RISK MANAGEMENT FRAMEWORK

APPROVED BY:	Board of Directors	**DATE:**	23 April 2010
APPROVING AUTHORITY	Board of Directors		
DELEGATION INSTRUMENT	Board Resolution – 28 May 2010		
CUSTODIAN:	General Manager Corporate Services		
COMMENTS:	Reviewed by Chief Financial Officer - 21 November 2008 Corporate Governance Review – February 2010 Reviewed by the Audit and Risk Committee – August 2013 Reviewed by the Board of Directors – 26 March 2015 Reviewed by the Board of Directors – 27 April 2018 Reviewed by the Audit and Risk Committee – 22 March 2021 Reviewed by the Board of Directors – 30 March 2021		

Table of Contents

Introduction

The Board of Directors of Far North Queensland Ports Corporation Limited (trading as Ports North) recognises that the management of risk is a key element of good corporate governance and has developed a Risk Management Framework that describes the manner in which risks are identified, assessed, monitored and reported. This Framework is supported by a strong system of internal control. The purpose of the risk management framework is to assist the organisation in integrating risk management into significant activities and functions including decision-making, at all levels of the organisation.

The management and oversight bodies within Ports North will:

- establish clear business objectives, identify and evaluate the significant risks to the achievement of those objectives, set boundaries for risk taking by development of its' risk appetite and apply risk treatment responses including risk mitigation where appropriate;
- incorporate risk management principals into management systems to address opportunities, protect people, the environment and company assets, facilitate effective and efficient operations and help to ensure reliable reporting and compliance with applicable laws and regulations;
- ensure the systems to manage risks are implemented and operating effectively;
- comply with all relevant internal policies and guidelines;
- provide an annual assurance regarding the extent of compliance with the Risk Management Framework;
- ensure communication and consultation with appropriate external and internal stakeholders occurs throughout the risk management process;
- promote an organisational culture that is risk aware and empowers staff to make informed decisions in accordance with Ports North Risk Appetite Statement;
- ensure that the necessary resources are allocated to managing risk;
- require the Chief Executive Officer, General Manager Finance and the General Manager Corporate Services to certify to the Board that the risk management and internal control system is operating efficiently and effectively in all material respects.

The Risk Management Framework will be implemented by:

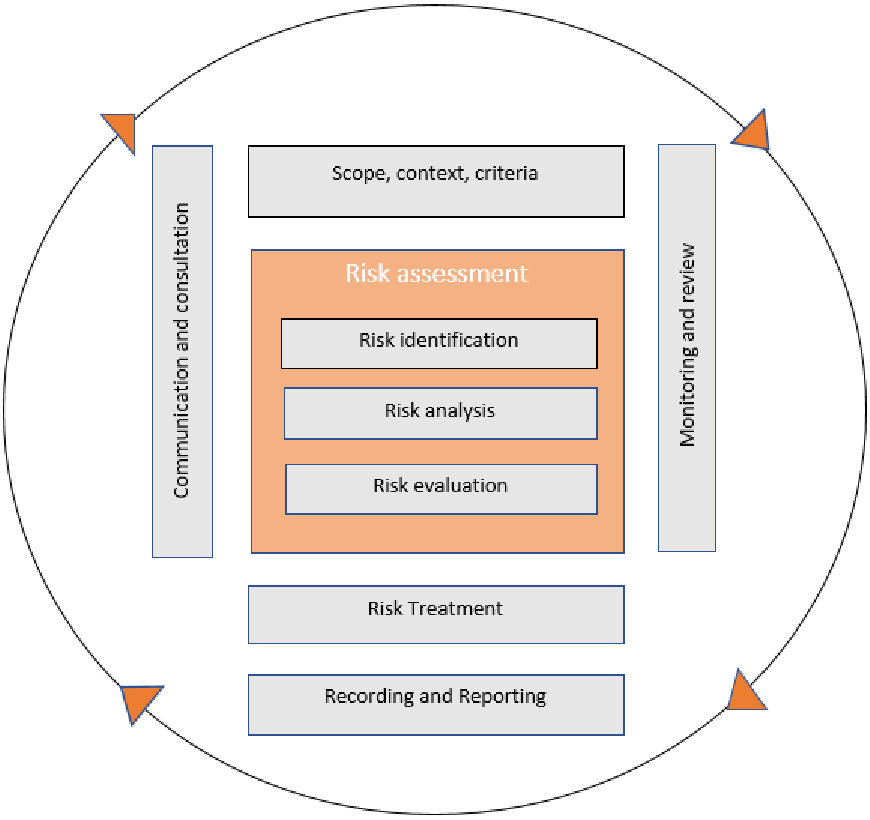
- establishing and implementing a formal risk management process;
- identifying from this risk management process specific project, operational and strategic risks;
- regularly monitoring and assessing the performance and effectiveness of the risk management process;
- ensuring the risk management process is overseen by the Audit & Risk Committee and the Board.

The Risk Management Framework includes the following key processes:

- Establishing the scope, context and criteria (objectives, stakeholders, operating environment);
- Identifying the risks (what can happen, how can it happen)
- Analysing the risks (consequence and likelihood)
- Evaluating the risks (actions, ownership and response)
- Treating the risks (identify risk treatment options, if any)
- Reporting and monitoring the risks.

The Risk Management Framework will incorporate a list of specific responsibilities for the management of risk.

The Risk Management Framework has been developed taking into consideration the guidance provided in the International Standard ISO 31000:2018 *Risk Management – Guidelines*, which recommends an integrated, structured, inclusive and dynamic approach to risk management. This approach is shown below. The relevant components of the standard will be outlined in this Framework, providing an explanation of how risk management will function in Ports North.



Source: AS ISO 31000:2018

Review

The Risk Management Framework will be reviewed every three years by the Custodian and Audit & Risk Committee and any recommended changes will be approved by the Board.

Related Documents

- AS ISO 31000: 2018 *Risk management – Guidelines*
- Corporate Governance Guidelines for Government Owned Corporations – February 2009 (Queensland Government).

