CoINVEST LIMITED ACN 078 004 985 t/as LeavePlus

POL028 [LGR002]

LeavePlus

The leave that **moves** with you

RISK MANAGEMENT FRAMEWORK (POLICY)

GOVERNANCE POLICY

CONTENTS

1. ABOUT THIS POLICY

1.1 Purpose

Effective risk management is imperative to enable the successful delivery of LeavePlus' strategic, financial, operational and compliance objectives.

This Risk Management Framework sets out how risk management informs LeavePlus' strategy, planning, policies and processes.

LeavePlus' Risk Management Framework aims to:

- Achieve the optimal balance of risk and reward and to actively manage the risks that may inhibit the achievement of the organisation's strategy;
- Assist LeavePlus Directors, Employees and Contractors to understand the organisation's risk profile and to act within risk appetite.
- Allow for the allocation of resources (human, financial, advocacy) to ensure that proper risk mitigation strategies are developed and implemented.
- Communicate the benefits of risk management and inculcate a positive risk management culture;
- Enable risk informed decision making in the management of the Construction Industry Long Service Leave Fund (**Fund**) and the Construction Industry Portable Long Service Leave Scheme (**Scheme**);
- Provide a structured and consistent approach to identifying, assessing, managing, and monitoring risks;
- Identify and describe the roles and responsibilities for managing risk across LeavePlus; and
- Provide a tool to LeavePlus Directors, Employees and Contractors which is user-friendly and can be used as an every-day reference in the performance of their duties.

1.2 Scope

This policy applies to all Directors, Employees and Contractors of LeavePlus.

1.3 Ownership and further information

The Legal and Compliance Team is responsible for developing, communicating and implementing this Policy.

1.4 Review and approval

This Policy will be reviewed biennially and approved by the Board.

Version	Policy Owner	Reviewer	Comments	Approved		Next review date
				By	Date	
2.3	Manager Governance & Risk	Chief Legal & Compliance Officer	Update of Standard, New Section 11 on GRC Platform, inclusion of Specialist Risk Registers, and minor wording & process updates.	Chief Legal & Compliance Officer	7-10-2024	

2.2	Board	Company Secretary	Update to Risk Assessment Criteria to include Information Security and incident levels in People/Safety.			
2.1	Board	Company Secretary	Update to Risk Assessment Criteria to include Member Satisfaction and update to Reputational consequence.	Board	20/2/2024	Nov 2025
2.0	Board	Company Secretary	Update of best practice, alignment of RAS and review cycle	Board	14/11/2023	Nov 2025
1.0	Board	Company Secretary	Initial policy	Board	20/09/2022	Sep 2023

2. GUIDING PRINCIPLES

The International Standard for Risk Management ISO 31000:2018 is based on 11 best practice principles. These principles underpin this Risk Management Framework and guide how risk can be effectively and efficiently managed at all levels of the organisation:

Creating and protecting value – risk management contributes to the achievement of LeavePlus' objectives and improves performance in areas such as corporate governance, project management, and health and safety of employees and visitors.

An integral part of all organisational processes – risk management is not a stand-alone activity performed in isolation. Rather, it is an integral part of our governance and accountability arrangements, performance management, planning and reporting processes.

Part of decision-making – risk management aids decision-makers to make informed choices, prioritise activities, and identify the most effective and efficient course of action.

Explicitly addressing uncertainty – risk management identifies the nature of uncertainty and how it can be addressed through a range of mechanisms, such as sourcing risk assessment information and implementing risk controls.

Systematic, structured and timely – risk management contributes to efficiency and to consistent, comparable and reliable results.

Based on the best available information – risk management draws on diverse sources of historical data, expert judgment and stakeholder feedback to make evidence-based decisions.

Tailored – risk management aligns with the internal and external environment within which we operate, and in the context of LeavePlus' risk profile.

Human and cultural factors – risk management recognises that the capabilities, perceptions and aims of people (internal and external) can aid or hinder the achievement of objectives.

Transparent and inclusive – risk management requires appropriate and timely involvement of stakeholders to ensure that it stays relevant and up to date. Involving stakeholders in decision making processes enables diverse views to be taken into account when determining risk criteria.

Dynamic, iterative and responsive to change – risk management responds swiftly to both internal and external events, changes in the environmental context and knowledge, results of monitoring and reviewing activities, new risks that emerge and others that change or disappear.

Continual improvement of the organisation – risk management facilitates continuous improvement of LeavePlus' operations by developing and implementing strategies to improve risk management maturity.

3. ABOUT RISK MANAGEMENT

Risk is defined as the effect of uncertainty on objectives. Risk is inherent in the pursuit of LeavePlus' strategic objectives and in the conduct of our business operations.

Risk Management is the process of identifying, assessing, and controlling threats to an organisation's objectives. These threats, or risks, may arise from a wide variety of sources including political and financial uncertainty, market volatility, regulatory or legal liabilities, strategic management miscalculation, human error, crime, accidents, natural disasters, IT security threats, and data related risks.

