Queensland
Good **jobs**
Better **services**
Great **lifestyle**

Queensland Government
Cyber Security Hazard Plan

Queensland Government

This publication has been compiled by the Cyber Security Unit of the Queensland Government Customer and Digital Group, Department of Transport and Main Roads

Contents

Authorisation Statement

Queensland adopts a comprehensive and all-hazards approach to disaster management but develops hazard specific sub-plans under the Queensland State Disaster Management Plan (QSDMP) when hazards have nuanced operational or coordination requirements. Cyber security has been identified as a hazard requiring the development of a sub-plan.

The Queensland Government Cyber Security Hazard Plan (the Plan) is issued under the authority of the Director-General, Department of Transport and Main Roads (DTMR). The Plan outlines the response and escalation pathway for cyber incidents with state-wide or national consequences, in support of DTMR as the lead agency for the management of the cyber security hazard in Queensland.

On behalf of the Director-General, the DTMR Cyber Security Unit and is responsible for developing and maintaining the Plan.

The Plan is hereby approved and recommended for distribution.

Neil Scales

Director-General

Department of Transport and Main Roads

23/05/2023

Introduction

The Queensland Government Cyber Security Hazard Plan (the Plan) outlines the Whole-of-Queensland Government (WoQG) response to cyber incidents with potential statewide or nationwide impacts. The Department of Transport and Main Roads (DTMR) is the lead agency responsible for the development and implementation of the Plan.

Aim

The Plan aims to respond to and protect Queensland communities from the potential consequences of a cyber crisis. It describes the interaction between the cyber security community, business continuity personnel and the emergency management sector to:

- reduce impacts to critical infrastructure, services and Government assets
- coordinate information flow between stakeholders
- communicate to the public when required for cyber incidents.

Objectives

The objectives of the Plan are to:

- outline the arrangements in place to manage cyber incidents with potential state-wide or nationwide impacts across the phases of prevention, preparedness, response, and recovery
- describe the strategic roles and responsibilities across Governments for the management of a cyber incident with potential state-wide or nationwide impacts
- outline Queensland's role in supporting the Australian Government's Cyber Incident Management Arrangements for Australian Governments (CIMA).

Scope and Application

The Plan will serve as a hazard-specific sub-plan under the Queensland State Disaster Management Plan (QSDMP).

The Plan:

- is supported by the Queensland Government Cyber Security Arrangements (QGCSA) which outline Queensland's operational cyber incident response
- aligns with the Australian Government's CIMA, which provide guidance on governmental collaboration and harm reduction in response to national cyber incidents
- should be read in conjunction with the overarching QSDMP and all subordinate arrangements. In the event of any conflict, the QSDMP will take precedence if specific guidance is required to protect life, property, or the environment.

All Queensland Government agencies are required to prepare for, respond to and recover from cyber incidents, and are responsible for developing and maintaining supporting agency specific plans, procedures and arrangements.

Recovery needs will be assessed and addressed in accordance with the Queensland Recovery Plan.

Reference Documents

A complete list of reference documents used to inform the preparation of the Plan are provided at Appendix 1.

Glossary

A table of acronyms used in the plan is provided at Appendix 2.

Review

The plan was current at the time of publication and will be subject to formal review and update with stakeholders at least every three years. More frequent reviews may be undertaken in the event of:

- structural or organisational change
- legislative change
- a cyber incident with statewide or nationwide impacts occurring, and/or
- annual planned exercise evaluations demonstrating a need for review.

Context

Cyber incidents are generally malicious in nature, seeking to deliberately damage, steal or disrupt.

During a cyber incident, an affected entity will likely be dealing with a threat actor who responds to incident management actions or mitigations undertaken by the entity reactively. This can have resounding and dynamic impacts on how a cyber incident unfolds and must be managed.

Rather than widespread damage of physical property, cyber incidents typically compromise security, information, and privacy, and can result in widespread harm to Queensland or further afield through:

- identity theft
- financial loss through fraud
- physical damage (e.g., property loss or bodily harm)
- psychological damage (anxiety, fear, distress, or worry that may be amplified in vulnerable groups or communities)
- reputational damage (brand damage incurred through a cyber attack which can erode staff, customer, or community trust and/or loyalty, and could also result in financial loss).

Hazard Definition

Cyber security is defined as "actions required to preclude unauthorised use of, denial of service to, modifications to, disclosure of, loss of revenue from, or destruction of critical systems or informational assets"[1].

Cyber criminals are increasingly exploiting digital connectivity for criminal activities. The term 'cybercrime' is often used to describe a broad range of criminal offences that are either dependent on or facilitated using computers or electronic devices.

A cyber incident is defined as:

- "an occurrence that:
- actually, or imminently jeopardises, without lawful authority, the integrity, confidentiality, or availability of information or an information system, or
- constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies."[2]

The Queensland Government defines a significant cyber incident (whether state-based or national) as any incident that has:

- the potential to cause, or is actively causing significant harm to people, or significant damage to property or the environment
- significant and widespread consequences for Queensland communities (whether state-based or nationwide).

