Enterprise Risk and Resilience Policy

Brief description

This Policy sets out GPC's commitment to manage enterprise risks diligently to create and protect value for GPC and their stakeholders and aims to promote the implementation of a consistent risk management culture throughout GPC.

Document information	
Current version	#1412364v16
First released	December 2002
Last updated	21/11/2023
Review frequency	Every 2 years or as required
Review before	29/02/2024
Audience	GPC Representatives, Contractors, Consultants

Document accountability	
Role	**Position**
Owner	Board
Custodian	Chief Executive Officer

Approved by	Board on 15/12/23

If you require any further information, please contact the Custodian.

The current version of this Policy is available on GPC's Intranet.

1 Terms and definitions

In this Policy:

"Business Continuity Plan or BCP" means a formal plan which guides the organisation in responding to a Disruption Event and assists it in the recovery, resumption and restoration of the organisation's Critical Business Functions.

"Critical Business Function" means a business function or part thereof identified as essential for survival of the organisation and achievement of its Critical Objectives.

"Critical Objectives" means objectives that must be prioritised / achieved during a period of disruption. (Note these may relate to requirements of external stakeholders.)

Terms that are capitalised and not otherwise defined in this Policy are defined in the GPC Corporate Glossary Instruction (as listed in Appendix 1 – Related documents).

2 Introduction

2.1 Purpose

GPC recognises that effective risk management is essential to support the achievement of our corporate objectives and is committed to managing enterprise risks diligently to create and protect value for GPC and its stakeholders.

The purpose of this Policy is to capture this commitment and to:

- promote the achievement of GPC's objectives through focused whole-of-business risk management practices that are aligned to GPC's Risk Appetite Statements (as listed in Appendix 2 – GPC Risk Appetite Statements), business value creation and protection;
- enhance internal business resilience through an integrated risk management process;
- develop and maintain capacity to efficiently anticipate, recognise, respond to, and recover from, an emergency, major business disruption and/or crisis event; and
- promote a risk intelligent organisational culture.

2.2 Scope

This Policy applies to all GPC Representatives and (unless otherwise specified) any other worker engaged under the direct management of GPC (for example Contractors, Consultants, agency resources, and volunteers). Where relevant, risk management requirements for external entities engaged by GPC must be included in contractual arrangements, and contractors must appropriately identify, assess, notify and manage risks related to GPC sites, including site-based activities according to all GPC Policies and Standards.

GPC recognises that all areas of the business face uncertainty in some situations or events (risks) that may have an effect on GPC's strategic objectives. The Policy therefore applies to all GPC's activities and operations.

2.3 Objectives

The aim of this Policy is to implement and embed a consistent risk management culture that promotes individual responsibility for the management of risk. This will be achieved through:

- sound governance practices;
- protecting and enhancing GPC's reputation;
- confident and informed decision making and planning;
- continuously reviewing GPC's exposure to risks and opportunities;
- promoting a risk intelligent organisational culture; and
- establishing the right balance between control and the risks GPC is willing to accept in the environment within which it operates.

3 Commitments

3.1 Risk management principles

In managing risk, GPC uses a risk management strategy and integrated risk and resilience framework that is based on the principles of *ISO 31000:2018 – Risk Management*.

Specifically, GPC will create and protect value for Stakeholders by:

- integrating risk management across all business processes, including (but not limited to) strategic planning, tactical (change and project management initiatives) and operational processes;
- providing a key decision-making process to enable informed decisions, distinguish between alternative options and priorities;
- ensuring alignment between risk management practices and GPC's vision, mission and values;
- promoting aligned assurance across specialist areas of risk management including (but not limited to) Health, Safety and Wellbeing, Environment, Information Security, Business Continuity, Compliance and Internal Audit;
- ensuring the process of managing risk is based on the best available information at the time, including historical data, modelling and forecasts, stakeholder feedback, past experience and subject matter expertise;
- ensuring that risk management architecture and processes are fit for GPC's purpose and are dynamically reviewed;
- taking human and cultural factors into account, recognising that the capabilities, perceptions and intentions of people can either facilitate or hinder the achievement of strategic objectives;
- being transparent and inclusive with an enterprise wide application; and
- facilitating continual improvement of the organisation and its control frameworks.

3.2 GPC risk appetite

Central to GPC's strategy for managing risk are GPC's Risk Appetite Statements (as listed in Appendix 2 – GPC Risk Appetite Statements) which have been developed by the Board. They summarise the amount of risk that GPC is willing to seek or accept in the decisions made in pursuit of GPC's objectives. They apply to the management of existing activities, as well as new opportunities. For each risk category identified by GPC, specific risk appetite statements and tolerances have been set.