Organisations which manage risks effectively and efficiently, particularly in times of volatility and uncertainty, are more likely to achieve their objectives at a lower overall cost.

LeavePlus is committed to embedding risk management into its organisational culture, governance and accountability arrangements, planning, reporting, project management, change management, performance review and improvement processes.

Risk management at LeavePlus should be:

- Performed in accordance with the International Standard for Risk Management ISO 31000:2018;
- Carried out in accordance with the responsibilities outlined in this Policy;
- Performed on a consistent basis taking into account the Risk Appetite and Tolerances of the Board by using the approved Risk Assessment Criteria (which should be reviewed together with this document); and
- Reported to the Board and the Audit, Risk and Compliance Committee as required under this Policy.

4. RISK MANAGEMENT FRAMEWORK OVERVIEW

The Risk Management Framework at LeavePlus is comprised of the various systems, processes and people within the organisation, who operate to assess, manage, monitor and mitigate all known and reasonably foreseeable sources of internal and external risks that could have a material impact on LeavePlus' ability to achieve its objectives, including to manage the Fund and to operate the Scheme in the interests of its members and in accordance with applicable law.

The Risk Management Framework is designed to enable LeavePlus to develop and implement strategies, policies and procedures to control and manage the risks it faces as well as monitoring the residual risks it may face even after controls are implemented.

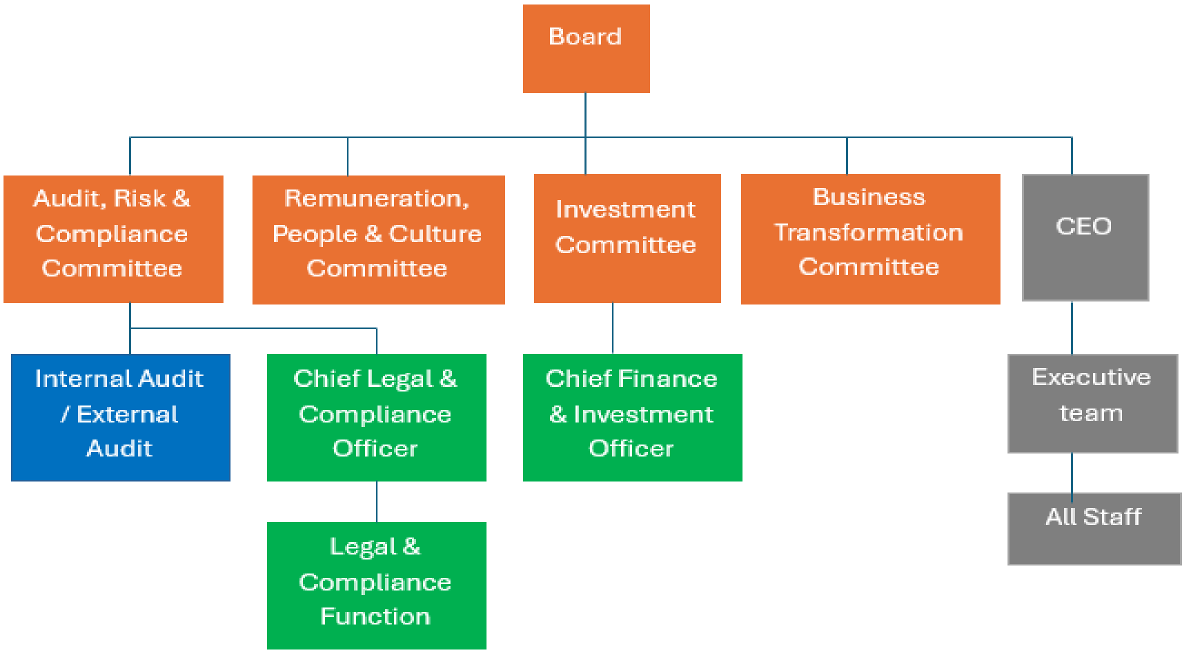
Management of risk is embedded into business as usual practices, using consistent language, approaches, documentation and tools.

5. RISK GOVERNANCE STRUCTURE

LeavePlus has adopted the three lines of defence model for risk management which sets out clear accountabilities for risk management across the organisation.

