Risk Management Policy

November 2022

Steadfast
THE STRENGTH YOU NEED

Contents

1. INTRODUCTION

The *Australian New Zealand Risk Management Standard (AS/NZS ISO 31000:2018)* defines risk management as "coordinated activities to direct and control an organisation with regard to risk".

The standard defines "risk" as the effect of uncertainty on objectives.

Both likelihood and consequences must be considered in assessing risk.

Risk arises in all aspects of the Company's operations and at all stages within the lifecycle of those operations. It offers both opportunity and threat, and must therefore be managed appropriately.

This policy confirms Steadfast's aim to adopt a strategic, consistent and structured enterprise-wide approach to risk management in order to achieve an appropriate balance between realising opportunities for gains and minimising losses. The policy reflects the *AS/NZS ISO 31000:2018* which provides the overall framework for risk management for the Company.

Risk management involves establishing an appropriate risk management infrastructure and culture, and applying logical and systematic risk management processes to all stages in the lifecycle of any activity, function or operation. By minimising losses and maximising gains, risk management enables the Company to best meet its organisational objectives.

2. POLICY INTENT

Risk management is an integral part of sound management practice and an essential element of good corporate governance, as it improves decision-making and enhances outcomes and accountability.

The aim of this policy is to ensure that the Company makes informed decisions with respect to the activities that it undertakes by appropriately considering both risks and opportunities.

The application of this policy and related framework will provide the basis for:

- more confident and rigorous decision-making and planning;
- better identification of opportunities and threats;
- pro-active rather than re-active management;
- improved incident management and reduction in loss and the cost of risk, including insurance premiums;
- improved stakeholder confidence and trust;
- a clear understanding by all staff of their roles, responsibilities and authorities for managing risk;
- better corporate governance; and
- development of a more risk aware organisational culture through enhanced communication and reporting of risk.

3. POLICY PRINCIPLES

3.1 Risk Overview

The Board is responsible for approving and reviewing the Company's risk management strategy and policy. The day to day aspects of risk and the implementation of mitigation measures is the responsibility of management.

The Board is also responsible for exercising due care, diligence and skill in relation to the Company in the areas of:

- integrity of financial and external reporting;
- external auditor's activities, scope and independence;
- management processes for the identification of significant business risks and exposures and reviewing and assessing the adequacy of management information and internal control structures; and
- whether the company is adequately managing risk relating to corporate governance and is maintaining appropriate controls against conflicts of interest and fraud.

The Board will overview management's application of the ASX Corporate Governance Council's principles and recommendations in respect of financial reporting and risk oversight.

3.2 Risk Management Approach

Steadfast's risk management approach is a continuous process aimed at ensuring the Company's strategic objectives are maintained.

The Board has responsibility for overseeing management's processes in identifying, assessing and monitoring risks associated with the Company's business operations and the implementation and maintenance of policies and control procedures to give adequate protection against key risks.

In determining the risk appetite of the Company, the Board has determined that the Company has a moderate tolerance for taking risk. Where Steadfast enters into a transaction or acts on a particular decision, the risks are justified by greater rewards and action taken to mitigate the exposure to risk. While Steadfast is willing to take on a moderate level of risk, Steadfast remains risk aware. As a result, management has incorporated risk management into strategic planning and decision making to understand and prioritise the management of material business risks.

Risk appetite is documented in Steadfast's *Risk Appetite Statement and measured quarterly by use of a scorecard*.

Risks will be managed according to the risk management framework detailed in *AS/NZS ISO 31000:2018* - displayed in Section 4 of this policy.

The risk management and internal control systems within the Company encompass all policies, processes, practices and procedures established by management and/or the Board to provide reasonable assurance that:

- established corporate and business strategies and objectives are achieved;

- risk exposure is identified and adequately monitored and managed;
- resources are acquired economically, adequately protected and managed efficiently and effectively in carrying out the Company's business;
- significant financial, managerial and operating information is accurate, relevant, timely and reliable; and
- there is an adequate level of compliance with policies, standards, procedures and applicable laws and regulations.

