Risk Management Policy

1 Purpose

The purpose of this policy and the framework within it is to ensure appropriate risk management procedures are in place and used to identify the risks to the business and maintain appropriate systems, controls and mitigants to manage these risks.

Risk is defined as “the effect of uncertainty on objectives” (ISO 31000).

Risk Management is the discipline of:

- identifying and assessing risk
- designing and implementing a risk mitigation plan – actions to avoid, reduce, share or accept risk
- monitoring risk within acceptable appetite levels.

2 Scope

The policy applies to all companies in the POAL group and all aspects of Risk Management.

3 Policy

All staff are required to apply the methodologies and processes established in this document in order to:

- Provide assurance risks are being:
    - Identified where they arise in the organisation;
    - Effectively controlled at an appropriate level of management; and
    - Accepted at an appropriate level of management.
- Allow POAL to recognise, prioritise and respond to risks arising from change; and
- Optimise allocation of resources to risk management.

4 Risk Management Framework

4.1 Responsibility for managing risk

Every employee has a duty for the management of risks in the area in which they work. When staff take up new roles their line manager has a responsibility to instruct them on the risks they face, the controls they are responsible for and any treatments they must action. Specific risk reporting requirements are listed in section 5 and specific management responsibilities are listed in section 6.

4.2 Risk Appetite

Risk appetite is the amount and type of risk the business is willing to pursue or retain – because an acceptance of a level of risk is necessary to achieve business objectives. The Board sets POAL’s risk appetite through approval of the Risk Appetite Table (Appendix 2). This table informs the quantitative and qualitative measures for risk evaluation in the Risk Matrix (Appendix 1).

4.3 Risk Identification & Assessment

Awareness of risk is an ongoing, daily activity for every member of staff or contractor that extends beyond their immediate work environment. Everyone needs to be mindful of the hazards they encounter and point out risks of these to others that may not be obvious.

Each business unit must review their internal and external environment to identify new risks that their business unit faces.

During annual planning each business unit must identify risks that are material to the achievement of their objectives and incorporate risk mitigation strategies into their plans. Treatment owners and target dates for completion must be agreed and incorporated into individual and team KPI's. Sufficient capital and operational budget must be requested to cover the cost of treatment plans.

Before decisions are made, the risks of each potential course of action must be identified and assessed, and used as an input into the decision making process.

Internal incidents and relevant external events must be reviewed in a timely manner to determine whether they identify new risks or impact on previously identified risks.

All managers are responsible for assessing their own risks by using the Risk Matrix (Appendix 1).

4.4 Risk Mitigation

Risk mitigations include ***controls*** (measures that maintain or reduce risk) and ***treatments*** (planned actions to lower risk). Each control must have a control owner and, where reasonably possible, a plan for checking the effectiveness of the control. Each treatment must have a treatment owner and an agreed target date for completion of the treatment. Risk owners remain accountable for the effectiveness of controls and the successful implementation of treatments.

The ***residual risk*** is the current risk which remains after taking into account effective risk mitigations in place, and is therefore the risk that the business needs to make a decision to accept or not. It is important this decision is made at an appropriate level (as specified in the Appendix 1) and with consideration of POAL's Risk Appetite. If the residual risk is not acceptable further mitigation is required or the activity stopped.

4.5 Risk Registers

The risk register records each non-trivial risk together with its risk mitigation plan. General Managers are responsible for ensuring their business unit(s) have a risk register and which is current.

Risk registers must include:

- Business unit name
- Risk register owner
- Date of last risk meeting
- List of all material risks currently faced

Each listed risk must include:

- Risk description
- Risk owner
- Date risk was last reviewed
- Residual risk assessment (amount of risk that remains after the controls are taken into account, based on the known effectiveness of those controls), comprising of:
    - Potential consequence (worst case)
    - Potential likelihood (of that worst case occurring)

    - Risk score (using the Risk Matrix in Appendix 1)
- List of controls in placeincluding:
    - Control owner
    - Assessment of control effectiveness
    - How control effectiveness is determined (control assurance process if any)
- If the current residual risk is above tolerance, a list of treatments planned to bring the residual risk down to be within tolerance, including:
    - Treatment owner
    - Planned treatment completion date

4.6 PortSafe

PortSafe is POAL's health and safety application for reporting and managing all health and safety risks. Risks recorded in PortSafe do not need to be repeated in business units risk registers.

4.7 Key Risks

Key Risks are those risks the Executive Team and the Board believe warrant definition as a Key Risk and are therefore reported to and considered by the Board.

A ***Key Risk Register*** will be maintained by the Governance & Risk Manager. Similar risks from multiple business unit risk registers may be combined into a single high-level risk on the Key Risk Register.

4.8 Risk Management Assurance

The risk management function will work closely with the Insurance and Internal Audit areas and other relevant external parties (e.g. Maritime NZ, NZ Customs) to ensure there is a common understanding of the purpose and effectiveness of controls that mitigate risks and ensure those risks which remain are acceptable.