3.3 Risk aware organisational culture

GPC promotes an organisational culture that is risk aware and empowers staff to make agile, informed and risk-based decisions in accordance with GPC's Risk Appetite Statements.

GPC recognises that risk management is an integral part of strategic focus and good management practices and is committed to establishing an organisational culture that ensures risk management is embedded consistently in its activities and business processes, reflecting the International Standard on Risk Management (ISO 31000:2018).

4 Implementation framework

4.1 Integrated risk and resilience framework

To ensure a coordinated, consistent and integrated enterprise risk management and resilience capability exists across all levels of the organisation, GPC employs an integrated risk and resilience framework that incorporates and aligns business functions and specialist areas of risk management across GPC, which include (and is not limited to):

- Enterprise risk management;
- Health and safety;
- Environment;
- Business continuity management;
- Security (Physical and information security over critical infrastructure, ICT networks, people, equipment and buildings);
- Insurance protection;
- Quality management;
- Policy & regulatory compliance;
- Asset management;
- Corporate business planning and budgeting;
- Financial control;
- Procurement and supply chain management;
- Resources management (people, capital and equipment);
- Information management and ICT Design;
- Port development;
- Corporate sustainability;
- Cargo handling operations.

4.2 Organisational resilience

In recognising that the concept of organisational resilience is the practical response to the needs of an enterprise to address the combined issues of security, preparedness, risk and survivability, GPC adopts a resilience approach to managing risks. GPC's resilience approach assists in developing the capability to deal with unexpected disruptions to business-as-usual activity.

GPC considers its level of organisational resilience to be an outcome of the effectiveness of its control and operating environment capabilities in dealing with foreseeable and unforeseeable risks. These capabilities are defined as follows:

- effective business as usual capability demonstrated through efficient and organised plans and processes (e.g. GPC's core set of capabilities) that assists GPC to resist the disruptive influences experienced in the normal course of doing business;
- ability to change and adapt by proactively responding to disruptions using non-routine management. These events include those triggered by, but not limited to, major disruptions (such as natural disasters) and other significant changes in its competitive or regulatory environment.

In order to mitigate impacts of disruption-related risks and support the achievement of corporate objectives, GPC requires the implementation of its established crisis management decision-making framework and business continuity management approach.

(a) Crisis management

To facilitate the active management of an incident or event with the potential to seriously affect GPC's ability to operate, profitability, reputation or seriously harm people, the environment, property or infrastructure, GPC has established the Crisis Management Procedure which provides the decision-making framework necessary to coordinate response activities following the onset of a disruptive event with the aim of minimising impacts on people, property, the environment, profitability, reputation and disruption on operations.

The Procedure also outlines the criteria for the formation of the GPC Crisis Management Team who is responsible for providing the strategic direction to enable the overall response and recovery effort during a disruption event.

For further details, refer to the Crisis Management Procedure.

(b) Business continuity management

GPC's business continuity management framework incorporates best practices principles and guidance from *ISO 22301:2019 – Societal security – Business continuity management systems – Requirements* and comprises the following elements in addition to this Policy:

- Business Continuity Management Standard;
- ResilienceONE (the BCM System); and
- Business Continuity Plans (BCPs) for GPC's Critical Business Functions.

Further details of these components are outlined within the Business Continuity Management Standard.

4.3 Supporting systems

There are two key systems supporting enterprise risk:

- SAI360 - is GPC's integrated risk management system. It is the approved system repository for all GPC risk registers;
- ResilienceOne - is GPC's business continuity management framework, used for BCM planning, testing and enforcement, by all GPC departments to mitigate risk outcomes.

5 Monitoring and review

The Audit and Risk Committee has been established to assist the Board in fulfilling its corporate governance responsibilities, by monitoring and reviewing GPC's Audit and Risk management systems and conformance to this Policy.

This Policy will be reviewed every two years or as other circumstances may require (e.g. to implement recommendations), as determined by the CEO in consultation with the Executive General Manager Safety & ESG.

