RISK POLICY

Approved by the Board of Philanthropy Australian on 2 March 2022

OVERVIEW

Philanthropy Australia (PA) recognises that the organisation is exposed to certain risks due to the nature of its activities and the environment in which it operates. The key to Philanthropy Australia's success is the effective management of risk to ensure its organisational objectives are achieved.

Risks arise due to the organisation's operational undertakings and from external sources. Risks occur in numerous ways and have the potential to impact financial performance, reputation, health and safety, membership and philanthropic community and the overall performance of the organisation.

Effective risk management is viewed as a key enabler and driver of the success of the organisation in meeting its strategic goals – not an inhibitor.

POLICY

To fully understand such risks, Philanthropy Australia has established a Risk Management Policy which provides the framework for how risk will be managed within the organisation. The Risk Management Policy is based on the Australian standard, principles and guidelines, and forms part of the governance framework of the organisation. It also integrates with the strategic planning process. The Policy addresses both strategic and operational risks.

- We will use our skills and expertise to identify risks across the organisation.
- Philanthropy Australia will identify operational controls in place that manage risk.
- We will assess the size or degree of risk by taking into consideration the potential impact to our operations.
- A Risk Register will be maintained containing material risks to the organisation, and risks will be ranked in a common and consistent manner.
- Risk treatment actions and plans will be developed for residual risks that are unacceptable to the organisation.
- Risks, and the effectiveness of the risk management system will be monitored on a regular basis.
- We will communicate and consult with relevant stakeholders on our approach to managing risk.

RISK APPETITE

The table below details the risk appetite descriptions for each key area of risk that has been identified.

Our tolerance for adverse risks will be used to determine which risks are treated through the development of risk control actions to manage residual risks to an acceptable level. During this process we will consider additional control measures to manage the risks to acceptable levels.

	Risk Appetite	Rationale
Strategic	Moderate to High	In order to achieve its objectives, PA must be willing to take and accept risk. PA is willing to take or accept a moderate to high level of risk in pursuit of its strategic priorities. There is low willingness to accept risks which have no alignment with our strategic direction or tarnish PA's credibility and its values.
Financial	Low-Moderate	PA needs to remain financially sustainable to continue to serve its purpose and achieve its aspirations. PA has no tolerance for irresponsible use of PA resources and unnecessary liabilities. We have a moderate risk appetite for being more commercially adept and explore avenues to diversify revenue streams through commercially viable arrangements and partnerships.
Membership	Low	PA does not accept risks that could result in a significant loss of its membership or revenue base, greater than 10%.
People	Low	PA recognises their people are key to success and will reduce risks at all times to enable their effectiveness The willingness to accept risks to the health, safety and wellbeing of staff, is very low. A strong culture of health and safety awareness and risk management is expected of all staff.
Reputational	Low- High	PA is willing to take risks that will inspire and enable more and better giving. We have a high-risk appetite to contribute to policy and practice discussions with government and the philanthropic community. We have a low-risk appetite for risks that will PA's brand and diminish its role as a significant contributor to the philanthropic community.
Operations	Low-High	PA has a low-risk appetite for business interruptions at critical periods of operations impacting staff and members. Whilst the ability to support operations on a day-to-day basis is important, PA has a high-risk appetite for change to ensure that PA has the right resources, staff and capabilities to optimise performance
Legal/Compliance	Low	PA seeks to comply with relevant statutory requirements to the best of its endeavours.
Governance	Low	PA has a low risk appetite for misconduct, fraud, harassment or discrimination and non-compliance behaviour that undermines the integrity of PA. We will achieve this through strong governance and management which will shape PA's culture for compliance, ethical conduct and living our values.

INTEGRATION WITH GOVERNANCE AND STRATEGIC PLANNING

The Risk Management Policy forms part of the governance framework and integrates with the strategic planning process. The Policy addresses both strategic and operational risks and the requirement of the organisation to operate in its regulatory environment.

ACCOUNTABILITY

Ownership of risks and risk treatment actions is the responsibility of the Board. The Board may assign the responsibility for management and reporting of these risks to key roles within the organisation, but at all times the Board is accountable for Risk. Philanthropy Australia has incorporated risk management accountability into Board, senior management and project roles that are required to report on risks and risk treatment actions.

RISK MANAGEMENT OVERSIGHT

Philanthropy Australia's Finance, Audit, Risk and Compliance Committee will oversee the Risk Management Policy and the organisation's exposure to risk. Oversight of the effectiveness of our risk management processes and activities will provide assurance to the Board and stakeholders and will support our commitment to continuous organisational improvement.

