Strategic Response Plan

Version: 2.0 | **Version effective date:** 14/11/2025
Supersedes: Crisis Management Plan v 1.6

Purpose

The Strategic Response Plan (**SRP**) provides a structured framework for managing situations that threaten the strategic objectives, reputation or viability of the Queensland Public Trustee (QPT).

It assists the Strategic Response Management Team (**SRMT**)[1] to make timely, coordinated, and informed decisions in situations that require urgent attention, place the organisation under significant pressure, are complex and inherently uncertain, involve multi-stakeholder interests, or attract intense or sustained external scrutiny.

Application

The SRP applies organisation-wide and is designed **for extraordinary situations that fall outside normal management processes and require coordinated executive leadership with strategic, adaptive and timely decision-making** – whether they arise suddenly or develop progressively.

The SRP includes the organisation's measures for prevention and preparedness, plan activation criteria, approach to strategic response, an agenda to guide SRMT meetings, and the responsibilities of the SRMT and supporting roles.

Activation

The SRP may be activated independently or alongside an Emergency Response Plan (**ERP**) or the Business Continuity Plan (**BCP**). Where an ERP or BCP incident escalates into a situation requiring a strategic response, the SRMT assumes oversight under this plan, while ERP and BCP teams continue managing operational response and recovery.[2]

The following illustrates situations where SRP activation should be considered.

- **Significant reputational threats** - sustained negative media coverage, activist campaigns, or events undermining public confidence.
- **High-profile regulatory, compliance, or legal matters** – investigations, inquiries, or enforcement actions attracting significant scrutiny.
- **Complex stakeholder issues** – competing demands from regulators, customers, employees, partners, or other stakeholders requiring coordinated executive leadership.
- **Strategic financial pressures** – affecting organisational stability, priorities, or long-term objectives.

[1] Refer to Appendix B in relation to SRMT composition and SRMT supporting roles.
[2] Further information on ERPs, BCP, and SRP activation and deactivation criteria, and examples of activation and interrelatedness, can be found in Appendix A of the QPT Resilience Planning Guide.

- **Cybersecurity or data breaches** – impacting regulatory obligations, customer trust, or reputation.
- **Sensitive workforce or industrial relations matters** – employee unrest, or workforce-related issues, drawing public attention.
- **Serious health or safety incidents** – fatalities, large-scale injuries, or incidents likely to trigger regulatory or public scrutiny.
- **Significant political, policy, or regulatory developments** – affecting organisational priorities or stakeholder relationships.
- **Board or executive leadership issues** – sudden leadership changes, governance failures, or situations impacting executive credibility.
- **Emerging strategic risks** – identified through strategic monitoring, foresight activities, or stakeholder intelligence, where early executive positioning may be required to manage impacts or prevent escalation.

Activation authority

Activation of the SRP is authorised by the Chief Executive Officer (CEO), who may act on their own initiative or by advice from SRMT members.

Escalation of potential situations

All staff must promptly escalate potential situations that may require a strategic response. Staff should notify their manager, who will assess the issue and escalate it to the relevant Director or Executive Director for escalation to the CEO, as appropriate.

Convening of SRMT

When a potential strategic response is required, the SRMT Coordinator, following direction from the CEO, will convene an SRMT as soon as practicable. At this meeting, the CEO will either confirm activation (if already decided) or decide whether activation is required, following advice and discussion with SRMT members.

SRMT members will be notified of the meeting through established communication channels and are expected to make themselves available as directed.

The SRMT Coordinator is to ensure meeting details, meeting agenda, and initial information are provided to all members in advance of convening.

Refer to Appendix A for an overview of the SRP process.

Prevention and Preparedness

Measures taken to reduce the likelihood and build organisational resilience to situations requiring a strategic response include the following, with the frequency of each measure governed by the associated policy, procedure, or program where the measure is already prescribed.

