# Risk Management Policy

## 1. Purpose

The purpose of this policy is to provide clear guidelines for the management of risk.

Risk is defined as “the effect of uncertainty on objectives”.[1]

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.

The Board requires that appropriate Risk Management procedures are in place and in use to identify the principal risks of the business and that appropriate systems are implemented to manage these risks.

## 2. Scope

The policy forms a part of POAL’s governance policies.

The policy applies to all companies in the POAL group and covers 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 that risks are being:
    - Identified and effectively controlled where they arise in the organisation; and
    - Escalated through the line management reporting structure to a level where they can be either effectively controlled or accepted
- 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 Risk Ownership

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

[1] Definition from ISO 31000

controls they are responsible for and any treatments they must action. Specific risk responsibilities are listed in section 4.

## 4.2 Risk Appetite

***Risk appetite*** is the amount and type of risk that the business is willing to pursue or retain - because an acceptance of a level of risk is necessary to achieve business objectives. The Board is responsible for determining POAL's risk appetite. The Board must be made aware of risks that may have a critical consequence (e.g. loss of life or serious injury, cessation of port operations for an extended period, significant environmental damage, significant reputational damage, and material financial loss) in order to provide guidance on what level of risk is acceptable.

Refer to Appendix 2 for the Risk Appetite Table. This table informs the quantitative and qualitative measures for risk evaluation.

## 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 risks they encounter and point out risks to others that may not be obvious.

At least annually 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.

Business units are responsible for assessing their own risks by using the POAL Risk Matrix (attached as Appendix 1).

## 4.4 Risk Mitigation

Risk mitigations include ***controls*** (procedures or policies that provide assurance) and ***treatments*** (planned actions to lower risk). Each control should have a control owner and, where reasonably possible, a plan for checking the effectiveness of the control. Each treatment should 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 risk which remains after all the risk mitigations are in place and is therefore the risk that the business is making a decision to accept. It is important that this decision is made at an appropriate level (as specified in the POAL Risk Matrix) and with consideration of POAL's Risk Appetite. The Board will provide guidance on accepting residual risk for Key Risks (see section 3.6).

## 4.5 Risk Registers

The risk register records each material risk together with its risk mitigation plan. General Managers are responsible for ensuring their business unit(s) has a risk register and that the risk register is kept 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 (after risk mitigations), comprising of:
    - Potential consequence (worst case)
    - Potential likelihood (of that worst case occurring)
    - Risk score (according to POAL Risk Matrix)
- List of controls in place, with each control having a:
    - Control owner
    - Control assurance process (if assurance process exists)
    - Date assurance process was last performed or reviewed
- List of treatments planned, with each treatment having a:
    - Treatment owner
    - Planned treatment completion date

## 4.6 PortSafe

PortSafe is a port-wide health and safety application. All health and safety risks must be included in PortSafe. Risks recorded in PortSafe do not need to be repeated in the business units risk register.

## 4.7 Escalation of High Risks and Extreme Risks

Managers are responsible for the reporting to their General Manager all newly assessed risks with a residual risk level (after controls) of Extreme or High. The General Manager is responsible for reporting these risks to the Executive and Board (via the monthly CEO Report).

## 4.8 Key Risks

***Key Risks*** are those risks with an Assessed Risk Level of High or Extreme plus other risks that the Executive Team believes warrant their inclusion as a Key Risk.

A separate ***Key Risk Register*** will be maintained by Governance and Risk Manager comprising of all Key Risks. Note similar risks from multiple business unit risk registers may be combined into a single high-level risk on the Key Risk Register. The Key Risk Register will be reviewed by the Executive team on an annual basis.

## 4.9 Board Risk Reporting

The full Key Risk Register will be presented to the Board for review on an annual basis. New Key Risks, and any material change to an existing Key Risk, will be reported to the Board at the next scheduled Board meeting within the monthly CEO report, in either the Current Issues or Risk and Compliance sections.

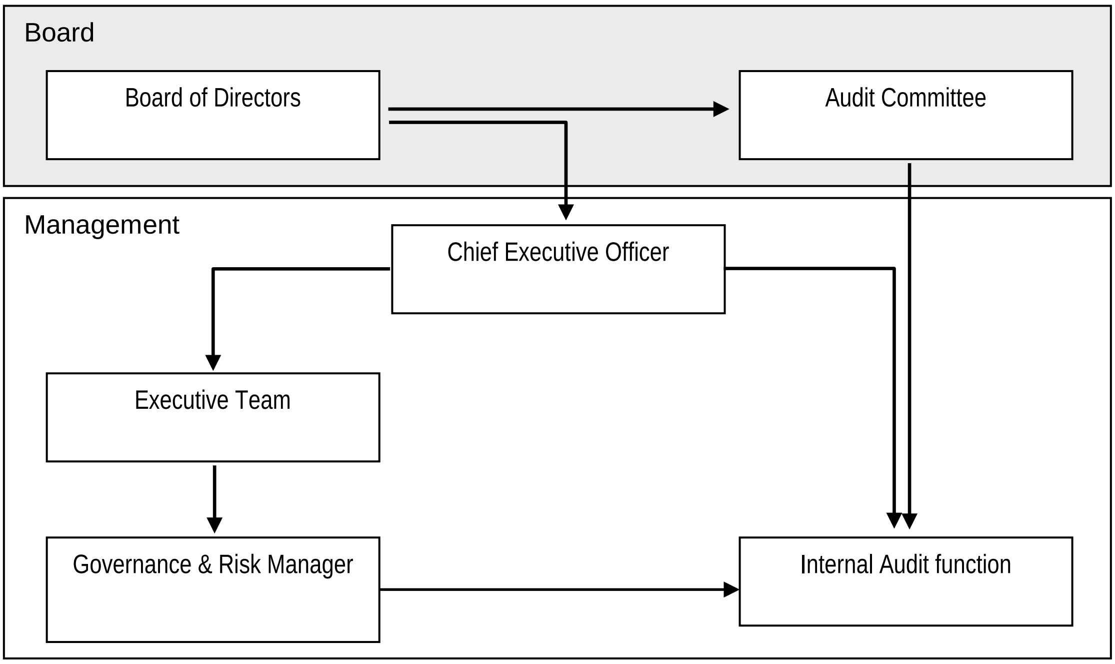
The Board will receive, on a regular basis, a Board paper on a pre-selected Key Risk prepared by the risk owner. Key Risks that are of a strategic nature will be discussed during the course of the Board's regular strategy discussions.