Glossary of Terms

"Consequence" – the outcome(s) of an event (for example, a loss, injury, disadvantage or gain) which affects the agency's ability to achieve its objectives.

"Control" – any action taken to manage risk.

"Cost" – of activities, both direct and indirect, involving any negative impact, including money, time, labour, disruption, good-will, political and intangible losses.

“Event” – occurrence or change of a particular set of circumstances.

“Hazard” – a source of potential harm or a situation with a potential to cause loss.

“Likelihood” – used as a qualitative description of probability or frequency of something happening.

“Loss” – any negative consequence, financial or otherwise.

“Major Project” – investment in construction or maintenance of plant, equipment or infrastructure, the value of which exceeds $2,500,000.

“Operational Risk” – those risks that arise in day to day operations, and which require specific and detailed response and monitoring regimes.

“Probability” – the likelihood of a specific event or outcome, measured by the ratio of specific events or outcomes to the total number of possible events or outcomes.

“Residual Risk” – the remaining level of risk after new controls or treatment measures have been taken into account.

“Risk” – the chance of something happening that will have an impact upon the achievements of Ports North’s objectives. It is measured in terms of consequences and likelihood.

“*Risk Coordinator*” – means the Manager Legal, Risk and Compliance.

“Risk Acceptance” – an informed decision by the risk owner to accept the consequences and the likelihood of a particular risk.

“*Risk Analysis”* – a systematic process to determine the nature of risk and the magnitude of their consequence.

“Risk Appetite” – the amount of risk that Ports North is prepared to accept or be exposed to at any point in time.

“Risk Assessment” – the overall process of risk identification, analysis and evaluation.

“*Risk Management”* – The coordinated activities to direct and control an agency with regard to risk.

“Risk Management Process” – the systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analysing, evaluating and monitoring risk.

“Risk Profile” – the documented and prioritised overall assessment of a range of specific risks faced by Ports North.

“*Risk Rating”* – the rating resulting from the application of Port North’s risk assessment matrix on the likelihood and consequence of a risk occurring.

“Risk Reduction” – selective application of appropriate techniques and management principles to reduce either the likelihood of an occurrence or its consequences, or both.

“Risk Register” – a system or file that holds all information on identifying and managing a risk.

“Risk Retention” – intentionally or unintentionally retaining the responsibility for loss, or financial burden of loss within the organisation.

“Risk Source” – element which alone or in combination has the potential to give rise to risk.

“Risk Tolerance” – the variation from the pre-determined risk appetite Ports North is prepared to accept.

“Risk Transfer” – shifting the responsibility or burden for loss to another party through legislation, contract, insurance or other means. Risk transfer can also refer to shifting a physical risk or part thereof elsewhere.

“Risk Treatment” – selection and implementation of appropriate options for dealing with risk.

“Stakeholder” – person or organisation that can effect, be affected by, or perceive themselves to be affected by a decision or activity.

“Strategic Risks” – significant risks that affect the organisation as a whole and will have an impact on the achievement of the Corporate Objectives and require oversight by the Board.