First line Management Control	Second line Risk Controls and Oversight Function	Third line Independent Assurance
All Employees and Contractors	Legal and Compliance Function	Internal Audit External Audit
• Risk ownership sits with operational line managers. • Adequate managerial control and supervisory controls are required to ensure compliance and to identify breakdowns or unexpected events. • Operational managers are responsible for: *Owning and managing risk and guiding the development of internal policies* *Implementing corrective actions to address process and control deficiencies* *Maintaining effective internal controls* *Executing risk and control procedures on a day-to-day basis* • All staff are responsible for controlling risks by using business control frameworks, internal policies and processes and adequate controls • All staff are responsible for reporting and escalating risks and issues including policy breaches and other control failures	• Second Line is designed to ensure the First Line is operating as intended. • The Governance & Risk function facilities and monitors the implementation of effective risk management practices in the following ways: *Provides the framework, training, and support for the First Line on risk and compliance* *Monitors risk management by the First Line and provides guidance and support, including on the development of policies and other internal controls* *Identifies and alerts the First Line to emerging risks and issues* *Monitors specific risks, adequacy of internal controls, reporting, compliance* • In relation to Scheme Compliance risks, managers and team leaders also have a role to play in the Second Line, by ensuring there are controls in place within the operational teams and processes that they are responsible for, to provide assurance over decision making and compliance with the Act and the Rules. • The Second Line is responsible for risk reporting to the various LeavePlus Board sub-committees and the Board, and for issues identification and escalation	• Internal Audit (IA) is established to provide the Board and Executive with assurance around: *Effective governance and risk management* *Internal controls* *How the First and Second Lines are operating* *Independent assessment of control objectives and plans* *Independent review of key business processes and functions* • LeavePlus has outsourced its IA function to RSM • The External Audit function conducts an independent assessment of the LeavePlus annual financial statements

The following diagram illustrates the key risk governance structures at LeavePlus that are in place to give effect to the three lines of defence model:


Board
Audit, Risk & Compliance Committee
Remuneration, People & Culture Committee
Investment Committee
Business Transformation Committee
CEO
Internal Audit / External Audit
Chief Legal & Compliance Officer
Chief Finance & Investment Officer
Executive team
All Staff
Legal & Compliance Function

Key

First Line of Defence
Second Line of Defence
Third Line of Defence

6. ROLES AND RESPONSIBILITIES

6.1 Board of Directors

The Board is ultimately responsible for ensuring that there is adequate and effective risk management framework in place. The Board achieves this through:

- Approval of the Risk Management and Compliance Frameworks;
- Approval and monitoring of the Board's Risk Appetite Statement;
- Regular risk and compliance reporting; and
- Establishing Committees of Directors to provide oversight of key risks, issues, policies and procedures.

6.2 Directors' Committees

The Audit, Risk and Compliance Committee, the Investment Committee, the Remuneration, People and Culture Committee, and the Business Transformation Committee have charters in place which outline the specific obligations, delegations and responsibilities of the respective committees.

The Audit, Risk and Compliance Committee has specific responsibility for monitoring and reporting to the Board on the maintenance of an effective risk management capability and ensuring that all "High" and "Very High" risks associated with LeavePlus' objectives are effectively managed.

The Investment Committee has specific responsibility for monitoring and reporting to the Board on investment related risks.

The Remuneration, People and Culture Committee has specific responsibility for monitoring and reporting to the Board on people related risks.

The Business Transformation Committee has specific responsibility for monitoring and reporting to the Board on risks relating to the delivery of Project Elevate, being the business transformation project being undertaken by LeavePlus.

6.3 Chief Executive Officer (CEO) and Executive Team

The Executive Team, led by the CEO, is responsible for promoting a strong risk and compliance culture and demonstrating a commitment to prudent risk management. The Executive Team will:

- Collectively consider risk in relation to key business decisions and hold each other to account through constructive challenge;
- Monitor key risk and performance measures in relation to their function, respond to issues and escalate to the CEO, Committees or the Board (as appropriate); and
- Ensure their function has the necessary capacity and capability to appropriately manage risk.

6.4 Risk Owners

Risk Owners are typically a General Manager and member of the Executive team, a manager of a business unit who is delegated accountability for managing certain risks and controls, or in certain circumstances a subject matter expert.

In fulfilling their responsibilities Risk Owners must:

- Implement the Risk Management Framework within their business unit or area of responsibility / expertise;
- Identify, assess and manage the risks that they have responsibility for and establish and maintain controls that act to reduce the risk levels and ensure controls are in place and operating effectively, in accordance with the requirements of this Policy;
- Ss required, put in place and ensure completion of risk action plans to respond to risks that they are responsible for that are outside of the desired risk tolerance;
- Report incidents, issues or breaches in accordance with this Policy and the Compliance Management Policy and escalate as appropriate; and
- Respond to and action any findings identified by internal or external audit.

6.5 Employees and Contractors

All employees and contractors have responsibilities for risk management.

They must:

- Understand the risks as they relate to their roles and functions, and be aware of how to manage and escalate appropriately; and
- When performing their duties, complying with all frameworks, policies, procedures and processes and escalating any breach or incidents on becoming aware of them.

6.6 Legal and Compliance function

Legal and Compliance Function, led by the Chief Legal & Compliance Officer and Manager Governance & Risk, are responsible for:

- Establishing and maintaining an effective risk management framework and reporting to the Audit, Risk and Compliance Committee, the Investment Committee, the Remuneration, People and Culture Committee, the Business Transformation Committee and to the Board, as appropriate;

- Developing risk capabilities in the business through training, education, advice and guidance including conducting risk workshops to support risk identification and evaluation;
- The relationship management with Internal Auditors and facilitating the work done by the internal audit function through co-ordinating audit activities within the business and providing input into the planning and scope of audits; and
- Providing technical support and where appropriate, effective challenge to the Executive Team, Committees and Board.