Preventative measure	Objective
Reform and Management Group (RMG)	
Review the Material Business and Strategic Risk Registers to monitor high-impact threats	Ensure ongoing visibility of strategic risks

Preventative measure	Objective
Endorse QPT's Risk Appetite Statement and ensure all organisational areas operate within those limits	Minimise unmanaged exposure
Strategic Response Management Team (SRMT)	
Oversee integration of external intelligence sources to identify potential strategic threats (regulatory and political, reputational, financial and economic, technology and cyber, stakeholder and multi-party complexity, safety, legal and litigation)	Anticipate emerging risks early and improve situational awareness
Confirm thresholds for escalation from incident to strategic response	Ensure timely SRP activation decisions
Participate in capability development exercises and after-action reviews, including lessons learned	Build SRMT readiness and leadership agility and
Strategy & Governance Division	
Monitor and support the updating of divisional and the Material Business and Strategic Risk registers and report to RMG for monitoring of any high-impact threats	Strengthen early detection of emerging risks
Support risk owners and program areas to ensure all risks associated with their area of responsibility are captured and appropriately updated	Reduce vulnerabilities before they escalate
Monitor statutory (laws and regulations) developments and assess their potential impact on the organisation	Prevent noncompliance-related incidents
Provide input into external intelligence sources to identify potential strategic threats	Improve situational awareness
Collaborate with SRMT to integrate strategic risk insights into organisational resilience testing exercises	Align organisational readiness with risk data and strengthen leadership readiness
Conduct after-action reviews within 20 work days following actual response situations (BCP and SRP), organisational resilience exercises, and near-misses	Capture lessons learned to avoid recurrence
Review organisational resilience testing program outcomes, track trends arising from after-action reviews, and integrate improvements into SRP updates	Reduce recurrence and strengthen response capabilities over time
Suggest additional SRP prevention and preparedness strategies against new or emerging risks	Keep plans current and relevant
Internal Audit	
Track unresolved audit findings and escalate to RMG if exposure exceeds agreed tolerances	Ensure risks don't remain unmanaged
Managers, Directors, Executive Directors	
Conduct regular operational risk assessments to identify vulnerabilities and stress-test critical controls	Address potential issues at source
Implement preventative maintenance programs for critical assets, infrastructure, and information technology systems	Reduce risk of service disruptions
Monitor key performance and risk indicators tied to operational stability	Detect issues before they escalate

Preventative measure	Objective
Report near-miss events and significant incidents	Enable early escalation and lessons learned
Participate in organisational resilience testing program exercises to assess operational response coordination	Build readiness within and across organisational areas
Maintain localised continuity response such as floor plans, emergency contacts, and response procedures	Improve mobilisation speed during emergencies
Information Technology	
Conduct penetration testing and vulnerability scans to identify security gaps	Detect weaknesses before exploitation
Monitor for unusual activity via Security Information & Event Management (SIEM) tools and automated alerts	Detect intrusions early
Patch system and update critical security software in line with vendor guidance	Prevent known vulnerabilities from triggering incidents
Test disaster recovery and data breach response procedures using simulations	Validate IT readiness for cyber events
Assist in integrating IT incident scenarios into the organisational resilience testing program	Build alignment between cyber and strategic response readiness
Develop cyber incident playbooks and pre-approved response templates	Enable rapid mobilisation during cyber events
Strategic Engagement and Community Education, and Media	
Monitor news platforms for reputational threats	Detect early signs of reputational triggers
Maintain a stakeholder engagement map and undertake regular communications at operational level	Strengthen relationships to manage sensitive situations
Prepare pre-approved holding statements, key messages and communication plans for identified risk scenarios	Enable rapid external communications
Develop internal strategic response communication protocols to inform staff during escalation events	Maintain trust and transparency internally
People & Culture	
Ensure mandatory training includes training to staff on incident reporting and escalation protocols	Improve early detection and transparency
Monitor workforce sentiment and wellbeing to detect emerging risks	Prevent staff-related strategic response situations
Ensure mandatory training embeds a speak-up culture and provides information on reporting channels	Encourage early identification of risks
Ensure robust Safety Management System, including integrated Psychosocial Risk Management Framework	Build workforce readiness for prolonged response and recovery actions
Procurement Services	
Ensuring a Contract Management Framework that includes requirements in relation to establishing supplier KPIs, collecting performance data, receiving regular contract performance reports, obtaining regular feedback from suppliers, managing	Ensure contractual arrangements are structured, monitored, and governed in a manner that supports supplier

Preventative measure	Objective
underperformance, and actively managing risk throughout the life of a contract	resilience and continuity and responsiveness
Implementation of a contract management system to assist organisational areas with management of supplier contracts and relationships	
QPT Procurement Policy requiring the use of whole-of-government template standard terms and conditions, with ICT Products and Services General Contract Conditions containing a supplier warranty for continuity of performance of supported software	Embed government preparedness requirements in supplier contracts to minimise supplier disruptions
Maintaining knowledge and awareness to whole-of-government emergency procurement procedures in an 'emergency situation'	Enables rapid, informed and transparent procurement in a sudden unforeseen event that can result in injury, loss of life or critical damage to property or infrastructure

