Policy

Organisational Resilience Policy

Version: 2.0 | **Version effective date:** 14/11/2025
Supersedes: Business Continuity Management Policy V.1.6

Scope

This policy applies to all organisational units, locations, and all staff.

It governs the development and alignment of QPT's Emergency Response Plans (**ERP**s), Business Continuity Plan (**BCP**), and Strategic Response Plan (**SRP**) and associated response and recovery procedures.

It applies to all activities undertaken to prepare for, respond to, and recover from disruptive events, regardless of their origin, scale, and duration.

Purpose

This policy outlines QPT's commitment to an integrated, organisation-wide framework that, during events that may impact on organisational stability or threaten the organisation's ongoing viability:

- strengthens and enhances organisational resilience to disruptive events
- enables coordinated efforts during disruptive events to protect people, property and assets
- maintains continuity of services and operations
- upholds stakeholder confidence and reputational integrity.

Policy statement

QPT recognises that disruptive events – whether internal or external, sudden or escalating – can have serious consequences for its staff, services and operations, finances, reputation, and long-term viability. It is committed to establishing, implementing, maintaining and maturing the capabilities required to ensure organisational resilience in the face of such events.

QPT adopts a cohesive approach to resilience that brings together emergency response, business continuity, and strategic response arrangements. These arrangements:

- provide a coordinated and scalable response to any disruptive event
- are developed and maintained in accordance with principles that prioritise effective preparedness, inclusive engagement, informed decision-making, and organisational learning
- incorporate the organisation's strategic objectives, operational context, and regulatory requirements.

The framework's resilience approach reflects best practice and recognised standards, and incorporates the intent, principles and structured guidance for robust, adaptable and effective resilience, of the following international standards:

- *AS ISO 22336:2025 – Security and resilience – Organizational resilience – Guidelines for resilience policy and strategy*
- *ISO 22316:2017 - Security and resilience – Organizational resilience – Principles and attributes*
- *ISO 22320:2018 - Security and resilience - Emergency Management – Guidelines for incident management*
- *AS ISO 22301:2020 - Security and resilience - Business continuity management systems – Requirements*
- *ISO 22361:2022 - Security and resilience - Crisis Management – Guidelines*

Integrated framework

QPT maintains an organisational resilience planning framework that ensures its ERPs, BCP and SRP are complementary and designed to work together, forming a fit-for-purpose, interdependent framework that enables timely escalation, seamless coordination, and appropriate leadership across all phases of a disruptive event.

Each plan fulfils a specific function within the broader response and recovery:

- **ERP** focuses on immediate actions to protect life, property and assets, and stabilise the situation.
- **BCP** enables the recovery and continuity of services and operations following an unplanned disruption.
- **SRP** facilitates strategic leadership and decision-making, executive oversight, and coordinated external communications during abnormal situations that threaten strategic objectives, reputation, or viability.

These plans may be activated **independently**, **simultaneously**, **or in sequence**, depending on the circumstances, severity, and operational effect of the disruptive event.

Plan development, maintenance and governance

The ERP, BCP and SRP are developed and maintained to ensure resilience arrangements remain current, practical, and capable of supporting a coordinated response to disruptive events.

Each plan is informed by structured risk and impact assessments, tailored to the organisation's operations, and address relevant legal, regulatory and strategic requirements.

Designated roles are responsible for ensuring that each plan is implemented, regularly tested, and updated as required to maintain effectiveness and consistency with this policy.