6.7 Auditors

The External Auditor and Internal Auditor roles are fulfilled via independent external appointments. These functions are required to perform an independent analysis and review of key business processes, controls and efficacy of the Risk Management Framework. The External and Internal Auditors have direct access to Committees and to the Board, as required.

7. KEY COMPONENTS OF THE RISK MANAGEMENT FRAMEWORK

Best practice sets out the following as the required key components of the Risk Management Framework:

1. Risk Management Policy & Plan;
2. Risk Appetite Statement;
3. Strategic and Business Plans;
4. Designated Risk Management Function;
5. Risk Register;
6. Risk System;
7. Attestation;
8. Risk Culture Assessment;
9. Workshops and Training; and
10. Review Process.

7.1 Risk Management Policy and Plan

This document sets out the required policy and planning elements for risk management at LeavePlus.

7.2 Risk Appetite Statement

Through this Risk Management Framework and its supporting processes, the Board of LeavePlus formally establishes and communicates its **Risk Appetite Statement**. That is, its willingness to take or expose the organisation to various risks, guiding Directors, Employees and Contractors in their actions and ability to accept and manage risks.

Understanding the Board’s appetite and tolerances for risk is critical to setting the risk management tone within LeavePlus and this enabling Risk Management Framework.

The Board monitors the environment in which LeavePlus operates and will adjust the Risk Appetite Statement as appropriate.

7.3 Strategic and Business Plan

LeavePlus considers that effective management of risk is integral to achieving its purpose.

Risk is defined as the effect of uncertainty upon objectives.

LeavePlus conducts strategic and business planning processes to define its objectives over the short and longer terms. Understanding of these objectives drives the risk management process.

Relevant plans are developed, approved, promulgated and referenced this document.

7.4 Designated Risk Management Function

The Manager Governance & Risk together with the broader Legal and Compliance team performs the Second Line of Defence activities with respect to risk management.

7.5 Risk Register

The Risk Register records details of the risks identified by Risk Owners and endorsed by the Executive Team. These risks are assessed in terms of the likelihood of occurring and the consequence if they happen.

The Risk Register also contains details of the controls and responsibilities which have been put in place to mitigate the risks and to lower the overall risk profile of LeavePlus.

The Risk Register is divided into various parts: Strategic Risk Register, Operational Risk Register, Project Risk Register, and Specialist Risk Registers.

Strategic Risk Register

Strategic Risks are risks that affect LeavePlus as a whole and relate to LeavePlus' ability to meet its objectives as outlined in its 2022-2025 Strategic Plan (objectives are linked to four focus areas: Member Experience, People & Culture, Manage and Administer the Fund; Systems, Processes and Governance).

Strategic Risks respond to challenges that might cause a particular strategy to fail, as well as any major risks that could affect LeavePlus' long-term positioning and performance. The management of these risks is crucial to the continued viability of LeavePlus and the Fund.

The status of Strategic Risks is reported to the Audit, Risk and Compliance Committee on a quarterly basis or more often as required. Investment and People Risks are also reported to the Investment Committee and Remuneration, People & Culture Committee respectively at their meetings.

The Strategic Risk Register must be reviewed annually by the Board and updated in line with the external context as well as the latest Strategic Plan and annual Business Plan.

Operational Risk Register

Operational Risks are risks that may affect LeavePlus' operations in a way that is not necessarily damaging to the organisation as a whole, but which may hinder its ability to achieve its objectives.

Operational risk can emanate from internal or external sources. Internal sources of risk can arise from people (e.g., poor training, errors, fraud) and processes (e.g., poor maintenance, accidents, and mishaps). Types of Operational Risk include: Occupational Health & Safety, Physical Risk, Security, Technology Risk (including cyber-crime), and Human Capital risks.

Operational risks are managed at the Extended Leadership team level.

Operational risks that are rated "High" or "Extreme" are also reported to the Audit, Risk and Compliance Committee on a quarterly basis or more regularly as required.

Project Risk Register

Project Risks are risks that may cause a particular project to fail, or which may hinder the delivery of the stated objectives of the project.

A risk assessment must be undertaken for all LeavePlus projects managed through the Project Management Office. Risks are managed by the relevant Project Manager and may vary in significance based on the project.

Specialist Risk Registers

Risks that may affect particular areas of the business or its operations may be captured and managed in specialist risk registers. These could cover items such as IT Security, Physical Security, OHS, Field Officers and the like.

7.6 Risk System

The Risk System is the process undertaken by LeavePlus in line with the International Standard for Risk Management ISO 31000:2018 to identify, analyse, evaluate and treat risks so that LeavePlus remains within the risk appetite set by the Board. The Risk System is outlined in detail in **Section 8** below.