Response

Once the SRP is activated, the response is to be guided by timely decision-making, coordinated leadership, and ensuring stakeholder confidence. SRMT leads the response by:

- Providing executive leadership and strategic direction.
- Making rapid, informed decisions based on verified information and credible intelligence.
- Ensuring information is verified, controlled, and communicated consistently.
- Protecting stakeholder confidence through accurate and transparent engagement.
- Aligning SRMT decisions with ERP and BCP activities to deliver a cohesive organisational response.
- Reassessing impacts and priorities regularly to adapt decisions as situations evolve.

SRMT meeting agenda

The following agenda:

- is to be used to support SRMT meetings held in response to both fast-moving and slower-evolving situations.
- applies to the initial meeting as well as subsequent meetings (shown in italics).
- establishes a consistent, structured approach adaptable to the pace, scale, and complexity of the situation.

Fast-moving situations:

- Keep meetings short and focused (15-30 minutes).
- Provide rapid updates and make rolling decisions.

Slower-evolving situations:

- Schedule longer meetings (60-90 minutes).
- Analyse developments in detail, test scenarios, and plan forward positioning.

- Maintain alignment with ERP/BCP activities and stakeholder communications if those plans are activated.
- If ERP/BCP are not yet activated, focus on assessing situational intelligence, making immediate strategic choices, and deciding on activation triggers.
- Monitor intelligence continuously and assess potential triggers for activation.
- Shape stakeholder perceptions proactively through deliberate communication planning.

Agenda Item	Actions
1. SRP activation	• Confirm whether SRP has already been activated by CEO. • If not yet activated, SRMT provide advice and recommendations to CEO to support CEO's activation decision. • Establish scope, objectives, and roles (with deputies). • Confirm SRP activation or decide if SRP activation is required. If not, set monitoring and interim coordination. • Add additional members or SMEs if needed. • Record activation decision and rationale. - *Reconfirm SRP activation status; adjust only if posture has changed.* - *Confirm any changes in roles, attendees, or accountabilities.* - *Reassess activation criteria if SRP not yet activated; decide on activation or continued monitoring.* - *Update earlier record of activation decision and rationale.*
2. Situation briefing	• Establish operational actions already taken (including ERP/BCP activation if applicable). • Capture a rapid 5W + H (fast-moving) – what, when, where, who, why, how; or review a structured intelligence summary (slower-evolving) - source, reliability, timeline, evolving context, uncertainties. • Assess current trend and escalation risk – worsening, stabilising, improving; likelihood of higher-level response. • Identify external reporting requirements (e.g. regulatory, insurer, contractual, partner). • Assess baseline stakeholder sentiment. - *Verify changes in operational actions since last meeting.* - *Update 5W+H (fast-moving) or structured intelligence summary (slower-evolving).* - *Reassess trend and escalation risk – worsened, stabilised, improved; escalation risk increased or decreased.* - *Update changes to external reporting requirements.* - *Assess stakeholder sentiment shifts.*
3. Information verification	• Confirm what is known, unknown, and requires verification. • Assign owners to confirm or disprove intelligence. • Build a structure information log. • Establish controlled processes for information flow. - *Confirm closure of previous information gaps.* - *Validate new intelligence inputs and reconcile conflicting information.* - *Refresh information log and ensure accuracy of updates.*

