RISK MANAGEMENT AND RESILIENCE POLICY

1. PURPOSE

The purpose of this Policy is to define the whole of business portfolio-wide principles-based approach to Risk Management (RM) and Organisational Resilience (OR) through the utilisation of an integrated framework to enable EQL to provide a structured approach to consistently delivering against risk management and organisational resilience objectives and strategies established by the EQL Group.

2. POLICY STATEMENT

The EQL Group is committed to embedding a risk management and organisational resilience approach across all levels of the business to support the delivery of strategic and operational objectives. This Policy sets out the overarching RM and OR architecture, principles and expectations to enable the EQL Group to utilise appropriate integrated practices in order to be a resilient, flexible, adaptable, and sustainable business.

3. IMPLEMENTATION

The EQL Board and Executive acknowledge that the organisation operates as a Government Owned Corporation under the Government Owned Corporations Act 1993 (Qld) in the capacity of a critical infrastructure owner and operator. This requires EQL to maintain delivery of efficient, effective, integrated and timely services to meet both the expectations of its customers and all other key stakeholders.

EQL recognises that organisational resilience is dynamic and emerges from the complex interaction between a wide-range of business processes. This policy incorporates the integration of risk management and organisational resilience for the EQL Group to develop, implement and maintain a robust and appropriate portfolio risk management and organisational resilience program.

Through collaboration, communication and education, the following business functions will align with the RM and OR management approach across the EQL portfolio:

- Health, Safety & Environment;
- Asset management (network and non-network functions and projects);
- Corporate business planning and budgeting;
- Corporate financial;
- Insurance ;
- Compliance, legal and regulatory management aspects;
- Quality management;
- Security management (critical infrastructure, electricity network, ICT, and physical - people, buildings, non-electrical equipment);
- Purchasing and supply chain management;
- Resources management (people, equipment and capital);
- Retail / trading management and all other Retail functions;
- Business disruption (emergency, disaster, business continuity, crisis situations); and
- Digital Information Management and ICT Design.

Risk Management

This policy articulates the responsibilities for the management of risk and ensures EQL uses its risk management capabilities to maximise value from assets, projects and other business opportunities.

EQL promotes a risk-aware portfolio-wide culture in all decision making. Through the skilled application of high quality, integrated risk analysis, our people will utilise risk effectively in order to enhance opportunities and reduce threats to deliver secure, affordable and sustainable energy solutions for our customers and the community.

Risk is an integral and unavoidable component of EQL's business and can have positive (opportunity) or negative (threat) characteristics which may impact the achievement of strategic and operational objectives. EQL has adopted a combined "top-down" "bottom-up" approach to risk management, which focuses on both setting the strategic direction and implementation of a robust control framework across the entire business. EQL is committed to:

- being proactive and effective in the identification and management of all risks;
- behaving as a responsible corporate citizen, protecting employees, contractors, customers, the community and the broader environment from unnecessary injury, loss or damage;
- achieving its strategic objectives by seeking opportunities to improve the business and optimise risk management; and
- finding the right balance between the cost of control and the risks it is willing to accept as the legitimate grounds for earning reward.

EQL's Risk Appetite Statement articulates the significant risks to which EQL is exposed and details the extent to which those risks will be accepted. The Board monitors EQL's adherence to the Risk Appetite Statement and the broader risk management process.

EQL's risk management architecture (adopting the principles of ISO: 31000) aims to create and protect value to the portfolio by:

- integrating across all business processes, including (but not limited to) strategic planning and all change and project management initiatives;
- providing a key decision-making tool to enable informed decisions, distinguish between alternative actions and prioritise;
- integrating risk as part of health and safety, environmental, asset, operational, project and strategic planning processes;
- ensuring the process of managing risk is based on the best available information available at the time, such as historical data, modelling and forecasts, stakeholder feedback, past experience and subject matter expertise;
- ensuring that risk management architecture and processes are tailored to the requirements of EQL and dynamically reviewed using the mechanisms defined within Board agreed processes;
- 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 via the portfolio-wide risk management tool; and
- facilitating continual improvement of the organisation and its control frameworks.

To support this approach, risk analysis is applied to all aspects of the business by management, staff and contractors, following the principles and processes as set out in the portfolio-wide Risk Management Standard (currently under development) and utilising the EQL Risk Evaluation (Consequence and Likelihood) Matrix to assess risk from an EQL portfolio perspective.

