

Risk Management Policy

Purpose

This document specifies the Generator Property Management Pty Ltd (GPM) policy and framework approach to managing enterprise risk, including how this approach will be integrated with the company's business planning processes, decision making structures and operational procedures.

Scope

This policy applies to all GPM employees and contractors, to all GPM workplaces, and to all GPM activities. It applies to all enterprise risk categories, including, but not confined to:

- finance and legal
- governance
- operating environment
- systems
- human resources, including work health, safety and welfare
- government
- stakeholders; and
- strategic delivery

Policy

1. Risk management objectives

Enterprise risk management creates and protects the value that the company generates for the Government and the people of NSW, as it works to achieve its vision and corporate objectives. It is integrated in all business decision making.

2. Risk management standards and structure

In managing enterprise risk, the company will apply and be guided by:
Australian/New Zealand Standard Risk management—principles and guidelines (AS/NZS ISO 31000:2018)

The company's enterprise risk management framework consists of:

- Risk management principles
- Risk management policy and procedures
- Risk management plans

3. Risk management principles

The company's framework and approach to managing risk are guided by the principles specified in AS/NZS ISO 31000:2018. These specify that risk management across all areas of the company must:

- create and protect value
- be an integral part of all processes
- be part of all decision making

Risk Management Policy

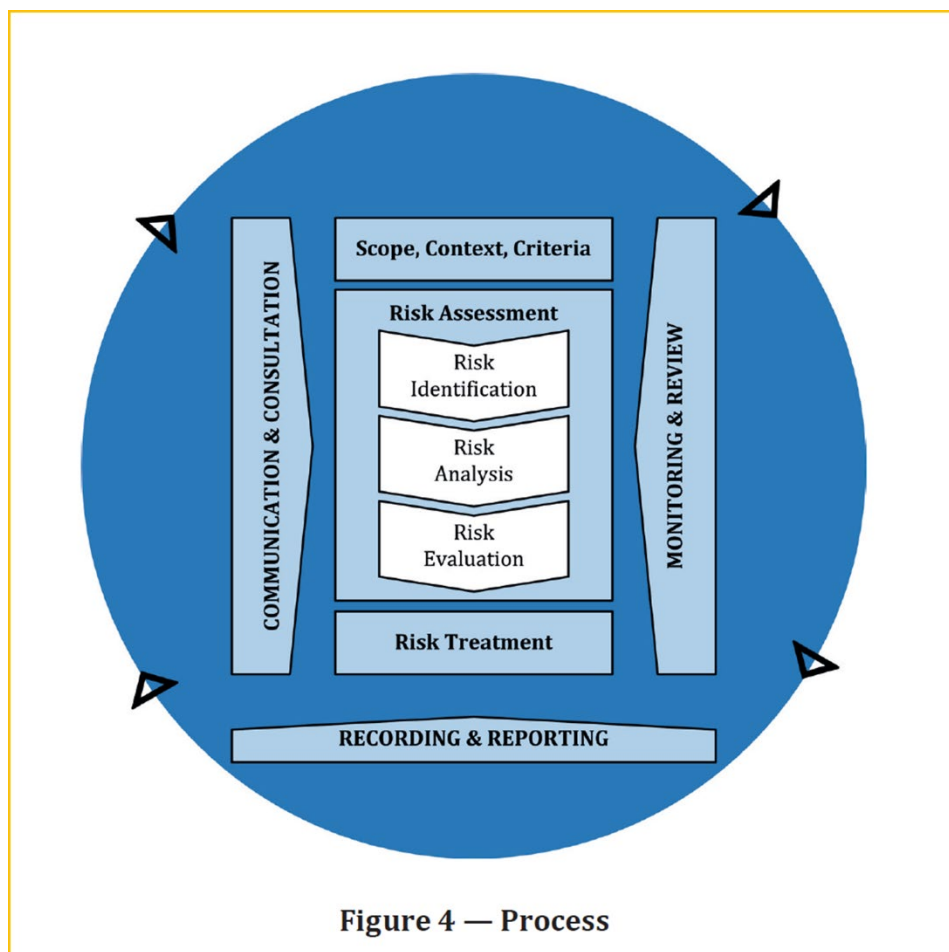
- explicitly address uncertainty
- be systematic, structured and timely
- be based on the best available information
- be tailored to the company's context and risk profile
- take human and cultural factors into account
- be transparent and inclusive
- be dynamic, iterative and responsive to change
- facilitate continual improvement.