Principles

The resilience framework is guided by the following principles, which provide a consistent and strategic foundation for emergency response, business continuity, and strategic response activities:

Principle	What this means for QPT
Risk-based and proactive preparedness with impacts in mind	Preparedness and mitigation efforts are informed by structured risk assessments and business impact analyses to ensure that arrangements address the most relevant threats and the most significant potential impacts. Readiness is underpinned by deliberate investment in planning, testing, training, and capability development to strengthen organisational resilience before a disruptive event occurs.
Inclusivity and cross-functional engagement	Resilience is built through inclusive engagement across all levels and functions of the organisation. Planning, response, and recovery efforts are informed by broad input to ensure arrangements are representative, practical, and collectively owned.
Clear accountability and escalation arrangements	Roles, responsibilities, and escalation pathways are clearly defined and regularly tested to support effective coordination, decision-making, and timely plan activation during disruptive events. Authority and accountability are exercised at the appropriate level, enabling confident, timely and coordinated action across all phases of disruptive event management.
Integrated and scalable coordination	Arrangements are integrated through a connected framework that enables alignment across local, operational, and strategic levels. Coordination is scalable to meet the demands of localised incidents, or complex, organisation-wide disruptions.
Rapid, proportionate, and coordinated response	Response actions are designed to be rapid, proportionate to the nature and scale of the disruptive event, and coordinated across relevant teams. Protection of people and property, limiting harm, maintaining continuity of services and operations, and containment and stabilisation of the situation are the focus.
Information integrity and situational awareness	Decisions during disruptive events are supported by timely, accurate, and verified information. Clear internal and external communication protocols enable situational awareness, minimise confusion, and strengthen trust within the organisation while maintaining credibility with external stakeholders.

Principle	What this means for QPT
Stakeholder confidence and assurance	Arrangements are developed and maintained to build and sustain the confidence of stakeholders – including staff, customers, partners, government, and the wider community. Arrangements demonstrate transparency, consistency, and organisational reliability in the face of disruptive events, preserving public reputation and fulfilling regulatory obligations.
Alignment with organisational objectives strategy and values, with continuous learning and adaptation	Resilience is strengthened when arrangements reflect the organisation's strategic objectives, values, and culture. Disruptive event management is guided by ethical decision-making and purpose-driven action that supports long-term sustainability and organisational integrity. Commitment to ongoing learning and adaptive improvement by systematically reviewing organisational performance following exercises, tests, and actual disruptive events. Lessons learned are used to strengthen capabilities, ensuring the resilience framework evolves in response to new risks, operational changes, and emerging best practices.

Requirements

QPT adopts a structured approach to addressing **Prevention**, **Preparedness**, **Response** and **Recovery** as key objectives of its organisational resilience framework and system.

The system comprises:

- A **business impact analysis (BIA)**, used to determine QPT's business continuity priorities and requirements, including to:
  - Identify services
  - Define impact areas and prescribe the possible consequences of disruption
  - Determine the level of impact for each service over time
  - Determine recovery metrics – Maximum tolerable period of disruption (**MTPD**) and Recovery time objective (**RTO**) for services
  - Assess service criticality – prioritise services based on importance and identify services critical to business continuity
  - Assess recovery capabilities and identify gaps
  - Map internal and external dependences, interdependencies, and supporting resources.

  The BIA will be overseen by the Reform and Management Group (RMG) and be reviewed:

  - comprehensively, at least every two (2) years, and
  - in response to material changes such as organisational restructures, new services and technologies, regulatory change, risk profile changes, incidents or audit findings.
- **Procedures for critical services** identified under the BIA, to:
  - guide response and recovery efforts, and support the restoration of normal operations within the specified RTO
  - include response strategies for operating with reduced capacity or no access to systems or locations that support delivery of the services and other relevant matters.
- **Testing programs** used to validate the effectiveness of the response and recovery strategies, sufficiency of supporting resources and staff readiness to perform their roles during a disruptive event.
- Disruptive **event monitoring, detection and notification** arrangements.
- **Procedures for activation and coordination** of response teams and initial impact assessment, communications, event containment and recovery.

The system reflects a continuous cycle of risk assessment and impact analysis, event monitoring, plan activation and evaluation, and readiness testing and improvement.

Policy review

This policy is to be reviewed every two (2) years, or earlier if there are significant changes in QPT's structure, services, risk profile, or regulatory requirements to ensure it is relevant and effective.

