Enterprise Risk Management Policy

Policy Owner: Chief Financial Officer

Version: June 2023

Table of Contents

1. INTRODUCTION

The Board of Directors (**Board**) and Executive Management of Cleanaway (the **Company**) are committed to the establishment of a sound system of risk oversight, management, and internal control.

Our growth and success depend on our ability to understand and respond to the challenges of an uncertain and changing world. This uncertainty generates risk, with the potential to be a source of both opportunities and threats. By understanding and managing risk, we provide greater certainty and confidence for all our shareholders.

2. ERM METHODOLOGY

This Policy requires that Cleanaway adopt and implement an Enterprise Risk Management (ERM) Methodology based on adherence to the International Standard on Risk Management, ISO 31000:2018. Adoption of a robust methodology as the basis for the development of all mandated risk registers supports our desire to operate within a sound system of risk oversight and management.

In accordance with this Policy, the Methodology must be reviewed at least annually, which aligns with the *ASX Corporate Governance Council Corporate Governance Principles and Recommendations* (Recommendation 7.2) that the Board or a Committee should:

a) review the entity's risk management framework (methodology) at least annually to satisfy itself that it continues to be sound, and that the entity is operating with due regard to the risk appetite set by the board; and

b) disclose, in relation to each reporting period, whether such a review has taken place.

A disclosure confirming compliance with this Policy and Recommendation 7.2 is provided to the Audit & Risk Committee annually.

3. RISK APPETITE

Cleanaway's appetite and tolerance to risk is articulated in a Risk Appetite Statement (RAS). In accordance with this Policy the RAS must be reviewed at least annually.

The RAS is documented in the Corporate Risk Register in accordance with the following process:

- Appetite is set depending on the nature of the risk – People, Earth, Markets, Assets or Financials. Under each of these categories various sub risks are identified and a risk appetite is set for each unique category.
- CWY has identified three levels of risk tolerance, cautious, balanced, or elevated. The current risk tolerance level is assessed for each sub-category of risk. In addition, the Company has identified a target risk tolerance. Where the current risk tolerance varies from the target, actions to bring it within the desired appetite are included in the Corporate and Functional Risk Registers.

4. RISK REGISTERS

Strategic Risks

The Policy requires that strategic risks are captured and managed in the Corporate Risk Register, Health & Safety Risk Register or the Environment Risk Register as follows:

Corporate Risk Register

In accordance with this Policy a **Corporate Risk Register,** developed in accordance with the **ERM Methodology** must be maintained which identifies and manages those risks that have the capability of affecting achievement of the Cleanaway's strategy and goals.

Health & Safety and Environment Risk Registers

These registers identify those risks that have the capability of breaching our Health, Safety or Environment Absolutes. Health, Safety and Environment Absolutes are the foundation on which Cleanaway operates in pursuit of its strategic objectives.

Risks captured within the Health, Safety or Environment risks registers are not duplicated in the Corporate Risk Register.

The Reporting Obligations outlined in Section 5 apply to the Corporate, Health & Safety and Environment Risk Registers.

Functional and Business Unit Risk

Risk may also be identified and managed at a functional level or business unit level. These risks are managed as follows:

Functional / Business Unit Risk Registers

Identify and manage risks specific to a function or business unit. Such risk registers are managed by the functional Head / General Manager and are overseen by the relevant Executive General Manager.

To the extent that a risk identified at a functional or business unit level may have the capacity (singularly or collectively) to impact on the achievement of a strategic objective they will be discussed and if it is agreed the risk meets the criteria for inclusion, it will be captured in the Corporate Risk Register. This is to ensure they are afforded the rigor imposed by Cleanaway's ERM methodology.

Where a functional risk register is **not** maintained management and the Executive General Manager must ensure that risks within the function that have the capacity to impact on the achievement of strategic goals and objectives or health, safety or environment Absolutes are appropriately captured in the applicable Corporate, Health & Safety or Environment Risk Register.