4. Enterprise risk management process

All staff are accountable, within their sphere of influence, to manage risks. Staff must use the risk management process specified in AS/NZS ISO 31000:2018 and outlined in Figure 1 to manage risk. This process must be:

- an integral part of all management
- embedded in culture and practices
- tailored to each business process in the organisation.

The Risk Management Process as per (AS/NZS/ISO 31000:2018)



Risk Management Policy

5. Risk management implementation

The Chief Executive Officer must:

- oversee implementation of the risk management framework, including information and training sessions and communication and consultation with employees
- oversee the implementation of the risk management process.

6. Risk management integration

The risk management process must be embedded within all management processes, including policy development, business and strategic planning and review, and change management processes.

Staff who oversee management processes, including setting policy, determining procedures, systems and rules, must ensure that the risk management process is embedded.

Management processes which must have the risk management process embedded within them include, but are not limited to:

- strategic and business planning and review
- organisational performance reporting and review
- budgeting and financial administration
- purchasing and procurement
- business continuity and disaster recovery planning
- work health, safety and welfare management
- environmental management
- project management, including capital projects
- human resource management, including workforce planning, recruitment,
- organisation development and change management
- stakeholder relationship management and service delivery.

7. Review and evaluation

The Chief Executive Officer must coordinate:

- monitoring risk management performance across the business
- periodically measuring progress against the risk management plans
- periodically reviewing to check that the Risk Management Framework including policy, procedures, understanding of detail and risk management plans continue to be appropriate to the department
- reporting to the Board on risk status, trends, understanding and progress with the risk management plans and how well the risk management policy is being followed
- review of the risk management framework.

In coordinating these activities, the Chief Executive Officer must work in cooperation with the company Board, its Auditors and all company staff.

8. Continuous improvement framework

The Chief Executive Officer must coordinate continual improvement of the risk management framework. All GPM staff should be proactive and involved in recommending improvements based on results of monitoring and reviews of the risking in their area of expertise.

Risk Management Policy

9. Risk management culture

The Chief Executive Officer will lead and advocate positive risk management behaviour within the company through:

- demonstrating the application of risk management in day-to-day activities
- communicating the benefits of risk management throughout the organisation
- incorporating measures of risk culture and attitude into performance management systems
- instituting positive reinforcement of effective risk management.

Procedures**Risk Register**

The Company Risk Register will consist a top down assessment of the strategic risks that the Company is exposed to and a bottom up assessment from within each operational area of the Business. The assessment of risks in the Risk register is to be undertaken in accordance with the principles set out *AS/NZS/ISO 31000:2018*..

These risks are to be recorded and ranked in the Corporate Strategic Risk Register to establish which risks are the most significant. Each of these risks is to be assessed for understanding of the detail necessary to quantify and control the risk. The most significant risks will be reviewed to ensure the key steps that need to be taken to control the risk, prepare to deal with the consequences if it materialises and the steps to be taken to increase understanding and mitigation of the risk are in place.

Each Officer will be accountable for establishing a bottom up assessment of all risks in their areas of control. These risks are to be recorded into the Risk Register for each area in the same manner as the Corporate Strategic Risk Register and are to be ranked to identify the most significant risk in their area. The most significant inherent risks are to be reviewed to ensure the key steps that need to be taken to control the risk, prepare to deal with the consequences if it materialises and the steps to be taken to increase understanding and mitigation of the risk are in place.