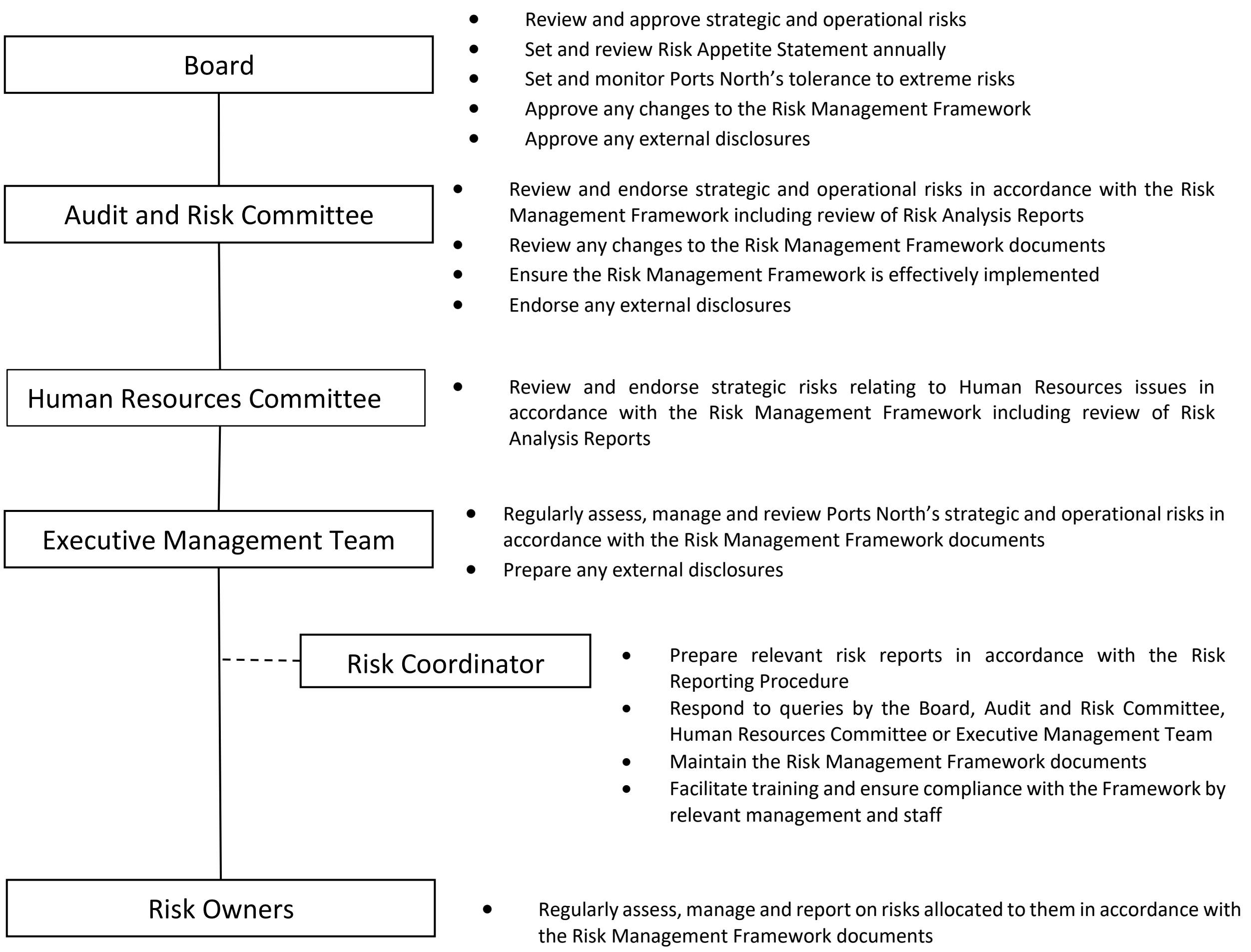
Risk Management Framework Overview

In order to implement consistent and standardised risk management practices across Ports North, the following Framework components have been developed as a guidance. Together, the Risk Assessment Procedure, Risk Reporting Procedure, Risk Appetite Statement and Risk Registers form the Risk Management Framework.

Document	Location	Description
Risk Assessment Procedure	Risk Management Framework Section 1	Provides guidance on how to identify, assess and treat risks; the actions and ownership associated with each risk rating and risk response option available for each risk.
Risk Reporting Procedure	Risk Management Framework Section 2	Defines the process that enables risk to be monitored and reported; identifies the content and frequency of reporting required to enable the Executive Management Team, Audit & Risk Committee, Human Resources Committee and Board oversight of the risk management process.
Risk Appetite Statement	Separate document	Provides guidance on Ports North’s willingness to assume or be exposed to a level of risk in order to achieve its objectives.
Risk Register	Separate document	Catalogues all strategic and operational risks identified. Shows the outcomes of risk assessments performed for risks identified including inherent, residual and target risk ratings, controls and actions.

Risk Management Responsibilities

A detailed list of risk management responsibilities for Ports North's Board, Audit & Risk Committee, Human Resources Committee, Management and staff have been provided in Attachment 1. A summary of these responsibilities is provided below.



Board

- Review and approve strategic and operational risks
- Set and review Risk Appetite Statement annually
- Set and monitor Ports North's tolerance to extreme risks
- Approve any changes to the Risk Management Framework
- Approve any external disclosures

Audit and Risk Committee

- Review and endorse strategic and operational risks in accordance with the Risk Management Framework including review of Risk Analysis Reports
- Review any changes to the Risk Management Framework documents
- Ensure the Risk Management Framework is effectively implemented
- Endorse any external disclosures

Human Resources Committee

- Review and endorse strategic risks relating to Human Resources issues in accordance with the Risk Management Framework including review of Risk Analysis Reports

Executive Management Team

- Regularly assess, manage and review Ports North's strategic and operational risks in accordance with the Risk Management Framework documents
- Prepare any external disclosures

Risk Coordinator

- Prepare relevant risk reports in accordance with the Risk Reporting Procedure
- Respond to queries by the Board, Audit and Risk Committee, Human Resources Committee or Executive Management Team
- Maintain the Risk Management Framework documents
- Facilitate training and ensure compliance with the Framework by relevant management and staff

Risk Owners

- Regularly assess, manage and report on risks allocated to them in accordance with the Risk Management Framework documents

Risk Appetite Statement and Risk Tolerance

Risk appetite sets the tone with regard to how much risk an organisation is willing to take in pursuit of its objectives and establishes internal boundaries for prudent decision making, risk taking and efficient governance.

Ports North's risk appetite statement has been developed in relation to the organisation's key corporate objectives and provides guidance on Ports North's willingness to assume, or be exposed to, a level of risk in order to achieve its objectives.

Ports North's risk appetite statement will be reviewed annually by the Board when it reviews Strategic Risks, or in light of changing circumstances.

The alignment of target risk ratings for strategic and operational risks against Ports North's risk appetite statement, will be reviewed and documented as part of the quarterly and annual review of risks.

Ports North's tolerance (any variation from the risk appetite Ports North is prepared to accept) to extreme risks is set by the Board as part of its review of the Risk Appetite Statement. The Board and Committees will monitor Ports North's tolerance to extreme risks as part of their ongoing review of Strategic Risks.

Section 1. Risk Assessment Procedure

Purpose

This section provides guidance on using Ports North's Risk Management Framework. It defines processes that enable risks to be identified, analysed, evaluated and treated in a consistent manner.

1.1 Scope, context and criteria

Establishing the context defines the basic parameters for identifying risks and sets the scope for the rest of the risk management process. It identifies key areas of risk exposure and the best means available for managing those risks. Generally context can be derived from external or internal factors.

External factors include:

- The business, social, regulatory, competitive, financial and political environment;
- Ports North's strengths, weaknesses, opportunities and threats;
- Key external stakeholders; and
- Key business drivers.

Internal factors include:

- Structure and culture;
- Internal stakeholders;
- Capabilities in terms of resources such as people, systems, processes and capital; and
- Goals and objectives and the strategies that are in place to achieve them.

Establishing both an external and internal context for risk identification ensures staff consider all threats and opportunities faced by Ports North. Practically, the internal and external context for Ports North is expressed by its risk categories. These categories are useful for performing a structured identification and analysis of risks, and allowing the logical reporting of risks by category.

Category	Description
Safety	Death or serious injury to an employee, contractor or member of the public on Ports North land or as a result of company operations. All other safety issues.
Stakeholder/Share holder	Failure to effectively engage and communicate with Government, community, customers and other stakeholders.
Major Projects	Failure to successfully deliver major projects, including project management and governance issues.
Infrastructure	Loss of reliability or availability, replacement time for failed equipment, lack of redundancy/contingency.
Financial	Contract risk, trade practices legislation, misappropriation of funds, fraud, fines.
Economic/Market	Loss of customers, failure to take advantage of improved market circumstances, currency fluctuation, interest rates, restrictions on growth.