Site and Operational Risks

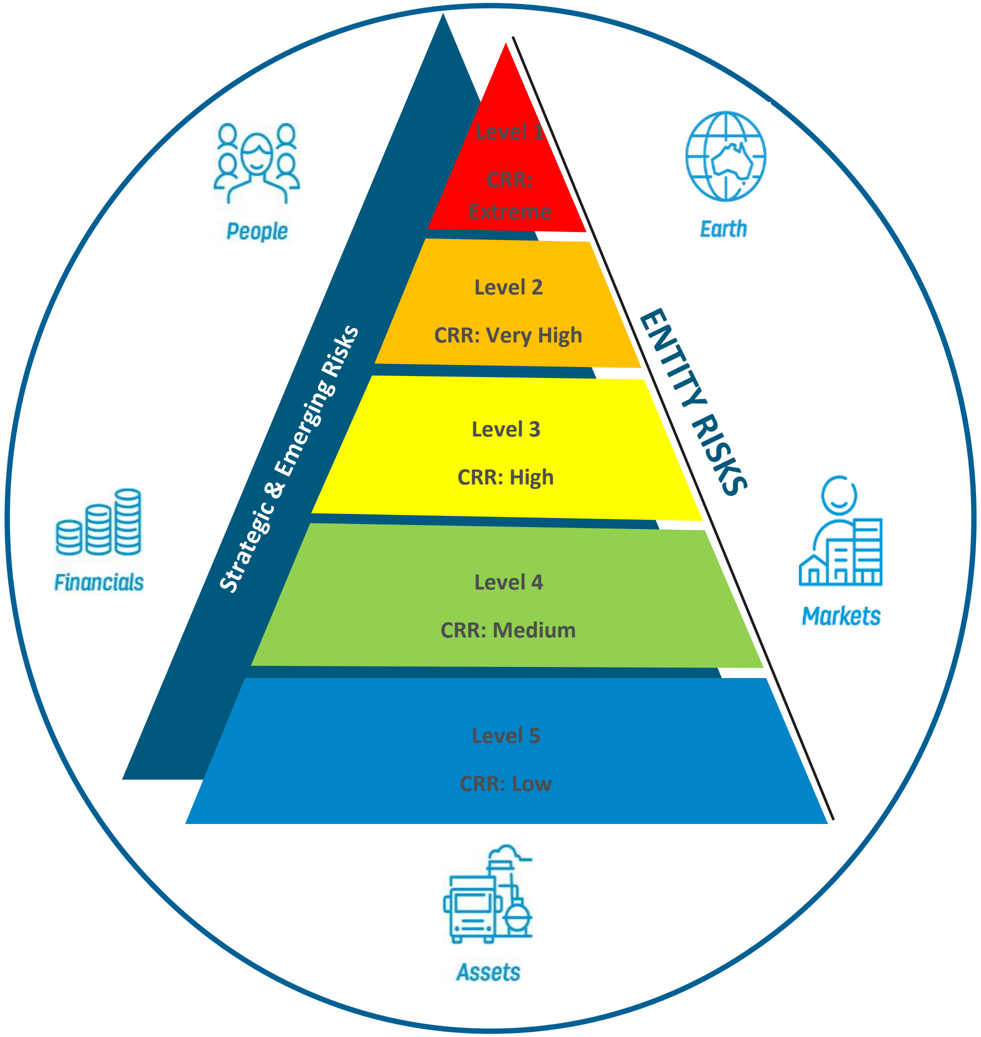
Risks at site level are captured via site risk registers or as part of Cleanaway's *Visual Management Board* methodology.

Diagram 1 Risk Structure

Key Definitions

- **Strategic Risks:** uncertainties or possible events (positive or negative) that could affect Cleanaway’s ability to achieve its strategic objectives.
- **Emerging Risks**: a new risk, or a familiar risk in a new or unfamiliar context.
- **Entity Risks**: uncertainties or possible events that might impact the achievement of a business’ objectives. The impact may be positive or negative.
- **CRR**: Current Residual Risk Rating

Risk Structure



Governance

Strategic, Emerging & Level 1 Risks

- Board (oversight)
- Executive Team (accountability)

Level 2 Risks

- Executive Team (oversight)
- Executive General Manager (accountability)

Level 3 Risks

- Executive General Manager (oversight)
- General Manager (accountability)

Level 4 Risks

- General Manager (oversight)
- Regional Manager (accountability)

Level 5 Risks

- Regional Manager (oversight)
- Branch Manager (accountability)

5. REPORTING

At a minimum the following reporting obligations are required in accordance with this Policy.