### 4.10 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. Responsibilities

### 5.1 Governance Structure




### 5.2 Board of Directors

The Board of Directors are responsible for:

- approval of the Risk Management Policy
- setting the tone and culture for risk management
- establishing POAL's risk appetite
- obtaining assurance on:
    - the effectiveness of the management of risks
    - the level of compliance with the Risk Management Policy

## 5.3 Chief Executive Officer

The CEO is responsible for:

- developing and maintaining the Risk Management Policy and ensuring it is implemented and effective
- setting the tone and culture for risk management
- delegating adequate authority and resources to staff to enable them to effectively identify and manage risks within the company's risk appetite
- providing appropriate, timely and accurate risk information to the Board on High and Extreme risks.

## 5.4 General Managers

Each General Manager is responsible for:

- supporting the effective implementation and operation of the Risk Management Policy
- championing initiatives to improve the management of risks
- reviewing risks that have been assessed with a residual risk level (after controls) of Extreme or High, and reporting these to the Executive team and the Governance and Risk Manager

## 5.5 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.

## 5.6 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

## 5.7 Governance and Risk Manager

The Governance and Risk Manager 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 and reporting the Key Risks Register to the Executive Team and the Board

- tracking the completion of risk treatments for Key Risks
- 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.

## 5.8 Audit Committee

The Audit Committee is responsible for ensuring the annual internal audit plan takes account of the key areas of risk.[2]

| | |
|---|---|
| **Board Approval:** | 19 March 2018 |
| **Policy Owner:** | Governance and Risk Manager |
| **Policy Review:** | Biennially |

[2] POAL Audit Committee Charter April 2017

# Appendix 1 – POAL 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 |

| Assessed Risk Level | 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 – if first aid required is self-administered – immediately back to work with 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 (as defined by WorkSafe) | Fatality or near miss that could result in a fatality |
| **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 overall morale, a few employees leaving, negative impact on recruitment outcomes | Large drop in morale, many employees leaving, remuneration increases required to keep existing and recruit new staff |
| **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. | Small drop in overall public perception or substantial drop in a stakeholder group.<br><br>Negative news stories or protests. | Substantial drop in public perception resulting in negative impacts on business strategy.<br><br>Material impact on our “licence to operate”. |

| Consequence | Insignificant | Minor | Moderate | Major | Critical |
|---|---|---|---|---|---|
| **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.<br>Material impact on our “licence to operate”. |
| **Operational** | Disruption of a non-critical process for less than 4 hours | Disruption of a non-critical process for 4-48 hours.<br>Disruption of a critical process for less than 4 hours. | Disruption of a non-critical process for more than 48 hours.<br>Disruption of a critical process for 4-24 hours.<br>Complete port shut-down for less than 4 hours. | Disruption of a critical process for more than 24 hours.<br>Complete port shut-down for 4-12 hours. | Disruption of a critical process for more than 1 week.<br>Complete port shut-down for more than 12 hours. |
| **Market** | Minor customer inconvenience - quickly forgotten | Dissatisfied customer with formal complaint requiring action | Dissatisfied customer resulting in reduction in total revenue of less than 1% | Loss of a below top 10 customer or reduction in total revenue of 1%-5% | Loss of a top 10 customer or reduction in total revenue of more than 5% |
| **Financial** | One-off financial loss of less than $1,000 | One-off financial loss $1,000 - $20,000 | One-off financial loss $20,000 - $500,000 | One-off financial loss $500,000 - $5M | One-off financial loss exceeding $5M |

**Level of Authority**

| Assessed Risk Level | | Approval to undertake risk activity (includes approving the risk assessment and risk mitigation strategy) |
|---|---|---|
| ☐ | Low (1-8) | Supervisor or Team Leader |
| ☐ | Medium (9-15) | Business Unit Manager or Direct Report to a GM |
| ☐ | High (16-22) | General Manager |
| ☐ | Extreme (23-25) | Executive Team or CEO |

# Appendix 2 – POAL Risk Appetite Table

The following table indicates the amount of risk POAL is prepared to assume in pursuit of its strategic 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 | | ✔ | |
| Regulatory compliance | ✔ | | |

**Risk domain** is the category the risk being assessed best fits should the risk eventuate. The risk domains used align with the consequences from the Risk Matrix specified in Appendix 1, with the addition of regulatory compliance.

**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.