Category	Description
Regulatory	Potential changes to legislation, failure to comply with legislation
Human Resources	Failure to attract and retain essential skills.
Environmental	Noise, contamination, exotic pests, heritage, native title, legislative change, loss or rescission of permit.
Extreme Events	Ports North is unable to recommence business in a timely manner following any extreme event e.g. cyclone, tsunami, earthquakes, terrorism.
Information	Loss of ICT capability, misappropriation of information.
Security	Loss of business associated with security event, riots, protests, sabotage, terrorism, error.
Fraud	Dishonest activity occasioning actual or potential financial loss to any person or entity including theft of money or other property by employees or external persons as well as deliberate falsification, concealment and/or destruction of documents.

Another important aspect of establishing the context is to determine the level of risks being identified. The levels of risk that operate in Ports North are described below:

Strategic Risks

Strategic Risks impact on the organisation's ability to achieve its strategic objectives. These risks are the most significant risks faced by Ports North and may affect the organisation's ability to maintain effective governance, conduct major initiatives, comply with and adapt to legislative and regulatory change, manage its stakeholder relationships, and respond to global and natural events. Strategic Risks are predominantly used by the Board, ARC, HRC and EMT to monitor and manage Ports North's risk environment.

Operational Risks

Operational Risks are associated with establishing and maintaining effective management over business level activities including financial, operational, health and safety, environmental, construction and maintenance management, corporate image, and human resources processes. Operational Risks will be focused at the Business Unit level and will be integrated into relevant Business Unit planning processes.

Project Risks

Risk management activities may be employed at a project level as part of project management. Whilst they may be associated with or inform the organisation's Strategic or Operational Risks and are assessed and defined using the same risk criteria, Project Risks are monitored and managed by the Project Manager and are not required to be reported to the Audit and Risk Committee or Board.

Defining Risk Criteria

Ports North has defined risk criteria to evaluate the significance of risk and to support decision-making processes. The risk criteria are detailed below as part of the process for risk assessment. The criteria have been defined taking into consideration the organisation's obligations and views of stakeholders.

1.2 Risk Assessment

Risk assessment is the overall process of risk identification, risk analysis and evaluation. A comprehensive identification and accurate description of all potential risks is critical for properly analysing and assessing Ports North's risks. Detailed below are the processes for identifying, describing and categorising risk.

Identifying Risk

New risks will emerge from time to time, and it is the responsibility of all staff to identify and ensure they are entered into the relevant risk register. Examples of situations where new risks may emerge include:

- Undertaking a new project;
- Implementing a new business process;
- Incidents leading to new risks being identified; or
- Changes in external factors leading to new risks (e.g. changes in legislation).

New risks must be added by the Risk Owner to the Risk Register within a week of the risk being identified.

When major projects are commenced or completed, or major changes are made to processes or activities, this should prompt a complete risk assessment of that project or process. Executive Managers are responsible for ensuring this takes place in accordance with the Risk Management Framework.

Identification of Risk as Strategic or Operational

Strategic Risks are those risks that Directors have determined are to be considered strategic. This determination will occur throughout the year as appropriate or at an annual strategic risks review. In addition to the risks Directors have determined to be Strategic, all Extreme rated risks will also be considered to be Strategic. All other risks are considered to be Operational Risks.

Describing Risk

Once identified, all risks will be stored in the relevant Strategic or Operational Risk Register. Risk Owners should complete the following fields of the register for each risk:

Risk	A short description of the identified risk.
Risk description	A more complete description of the risk including an explanation of cause and outcomes (see information below).
Risk owner	The person responsible for monitoring and reporting the risk.
Category	The general category under which the risk will be classified. See section 3.1.

The following factors should be considered to enable a consistent description of newly identified risks:

- The source or cause of the risk;
- The effect of the risk on business objectives;
- When, where, why and how risks are likely to occur; and
- Who might be involved or impacted.

A good way of describing risks is giving cause and outcome, that is:

> *"[something happens] leading to [outcomes expressed in terms of impact on objectives]".*

For example:

> *"Poor weather leads to delays in project completion",* or
> *"A chemical spill into waterways damages the organisation's reputation in the community"*

1.3 How to Assess Risk

Ports North's risk assessment approach uses Consequence and Likelihood to determine risk rating. Risks are evaluated by first identifying the worst credible consequence that could evolve from a risk event, and then evaluating the Likelihood of that event occurring. The combination of Consequence and Likelihood is represented in the risk matrix, and will determine the overall risk rating allocated to that risk.

Consequence Descriptor Scale

Consequence is the outcome or impact of an event that may influence the achievement of objectives. Various descriptors are provided below as guidance for determining the consequence rating of a particular risk. If multiple descriptors apply to a risk the worst credible consequence rating should always be used.

	Example Consequence Descriptors					
	People	**Total Financial Loss ($M)**	**Environment**	**Legal Sanction**	**Community Profile**	**Community Impact**
Minor	Injury no lost time	Up to 0.1 per annum recurring loss. Or non-recurring loss of up to 0.4	No or minimal impact on the environment. No reporting required according to legislation.	Minor, non-deliberate breach with no sanction. Little or no cost implication for business.	Few community complaints or minor adverse media coverage. Negligible impact on reputation.	Isolated community disruption up to 1 day, negligible economic impact.
Medium	Injury with lost time. No permanent impairment.	0.1 to 0.75 per annum recurring loss or non recurring loss of 0.4 to 3.0	Site impact that is easily containable. Environmental impact report to authorities as required.	Technical breach of contractual or legislative conditions. Incident requires complex legal issues to be addressed.	Widespread local community complaints or limited adverse regional media coverage.	Isolated community disruption up to 3 days with limited adverse economic impact.