Agenda Item	Actions
4. Impact assessment	• Identify immediate and potential impacts on stakeholders, workforce, reputation, financial exposure, operations, project delivery, legal exposure and regulatory obligations. • Assign severity ratings to each impact area (rapid in fast-moving, detailed in slower-evolving). • Assess strategic implications, including reputational standing, regulatory posture, financial stability, long-term objectives, and operational dependencies. • Define escalation triggers and thresholds linked to assessed impacts. • Record all impact ratings and triggers. - *Update new or emerging impacts; adjust severity ratings as required.* - *Verify the completion and status of mandatory reporting obligations identified earlier.* - *Validated impact ranges with new intelligence and reconcile against earlier assessments.* - *Capture secondary and tertiary effects and assess their influence on escalation triggers.* - *Refresh the record of the impact ratings and triggers.*
5. Set strategic priorities	• Define stabilisation and positioning priorities to limit escalation (e.g. control situation, protect people, secure assets). • Set near-term objectives – next 1-3 hours if fast-moving, or short-term while balancing medium- to long-term positioning if slower-evolving. • Allocate responsibilities, owners, and timelines for priority actions. - *Review progress of earlier actions and reset priorities if required.* - *Adjust or reconfirm objectives based on updated impacts and intelligence.* - *Reallocate SRMT resources as needed.* - *Update priorities and responsibilities in the SRMT Decision Log.*
6. Strategic options and risk monitoring	• Consider immediate courses of action to contain the impact and stabilise the situation. • Develop scenario-based options: best-case, most-likely, and worst-case. • Identify decision thresholds and pre-conditions for activating each option. • Establish early warning indicators and assign responsibilities for horizon scanning. - *Expand to review long-term strategic risks and potential response pathways.* - *Revisit and refine scenarios using new intelligence.* - *Reconfirm decision thresholds; approve pre-emptive actions and define triggers for implementation.*
7. Stakeholder mapping & communications	• Identify affected/high-priority stakeholders; map strategic stakeholders where pace allows. • Agree messaging priorities and initial engagement approach, including communication channels. • Define communication objectives for stakeholder groups and draft holding lines. • Confirm spokesperson and assign Communication and Media Leads with approval pathways.

Agenda Item	Actions
	• Establish monitoring arrangements for stakeholder sentiment and expectations. • Approve initial public statements and confirm regulatory/government engagement requirements. - *Review and adjust stakeholder map for new and emerging stakeholders.* - *Review stakeholder sentiment and expectations; adjust communication priorities accordingly.* - *Approve new and updated statements, messaging, or engagement strategies.* - *Reconfirm communication responsibilities and coordination with ERP/BCP.*
8. Coordination with ERP/BCP	• Review operational activation status of ERP/BCP and current posture. • Ensure SRMT actions remain aligned with, but distinct from ERP/BCP operational response. • Confirm operational dependencies and escalation thresholds. • Identify gaps or overlaps between strategy and operations. • Direct adjustments and establish reporting cadence between SRMT and ERP/BCP leads. - *Review ERP/BCP operational status and posture.* - *Reconfirm cross-team alignment and ensure operational response and recovery actions support SRTM strategic priorities.* - *Review updates from ERP/BCP leads and reconcile constraints and overlaps.* - *Confirm communication coordination between SRMT and ERP/BCP structures.*
9. Resource and capability alignment	• Identify available people, facilities, systems, and funding. • Approve urgent reallocations or requests for external support. • Priorities resources against immediate objectives. - *Confirm changes in resource availability or constraints.* - *Review progress of earlier resource decisions.* - *Adjust allocations or request further support.*
10. Action tracking and decision log review	• Summarise key decisions made; record in Decision Log. • Confirm assigned actions, owners, and deadlines; capture in Action Tracker. - *Reconcile Action Tracker as to status of earlier actions; reconfirm or reassign owners if required.* - *Summarise key decisions made; record in Decision Log.* - *Confirm assigned actions, owners, and deadlines; capture in Action Tracker.*
11. Confirm next meeting cadence	• Confirm SRMT meeting cadence (duration and frequency). • *Reconfirm SRMT meeting cadence - adjust cadence if developments accelerate or slow, pivot to 'trigger-based' meetings where updates occur at significant shifts.*

The SRMT should continue using the agenda to guide meetings for as long as the situation requires active strategic management. Meetings should be held at the agreed cadence, using the SRMT Whiteboard (optional – Appendix C), the Situation Report (Appendix D) and the Decision Log & Action Tracker (Appendix E) to track verified information, assess evolving impacts, and make informed decisions.

Recovery

The recovery phase begins once the situation stabilises and no longer requires active executive-level oversight, but continues to demand strategic coordination and stakeholder management.

SRMT leads the transition from response to recovery, setting the overall recovery objectives and ensuring alignment with organisational priorities. Recovery priorities are informed by outputs from SRMT meetings.

While operational recovery activities may continue under ERP or BCP, SRMT maintains oversight of strategic issues such as stakeholder confidence, regulatory positioning, reputational management, and future risk exposure.

The phase concludes when stable operations are restored, stakeholders are reassured, and any lessons learned are captured to strengthen organisational resilience.