5 Risk Management Reporting and Register Updates

Report to	Action by	Report or update	Frequency
Board	CEO**	New high or extreme risks	Immediately
		Key Risks; new, emerging, material change to existing (CEO report)	Every meeting
		Key Risk heat maps	Quarterly (post Board committee review) and with strategy/plan
		Risk assessment and mitigation plan	All project/ capex approval papers
		Specified report on a Key Risk	As required by the Board
Board Committees*	CEO**	Key Risk heat map (changes and issues)	Every meeting
		Progress on mitigating Key Risks outside tolerance	Every meeting
		Key Risk register	6-monthly
CEO	Executive Team	Key risk register update	6-monthly (prior to Board committee review)
	Management	New high or extreme risks	Immediately
n/a	Business Unit Manager	Full business unit risk register update	Annually
		Risk register update	Immediately a new risk identified
n/a	Risk owner	Risk register update	As soon as actions are completed
n/a	Governance & Risk Manager Senior Manager Safety & Wellbeing	Key Risk register update	As soon as a new Key Risk is identified or actions are completed
		Key Risk heat map update	Quarterly (prior to Board Committee review)

* Health & Safety Committee – health and safety risks, Audit & Risk Committee – all other risks.

** Supported by Governance & Risk Manager and Senior Manager Safety & Wellbeing

6 Responsibilities

These responsibilities are in addition to the reporting responsibilities shown above.

6.1 Board of Directors

The Board of Directors, supported by the Audit & Risk Committee and the Health & Safety Committee, is responsible for:

- approval of the Risk Management Policy
- setting the tone and culture for risk management
- participating in the identification, assessment and mitigation of Key Risks through regular consideration of the Key Risk heat maps
- acceptance or otherwise of the risk assessment for Key Risks and agreeing actions to be taken to reduce unacceptable risks or stopping activities with unacceptable risks
- ensuring the annual internal audit plan takes account of the key areas of risk.

6.2 Chief Executive Officer

The CEO is responsible for:

- developing and maintaining the Risk Management Policy and ensuring it is implemented, complied with and effective
- setting the tone and culture for risk management
- participating in the identification, assessment and mitigation of Key Risks through regular consideration of the Key Risk heat maps
- agreeing actions to be taken to reduce unacceptable Key Risks or stopping activities with unacceptable risks
- delegating adequate authority and resources to staff to enable them to effectively identify and manage risks within the company's risk appetite.

6.3 General Managers

Each General Manager is responsible for:

- ensuring effective implementation and operation of the Risk Management Policy in their area of responsibility
- championing initiatives to improve the management of risks
- reviewing all risk registers to determine appropriateness of assessment, controls and mitigations.

6.4 Managers

Each Manager is responsible for:

- taking responsibility for managing risk, safety, health and compliance in their own area of responsibility
- identifying the risks relating to own area (operational, financial, political etc.) and ensuring that there are adequate mitigation strategies in place to effectively manage those risks
- maintaining knowledge about the key risks
- keeping their business unit risk register current and ensuring their General Manager is informed on their risks and risk mitigation strategies

6.5 All staff

All staff are responsible for:

- identifying potential risks within their business area
- identifying perceived shortcomings in risk controls
- the timely completion of risk treatments
- complying with the Risk Management Policy.

6.6 Governance & Risk Manager and Senior Manager Safety & Wellbeing

The Senior Manager Safety & Wellbeing (for health and safety risks) and the Governance & Risk Manager (for all other risks) is responsible for:

- providing the tools and advice to enable managers to implement the Risk Management Policy
- monitoring the application and effectiveness of the Risk Management Policy
- maintaining the Key Risks Register
- maintaining the Key Risk Heat Map
- tracking the completion of risk treatments for Key Risks
- supporting the CEO by providing the reporting required in section 5 to the relevant Board Committee and to the Board
- coordinating company-wide initiatives to improve processes that identify and manage risks
- advising, coaching and training staff on risk management techniques
- assisting the internal audit function to provide assurance on risk management.

Board Approval:	Approved 22 November 2021
Policy Owner:	Governance & Risk Manager
Policy Review:	Biennially

Appendix 1 – Risk Matrix

Likelihood	Consequence				
	Insignificant	Minor	Moderate	Major	Critical
Almost certain	9	12	20	23	25
Likely	4	11	17	21	24
Possible	3	10	16	18	22
Unlikely	2	6	13	14	19
Rare	1	5	7	8	15

Risk Rating	Low (1-8)	Medium (9-15)	High (16-22)	Extreme (23-25)

Likelihood	Description of Likelihood
Almost certain	Almost certain to occur within the foreseeable future. Greater than 80% probability that the risk will occur within next 12 months (and likely to have multiple occurrences).
Likely	Likely to occur within the foreseeable future. 50% - 80% probability that the risk will occur within next 12 months
Possible	May occur within the foreseeable future. 20% - 50% probability that the risk will occur within next 12 months (between a 1 in 2 and a 1 in 5 year occurrence).
Unlikely	Not likely to occur within the foreseeable future. 2% - 20% probability that the risk will occur within next 12 months (between a 1 in 5 and a 1 in 50 year occurrence).
Rare	Will only occur in exceptional circumstances. Less than 2% probability that the risk will occur within next 12 months (less than 1 in 50 year occurrence).