Organisational Resilience

EQL is committed to managing disruptive risks to the business through the design and implementation of a fit-for-purpose organisational resilience approach to strengthen EQL's ability to be able to respond to short term shocks – such as natural disasters or significant changes in market dynamics – and take advantage of long term trends and challenges. Ensuring business continuity and to safeguard Queensland's electricity distribution network and critical assets to support the social and economic wellbeing of Queensland. EQL understands the significant consequential impacts on communities, businesses and governments should this service be degraded or rendered unavailable for an extended period.

The EQL Organisational Resilience Framework includes emergency, crisis and disaster management, business continuity management and security management (including protective and cyber security) arrangements for the management of foreseeable and unforeseeable risks and threats to the continuity of essential services and critical business functions. It is an all hazards approach to the management of actual or potential threats to EQL's strategic objectives and values, financial stability and long term ability to do business.

EQL's Organisational Resilience strategy is in alignment with the Australian Government's Critical Infrastructure Resilience Strategy, and Australian and Internal Standards, Guides and industry best practice.

EQL's Organisational Resilience is based on the following principles:

- Appropriateness (Appropriate risk management of disruptive threats by implementing fit-for-purpose prevention and mitigation measures identified through risk assessments and risk management plans that address a broad range of hazards and their consequences.)
- Effectiveness (Building capacity within EQL to be able to effectively respond to business disruptions with appropriate and contemporary emergency/crisis management, business continuity and recovery plans that are continually improved through ongoing assurance activities to ensure optimal resiliency.)
- Continual Improvement (Creating an organisational culture that has the ability to efficiently and safely provide service during interruptions, emergencies and disasters, and return to full operations quickly; through the continual assessment of threats and hazards, and analysis and application of learnings from incidents, near misses and events; and making use of contemporary bodies of knowledge on organisational resilience.)

Roles and Responsibilities

This policy applies to the EQL Group, its officers, employees and contractors (where applicable) and any other personnel notified that this policy applies to them.

To achieve both RM and OR objectives, EQL expects that its employees and contractors, regardless of their appointment level, will uphold their employment responsibilities and in doing so will positively influence EQL's RM and OR.

Role / Position	Responsibilities
EQL Board	EQL's Board retains ultimate responsibility for risk management and organisational resilience and for determining the appropriate level of risk that the Board is willing to accept in the conduction of EQL's business activities. The Board is responsible for approving this policy, the risk appetite statement and risk evaluation matrix and is responsible for oversight of business critical / strategic risks and the adequacy of the risk management framework.
Board Committees	The Board Committees will monitor and as necessary make recommendations to the Board in respect to the adequacy and effectiveness of the Risk Management and Organisational Resilience strategy and approach. The Board committees will review for Board approval this policy, risk appetite statement and risk evaluation matrix. The Board committees will provide oversight, discuss and refer business critical / strategic risks and the risk management framework to the Board as appropriate.
Executive Leadership Team (ELT) **(Chief Executive Officer (CEO) & Executive General Managers (EGMs), (both individually and collectively)**	Ultimate accountability for ensuring that the EQL Group has identified and managed significant portfolio risks and has effective risk management and organisational resilience strategies. Each executive is accountable for ensuring portfolio risks are identified and managed within their business unit and for having appropriate crisis, disaster, incident, emergency management and business continuity planning in place. Responsible for promoting risk management and organisational resilience practices within their business units, and how they enable and support the achievement of team and business work plans to support achievement of organisational objectives.
General Managers	Responsible for ensuring portfolio risks are identified, managed and escalated / referred to the ELT/ EGM's (as appropriate) within their teams and for having appropriate crisis management and business continuity planning in place. Responsible for promoting risk management and organisational resilience practices within their teams, and how they enable and support the achievement of team and business unit work plans.

Role / Position	Responsibilities
Line Managers and Supervisors	Responsible for ensuring risks are identified, managed and escalated / referred to the GM/EGMs (as appropriate) within their teams and for having appropriate crisis management and business continuity planning in place. Responsible for promoting risk management and organisational resilience practices within their teams, and how they enable and support the achievement of team work plans.
Risk Coordinators	Responsibility for maintaining the business unit risks register, engagement with business unit management teams on existing and emerging risks, mitigations, escalation and de-escalation of risk and the risk reporting for the business unit. They monitor and challenge risk mitigation plans developed and implemented within the business unit. The business unit risk coordinators actively collaborate cross-functionally with other Risk Coordinators and the Portfolio Risk Management team. They are responsible for promoting risk management practices within their business unit / teams, and how they enable and support the achievement of team and business work plans.
Portfolio Risk & Compliance team	Accountable to the EGM SPI for the development, implementation and continuous improvement of RM and OR architecture, strategies and framework including terminology, accountabilities, principles, practices, systems, tools, reporting, communication and training.
Other Employees, Contractors and subcontractors	Responsible for familiarising themselves with this Policy and the supporting strategies, processes and plans that affect their workplace activities, incorporating risk management and organisational resilience practices into their day to day activities and reporting and escalating all events, risk concerns, issues and breaches.