7.7 Attestation

At the end of each financial year, Risk Owners are required to self-assess and attest to the operating effectiveness of the controls managing all risks in their business unit or area of responsibility.

7.8 Risk Strategy and Risk Culture Assessment

LeavePlus has implemented a Risk Culture Assessment process covering 10 elements to support its strategy to become a risk informed organisation. These 10 dimensions to be progressively assessed are as follows:

RISK BEHAVIOR

1. **Leadership**

Leaders at every level deliberately and consistently champion risk management, setting a clear tone and role-modelling appropriate risk behaviours to instil the desired risk culture throughout the entity.

2. **Decision-Making and Challenge**

There is a demonstrated willingness to proactively consider diverse viewpoints and to give and receive constructive challenge across the entity.

3. **Communication and Escalation**

Risk issues are openly communicated across the entity, supported by an environment where people feel safe to speak up without fear of retribution.

4. **Risk Capabilities**

The level of skills and learning, well-being, processes, systems and data across the three lines of defence support effective risk management practices and behaviours.

5. **Alignment with Purpose and Values**

The entity's espoused Purpose and Values promote and support good risk management practices and behaviours.

RISK ARCHITECTURE

6. Risk Culture Assessment and Board Oversight

The Board has a robust approach for overseeing the assessment of risk culture in order to form a view, identify desirable changes and ensure steps are being taken to address these changes.

7. Risk Appetite and Strategy

Business and strategic decisions align with the Risk Appetite Statement.

8. Risk Governance and Controls

Across the entity there is effective oversight of risk, and risk management is supported by appropriate risk frameworks, policies, controls and reporting.

9. Responsibility and Accountability

Responsibilities and accountabilities for risk are clearly understood, embraced and discharged across the three lines of defence.

10. Performance Management and Incentives

Good risk management behaviour is rewarded, and poor risk behaviour has proportionate consequences.

7.9 Workshops and Training

The Legal and Compliance team must provide on an annual basis or as required:

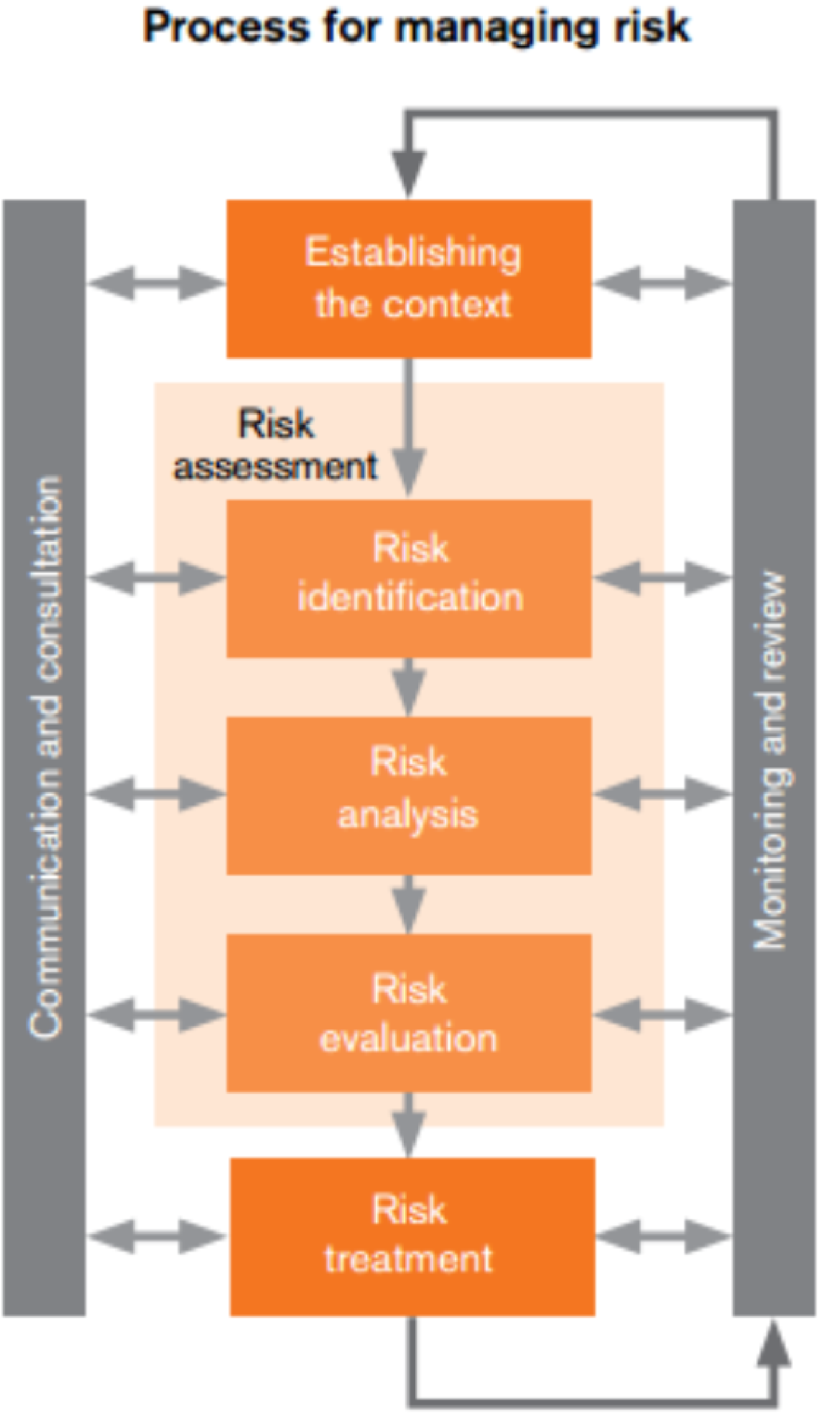
- Training for new Risk Owners;
- Refresher training to all Risk Owners; and
- A Risk Management Workshop for the Leadership Team.