Definitions

Term	Definition
Business continuity	The capability of an organisation to continue the delivery of products and services within acceptable time frames at predefined capacity during a disruption. *AS ISO 22301:2020, clause 3.3**
Business continuity plan (**BCP**)	Documented information that guides an organisation to respond to a disruption, and resume, recover and restore the delivery of products and services consistent with its business continuity objectives. *AS ISO 22301:2020, clause 3.4**
Disruption	An incident, whether anticipated or unanticipated, that causes an unplanned, negative deviation from the expected delivery of products and services according to an organisation's objectives. *AS ISO 22301:2020, clause 3.10**

Term	Definition
Disruptive event	Any actual or potential situation – whether sudden or escalating, internal or external – that interrupts, impairs, or threatens to interrupt or impair an organisation's ability to deliver services, maintain normal operations, protect people, property and assets, or that threaten its strategic objectives, reputation, or viability. Disruptive events can vary in scale, duration, origin, and complexity. Examples of disruptive events include, but are not limited to, emergencies, natural disasters, system and equipment failures, cyber incidents, supply chain disruptions, security breaches, or situations that have the potential to significantly damage the organisation's reputation or threaten its viability.
Emergency	Sudden, urgent, usually unexpected occurrence or event requiring immediate action. *AS ISO 22300:2019, clause 3.7^*
Emergency response	Overall approach for preventing emergencies and managing those that occur. *AS ISO 22300:2019, clause 3.78 (emergency management)^*
Emergency Response Plan (**ERP**)	Document setting out the organisation's procedures, roles, and responsibilities to enable a timely and coordinated response to incidents or emergencies. It supports the protection of life, minimisation of harm to people and property, and the restoration of safe and stable conditions.
Staff	Any person who carries out work for the QPT, including work as a QPT employee, contractor or subcontractor (or their employee), trainee, work experience student, employee of a labour hire company or a volunteer.
Strategic response	Coordinated activities to lead, direct and control the organisation with regard to an abnormal situation that threatens the organisation's strategic objectives, reputation, or viability and requires a strategic, adaptive and coordinated response. To assist with clarity in ensuring the most appropriate organisational resilience plan is activated, QPT's **Organisational Resilience Framework** substitutes 'strategic response' for 'crisis management' when aligning with *ISO 22361:2022 Security and resilience – Crisis management – Guidelines.*
Strategic Response Plan (**SRP**)	Document specifying the procedures and associated resources to be applied by whom and where for the organisation's strategic response.
Organisational resilience	The ability of an organisation to absorb and adapt in a changing environment – *clause 3.4, ISO 22361:2017 - Security and resilience – Organizational resilience – Principles and attributes.*

** AS ISO 22301:2020 Security and resilience – Business continuity management systems – Requirements*
^ AS ISO 22300:2019 Security and resilience - Vocabulary

Legislation and other compliance obligations

- *Financial Accountability Act 2009* (Qld)
- *Financial and Performance Management Standard 2019* (Qld)

Organisational Resilience Policy

Supporting documents

- QPT Emergency Response Plans*
- QPT Business Continuity Plan
- QPT Strategic Response Plan
- QPT IT Disaster Recovery Plan*
- QPT Privacy Data Breach Response Plan
- QPT Risk Management Policy
- QPT Risk Management Procedure

** QPT internal document*

Related resources and information

- AS ISO 22336: 2025 Security and resilience – Organizational resilience – Guidelines for resilience policy and strategy
- ISO 22316:2017 Security and resilience – Organizational resilience – Principles and attributes
- ISO 22320:2018 Security and resilience – Emergency management – Guidelines for incident management
- AS 3745-2010 Planning for emergencies in facilities
- AS ISO 22301:2020 Security and resilience – Business continuity management systems – Requirements
- ISO 22361:2022 Security and resilience – Crisis management – Guidelines
- AS ISO 22300:2019 Security and resilience - Vocabulary
- AS ISO 31000:2018 Risk Management – guidelines
- Queensland Government Disaster Management

Contact

For further information, please contact:

Compliance Systems & Governance

Email: compliance@pt.qld.gov.au