Definitions

Term	Definition
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 – *clause 3.4, AS ISO 22301:2020.**
Credible intelligence	Verified, reliable, and high-confidence information obtained from trusted internal or external sources that indicate a potential or emerging situation requiring strategic consideration by the SRMT. It may relate to threats, risks, opportunities, or stakeholder developments and is used to inform decisions, trigger early escalation, or active the SRP proactively before impacts fully materialise.
Critical service	A service essential to the organisation's ability to meet its objectives, legal or regulatory obligations, or stakeholder expectations, and which must be resumed within an acceptable timeframe to prevent unacceptable impact following a disruption.
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 – *clause 3.10, AS ISO 22301:2020.**
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.

Term	Definition
	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.*^
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 22361:2022.*
Situation Report (SitRep)	Summary, either verbal or written, outlining the current state and potential development of an incident or crisis and the response to it – *clause 3.9 ISO 22361:2022.*

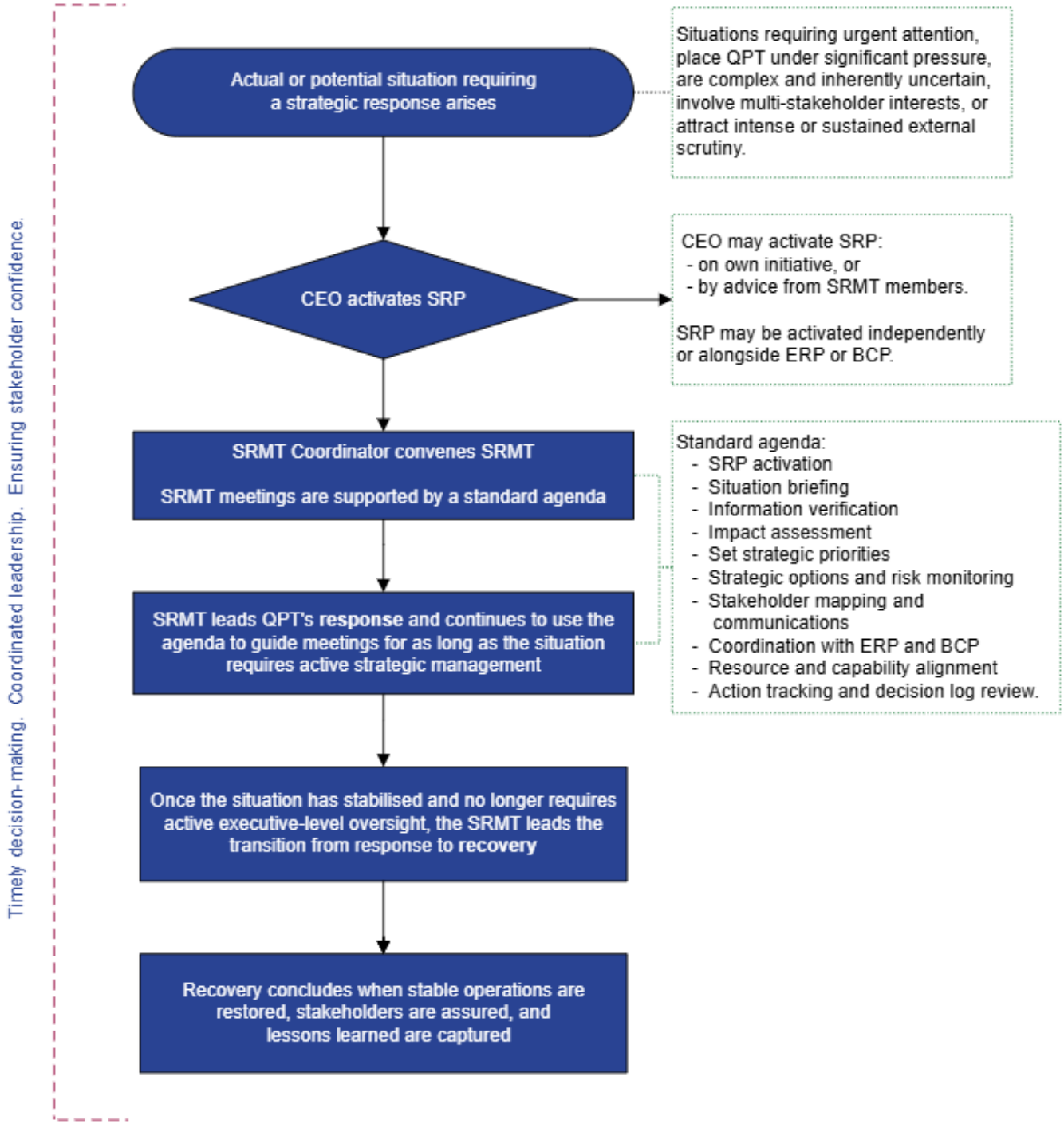
** 22301:2020 Security and resilience – Business continuity management systems – Requirements.*
^22361:2022 Security and resilience – Crisis management – Guidelines.