	Example Consequence Descriptors					
	People	Total Financial Loss ($M)	Environment	Legal Sanction	Community Profile	Community Impact
Major	Permanent impairment affecting quality of life.	0.75 to 2.5 per annum recurring loss or non-recurring loss of 3.0 to 10.0	Temporary damage to habitat or environment. May incur cautionary notice or infringement notice.	Contractual or legislative breach leading to requirement to operate under limited regulatory restrictions or orders. Serious incident requires legal representation.	Extensive community complaints or extended adverse regional media coverage.	Widespread community disruption up to 7 days with adverse economic impact.
Critical	Fatality.	Over 2.5 per annum recurring loss or non-recurring loss of over 10.0	Permanent impact on environment. Serious or repeated breach of legislation or license conditions. Prosecution.	Contractual or legislative breach leading to significant fines or operation under regulatory conditions. Possible imprisonment for Board/ senior management.	Extensive community complaints and adverse state or national level media coverage. Long-term damage to reputation.	Widespread, extended (> 7 days) community disruption with significant adverse economic impact.

Likelihood Descriptor Scale

Risk Likelihood is determined as the chance of the nominated consequence occurring. As with Consequence, the worst credible case rating should always be taken in the assessment of risks.

Descriptor	Probability	Description
Almost Certain	Estimate 90%+ chance of occurring	The event is likely to occur within the next year
Likely	Estimate 50 to 90% chance of occurring	The event is likely to occur within the next 1-2 years
Unlikely	Estimate 10 to 50% chance of occurring	The event is likely to occur within the next 2-10 years
Rare	Estimate <10% chance of occurring	The event is likely to occur less than once every 10 years

Risk Matrix

Once the likelihood and consequence of an event are estimated using the above scales, they are combined to assign a risk rating using the following matrix. The risk rating is used to prioritise risks and also determines the relevant actions and ownership that must take place.

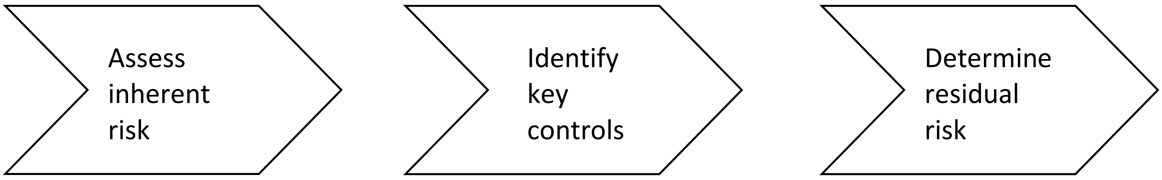
	Consequence			
Likelihood	**Minor**	**Medium**	**Major**	**Critical**
Almost Certain	Moderate	High	Extreme	Extreme
Likely	Low	Moderate	High	Extreme
Unlikely	Low	Moderate	High	Extreme
Rare	Low	Low	Moderate	High

The risk rating can also be expressed as a number between 1 and 16, which will permit further differentiation between risk ratings of the same level, as outlined in the table below.

	Consequence			
Likelihood	**Minor**	**Medium**	**Major**	**Critical**
Almost Certain	5	9	13	16
Likely	3	7	11	15
Unlikely	2	6	10	14
Rare	1	4	8	12

1.4 Risk Assessment Steps

Risks are evaluated in terms of their inherent, residual and target risk ratings. In summary, the following process should be used to assess risks:



Assess Inherent Risk

Inherent risk is the risk level of an activity before the implementation of any control measures or risk treatments. Inherent risk is determined by considering the inherent Consequence and Likelihood of each risk. The following fields of the risk register should be completed for this section:

Inherent Consequence	The outcome or impact of an event, which is determined according to the consequence descriptor scale in the Risk Assessment Procedure. Each risk should be considered in terms of its worst credible consequence <u>before</u> controls are considered.

Inherent Likelihood	The chance of the stated consequence occurring, which is determined according to the likelihood descriptor scale included in the Risk Assessment Procedure.
Inherent Rating	Inherent rating is automatically determined from the inherent consequence and likelihood ratings by referring to the risk matrix.

Identify Key Controls

Following identification, assessment and evaluation of the risk, it is important to identify controls that reduce or mitigate that risk. Risk Owners must identify and note all processes or methods implemented by Management to reduce the likelihood of a risk occurring. Controls may involve the implementation of policies, standards, procedures or physical action. The following fields of the risk register should be completed for this section:

Control Description	Key controls for each risk should be appropriately documented in this field.

Determine Residual Risk

Residual risk is the risk remaining after implementation of control measures. It should be based on the effectiveness of controls to reduce the inherent risk rating. Residual risk is determined by considering the residual consequence and likelihood of each risk (i.e. after controls are considered). The following fields of the Risk Register should be completed for this section.

Residual Consequence	The outcome or impact of an event, which is determined according to the consequence descriptor scale in the Risk Assessment Procedure. Each risk should be considered in terms of its worst credible consequence after controls are considered.
Residual Likelihood	The chance of the stated consequence occurring, which is determined according to the likelihood descriptor scale included in the Risk Assessment Procedure.
Residual Risk Rating	Residual risk rating is automatically determined from the residual consequence and likelihood ratings by referring to the risk matrix.

1.5 Risk Evaluation: Actions, Ownership & Response

The Residual risk rating will be used to determine appropriate actions for each risk, enable prioritisation of key risks and guide responsibilities for the management, monitoring and reporting of each risk. Once Residual risk is determined, Risk Owners must report the risk to the appropriate level of Management as outlined below. (Note that detailed guidance regarding ongoing risk reporting is provided in Section 2).

Actions and Ownership

The residual risk level for each risk carries with it requirements for initial approval and reporting as follows.