3.3 Roles and Responsibilities

3.3.1 Board of Directors

- champion the Company's governance and risk management processes;
- determine the Company's risk appetite and tolerance;
- establish an Audit & Risk Committee and provide the Committee with adequate direction;
- review recommendations from the Audit & Risk Committee and determine future actions; and
- publicly report and make the necessary disclosures relating to risk as required.

3.3.2 Audit & Risk Committee

- to monitor the adequacy of the risk management framework and satisfy itself that the Group is operating with due regard to the risk appetite set by the Board including satisfying itself that the risk management framework deals adequately with contemporary and emerging risks such as conduct risk, digital disruption, cyber-security, privacy and data breaches, sustainability and climate change;
- it is noted that where from time to time circumstances dictate that the Group needs to operate outside the current risk appetite set by the Board, the matter should be brought to the attention of the Board;
- review management's approach to the management of risks, (including economic dependency, the adequacy of insurance arrangements, business continuity planning, regulatory compliance, subsidiary compliance, reputational and exposures to movements in premium and commission rates);
- to assess whether audit plans developed by the internal and external auditor are consistent with the financial and operating risks facing the organisation;
- management to provide the Committee with the Risk Appetite Statement for approval each year in November;
- to oversee the preparation of a summary of the main internal and external risk sources that could adversely affect the Group's prospects for future financial years, for inclusion in the operating and financial review section of the directors' report;
- to review and assist management's approach to ensuring that there are adequate procedures in place to manage the risks associated with subsidiaries;

- to annually review and make recommendations to the Board in relation to the Risk Management Policy; and
- to assess whether the Group has any material exposure to economic, environmental and social sustainability risks and recommend to the Board how to manage those risks.

3.3.3 Managing Director & CEO/Senior Management

- develop the Company's strategic risk profile by identifying and prioritising material business risks;
- review the Company's risk profile periodically;
- review and assess the current and planned approach to managing material business risks;
- review and monitor the status of risk treatment strategies;
- periodically report on material business risks to the Board/Audit & Risk Committee; and
- implements the risk management framework across the different areas of operations.

3.3.4 Managers and Supervisors

- monitor the material business risks for their areas of responsibility;
- provide suitable information on implemented treatment strategies to senior management to support ongoing reporting to the Board; and
- check staff are adopting the Company's risk management framework as developed and intended.

3.3.5 Chief Risk Officer

- coordinates the implementation of the risk management framework, risk profile and treatment strategies;
- facilitates, challenges and drives risk management development within the Company; and
- reports to the Chief Executive Officer, senior management, executive management and Audit & Risk Committee at regular intervals on the risk management process.