Contact

For further information, please contact:

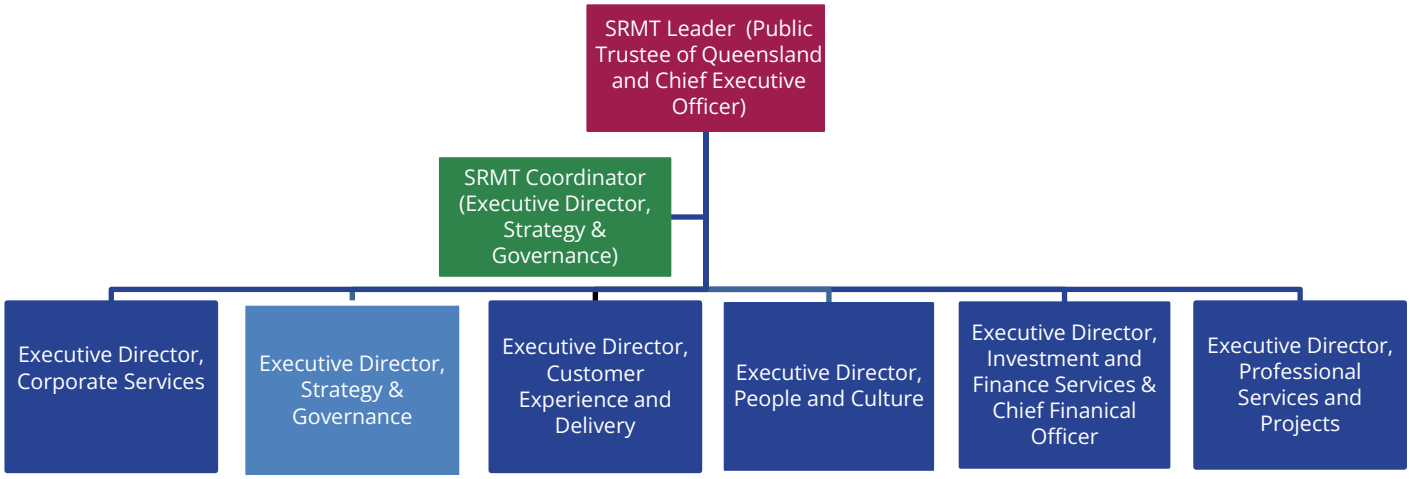
Compliance Systems & Governance
Email: compliance@pt.qld.gov.au

Appendix A: Strategic Response Plan Process – Overview



Appendix B: SRMT and supporting roles

Strategic Management Response Team



In addition to their membership on SRMT, individual members may also be assigned specific supporting roles.

Where specialised expertise is required, supporting roles may also be assigned to individuals outside of SRMT members, such as Directors and Managers, technical specialists, or external advisors.

Position	Responsibility
SRMT Lead - Chair (Public Trustee of Queensland and Chief Executive Officer - PTQ and CEO)	• Leading the SRMT. • Provides overall strategic leadership and authority during a strategic response situation. • Authorises activation and deactivation of the SRP. • Chairs SRMT meetings, ensures procedural compliance and drives decision-making. • Acts as primary liaison with the Attorney-General, Audit & Risk Management Committee (ARMC) and Public Trust Office Investment Board (PTOIB). • Reviews and authorises internal and external messaging on matters of significance during a strategic response.
Deputy SRMT Chair (Executive Director, Strategy & Governance)	• Ensures continuity of leadership if the SRMT Lead is unavailable. • Assumes SRMT Lead responsibilities when required. • Supports the SRMT Lead with meeting facilitation and governance.
SRMT Members	**Strategic Leadership and Decision-Making** • Actively contribute to timely, informed decisions. • Assist in setting the organisation's strategic response objectives and priorities. • Provide advice on SRP activation, escalation, de-escalation, and stand-down. • Support unified, coordinated decision-making across SRMT.