4. REFERENCES

AS/NZS ISO 31000:2009 *Risk management—Principles and guidelines*

ISO Guide 73 *Risk management—Vocabulary*

ISO 22316:2017 *Security and resilience — Organisational resilience — Principles and attributes*

(American National Standards Institute) ANSI/ ASIS.SPC.1:2009 *Organizational Resilience: Security, Preparedness and Continuity Management Systems – Requirements with Guidance for Use*

ISO 22301:2012 *Societal security - Business continuity management systems – Requirements*

BS 65000:2014 Guidance and Organisational Resilience; and ASIS SPC.1-2009 Organisational Resilience: Security, Preparedness, and Continuity Management Systems – Requirements with Guidance for Use.

Disaster Management Act 2003 (Qld)

5. DEFINITIONS

For the purpose of this Policy the following definitions apply:

Organisational Resilience

Organisational resilience is the ability of an organisation to absorb and adapt in a changing environment to enable it to deliver its objectives and to survive and prosper.

(Source: ISO22316-2017)

In the EQL context it involves the management of disruptive risks and our ability to prevent disruptions from occurring; or when struck by a disruption, have the ability to withstand the impact, respond quickly and recover rapidly.

Business Continuity

Is defined as the capability of the organisation to continue delivery of products or services at acceptable predefined levels following a disruptive incident.

(Source: ISO 22301:2012)

Critical Infrastructure

Critical infrastructure underpins the functioning of Australia's society and economy and is integral to the prosperity of the nation. It enables the provision of essential services such as food, water, medical care, energy, communications, transportation and banking. Secure and resilient infrastructure supports productivity and helps to drive the business activity that underpins economic growth.

(Source: Australian Government Attorney General's Department)

Incident

An incident is a localised event that can be managed as part of normal business operations, using business as usual processes and plans. An incident is any occurrence that has resulted in, or has the potential to result in adverse consequences to people, the environment, the network, or our business.

Emergency

An emergency is defined as a situation, threat or hazard (unexpected or otherwise) that has placed (or has the potential to place) the safety of people, the reputation of EQL or the continuity of EQL's network or business operations and activities at a greater risk than what can be managed by normal business operations. And requires an immediate coordinated response to reduce the risk to an acceptable level.

Crisis

A crisis is an inherently abnormal, unstable and complex situation that represents an actual or potential threat to the strategic objectives, reputation or existence of an organisation. A crisis will typically present significant risk to EQL's reputation, financial stability and regulatory compliance; and long term ability to do business.

Organisational Resilience

Organisational resilience is the ability of an organisation to absorb and adapt in a changing environment to enable it to deliver its objectives and to survive and prosper.

(Source: ISO22316-2017)

In the EQL context it involves the management of disruptive risks and our ability to prevent disruptions from occurring; or when struck by a disruption, have the ability to withstand the impact, respond quickly and recover rapidly.

Disaster

A disaster is a serious disruption in a community, caused by the impact of an event, that requires a significant coordinated response by the State and other entities to help the community recover from the disruption. A disaster is a state or national declaration to which EQL's arrangements align as the owner/operator of critical infrastructure.

(Source: QLD Disaster Management Act).

Risk

effect of uncertainty on objectives

(Source: ISO Guide 73 Risk management—Vocabulary)

Risk Management

coordinated activities to direct and control an organisation with regard to risk

(Source: ISO Guide 73 Risk management—Vocabulary)

this Policy

This Policy and any related documents

6. ENFORCEMENT

The RM and OR Policy, applies to the activities of Energy Queensland Limited and all subsidiaries, Directors, Officers, Management and employees. It is expected that all contractors and / or subcontractors engaged by Energy Queensland Limited or its subsidiaries will abide by this Policy.

A breach of this Policy should be reported to your line-manager or, where this is not appropriate, your manager once-removed or the Risk and Compliance team.

To ensure that the Board has sufficient oversight of EQL's RM and OR processes and activities, on an annual basis, Management will provide an update on the implementation of this Policy (in accordance with the Risk and Compliance Committee Charter).

7. VARIATION

This Policy is not intended to detract from, or add to, any rights held by a person covered by this Policy under a contract of employment or enterprise agreement. Subject to any consultation obligations, EQL may vary, add to, withdraw, or replace this Policy, at its discretion, at any time.

8. CATEGORY

Governance