The combination of individual area risk registers with the Corporate Strategic Risk Register will ensure all risk are assessed on the same basis and the most significant are identified at the highest level for reporting to the Board with their management plans.

The Corporate Strategic Risk Register is to be reviewed annually or if there is a significant change in operations and the results of this review reported to the Board along with the Risk management actions status for the most significant risks.

Roles and responsibilities**Chief Executive Officer**

The Chief Executive Officer is accountable for ensuring the effective implementation of the enterprise wide risk management framework. This includes:

- Implement this Board approved policy.
- In consultation with the Board communicated the agreed risk appetite.

Risk Management Policy

- ensuring the enterprise risk management framework is implemented and the risk register is reviewed regularly.
- communicating the benefits of risk management throughout the organisation.
- aligning risk management objectives with the company's objectives and strategies.
- monitoring risk management performance.
- ensuring legal and regulatory compliance.
- allocating necessary resources to enterprise risk management.
- coordinate establishment of accountability, authority and appropriate competence for managing risk, including implementing and maintaining the risk management process and ensuring adequacy, effectiveness and efficiency of controls.
- coordinate the integration of risk management into company processes, ensuring that risk management is part of, not separate from these processes.
- coordinate a company-wide management framework for risk management.
- coordinate internal communication and reporting mechanisms to support accountability and ownership of risk.
- ensuring staff are implementing the risk management policy as intended.
- implementing, monitoring and continuously improving the effectiveness of mitigation strategies.
- reviewing recommendations from the company Auditors and,
- reporting routinely on the status of risk management activities and risks to the Board.
- reviewing and ensuring the risk management framework remains appropriate.
- reviewing whether a sound and effective approach has been followed to develop risk.
- working with staff to embed risk management into day to day decision making.

All Staff

All staff are responsible for the management of risk within their sphere of influence. This includes:

- using a risk management approach in all decision making.
- familiarisation with the risk management process and its application within their areas of responsibility.
- identification, assessment, reporting in a Risk Register and management of risk in their area of responsibility.
- applying risk plans in their areas of responsibility by identifying, communicating and responding to expected or emerging risks.

Definitions

- **Enterprise Risk Management (ERM):** includes the methods and processes used to manage risks and seize opportunities related to the achievement of our corporate and business objectives.
- **Objectives:** are specific, realistic and measurable goals which enable the company to deliver on its priorities within a given period of time as expressed in our Strategic Plan.
- **Risk:** the effect of uncertainty on objectives.

Risk Management Policy

- **Risk management:** the coordinated activities to direct and control an organisation with regard to risk.
- **Risk management framework:** the totality of the structures, methodology, procedures and definitions that an organisation uses to design, implement, monitor, review and continually improve its risk management processes.
- **Risk management policy:** clarifies the company's objectives for and commitment to risk management.
- **Risk management procedures:** the systematic application of management policies and practices to the tasks of communicating, consulting, establishing the context, identifying, analysing, evaluating, treating and monitoring and reviewing risk.
- **Risk register:** Part of the risk management plan that identifies risks, evaluates them and identifies current or future risk controls to modify the risk.

Elements include:

- **Risk owner:** the person or entity with the accountability and authority to manage a risk.
- **Controls:** measures that modify risk such as processes, policies, devices, practices or other actions that act to minimise negative risks or enhance positive opportunities.
- **Risk appetite:** the amount and type of risk that an organisation is prepared to pursue, retain or take. The company's risk appetite is articulated through its descriptions of consequence and likelihood, its matrix for rating risk and its risk registers.
- **Risk tolerance:** an organisation's or stakeholder's readiness to bear the risk after risk treatment in order to achieve its objectives.
- **Risk assessment:** the overall process of risk identification, risk analysis and risk evaluation.

Review:

This document will be subject to review every 2 years or as required to meet GPM's business requirements. Regular internal audits may also be conducted.

Authorised:



David Wood
Chief Executive Officer