Position	Responsibility
	Situation Awareness and Intelligence • Stay informed on the current situation using SitReps, verified updates, and Whiteboard summaries. • Identify and communicate credible intelligence, risks, and triggers relevant to their area of responsibility. • Highlight potential strategic, reputational, regulatory, or operational impacts for SRMT consideration. • Distinguish between verified information, assumptions, and unknowns when briefing the SRMT. • Lead assigned supporting role where applicable. • Coordinate with other SRMT members and supporting roles, to ensure alignment and consistency. **Stakeholder and Communications** • Provide input on key messages for internal and external stakeholders. • Escalate any mandatory reporting obligations linked to their area of responsibility. • Monitor stakeholder sentiment, risks, and pressures relevant to their area of responsibility. **Resource and Financial Accountability** • Identify and escalate critical resource requirements relevant to their area of responsibility. • Flag any significant financial implications for SRMT consideration. • Support accurate cost tracking through inputs to the Strategic Response Cost Tracker. **Recovery and Transition Participation** • Support the SRMT in deciding when to shift from response to recovery. • Provide input into recovery objectives and any ongoing dependencies relevant to their area of responsibility. **Governance and Continuous Improvement** • Participate in post-event reviews and provide lessons learned. • Support updates to the SRP, training programs, and organisational resilience strategies.
SRMT Coordinator (Executive Director, Strategy & Governance)	• Ensures efficient information flows between SRMT members. • Coordinates meeting agendas, actions, and decisions. • Maintains the SRMT Whiteboard, Decision Log & Action Tracker and SitRep. • Tracks progress of assigned actions to ensure accountability. • Supports SRMT Lead with communications, and distributes approved SitReps and updates.
Subject Matter Experts (as co-opted)	• Provide technical or specialist advice depending on the nature of the situation (e.g. information technology, cyber, health and safety). • Participate in SRMT deliberations only for as long as their expertise is required.

Supporting roles

Position	Responsibility
Intelligence Lead	• Monitors, verifies, and assesses incoming intelligence, distinguishing between credible intelligence and unverified data. • Maintains a facts vs assumptions vs unknown grid. • Tracks triggers, and supports SRMT decision-making with scenario insights.
Operations Lead (ERP/BCP Liaison)	• Coordinates with ERP/BCP leads to ensure alignment between strategic SRMT decisions and operational response. • Provides updates on critical services, dependencies, and resource status.
Communications Lead	• Manages internal and relevant external communications, ensuring consistent messaging to staff, SRMT members, and operational teams. • Works closely with the Media Lead.
Stakeholder Engagement Lead	• Manages strategic relationships with regulators, government, government agencies, customers, partners, and advocacy groups. • Ensures SRMT decisions consider stakeholder sensitivities and required engagement cadence.
Media Lead	• Manages media communications and strategy, manages spokespeople, develops holding statements, and monitors public sentiment and reputational risks. • Often works with external 'crisis communications' advisors.
People Lead	• Focuses on staff safety, wellbeing, and workforce impacts. • Ensures messaging supports morale and workforce continuity.
Legal Lead	• Provides advice on regulatory exposure, liabilities, investigations, mandatory reporting obligations, and contractual implications. • Ensures SRMT decisions are legally sound and defensible. • Coordinates with insurers to ensure timely notifications, claim viability, and alignment between SRMT actions and policy coverage conditions.
Compliance & Governance Lead	• Ensures SRMT decisions meet regulatory and governance obligations. • Tracks mandatory reporting deadlines and ensures submissions are coordinated across stakeholders.
Financial & Commercial Lead	• Provides oversight of financial exposure, scenario-based cost impacts, insurance considerations, and commercial dependencies (e.g. supplier risks). • Tracks and maintains SRP-related costs.

Appendix C: SRMT Whiteboard (optional use)

1. Situation Overview & Strategic Objectives

SitRep #/ Date [SRP-SITEREP-DD/MM/YYYY]	**Current Status** [Contained/Escalating/ Monitoring]	**Trigger for Activation**	**Current Phase** [Fast-moving/Slow-moving]	**Lead Coordinator** [Name and role]

Strategic Objectives – What we are trying to achieve:

Example:

1. Preserve stakeholder confidence.
2. Maintain regulatory compliance.
3. Limit reputational harm.
4. Preserve financial stability.
5. Position organisation for recovery.

2. Critical Facts, Assumptions & Information Requirements

Verified Facts [List validated facts]	**Key Assumptions** [List assumptions affecting decisions]	**Information Gaps** [List gaps needing confirmation]

Information Needed [Example: Regulator's position]	**Owner**	**Deadline** [DD/MM HH:MM]	**Impact** [Example: Impact on communications/customers]
1.			
2.			