Consequence	Insignificant	Minor	Moderate	Major	Critical
Safety and Wellbeing	Very minor injury, self-administered first aid, immediately back to work, no impact on performance	Minor injury or illness requiring first aid, treatment on site, back to work with no LTI	Injury or illness requiring off-site medical treatment and/or LTI	Notifiable injury or illness such as serious harm (as defined by WorkSafe), or near miss involving the same	Fatality or near miss that could result in a fatality or fatalities
Employee engagement	Minor impact on one employee	Minor impact on limited number of employees or prospective employees	Minor widespread impact or major impact on a limited number of employees	Small drop in morale, a few employees leaving, negative impact on recruitment outcomes	Large drop in morale, many employees leaving, impact on remuneration to retain and recruit
Public reputation	Isolated minor complaint from member of public	Multiple complaints from a stakeholder group that are easily resolved	Multiple complaints from a stakeholder group that are not easily resolved	Drop in overall public perception or substantial drop in stakeholder group, negative news stories or protests	Substantial drop in public perception, negative impacts on business, material impact on “licence to operate”
Environmental	No effect on environment	Insignificant fleeting effect on environment	Minor short-term effect on the environment	Moderate short-term or minor long-term effect on environment	Significant short-term or moderate long-term effect on environment

Consequence	Insignificant	Minor	Moderate	Major	Critical
Operational continuity	Disruption of non-critical process for <4 hrs	Disruption of non-critical process 4-48 hrs. Disruption of critical process <4 hrs	Disruption of non-critical process >48 hrs. Disruption of critical process 4-24 hrs. Complete port shut-down <4 hrs.	Disruption of critical process >24 hrs. Complete port shut-down 4-12 hrs.	Disruption of critical process for >1 week. Complete port shut-down for >12 hrs.
Market reputation	Customer inconvenience quickly forgotten	Dissatisfied customer formal complaint requiring remedial action	Dissatisfied customer resulting in lost revenue	Dissatisfied customer resulting in lost ship call	Dissatisfied customer resulting in multiple lost ship calls
Financial	Loss <$1k	Loss <$20k	Loss <$500k	Loss <$5M	Loss $5M or more
Legal & regulatory compliance	Contract breach not required to be remedied or notified. Legislative/ Regulatory non-compliance not required to be remedied or notified.	Contract breach able to be remedied without third party involvement. Legislative/ Regulatory non-compliance able to be remedied without notification.	Contract breach requiring dispute mediation. Legislative/ Regulatory non-compliance requiring mandatory reporting.	Contract breach requiring District Court litigation. Legislative/ Regulatory non-compliance resulting in sanction or prosecution.	Contract breach requiring High Court litigation. Legislative/ Regulatory non-compliance resulting in sanction or prosecution.

Residual Risk Rating	Lowest level Risk owner	Approval of risk assessment, risk mitigation strategy and to undertake risk activity
Low (1-8)	Supervisor or Team Leader	Business Unit Manager or Direct Report to a GM
Medium (9-15)	Business Unit Manager or Direct Report to a GM	GM
High (16-22)	General Manager	CEO (and Board for Key Risks)
Extreme (23-25)	CEO	Board

Appendix 2 – POAL Risk Appetite Table

The following table indicates the amount of risk POAL is prepared to assume in pursuit of its objectives. Use the table when reviewing risk to guide the decision on whether the risk controls and treatments are sufficient.

Risk domain	Risk averse	Balanced	Risk tolerant
Safety and wellbeing	✔		
Employee reputation		✔	
Public reputation		✔	
Environmental protection	✔		
Operational continuity		✔	
Market reputation		✔	
Financial performance		✔	
Legal and regulatory compliance	✔		
Commercial			✔

Risk domain is the category the risk is being assessed against. Risks may require assessment against more then one risk domain. The qualitative measures in the consequence table are informed by the risk appetite for each domain. The risk rating is assessed using the highest rated outcomes from all relevant domains.

Risk averse indicates domains where POAL will take all reasonable practical steps to avoid and/or mitigate the risk.

Balanced indicates domains where POAL has flexibility in its approach to the risk, to ensure an appropriate balance between risk and reward.

Risk tolerant indicates domains where POAL is willing to take on more risk in the search for greater reward.