6 Appendices

6.1 Appendix 1 – Related documents

(a) Gladstone Ports Corporation documents

The following documents relate to this Policy:

Type	Document number and title
Tier 1: Policy	N/A
Tier 2: Standard/Strategy	#829152 Enterprise Risk Management Standard #852778 Business Continuity Management Standard
Tier 3: Specification/ Procedure/Plan	#872678 Crisis Management Procedure #936233 Enterprise Risk Management Procedure
Tier 4: Instruction/Form/ Template/Checklist	#1621179 GPC Corporate Glossary
Other	#159390 Board Charter #106187 Audit and Risk Committee (ARC) Charter

6.2 Appendix 2 – GPC Risk Appetite Statements

When reading GPC Risk Appetite Statements, it is important to note:

- it is not a substitute for, but an adjunct to, GPC's extensive and comprehensive risk management framework, and is consistent with the organisation's risk matrices for individual risk areas;
- it is developed to guide decision-making, to allocate response to the level of risk which is considered acceptable; and the requirements for escalation and reporting. The Risk Appetite Statement is a 'trigger for decision making, escalation and reporting (as applicable) versus being a 'rule based parameter'.

Risk Category	Appetite				
	Very Low	Low	Medium	High	Very High
Health and Safety	(3)				
Compliance		(5)			
Reputation		(5)			
Financial			(7)		
Customer Experience			(7)		
People		(5)			
Delivery of Core Operations & Services			(7)		
Information Management		(5)			
Security (including cybersecurity)	(3)				
Major Change Failure		(5)			
Governance		(5)			
Environment		(5)			

Table 1: Risk Category Appetite Levels

(a) Health and Safety

GPC has a **very low appetite** for risk in practices or behaviours that lead to the harm of staff, contractors or visitors on or in our sites (within our control) or when undertaking related operating activities.

GPC has, within this very low appetite for health and safety risk, the following tolerance (controls/limits):

- a very low tolerance for inadequate or untimely remedy and reporting of breach incidents, or near misses;
- no tolerance for negligent or deliberate violations of health and safety obligations.

(b) Compliance

GPC has a **low appetite** for breaches in applicable legislation, regulation, government policy or direction, industry codes and standards.

GPC has, within this low appetite for compliance risk, the following tolerance (controls/limits):

- no tolerance for non-compliance with formal performance agreement between the Board and its shareholding Ministers (the Statement of Corporate Intent);
- no tolerance for activities being undertaken in a matter that breaches the requirements of its approvals;
- no tolerance for breaches in workplace health and safety laws or the organisation's workplace health and safety policies and procedures;
- a very low tolerance for inadequate or untimely remedy and reporting of breach incidents, or near misses.

(c) Reputation

GPC has a **low appetite** for risk in the conduct of any of its activities that puts its reputation, or the reputation of its stakeholders in jeopardy, could lead to undue adverse publicity, or could lead to loss of confidence by customers, the communities it serves, operates in, or is funded by.

GPC has, within this low appetite for reputational risk, the following tolerance (controls/limits):

- medium tolerance for activities that may impact its social licence to operate in the communities it operates in, where such activities are in accordance with approved strategies, plans and communications.

(d) Financial

GPC has a **medium appetite** for risk to its short to medium-term financial performance in pursuit of long-term financial sustainability and overall financial strength.

GPC has, within this medium appetite for financial risk, the following tolerance (controls/limits):

- no tolerance for fraud or corruption perpetrated by its Representatives, Contractors or Consultants.
- very low tolerance for inadequate or infrequent financial forecasting to support both the short-term and long-term financial sustainability of the organisation.
- high tolerance for investment in innovative opportunities which can enable and drive the pursuit and achievement of strategic objectives and initiatives.

(e) Customer experience

GPC has a **medium appetite** in accepting this risk subject always to ensuring that potential benefits and risks are fully understood before developments are authorised and that sensible measures to mitigate risk are established.

GPC has, within this medium appetite for risk to the customer experience, the following tolerance (controls/limits):

- no tolerance for activities being undertaken in a manner (or with an outcome) that breaches undertakings in the Statement of Corporate Intent as they relate to customer experience;
- no tolerance for conduct that is in breach of the customer service standards set out in the Code of Conduct.

(f) People

GPC relies on motivated and high calibre Employees to perform its functions. GPC aims to create an environment where Employees are empowered to the full extent of their abilities. GPC has a **low appetite** for losses to the value of the organisation's competencies, knowledge and skills. GPC places high importance on a culture of integrity in conduct, performance excellence, equality and diversity, dignity and respect, collegiality, feedback, and the development of staff. GPC takes very seriously any breaches of its Code of Conduct. GPC has a **very low appetite** for behaviour or conduct which does not meet the standards set out in the Code of Conduct.