3. Strategic Priorities & Key Challenges (top 3)

For fast-moving situations → focus on containment. For slow-moving → focus on positioning and forward planning.

Priority	**Owner**	**Deadline** [DD/MM HH:MM]	**Mode Focus** [Fast/Slow]	**Status** [Pending/In Progress]
1.				
2.				
3.				

Key Challenges/Pressures

Challenge/Pressure [Example: Regulatory scrutiny increasing]	**Impact/Notes** [Requires pre-approved communications]

4. Stakeholder Sentiment & Key Messages

Stakeholder Sentiment

Stakeholder	**Impact** [Low/Medium/High]	**Sentiment** Stable Watch Concerned	**Action/Message** [Message or next action]	**Owner** [Name and role]

Key Messages

Audience [Staff / Regulators/ Media, etc]	**Key Message** [Approved holding statement]	**Owner**	**Last updated** [DD/MM HH:MM]
1.			
2.			
3.			

5. Escalation Triggers & Scenario Planning

Escalation Triggers

Trigger/Indicator	**Owner**	**Planned Response** [Pre-agreed action]

Scenario Planning

Scenario	**Impact**	**Response Pathway** [Planned actions]	**Owner**
Best case			
Most Likely			
Worst case			

6. Key SRMT Decisions & Actions

Decision	**Owner**	**Rationale** [Reason for decision]	**Date/Time** [DD/MM HH:MM]
1.			
2.			
3.			

Assigned Actions

Action	**Owner**	**Deadline** [DD/MM HH:MM]	**Status** [Pending/In Progress/Complete]
1.			
2.			

7. Next SRMT Meeting & SitRep

Next Meeting Time [DD/MM HH:MM]	**SitRep Release** [DD/MM HH:MM]	**Cadence** [Hourly/Daily/Weekly/Monthly]

Appendix D: Situation Report (SitRep)

SitRep #	Date / Time Issued	Prepared By	Approved By	Distribution
[SRP-SITEREP-DD/MM/YYYY]				

Executive Summary

SRP activated at [HH:MM] due to [trigger/event]. Current status: [Stable/Escalating/Controlled]. Key priorities: [Priority #1], [Priority #2], [Priority #3]. Next SitRep scheduled for [HH:MM DD/MM].

Current Situation & Strategic Objectives

Current Situation	Response Mode	Strategic Objectives
[Brief confirmed situation summary, 2-3 lines]	[Fast-moving / Slow-moving]	Example: 1. Protect stakeholder confidence 2. Maintain regulatory compliance 3. Preserve operational integrity.

Top 3 Strategic Priorities

Priority	Owner	Deadline [DD/MM HH:MM]	Status
1.			[Pending/In Progress/Complete]
2.			
3.			

Stakeholder Sentiment Snapshot

Stakeholder Group	Sentiment Stable 🟢 Watch 🟡 Concerned 🔴	Approved Message
Regulators		[Key approved message]
Customers		
Staff		
Media		

Immediate Next Steps

1.
2.
3.
4.

Appendix E: SRMT Decision Log & Action Tracker

This template can be used by SRMT to record all key decisions made during a strategic response, along with linked actions, ownership, timelines, and progress updates.

SRP Reference	Situation / Event ID	Version	Prepared By	Approved By
[SRP-SRMT-DLOG-XX]	[Event name / ID]	[v1.0]	[Name / Role]	[SRMT Lead / CEO]

Last updated: [DD/MM/YY HH:MM]

1. SRMT Decision Log

Decision#	Decision Summary	Rationale	Decision Maker	Risk	SitRep#	Owner	Date & Time	Status*
D-001			[CEO/SRMT Lead, SRMT Consensus]	[High Medium Low]		[Responsible person]		

- Log only formally agreed decisions authorised by the SRMT.
- Risk rating reflects information certainty when decision was made.
- Link decisions to relevant SitRep reference for traceability.

2. Linked Action Tracker

Action #	Linked Decision#	Action description	Owner	Deadline	Dependencies	Status*	Notes
			[Responsible person]		[Pre-conditions Dependencies]		[Additional details, risks, impediments]

- Track all actions to SRMT decisions for accountability.
- Use sequential numbering for traceability e.g. A-001, A-002.
- Ensure dependencies are recorded.

* Status

Pending → Awaiting SRMT or CEO approval
Approved → Decision/action signed off and progressing
In Progress → Action underway
Complete → Fully executed
Revised → Superseded based on new information