REPORTING, MONITORING AND REVIEW

The Senior Management Team of Philanthropy Australia will monitor risks and treatment actions on an ongoing basis with a review of the risk register to be undertaken by the Senior Management Team on a monthly basis. The Finance, Audit, Risk and Compliance Committee will review the Risk Policy and Risk Register on a semi-annual basis. Performance of the risk management system and outstanding residual risk treatment actions will be reported to the Board annually.

Formal reviews of both the risk management system and the Risk Register will take place on an annual basis and the FARC Committee & Board will assess the effectiveness of the Risk Policy annually.

Date established:	July 2018
Date of review:	November 2022
Board Approved:	2 March 2022

Risk Management Process

PURPOSE

This Risk Management process must be read and aligned to the Philanthropy Australia (PA) Risk Policy. This establishes a risk assessment framework and management process for Philanthropy Australia.

The PA Board understands and accepts that risk management is an integral part of good governance and essential to effective management practice. It is an iterative process consisting of steps that, when undertaken in sequence, enable continuous improvement in decision-making and facilitate continuous improvement in performance.

To be most useful, it should be embedded in PA culture, best achieved when it forms a basis of our operations, practices and processes rather than undertaken as a separate activity.

RESPONSIBILITY & ACCOUNTABILITY

The Board of PA has ownership & responsibility for management of risks.

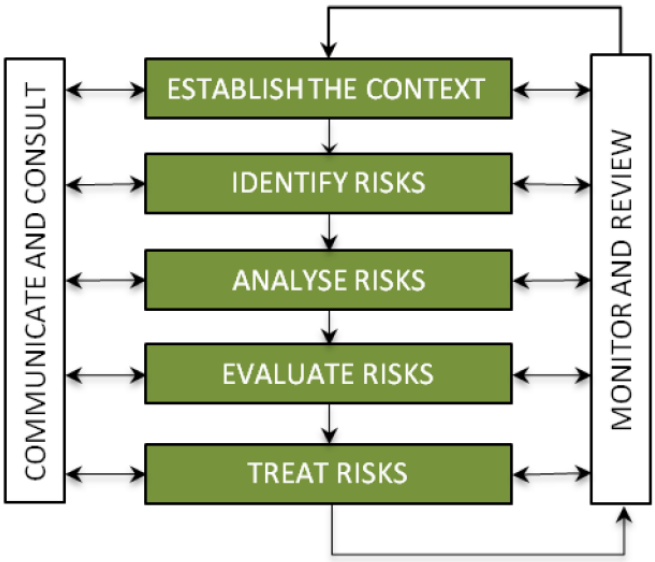
They have delegated the monitoring of financial, strategic, operational, legal and regulatory due diligence and risk management to the sub-committee of the Board, the Finance, Audit, Risk & Compliance Committee (FARCC) (Guideline 14, 1(h)).

Risks must be reported at least annually to the Board (G14, 6.12)

The CEO has the responsibility (within their Position Description) to manage the implementation and timely reporting of the risk management framework and policy, through the FARC Committee, to the Board.

1. RISK ASSESSMENT

PA shall establish arisk assessment process that identifies threats and vulnerabilities, and ensures mitigation and monitoring is in place. The risk assessment process is represented as follows:



To execute this process the PA Board has delegated to the CEO and the Senior Management Team (SMT) team responsibility for ensuring the process is carried out and outomes reported back to the Board, through the FARCC bi-annually. The Board will also contribute to the review, via the FARCC and at each Board meeting.

2. RISK ASSESSMENT PROCESS

PA needs to execute each component as showed above.

2.1. Context Establishment & Risk Identification

Formal risk assessments are to be conducted as part of the following aspects of PA operations (not exhaustive), and clearly define the scope and context (including what is in and out) of the risk analysis;

- Development and ongoing management of all business and strategic plans;
- Key decision making processes (e.g. investment decisions);
- Implementation of new systems and processes;
- Compliance with applicable legal and regulatory requirements and obligations;
- Collaborations with other NFP's, businesses and organisations; and
- Management of government-funded projects, and private trust and foundation projects;

2.2. Identify the Risks

PA will identify the people, process or technology related to the context of each activity of the annual plan's operational strategy.