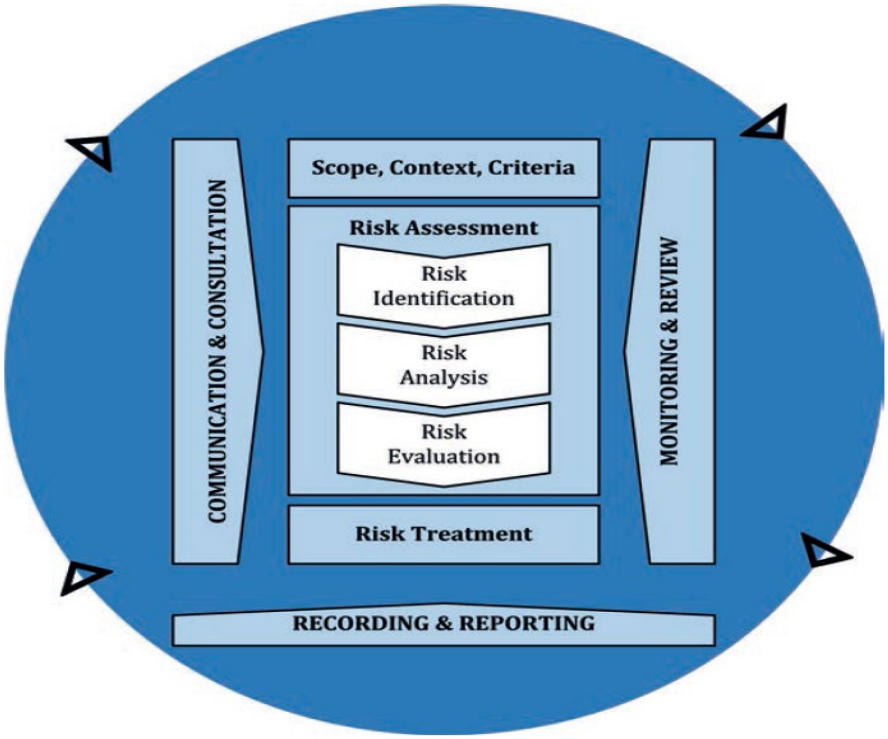
3.3.6 Individual staff

- recognise, communicate and respond to expected, emerging or changing material business risks;
- contribute to the process of developing the Company's risk profile; and
- implement treatment strategies within their area of responsibility.

4. RISK MANAGEMENT FRAMEWORK

The Company's risk management framework is based on AS/NZS ISO 31000:2018.

The risk management process is illustrated by the following diagram:



* Risk Management Process - Overview, "Risk Management Guidelines Companion to AS/NZS ISO 31000:2018".

4.1 Understanding the organisation and its context

Establishing the context means the Company considers both external and internal factors when identifying and managing risks associated with the achievement of strategic and operational objectives.

- **Roles and Responsibilities**
  The Board of Directors is ultimately responsible for establishing the context for risk management at the Company level; however, this may also be performed at various other levels within the Company.

4.2 Risk Assessment

Risk assessment means the overall process of risk identification, risk analysis and risk evaluation. A risk register is used in order to assess risk.

4.2.1 Risk identification

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

4.2.2 Risk Analysis

Risk analysis means considering the range of causes, sources of risk, consequences and likelihood to produce a risk rating. The rating can then be used to determine further management by the Company.

4.2.3 Risk Evaluation

Risk evaluation means the level of risk identified during risk analysis can be ranked and prioritised according to a consistent overall ranking and rating system.

- **Roles and Responsibilities**
  The Audit & Risk Committee has delegated the preparation and maintenance of the risk register to the Chief Risk Officer. The management team plays an active role in risk assessment (i.e. risk identification, risk analysis and risk evaluation). The Audit & Risk Committee reviews the top ten current and emerging risks including the risk management strategies in place based on management's assessment.

4.3 Risk Treatment

Risk treatment means selecting one or more options for addressing risk. This involves formulating and selecting risk treatment options, planning and implementing risk treatment, assessing the effectiveness of that treatment, deciding whether the remaining risk is acceptable and if not acceptable, taking further treatment.

- **Roles and Responsibilities**
  Risk treatment is different depending on the associated risk. Therefore, each individual risk identified; where risk treatment is required, will have assigned personnel or groups responsible for carrying out the risk treatment. The Chief Risk Officer is responsible for coordinating and managing the process.

4.4 Communication and Consultation

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

- **Roles and Responsibilities**
  Communication and consultation is a continuous process evident at all levels within the risk management process. Roles and responsibilities are dependent on the specific stage or component of the framework. For example, the Board of Directors is responsible for communicating aspects of establishing the context, while the Audit & Risk Committee is responsible for communicating risk assessment. The Chief Risk Officer is responsible for coordinating and managing the process.

4.5 Monitoring and Review

Continual monitoring and review improves the quality and effectiveness of process design, implementation and outcomes.

- **Roles and Responsibilities**
  Monitoring and review is a continuous process evident at all levels within the risk management framework. Roles and responsibilities are dependent on the specific stage or component of the framework. For example, the Board of Directors is responsible for monitoring and reviewing the risk appetite of the Company and the implementation of a risk management framework, while individual personnel or groups are responsible for monitoring or reviewing their

assigned risk mitigation action plans. The Chief Risk Officer is responsible for coordinating and managing the process.

4.6 Recording and reporting

The risk management process and its outcomes are documented and reported through appropriate mechanisms.

5. Review and publication of this policy

The Board will review this policy annually. The Board may, in its discretion, adjust or exclude a specific requirement of this policy from time to time, either generally or on a case by case basis. This policy may be amended, ceased or replaced, by resolution of the Board.

A copy of this policy will be available on the Steadfast website. Key features will be published in the corporate governance statement.

November 2022