable/ unrecoverable reputational damage.

These descriptions are examples of what impact your risk might have across four areas (Operational, Medical/Wellbeing, Financial, Reputational). These link back to the risk appetite we have discussed and helps build a common and consistent understanding of what each risk might mean when we look at the collective risks across the organisation. Say for instance every team keeps coming back with major financial impact risks – the Board and Executive may need to think about what more can be done to mitigate the organisational finance risk.

Table Three: Inherent risk rating

Now you have a likelihood and a consequence rating, you can rate your risk without any action taken. This is often called the “inherent risk rating”. Once you have taken actions to mitigate the risk, it is called the “residual risk”.



		IMPACT (CONSEQUENCE) RATING				
LIKELIHOOD		(1) Insignificant	(2) Minor	(3) Moderate	(4) Major	(5) Catastrophic
	(5) Almost Certain	(5) Moderate	(10) High	(15) Very High	(20) Extreme	(25) Extreme
	(4) Likely	(4) Moderate	(8) High	(12) Very High	(16) Very High	(20) Extreme
	(3) Probable	(3) Low	(6) Moderate	(9) High	(12) Very High	(15) Very High
	(2) Unlikely	(2) Low	(4) Moderate	(6) Moderate	(8) High	(10) High
	(1) Rare	(1) Low	(2) Low	(3) Low	(4) Moderate	(5) Moderate

To use the above table, you take the number or the rating of the likelihood table and match it to the column on the left. Then you find the number or rating of the impact table, and find it in the row in the above table.

Inherent Risk Example: Say we are assessing the risk of fraud occurring to a program in a project in Australia. We know fraud happens in the sector but it has not occurred in MP. We know it could occur though so we say it is ‘unlikely’. Yet, if fraud was to happen, it would have some ‘major’ consequences. It would disrupt the program and the larger organisation as the legal reporting and investigations response occurs. It would likely damage morale and wellbeing of some people. Depending on the severity, it may result in the entire program being ceased along with a withdrawal or reduction in donor or fundraising money. It would absolutely damage the organisation’s reputation. So, this means we match the unlikely up with the major impact rating which means the overall risk rating is HIGH.

Step Four: Actions

Once you have a risk rating for each of your risks, it’s time to think about what action you can take to reduce the residual risk of the moderate, high, very high or extreme risk. Table four provides you with broad instructions on what actions you will need to take, often as part of a team, organisation or partnership.

Risk Leve	Actions/Acceptance
Low	Activity can proceed.
Moderate	Activity can proceed. With reasonable actions the risk can be mitigated, and all reasonable steps have been taken to lower the risk.
High	Activity can proceed only if there is a clear logic demonstrating a correlation between threats/hazards and reasonable actions to mitigate or lower the risks they pose.
Very High	Activity should not proceed until the risk level is lowered or has passed. Senior management permission must be sought for activities to occur and only where it is justified by exceptional circumstances or mission criticality. Monitoring and review must occur at a minimum, quarterly with Board of Director annual approval.
Extreme	Activity cannot proceed until risk level is lowered.

There are three broad kinds of actions (or controls) you can take to mitigate risk.

Preventative	Are controls you put in before a risk event occurring that aim to reduce the likelihood of it occurring (e.g. the need to authorise a payment prior to the money being transferred or handed over).
Detective	Are active after a risk event and aim to identify failures or breaches (e.g. bank reconciliations to identify unauthorised payments).
Corrective	Also occur after an event but aim to learn from it and make sure it does not happen again (e.g. creating this guidance note to help you manage risk is a great example).

Once you have a list of actions you can, will or have taken to reduce the risk. You can step through the likelihood, consequence and risk rating steps again. The result of this process is what is your residual risk.

Residual Risk Example: If we stick with the example of our fraud incident. We might increase the number of people who provide approvals, provide fraud prevention training and put a new payment system in place. Now, if we consider the likelihood the risk is rare. If we look at the harm consequence is still major though. Yet, the residual risk rating has dropped to moderate. Good job!

Step Five: Monitor

You now have all of your controls in place. You have your approvals to operate and your activity is running smoothly. But, how do you know it is? Monitoring the system you put in place that tells you it is working and that if there are any changes to the risk appetite or environment, you will know.

One example is how will you know that your insurances to operate is current? When will you know that all of a sudden you have a higher financial or personal liability risk than when you first began? A useful way of monitoring is identifying things that will show MP and your team that the controls are working. You can also monitor by scheduling reviews, get feedback from partners, staff and people you help. You might like someone outside of your team to look at your approach and see if they can see any improvements. You may ask for a risk management expert to come in from outside the organisation to provide you with more ideas or check how things are going. The more confident you can be, the less likely you will be caught by surprise and need to enact a crisis response plan.

Step Six: Risk Reporting

The Risk Assessment and Register is a tool that can help you report risk clearly, timely, accurately and with relevance. Reporting risk this way, is more likely to result in good decision making. Managers and leadership are responsible for reporting on the status of different risks. The Audit and Risk Committee is responsible for ensuring appropriate action and resources are allocated and that the Management Committee (for full details see the Terms of Reference) are informed according to the Risk Appetite.

MP managers, decision makers and partnership leads are responsible for ensuring that the following instances are reported immediately to a member of the executive or Board:

- an extreme or very high-risk rating
- high risk ratings on the same issues appearing across multiple risk registers
- when there is 10% or more financial risk to a program or budget
- when harm is expected to occur to any person
- risk of sustained or adverse media coverage.

To ensure the Management Committee are informed and are able to fulfil their obligations to safeguard people, the organisation, partnerships and the rights holders you work for, you can use the following template to report Very High and Extreme Risks.

Details of the risk	**Risk Rating**	**Recommended actions**	**Risk Owner/s**
Insert the type of risk, the likelihood and impact rationale and why you are unable to reduce the risk without executive support. What will happen if this risk is not mitigated?	What is the residual risk rating.	What actions do you need from the Board or your management team? What resources, action, support?	Your name, team and position and your supervisors details if relevant.

8. Related Policies and Procedures

MP must comply with Australian laws. While MP is not expected to have specialised legal knowledge, it is responsible for ensuring compliance with the law, and should therefore have some familiarity with relevant legal obligations, including those that may arise under local in-country laws and regulations. This includes, but not limited to:

- Governance under Corporations Act 2001 (ASIC and ACNC).
- Fraud under Commonwealth Criminal Code (Part 7.3 relating to fraud).
- Privacy under Privacy Act 1988.

- Child protection under Commonwealth Law.
- Gender Equality Act.
- Australian Tax Law and GST Legislation.
- Privacy Law.
- Counterterrorism under Australian counter-terrorism legislation.

Other supporting documents

- ISO 31000:2018
- ACFID Quality Assurance Framework
- ACNC Governance and External Conduct Standards

Document Control	
Risk Level:	Very High (one year)
Approval Date:	Operationally approved: 9/05/2023
Next Review Date:	9/05/2024
Responsible Position:	Operations Manager