Philanthropy Australia identifies Risk under these categories;

- Strategic (including environmental)
- Financial
- People

Membership

- Reputational
- Operations
- Legal/Compliance
- Governance

Consider the following as part of the risk identification process:

- All knowable material risks (threats and opportunities) able to impact the successful achievement of the particular objectives being considered; including
- Those risks beyond the control of Philanthropy Australia;
- The PA Board approved Strategic Plan;

- Assessment must include those risks associated with the processing, storage, transmission or protection of personal information and cardholder and bank account data.
- Knock-on effects as a result of particular consequences; and
- The risk of not pursuing identified opportunities.

2.3. Risk Analysis

Risk analysis is the process of developing a thorough understanding of identified risks. During the risk analysis phase appropriate consideration is given to:

- The causes and sources of the risk;
- The potential exposure to PA;
- The current controls in place;
- The current effectiveness of exisiting controls;
- The potential consequences resulting from the risk (positive and negative);
- The likelihood that the identified consequences will occur;
- Factors affecting consequence and likelihood;
- Interdependence of identified risks;
- The level of confidence associated with the determinations of consequence and likelihood; and
- Any known uncertainties resulting from gaps in expertise, information or resources.

2.4. Risk Rating

PA will determine the Current Risk Rating as follows:

- Consider all possible consequences of the risk and the corresponding likelihood using the specified Risk Assessment Criteria;
- Take due account of current controls and the associated control effectiveness; and
- Select the most appropriate Current Risk Rating based on the assumption of the most likely consequence occurring and the corresponding likelihood of occurrence.

2.5. Risk Profiling / Evaluation

PA will evaluate the risks defining probability (likelihood) and impact, resulting in a risk score that will help allow prioritization, allowing focus of the efforts PA should use.

The qualitative model uses two assessment criteria tables, as described below:

- Table A - Likelihood Criteria – A detailed guide for selecting the **likelihood** of a risk using one of five different measures – probability of occurrence, qualitative judgement or frequency of recurrence (use a singular or combination approach to determine likelihood).
- Table B - Consequence Criteria – Detailed criteria for selecting threat **consequence** levels. This table outlines a range of consequence categories aligned to the PA's objectives, and includes five levels of consequence (where 1 is the lowest and 5 is the highest).

The resulting risk score enables decisions to be made about the management approach to which risks require further action, the exisiting management controls and actions, and the treatment priorities.

- Table C - Risk Rating – The matrix for determining the risk rating by bringing together consequence and likelihood

Table A - Likelihood Assessment Table

Level	Likelihood	Likelihood description	Level of Likelihood value
1	**Rare**	This event may occur in exceptional circumstance. Less than once in 15 years	1 - 3
2	**Unlikely**	This event could occur sometime. At least once in 10 years	4 - 5
3	**Possible**	This event should occur at some time. At least once in 3 years	6 - 9
4	**Likely**	This event will probably occur in most circumstances. At least once per year	10 -15
5	**Almost Certain**	This event is expected to occur in most circumstances. More than once per year	16 -25

Table B -Consequence Assessment Table

	Minor / No Impact	Moderate	Significant	Serious	Extreme
	1	2	3	4	5
Financial: Balance Sheet / Cash-flow	Impact on bottom line Less than 10k Negligible impact on liquidity / cash flow	Impact on bottom line 20k to 50k Liquidity / cash flow impact absorbed under normal operating conditions	Impact on bottom line 50-100k Liquidity / cash flow may be affected and will effect ability to pay bills	Impact on bottom line 100-250k Liquidity / cash flow may be adversely affected and will effect ability to pay bills and meet payroll	Impact on bottom line more than 250k Imminent liquidity / cash flow problem. Receivership
Members	Loss of <1% Members	Loss of <5% Members	Loss of <10% Members	Loss of <20% Members	Business failure due to loss of >25% Members
Regulatory / Legal	Possible request from regulator for a summary report when normal operations resumed. Individual legal case	Regulator takes an interest requesting regular updates Individual legal cases	Regulator on site requesting formal report. Potential to incur penalties Small scale class action (>20)	Suspension of Licence or service Penalty warning issued Medium scale class action (20-100)	Business failure due to loss of Licence or closure of Service. Penalties incurred. Large scale class action (>100)