Strategic Risks:

Strategic Risk Rating	Actions and Ownership
Extreme	• All risks classified as Extreme are deemed to be strategic. • All new Extreme risks must be reported to the CEO immediately and to the Chair of the Board within 24 hours of being identified. • All new Extreme risks are deemed intolerable and the activity giving rise to these risks must not be undertaken until either the Board approves the risk and decides on an appropriate response, or the risk rating is reduced. • Where management believe a current risk should be rerated to Extreme, already existing activity giving rise to this risk can continue until the next ARC or Board meeting has considered the risk provided that the risk has been reported to the Chair as described above. • All Extreme risks must have Risk Analysis Reports prepared within one month of the risk being identified. The Risk Analysis Report must be reported to the next Board meeting and reviewed at the next HRC meeting (for Human Resources issues) or the next ARC meeting (for all other types of Extreme risks). • Risk ratings must be reviewed by the CEO, GMCS, GMF and Risk Owner on a quarterly basis. • Risk Analysis Reports must be reviewed and monitored quarterly by EMT and ARC, or HRC (for Human Resources issues) on an annual basis. • Extreme risks must be reported to the Board, and ARC or HRC (for Human Resources issues) and EMT, in accordance with the risk reporting procedure.
All other Strategic Risks	• Any reassessed risk where the rating is increased to High, must be reported to the Executive Manager immediately and to the CEO within 24 hours of being identified. • Risk Analysis Reports must be prepared for High rated strategic risks and monitored by the ARC or HRC (for Human Resources issues) and EMT, on an annual basis. • High risks must be reported to the ARC or HRC (for Human Resources issues) and EMT, in accordance with the risk reporting procedure.

The Risk Analysis Report template is provided in Attachment 2.

Operational Risks:

Operational Risk Rating	Actions and Ownership
High	• Any new or reassessed risk must be reported to the Executive Manager immediately and to the CEO within 24 hours.

	• The Operational Risk Register must contain details of controls and risk treatment actions for High rated Operational Risks. • High rated risks must be reported to the ARC or HRC (for Human Resources issues) and EMT, in accordance with the risk reporting procedure.
Moderate	• Any new or reassessed Moderate risks must be reported to the relevant Executive Manager within one week. • Executive Managers should determine the relevant risk response for all Moderate risks. • Moderate risks must be reported to the ARC or HRC (for Human Resources issues) and EMT, in accordance with the risk reporting procedure.
Low	• Managers and Supervisors will be responsible for monitoring Low rated risks relating to their organisational area. • Low risks must be reported to the ARC or HRC (for Human Resources issues) and EMT, in accordance with the risk reporting procedure.

Risk Response

Management must prioritise the key risks and determine suitable responses for each key risk.

Activities to manage risks can vary depending on management's acceptance or non-acceptance of the risk level. There are four basic approaches for management to choose from when a risk has been identified and assessed. These should be communicated to the Risk Owner and appropriate action should be taken.

Tolerate	Indicates Management are comfortable with residual risk levels and no further action is required.
Treat	Indicates Management are not comfortable with the residual risk levels and that risk mitigation actions can be implemented to reduce the risk to a level which management is comfortable with.
Transfer	Indicates Management are planning or have transferred the risk to another party, through the use of insurance or other methods.
Terminate	Indicates Management are not comfortable with the residual risk levels and no risk mitigation actions can be implemented to reduce the risk to an acceptable level. Consequently the activities leading to the risk are discontinued.

Determine Target Risk

Based on this decision by Management, Risk Owners will then be required to identify the target risk rating, which refers to the desired level of risk that can be achieved in the next three years (i.e. 'tolerate' will mean Target risk equals Residual risk while 'treat' will mean Target risk is less than Residual risk). The following fields of the risk register should be completed for defining Target risk.

Target Consequence	The outcome or impact of an event, which is determined according to the consequence descriptor scale included in the Risk Assessment Procedure. Each risk should be considered in terms of its target consequence once all future actions are implemented.
Target Likelihood	The chance of the stated consequence occurring, which is determined according to the likelihood descriptor scale included in the Risk Assessment Procedure.
Target Risk Rating	Target risk rating is automatically determined from the target consequence and likelihood ratings by referring to the risk matrix.

1.6 Risk Treatment

For risks where there is a difference between Residual and Target risk (i.e. where further actions are required), the Risk Owner should identify actions (treatments) that will be implemented to enhance the level of control effectiveness. Not all risks will require actions, however, Management should clearly identify key risks where actions are required.

Risk treatment involves identifying the range of responses available for treating risks, assessing these options, and preparing and implementing the most appropriate treatment actions. These actions should consider the most appropriate option based on its cost benefit to Ports North and its integration with existing controls.

The following aspects of each risk treatment action should be noted in the risk register:

Action	Describes each of the risk treatment actions that will take place.
Responsible Person	For each action the person responsible for implementing that action should be noted.
Due Date	The due date for completing the risk treatment action.

Information regarding treatment actions will form part of the ongoing monitoring of risks. Once an action has been implemented (completed) it should be added into the controls and should trigger a reassessment of the residual risk rating.

Section 2. Risk Reporting Procedure

Purpose

This section defines processes that enable risks to be monitored and reported to meet the requirements of Ports North's Risk Management Framework. It describes the process, content and frequency of risk reporting.

Introduction

Risk reporting allows Ports North to manage and monitor key risks at all levels of the organisation. It represents how risks are communicated and helps ensure appropriate people are receiving timely risk information to enable informed decision-making and the selection of appropriate risk management actions.

The following reporting requirements are outlined in this guideline:

- Risk review and monitoring requirements.
- Risk reports to the ARC.
- Risk reports to the HRC.
- Risk reports to the Board.
- Risk register review.

2.1 Risk Review and Monitoring Requirements

Ongoing monitoring of risks is essential to ensure risks and control strategies remain relevant and effective, and that any changes in risk are identified and managed in a timely manner. Factors that affect the Consequence or Likelihood of an outcome change and it is, therefore, necessary to monitor risks frequently.

Communication and Consultation

Communication, consultation and regular feedback must take place during the risk management process. Communication involves sharing information with targeted audiences and participants providing feedback which contributes to and shapes decisions or other activities.

The Risk Register is used to maintain a record of all risks identified in Ports North.

Each risk is assigned a Risk Owner who is required to review and update their risks on a quarterly basis in preparation for risk reports. If a significant change in risk rating is detected outside these formal reviews (e.g. implementation of a significant control), the Risk Owner is required to update the Risk Register within one week. The risk register is used to generate risk reports, so accurate information is required.