7.10 Review process

A review process is required to ensure that the Risk Management Framework is effective in identifying, measuring, evaluating, monitoring, reporting and controlling or mitigating material risks.

8. RISK SYSTEM

The process for managing risk at LeavePlus follows the Australian Standard and is described as follows:



8.1 Risk Identification

Risk identification defines the “risk” problem and provides insight into “uncertainty” and the possible effect on the achievement of objectives.

The Legal and Compliance team will facilitate a workshop with the Extended Leadership Team, at least annually (and more frequently if material risks or risk appetite changes) to review the Risk Register and to consider whether all material risks have been identified.

8.2 Risk Analysis and Evaluation

These are separate steps in the Risk System process but are usually undertaken together.

Risks will be analysed to:

- Identify the source and cause;
- Assess current controls, effectiveness, and determine gaps;
- Determine the potential impact(s) and consequence levels;
- Determine how likely that impact is; and
- Determine the risk rating = impact (consequence) x likelihood.

Risks will be evaluated to:

- Escalate to necessary reporting levels;
- Prioritise risks;
- Consider options;
- Decide what action is required; and
- Identify resources required.

Risks must be assessed in line with LeavePlus’ Risk Assessment Criteria (see below). LeavePlus will assess all risks by applying a rating to the risk that identifies the probability of the risk occurring and the impact to LeavePlus if the risk is realised. Consequence and likelihood scales and a matrix are in place and included in the risk register and incident and breach register.

Risk Owners must consider the **inherent risk** as well as the **residual risk** after taking into account the controls in place to modify the risk.

Considering both the design and operating effectiveness of controls is a critical aspect of the risk management process. Multiple controls may exist and some will be more important or effective than others. Failure of controls could lead to an undesirable event.

Key questions that a Risk Owner should consider include:

- What are the current control(s) in place that would reduce this risk?
- Why is this control important in reducing this risk?
- How effective is the control at reducing this risk?
- Who is going to assess whether the control is effective?

Control effectiveness can be assessed as either:

- Effective
- Partially Effective
- Ineffective

After the controls have been identified, assessed and rated, a decision can be made as to whether additional controls are required.

9. RISK ASSESSMENT CRITERIA

9.1 Consequence

Level	Financial	Information Security	Service Delivery	Member Satisfaction	Project / Initiative	Reputational / Political	People / Safety	Compliance / Conduct
Severe	**Accrued funding ratio** of <100% Floor - ratio of >135% **Potential unplanned operating cost** of >$50M	Virus or Malware affecting multiple sites and NOT contained. Multiple failures in infrastructure including failures within DR capability. Manual recovery required. Successful Hack, multiple systems compromised.	Loss of major service or critical business system for >10 working days Data breach affecting >10% members	Severe widespread member dissatisfaction evidenced by level of complaints across all member classes Severe widespread adverse social media or mainstream media commentary by members >1 member complaint to a regulator resulting in regulatory investigation	Greater than 50% change in cost, time, or scope Risk of primary intended benefits of significant projects or initiatives not being realised	National negative media coverage Total loss of confidence from Government or broader industry Fraud or theft that results in: • Widespread negative perception affecting the LeavePlus' overall reputation • Significant media scrutiny and public outcry • Requires immediate and comprehensive reputation recovery efforts • Potential for long-term damage to public trust and relationships	One or more deaths or injuries that include lifetime disabilities Multiple key staff leave within a short period of time Extremely high 12-month rolling voluntary staff turnover (>30% all staff, >50% frontline) Any actual incident requiring immediate emergency services.	Significant breach with prosecution and/or significant fines Investigation by a regulatory or audit body that could lead to prosecution and/or significant fines Serious civil litigation >$5M or Class actions
Major	**Accrued funding Ratio** between 105%-101% Floor – ratio between 125%-134% **Potential unplanned operating cost** of $10M-$50M	Virus or Malware affecting multiple sites and NOT contained. Multiple failures in infrastructure components requiring activation of DR Plan. Uncontained DDOS attack. Web servers defaced and compromised. Successful Hack, single system compromised.	Loss of major service or critical business system for 5-10 working days Data breach affecting 5%-10% of members	Significant widespread member dissatisfaction evidenced by level of complaints specific to a member class Significant widespread adverse social media or mainstream media commentary by members 1 member complaint to a regulator resulting in regulatory investigation	Greater than 20-50% change in cost, time, or scope Risk that most benefits of significant projects are not realised	State-wide negative media coverage. Significant relationship difficulties with Government or industry categories. Fraud or theft that results in: • Significant negative attention from multiple stakeholder groups. • Tangible harm to the LeavePlus' reputation. • Requires a comprehensive reputation management strategy and communication plan. • Possible legal or regulatory repercussions	Injury involving long-term hospitalisation and significant rehabilitation (significant lost time) Some key staff leave within a short period of time Very low staff morale and/or very high 12-month rolling voluntary staff turnover (20-30% all staff, 40-50% frontline) Any incident requiring emergency services.	Major breach of regulation with significant penalties. Civil litigation $1-5M Adverse finding by a regulatory or audit body. Compliance breaches indicate a systemic or cultural failure.