Reputation / Relationships	Media annoyance, little or no stakeholder interest	Limited complaints Minor, adverse media attention. Minor stakeholder complaints that can be readily managed.	Numerous complaints Adverse media attention and/or heightened concern. Reputation impacted with some stakeholders. Some stakeholder criticism / negativity	Significant adverse media/public attention on a state level. Reputation impacted with significant number of stakeholders. Significant stakeholder criticism / negativity lasting weeks.	Sustained and widespread outrage by public or media on a national level. Reputation impacted with majority of key stakeholders. Sustained stakeholder criticism / negativity lasting months. Business failure due to perceived incompetence or faith in the organisation
Employees	5% of staff unable to perform work staff unable to perform 5% of their business activities	10% of staff unable to perform work staff unable to perform 20% of their business activities	20% of staff unable to perform work staff unable to perform 20% of their business activities	50% of staff unable to perform work staff unable to perform 50% of their business activities	>80% of staff unable to perform work staff unable to perform >80% of their business activities
Safety	No workplace injuries No Harassment	injuries reported: 1-2 (minor in nature) Staff reported Harassment; not official	injuries reported: >2 Staff reported Harassment; Officially & formally	serious injuries reported >0 Staff Harassment; Legal proceedings	workplace death Staff Harassment; legal proceedings

Table C – Risk Rating:

			CONSEQUENCES				
			Minor	Moderate	Significant	Serious	Extreme
			1	2	3	4	5
LIKELIHOOD	Almost Certain	5	Moderate	Serious	High	High	High
	Likely	4	Low	Moderate	Moderate	High	High
	Possible	3	Low	Moderate	Moderate	Moderate	High
	Unlikely	2	Low	Low	Moderate	Moderate	Moderate
	Rare	1	Low	Low	Low	Low	Moderate

2.6. Risk Owners

Risk Owners are accountable for assuring the effectiveness of controls, treatment and mitigation strategies, appropriateness of the risk rating and all associated monitor and review requirements and arrangements.

2.7. Residual Risk Treatment Strategy

The decision to accept/tolerate a residual risk and the associated exposure will consider;

- Whether the residual risk is being controlled to a level that is reasonably achievable;
- Whether it would be reasonably practicable and cost effective to further treat the residual risk; and

- Whther the residual risk is wtihin the risk appeite for risks of that type.

and would be best described as risk reduction, risk sharing/transference, risk avoidance and risk acceptance;

a. Risk Reduction

To be used when the strategy is to influence the likehood of occurence (eg reduction); or reduce the severity of loss the consequences, as appropriate, i.e. to reduce disbenefits (losses) or increase the benefits (gains). This may include emergency response, contingency and disaster recovery plans;.

b. Risk Sharing/Transference

To be used when the strategy is to share the risk with third parties through insurance and/or service providers.

c. Risk Avoidance

To be used when PA decides to eliminate the risk by withdrawing from or not becoming involved in the activity that allows the risk to be realized.

d. Risk Acceptance

To be used when PA decides to accept a particular risk because it falls within its risk-tolerance parameters and therefore agrees to accept the cost when it occurs.

Risks outside the approved Risk Appetite must be reported to Board at each meeting.

Residual Risk treatment will involve the design of controls to treat causes and the impact of consequences (e.g. business continuity plans, crisis management plans, etc.).

It will also involve deciding and recording when, by what means and by whom, control checking will take place. A number of treatment options may be considered and applied.

Selection of the most appropriate treatment option will involve Cost Benefit Analysis (CBA) where appropriate. In general, the cost of treating risks shall be commensurate with the benefits obtained.

When conducting a CBA and there is uncertainty about the costs to be incurred or benefits to be gained, the analysis should take explicitly into account that uncertainty. Where it is difficult to quantify costs (benefits or disbenefits), then a qualitative assessment will be undertaken.

Where safety, environment, legal, reputation and community requirements override simple financial cost benefit analysis, a qualitative benefit analysis will be used.

Residual Risk treatment actions will be resolved into a number of specific tasks and these will be allocated to Risk Owners who will be responsible for their timely completion.

2.8. Tool

The CEO & SMT shall document the risk assessment process through the Risk Register.

3. RISK MONITORING

3.1. Reporting

The CEO and the SMT shall assess risk ongoing as activities and strategies adapt throughout the year.

The CEO will report formally through the FARCC to the PA Board twice a year, but will raise any emerging risks outside the risk appetite with the FARCC & Board as soon as practical.

Annually, the PCI DSS environment will be fully reviewed to ensure it has been reflected in all controls and systems that protect PA cardholder and personal data.

3.2. Risk Management

All stakeholders identified as responsible during the Risk Assessment meeting as Risk Owners shall follow-up their risks to verify if the risk exposures change.