When performing a review of their risks, Risk Owners should focus on the following attributes in the Risk Register:

- Risk information (risk name, risk description, owner, category, controls);
- Risk ratings (inherent and residual likelihood, consequence and risk rating); and
- Risk treatments, if applicable (action, responsibility, timeframe).

The Board shall review all Strategic Risks annually. The Board and ARC will monitor Strategic and Operational Risks according to the Risk Reporting Procedures outlined in this Section.

2.2 Review of Risks by Risk Owners

Quarterly Risk Review

On a quarterly basis, Risk Owners will receive copies of Risk Analysis Reports and Risk Registers from the Risk Coordinator.

Risk Owners must review the Risk Analysis Reports and Risk Registers and provide details of any changes and instructions for action to the Risk Coordinator, to enable the Risk Coordinator to update the Strategic and Operational risks and prepare Risk Reports to Audit and Risk Committee and Board of Directors.

2.3 Risk Reports to the Audit and Risk Committee

For each ARC meeting, Management will submit a report to the ARC that contains the Risk Dashboard, Action Plan and commentary regarding all Strategic Risks. In addition the report will provide commentary on the overall distribution of Operational Risks. The risk report will contain a number of sections as specified below:

Detailed Discussion of Specific Risks	• This section lists the Strategic Risks that have been considered in detail at previous meetings. • It also provides commentary in relation the Strategic Risks being reviewed in detail that meeting. • Risk Analysis Reports will be presented in the risk report, for those Strategic Risks being reviewed in detail.
Update on Risk Framework and Profile	• This section summarises the current status of Ports North’s Strategic and Operational Risk profiles. • It also provides commentary on the status of any risk activities that have been undertaken in the last quarter.
Risk Summary	• This section will provide an overall summary in graphic format of the current classification of all: ○ Strategic Risks; and ○ Operational Risks. • Notes relating to any change in the numbers of risks in each of the four classifications (i.e. Extreme, High, Moderate and Low) will also be included.

Risk Change Report	- The Risk Change Report summarises any relevant changes to Ports North's Strategic Risk Registers: o All new or re-rated Strategic Risks, including comments relating to any changes; and o Any Strategic Risks that have been closed.
Responses to ARC Requests	- Detailed responses to requests made by the ARC.
Risk Dashboards and Action Plans	- The following Dashboards will be presented in the risk report: o Dashboard of all Strategic Risks; o Risk Action Plan for Strategic Risks.

The ACR should review the risk report and provide changes and instructions for actions by Management. For each meeting, the ARC should also nominate 2-3 strategic risks that will be discussed in further detail at the next meeting.

Management will provide copies of the Risk Analysis Reports for those risks being reviewed in detail and be prepared to provide further information regarding that risk (e.g. background, controls, trends and treatment actions) and answer any further questions from the Committee.

2.4 Risk Reports to the Human Resources Committee

Management will submit an annual report to the HRC that contains Risk Analysis Reports and commentary regarding all Human Resources related Strategic Risks.

The HRC should review the risk report and provide changes and instructions for actions by Management. Management will be prepared to provide further information regarding that risk (e.g. background, controls, trends and treatment actions) and answer any further questions from the Committee.

2.5 Risk Reports to the Board

The Board will receive a Quarterly Report that contains the following sections:

Update on Risk Framework and Profile	- This section summarises the current status of Ports North's Strategic and Operational Risk profiles. - It also provides commentary on the status of any risk activities that have been undertaken in the last quarter.

Risk Summary	• This section will provide an overall summary in graphic format of the current classification of all: ○ Strategic Risks; and ○ Operational Risks. • Notes relating to any change in the numbers of risks in each of the four classifications (i.e. Extreme, High, Moderate and Low) will also be included.
Risk Change Report	• The Risk Change Report summarises any relevant changes to Ports North's Strategic Risk Registers: ○ All new or re-rated Strategic Risks, including comments relating to any changes; and ○ Any Strategic Risks that have been closed.
Responses to Board Requests	• Detailed responses to requests made by the Board.
Risk Dashboards and Action Plans	• The following Dashboards will be presented in the risk report: ○ Dashboard of all Strategic Risks; ○ Risk Action Plan for Strategic Risks.

2.6 Risk Analysis Reports

Risk Analysis Reports are required for all Strategic Risks.

Risk Action Plans are required for all Strategic Risks where the Residual risk is greater than the Target risk.

A template for the Risk Analysis Report is provided in Attachment 2 and a template for the Risk Action Plan is provided in Attachment 3.

Risk Analysis Reports and Risk Action Plans should be reported according to the following procedures:

Strategic Risks	Newly developed Risk Analysis Reports should be provided to the Chief Executive Officer for approval within one month of the risk being identified.
	Risk Analysis Reports for those risks being considered by the ARC or HRC should be provided to the relevant ARC or HRC meeting.
	Updated Risk Action Plans should be provided at each relevant ARC or HRC meeting.

2.7 Annual Risk Register Review

The Board will review the Strategic Risks annually. The Board will receive an annual report containing a table of all existing Strategic Risks.

Attachment 1: Responsibilities under Risk Management Framework

Board of Directors	The Board will regularly monitor Ports North's Strategic Risks and approve any documentation / disclosures provided by the ARC. In summary, the Board will: • Review and approve Strategic Risks annually. • Set and review Risk Appetite Statement (including risk tolerance) annually. • Review and approve any changes proposed by Management to Strategic Risks. This includes approval of any changes to the ratings of these risks. • Monitor all Strategic Risks on a Quarterly basis. • Approve any changes to the Risk Management Framework as specified by the ARC; and • Approve any external disclosures relating to risk processes.
Audit and Risk Committee	The ARC will assist the Board with reviewing risk management processes and Ports North's progress in implementing agreed risk management strategies. In summary the ARC will: • Review and endorse Strategic and Operational Risks in accordance with the Risk Reporting Procedure; • Review and endorse changes to the Risk Management Framework, as submitted by the Executive Management Team; • Ensure the Risk Management Framework is being effectively implemented and applied across the organisation; • Monitor the alignment of target risk ratings with risk appetite and Ports North's risk tolerance; and • Endorse any external disclosure relating to risk processes of Ports North for Board approval. • Review Strategic Risks in detail by considering the relevant Risk Analysis Reports and Action Plans. In addition to their usual roles, compliance and internal audit functions may be employed to enable evaluation of risk management practices and check the effectiveness of key controls identified in the Ports North risk profile. This activity will be overseen by the ARC. A more detailed overview of the ARC's responsibilities can be found in the Audit and Risk Committee Charter.