GPC has, within this very low appetite for human resources behaviour risk, the following tolerance (controls/limits):

- no tolerance for behaviours or actions that result in harm to employees, contractors or visitors (within its control and responsibility);
- no tolerance for conduct that is unlawful or unethical or otherwise in breach of the Code of Conduct.

(g) Delivery of core operations and services

Whilst the ability to support operations on a day-to-day basis is important, GPC has a **medium appetite** for change to ensure that GPC has the right strategies, infrastructure, facilities and resources, staff capabilities, organisation structure and culture to optimise performance. Such changes will be in accordance with approved strategies, plans and budgets to ensure existing and future assets are procured, operated and maintained to meet strategic plans.

(h) Information management

GPC has a **low appetite** for the compromise of processes governing the use of information, its management and publication.

GPC has, within this low appetite for information management risk, the following tolerance (controls/limits):

- no tolerance for the unauthorised access to, or disclosure, of commercially sensitive and/or private information of the organisation or its customer; and
- no tolerance for conduct that is in breach of the confidential information protection standards set out in the Code of Conduct.

(i) Security (including Cybersecurity)

GPC has a **very low appetite** in relation to damage to GPC critical infrastructure and information assets from threats arising from physical security breaches and malicious cyber-attacks. GPC aims for strong internal processes and continuous improvement of robust physical and information security controls.

GPC has, within this very low appetite for security risk, the following tolerance (controls/limits):

- no tolerance for malicious or mistaken actions which aid the bypass of physical security and cybersecurity controls leaving commercially valuable and/or private information of the organisation or its customers vulnerable;
- no tolerance for malicious actions which aid the bypass of maritime security zones; and
- medium tolerance for the pursuance of projects and strategies which strengthen and continuously improve GPC's physical security and cybersecurity protocols and controls.

(j) Major change failure

GPC has a **low appetite** for incidents or impacts which are generated by poor change management practices.

GPC has, within this low appetite for major change failure risk, the following tolerance (controls/limits):

- a very low tolerance for incidents or impacts which are generated by poor capital expenditure project management practices and which compromise agreed project outcomes (more specifically project timeframes, project financial allocation and project resourcing in relation to capital expenditures).

(k) Governance

GPC has a **low appetite** for the compromise of processes and practices that are in breach of approved governance standards and procedures.

(l) Environment

GPC has a **low appetite** for risk in practices or behaviours beyond approval conditions that lead to environmental harm on or in our sites (within our control) or offsite when undertaking related operating or project activities.

GPC has, within this low appetite for environment risk, the following tolerance (controls/limits):

- a low tolerance for inadequate or untimely remedy and reporting of breach incidents, or near misses;
- no tolerance for negligent or deliberate violations of environmental obligations.

6.3 Appendix 3 – Revision history

Revision date	Revision description	Author	Endorsed by	Approved by
Dec 2002	#81517 approved			Board
26/02/10	#159385 approved			Board
26/02/14	#924357 approved			Board
29/08/19	#1412364 v1 – 9 reviewed v10 – Board approved 29/08/19 and published 02/09/19	Sohana Maharaj, Chief Governance Officer	EMT	Board
30/06/20	v11 – reviewed in accordance with GPC's Risk Review Framework v12 – EMT approved 02/09/20 and published 03/09/20	Mariette Lansdell, Deputy Company Secretary	Rufus Gandhi, General Counsel and Company Secretary	EMT
10/09/20	v13 – Include an Environment risk appetite statement	Mariette Lansdell, Deputy Company Secretary	Rufus Gandhi, General Counsel and Company Secretary	Board
22/09/20	v14 – Minor amendment to add two paragraphs to 6.2(k) Environment	Mariette Lansdell, Deputy Company Secretary	Rufus Gandhi, General Counsel and Company Secretary	EMT
11/08/21	V15 – updates to Risk Appetite Statements, change reference to Committee Charters from Governance, Risk and Compliance (GRC) Committee to Governance and People (GAP), and Finance, Investment, Commercial, and Audit (FICA) Committee to Finance, Audit and Risk (FAR) Committee	Mariette Lansdell, Acting Company Secretary	Rufus Gandhi, General Counsel and Company Secretary	EMT & Board
21/11/2023	V16 – Administrative Amendment: Change reference to Committee from Finance, Audit and Risk (FAR) to Audit and Risk Committee (ARC) Full review to occur early 2024.	Kylee Lockwood, Acting Risk and Governance Project Lead	Executive Leadership Team and CEO	Board