Level	Financial	Information Security	Service Delivery	Member Satisfaction	Project / Initiative	Reputational / Political	People / Safety	Compliance / Conduct
Moderate	**Accrued funding ratio** between 109%-106% Floor – ratio >120% **Unplanned operating cost** of $3M-$10M	Virus or Malware affecting multiple sites. Has been contained. Single infrastructure component failure, or multiple components operating in degraded state. Contained DDOS attack or Web defacement. Unsuccessful Hack. Information loss 100 to 250 records.	Loss of major service or critical business system for 1-5 working days Data breach affecting 2%-5% members	Moderate broad-based member dissatisfaction evidenced by level of complaints within a specific member class Moderate broad-based adverse social media or mainstream media commentary by members	A 10-20% change in cost, time, or scope Risk that some key benefits of significant projects or initiatives are not realised	Some negative attention from local media Moderate adverse attention from or disengagement by Government or Industry. Fraud or theft that results in: • Noticeable impact on public perception within certain stakeholder groups. • Requires proactive communication and targeted reputation management efforts. • Potential for some negative media coverage	Medical treatment required with a period of rehabilitation (some lost time) Low staff morale and/or moderate 12-month rolling voluntary staff turnover (15-20% all staff, 30-40% frontline). Staff grievances requiring external resolution (e.g. Fair Work Commission) Any perceived incident requiring emergency services.	Serious breach of regulation with investigation or report to regulator. Potential for prosecution and/or moderate penalties.
Minor	**Accrued funding Ratio** between 114%- 110% **Unplanned operating cost** of <$3M	Virus or Malware affecting multiple machines but contained. Single infrastructure component degraded but functional. Information loss <100 records.	Loss of a minor service or non-critical business service for >5 days Loss of a major service or critical business system for up to 1 working day Data breach affecting 0.5%-2% members	Some member complaints Some adverse social media or mainstream media commentary by members	A 1-10% change in cost, time, or scope Risk that some key benefits of significant projects or initiatives are delayed or deferred	Low level mention or interest in local media, quickly remedied Fraud or theft that results in: • Some negative attention from specific stakeholders. • Limited impact on overall reputation. • Can be resolved with relatively minor corrective actions	Minor injury / health effects (lost time injury or restricted work <5 days lost) Some voluntary staff turnover on a 12-month rolling basis (<15% all staff, <30% frontline) Series of staff complaints managed internally Any minor incident requiring P&C and / or Executive assistance.	Reportable incident to regulator, no follow up Minor breach

Level	Financial	Information Security	Service Delivery	Member Satisfaction	Project / Initiative	Reputational / Political	People / Safety	Compliance / Conduct
Insignificant	**Potential unplanned cost** can be dealt with within budgets	Virus or Malware on a single machine. No impact in core infrastructure. No evidence of information loss.	Loss of a minor service or non-critical business system for <1 working day Data breach affecting less than 0.5% members	Isolated member complaints Isolated social media or mainstream media commentary by members	<1% change in cost, time, or scope Risk that secondary / ancillary benefits of significant projects or initiatives are delayed	Issues resolved as part of normal internal management process No media interest Fraud or theft that results in: • Minimal impact on public perception. • Limited awareness or concern among stakeholders. • Easily addressable and correctable without significant public attention	Near misses, first-aid or minor medical treatment Isolated staff complaints Minor incident requiring no intervention or colleague / manager support.	Not reportable to regulator

9.2 Likelihood

Rare	Unlikely	Possible	Likely	Almost Certain
The event may occur only in exceptional circumstances, never heard of in industry Once in a 30-year period Less than 5% chance of occurring within a project	The event could occur at some time, heard of in the industry Once in a 10-year period 5-30% chance of occurring within a project	The event may occur at some time May occur once in a 3-year period 30%-70% chance of occurring within a project	The event will probably occur in most circumstances May occur at least annually 70%-90% chance of occurring within a project	The event is expected to occur in most circumstances Will occur several times a year to monthly 90%-100% chance of occurring with a project