Human Resources Committee	The HRC will assist the Board with reviewing Human Resources Related Strategic Risks. In summary the HRC will: • Review and endorse Human Resources related Strategic Risks in detail by considering the relevant Risk Analysis Reports and Action Plans.

Chief Executive Officer	The CEO will be responsible for ensuring the Risk Management Framework is implemented and consistently applied across the organisation. In summary, the Chief Executive Officer will: • Review and approve Strategic and Operational Risks in accordance with the Risk Reporting Procedure; • Ensure the Risk Management Framework is implemented and applied; • Keep the Board and ARC informed about the status of risk management activities and Strategic and Operational risks in a timely manner; and • (With the General Manager Finance) state to the Board that:- o the statement regarding financial reports is founded on a sound system of risk management and internal compliance and control which implements Board policies; and o the risk management and control system is operating efficiently and effectively in all material respects.

Executive Management Team	The EMT has scheduled risk as a standing agenda item at its monthly meetings., The EMT's responsibilities will be fulfilled through: • Monitoring risk management across Ports North in accordance with the Risk Management Framework; • Regularly assessing, managing and reporting on Ports North's Strategic and Operational risk profiles in accordance with the Risk Reporting Procedure; and • Preparing external disclosures relating to risk processes of the organisation which may be required, and submitting these to the ARC for review and approval. In addition to their usual roles, compliance and internal audit functions may be employed to enable evaluation of risk management practices and check the effectiveness of key controls identified in the Ports North risk profile. This activity will be coordinated by the Executive Management Team.

Risk Coordinator	The Risk Coordinator provides a central resource for managing the Risk Management Framework and providing guidance to Management and staff regarding its application. The Risk Coordinator's responsibilities include: • Preparing risk reports to the Board, ARC and HRC; • Responding to any queries by the Board, ARC, HRC or Risk Owners; • Maintaining Framework documentation; • Facilitating risk management training sessions as required; • Coordinating processes to ensure risk owners comply with the Risk Management Framework; and • Coordinating annual Risk Management Framework review processes.

Risk Owner	Risk Owners are those Ports North staff who have been allocated a risk and are responsible for managing, monitoring and reporting on the status of the risk on a regular basis. Risk owners should follow the Risk Management Framework in fulfilling their responsibilities.

Managers	Across Ports North, personnel who supervise and manage other staff will be responsible for ensuring that: • Individuals who report to them incorporate risk management into their planning and decision making processes; • Projects and operations include the ongoing identification, assessment and management of all reasonably foreseeable risks arising from their activities; • Appropriate measures are developed and implemented to manage identified risks for themselves and their direct reports through ongoing risk assessments and monitoring of the effectiveness of controls; • Training takes place to ensure personnel are appropriately skilled in identifying and managing risks; and • Risk management processes are appropriately documented.

All Staff	Across Ports North, personnel who become aware of potential or actual risks will be responsible for ensuring that: • Risks are reported to their line manager as soon as practicable

Attachment 2: Risk Analysis Report Template

Risk Analysis Report

Risk # ______	**<RISK>**		
Risk description	<ENTER A DESCRIPTION OF THE RISK>		
Risk owner	<________>	**Date prepared**	<__________>

Inherent risk assessment			**Residual risk assessment**			**Target risk assessment**		
Critical	Likely	**Extreme**	Critical	Unlikely	**Extreme**	Critical	Rare	**High**

Summary of key issues/trends/ emerging factors

<PROVIDE A SUMMARY OF KEY ISSUES/ TRENDS AND EMERGING FACTORS FOR THIS RISK>

Current controls

Control	Responsible person	Last review date	Comments

Risk Treatments (actions)

Proposed actions	CBA?* (A/R)	Impact on risk rating (H/M/L)	Resource requirements	Responsible person	Due date	Comments/ current status

*CBA = Was a cost benefit analysis performed? (Accept/Reject)

Assurance Activities

Audit function	Current audits being undertaken	Frequency

Review and Approval

Version	Reviewed by	Approved by	Date

Risk Appetite Statement Alignment

Corporate objectives

1 Identify and develop new trade and business opportunities and grow existing business to provide value to Ports North and its shareholders
2 Manage and develop Port Property to provide sustainable commercial return to Ports North and its shareholders
3 Plan, develop and manage Port Infrastructure and assets to improve Port efficiency, meet the needs of customers and contribute to sustainable regional development
4 Maintain organisational capability and governance system to deliver the business requirements and maintain the organisation's reputation

	Where Ports North has an appetite for risk:	
1	Where the risk aligns with the achievement of corporate objectives	
2	Where the risk improves stakeholder or customer outcomes and/or contributes to regional economic growth	
3	That improve safety or port efficiency	
4	That improve the sustainability of our operations (socially, culturally, financially, environmentally)	
	Ports North *does not* have an appetite for risks:	
1	That result in a breach of our legal or regulatory obligations	
2	Where the outcome is likely to be corrupt, unethical or negatively impacts the organisation's reputation	
3	That detract from achievement of our corporate objectives	
4	That impact on our ongoing financial stability or solvency	
5	That contribute to significant safety and environmental incidents	
6	Which we do not consider we can adequately manage or mitigate, or which may have adverse consequences of such a nature that they may unduly impact on our ability to operate in the manner and at a level at which we aspire to operate	

Attachment 3: Risk Action Plan

Number	Risk	Possible Treatment Option	Due Date for Implementation	To be actioned by	Status	Revised Completion Date