- Status of risks, controls, and risk treatment plans, as contained in the functional and corporate risk register will be reported upon as appropriate via the Monthly Operating Report (MOR) process.
- The Head of Risk and Audit will facilitate the ongoing review of the Corporate Risk Register by risk owners and Executive Team (ET), and at least twice annually will conduct a workshop to review the register with all risk owners and ET.
- The Head of Risk and Audit will review the Health & Safety and Environment Risk Register at least quarterly and will consider:
  - The rigor of the process to identify, evaluate, analyse, and treat risks
  - Whether the ERM Methodology has been appropriately applied in the development of the register
  - The adequacy of controls to address the risk
  - Assurance activities directed at these risks
  - The suitability of the actions in place to enhance controls and bring risk in line with our appetite – and ensure monitoring in place

  and will report findings in relation to these activities to management and Board committees as appropriate.
- The Corporate Risk Register is to be tabled at the Audit & Risk Committee at least twice annually.
- The Head of Risk and Audit will report compliance with this Policy and ASX Recommendation 7.2 annually to the Audit & Risk Committee.
- The Health & Safety and Environment Risk Registers are to be tabled at the Sustainability Committee regularly in line with the Committee's approved standing agenda.

6. ROLES AND RESPONSIBILITIES

Board

Ensure the Audit & Risk Committee and the Sustainability Committee discharge their responsibilities in relation to risk management as outlined in this Policy.

Receive any risk reports from the respective committees which warrant consideration by the Board such that the Board can satisfy itself that it is discharging its obligations in relation to the oversight of risk.

Audit & Risk Committee

Receive and review the Corporate Risk Register in accordance with this Policy. Make relevant enquires and satisfy itself that risk is appropriately identified and managed in accordance with the ERM methodology.

Receive and consider the annual declaration from the Head of Risk and Audit in relation to the risk methodology and operating with due regard to the risk appetite and make appropriate enquires.

Sustainability Committee

Receive and review the Health and Safety and Environmental Risk Registers in accordance with this Policy. Make relevant enquires and satisfy itself that risk is appropriately identified and managed in accordance with the ERM Methodology.

Chief Financial Officer

Review risk reports prepared by the Head of Risk and Audit for tabling at the Audit & Risk Committee.

Make enquiries as necessary to be satisfied that risk is being managed in accordance with the ERM Methodology and this Policy.

EGM Health, Safety & Environment

Review reports prepared by the Head of Health and Safety and the Head of Environment for tabling at the Sustainability Committee.

Make enquiries as necessary to be satisfied that risk is being managed in accordance with the ERM Methodology and this Policy.

Executive Team

Review risks owned by you or your reports.

Participate in risk register workshops.

Ensure risk management including the implementation status of risk treatment plans is actively monitored and reported via the MOR process.

Head of Risk & Audit

Review and recommend amendments to the ERM Policy and Methodology as required.

Facilitate the Corporate Risk Register process and twice annual reporting to the ARC

Review and assist as required to ensure that functional risk registers are maintained and review and monitor the risk management process for the functional risk registers as outlined in this Policy

Provide the annual attestation to the Audit & Risk Committee that the ERM Methodology remains fit for purpose and confirm that the Company is operating with due regard for the risk appetite set for the Company.

Provide subject matter expertise in relation to the management of risk across the Company.

Head of Health and Safety & Regulatory Compliance

Manage the H&S risk register and risk management process and complete reporting as required by this Policy.

Head of Environment & Regulatory Compliance

Manage the Environment risk register and risk management process and complete reporting as required by this Policy.

Business Unit Heads and Managers

Manage risk within their function in accordance with this Policy.

Branch Managers

Responsible for managing day to day risk at their sites and reporting in accordance with this Policy and applicable site level guidance.

All Employees

Responsible for managing risk as directed and for raising risk concerns with their manager.

Version control table

Document description	Risk Management Policy
Document owner	Head of Risk and Audit
Document approved by	Cleanaway Board of Directors
Version number	2.0
Last review date	June 2023
Approval date	June 2023
Next review date	June 2024