9.3 Risk Rating

Consequence					
Severe	High	High	High	Extreme	Extreme
Major	Medium	Medium	High	Extreme	Extreme
Moderate	Low	Medium	Medium	High	High
Minor	Low	Low	Medium	Medium	High
Insignificant	Low	Low	Low	Medium	Medium
	Rare	Unlikely	Possible	Likely	Almost Certain
	Likelihood				

9.4 Risk Treatment

Risk treatment strategies (mitigation actions) identified in the risk register may include:

- Acceptance of the risk, where the impact of the risk is neither material nor sufficiently cost effective to treat;
- Controlling or reducing the likelihood of the risk through the implementation of documented policies, procedures, checklists, monitoring and reporting and responding;
- Transferring the risk through insurance, where applicable or to other parties through service agreements;
- Mitigation of risk and reduction or risk consequences by implementation of plans and guides, such as the Business Continuity Plan (BCP);

- Avoidance of activities or events that would give rise to risks of an unacceptable level; and
- Modification of a risk through modification of an activity thus reducing/removing any unacceptable risks.

9.5 Risk Treatment Plan

Where a risk has been identified outside the Board's risk appetite or tolerance, a Risk Treatment Plan must be completed to outline the proposed action to be taken to further manage the risk. The Risk Treatment Plan should outline:

- The target risk rating;
- The specific actions which are to be taken to move the risk towards the target risk rating;
- The responsible person;
- Identify a time for completion;
- Date for future review;
- Any resources required for the response/treatment; and
- Future actions for reporting and monitoring.

The table below outlines the timeframes for a required Risk Treatment Plan is needed and the monitoring frequency for those treatment plans:

Residual Risk Rating	Treatment
Extreme	Action plan(s) must be established within 1 week and action progress reviewed at least monthly
High	Action plan(s) to be established for any risk with a control effectiveness of less than strong, within 1 month. Risk is reviewed at least quarterly.
Medium	Consider action plans for controls rated less than strong. Must be reviewed annually.

10. RISK REPORTING AND MONITORING

The following reporting regime must be adhered to at LeavePlus on a continuous basis:

- The Strategic Risk Register must be reviewed annually by the Board and updated in line with the external context as well as the latest Strategic Plan and annual Business Plan.
- Status and Risk Treatment Plans for all "High" and "Extreme" risks reviewed by the Executive are to be reported to the appropriate Board Committee;
- Quarterly Risk Reporting to the Audit, Risk and Compliance Committee (comprising the Strategic Risk Register and extracts of other Risk Registers, as appropriate);
- Monthly review of outstanding Internal Audit actions and Risk Treatment Plans by the Executive; and
- Risk workshops conducted with the Extended Leadership Team at least annually or more often as required.

Extended Leadership Team members should discuss any material changes to all "High" and "Extreme" rated risks in their business unit or area of responsibility with the Legal and Compliance team once they are aware of the change. Any other concerns related to risks should be addressed with a member of the Legal and Compliance team at the earliest convenient time.

11. GRC (GOVERNANCE RISK & COMPLIANCE) PLATFORM

LeavePlus has implemented a GRC Platform (Drova) as its enabling technology for capturing, documenting and maintaining its risks & controls, its compliance obligations, its KRI's, relevant registers and associated governance, risk and compliance activities.

It is used to provide relevant reports to all levels of the LeavePlus business.

The Manager Governance and Risk is the owner of the GRC Platform

12. KEY TERMS

Control: An activity or action (process, policy or procedure) that 'controls' a risk materialising or prevents a breach of a compliance obligation.

Breach or Incident: A breach of internal policies, processes or regulatory or legal obligations. A control failure or process or procedural issue which requires attention and potentially the implementation of additional controls.

Risk Appetite: The type and amount of risk LeavePlus is willing to accept to achieve its strategic plan and business objectives. LeavePlus' risk appetite is set out in the Risk Appetite Statement.

Risk Register: A register of identified and assessed risks (strategic, operational, project, specialist). The register also includes the controls and treatment plans (where applicable).

Inherent Risk: The amount of risk that exists in the absence of controls.

Residual Risk: The amount of risk remaining after controls and mitigation strategies are accounted for.

13. RELATED INFORMATION

13.1 Codes and Better Practice

ISO 3100:2018 Risk Management.

13.2 Related Policies and Procedures

- Board Charter [POL034]
- Audit, Risk and Compliance Committee Charter [POL038]
- Investment Committee Charter [POL037]
- Remuneration, People & Culture Committee Charter [POL039]
- Business Transformation Committee Charter [POL030]
- Internal Audit Plan (Strategic Internal Audit Plan)
- Policy Development Framework Policy [POL027]
- Compliance Management Framework [POL038]
- Risk Appetite Statement [POL029] and Strategic Risk Register
- Incident and Breaches Register
- Strategic and Business Plans.