The Importance of Cyber Security

In today's digital economy, all sectors of government, society and industry rely on Information and Communications Technology (ICT) to:

- increase productivity and drive economic growth
- connect communities
- preserve confidentiality and trust
- maintain infrastructure integrity
- provide a platform for the safe and secure exchange of goods and services (commerce).

While beneficial, an increased reliance on technology and digital assets exposes Queensland to cyber security risks.

Cyber security poses a risk to all areas of the Queensland community, and to any individual or organisation that holds information that could be exploited. No one is 100 per cent protected from cyber security risks, and the potential impact a cyber incident may pose is directly proportionate to the effectiveness of hazard mitigation and risk management strategies in place.

1. International Standard: IECT/TS 62443-1-1 ed. 1.0
2. NIST Privacy Framework Version 1.0

Critical assets and systems are subject to a range of ownership and governance structures. Effective cyber security arrangements rely on the definition of clear roles and responsibilities for a wide range of government entities, corporations, and private businesses.

Cyber Security Risk Environment

The global cyber security landscape is deteriorating, with a notable uptick in political and geopolitical hacktivism, espionage, industrial sabotage, and financially driven cybercrime. The capability of cyber criminals is rapidly increasingly spurred by the possibility of large-scale financial returns, and cyber incidents are now a normal occurrence rather than a remote possibility. Insurers are now approaching cyber risk in the equivalent manner to natural disaster risk.

In 2021–2022, the Australian Cyber Security Centre (ACSC) Annual Cyber Threat Report noted[3]:

- one new cybercrime report was made approximately every seven minutes
- more than 76,000 cybercrime reports were made to ReportCyber
- 29 per cent (approximately 22,040) of these reports were attributed to Queensland (Queensland reports disproportionately higher rates of cybercrime relative to the population)
- medium-sized businesses had the highest average loss per cybercrime where a financial report occurred.

Ransomware attacks continue to escalate in scope and severity, as noted globally but also when considering notable Australian attacks such as those experienced by Optus, Medibank, and Fire and Rescue Victoria.

The ACSC has noted that authorities in the United States, Australia and the United Kingdom have observed an increase in sophisticated, high-impact ransomware incidents against critical infrastructure organisations. In 2021, the Australian Signals Directorate Director-General advised of a 60 per cent increase in ransomware attacks against Australian entities, and quoted[4] studies by AustCyber indicating that a single significant cyber attack against Australia could cost $30 billion and 160,000 or more jobs.

These themes continue to be echoed in the present-day, by the '2022 Official Cybercrime Report' published by Cybersecurity Ventures and eSentire, which notes that global cybercrime damage costs are expected to grow by 15 per cent a year, reaching

$US10.5 trillion annually by 2025, up from $US3 trillion in 2015[5].

3. https://www.cyber.gov.au/sites/default/files/2022-11/ACSC-Annual-Cyber-Threat-Report-2022.pdf
4. https://www.aph.gov.au/Parliamentary_Business/Hansard/Hansard_Display?bid=committees/commjnt/27d1412f-0716-454a-9b40-c8e8276eb931/&sid=0005
5. https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/

Prevention

The risk of a cyber incident cannot be eliminated, so efforts are focused on understanding and reducing the risk of exposure and/or impact of a cyber incident. Prevention activities for cyber security are increasingly being integrated as business-as-usual practice, underpinned by systematic risk management. Cyber security is no longer an ICT problem, but a business risk.

Queensland Government Cyber Security Unit

The central DTMR Cyber Security Unit (DTMR CSU) is responsible for supporting the development of Queensland's cyber security industry and local cyber security workforce as well as managing several WoQG cyber security services.

The CSU team provides:

- cyber security leadership
- guidance on governance, policy, and standards
- a coordinated response to cyber incidents
- progression of cyber security capability development across government.
- advocacy for cyber security awareness
- policies and practices.

The CSU also hosts communities of practice for Queensland Government ICT professionals, who meet on a regular basis to collaborate, share information, and generally expand their knowledge and cyber security skills.

Queensland Government Information Security Policy

The Queensland Government Information Security Policy (IS18) ensures all departments apply a consistent, risk-based approach to the implementation of information security.

Under IS18, Queensland Government entities (departments, and entities that choose to voluntarily adopt IS18) are responsible for classifying information and information assets according to their business impact. They are also responsible for determining and applying appropriate controls to safeguard information and information assets in a consistent manner.

In addition to extensive technical and cyber awareness uplift, major improvements under IS18 include agencies:

- aligning to international best practice cyber-governance based on ISO27000 standards
- continuously maturing and reporting on the implementation of the Essential Eight mitigation strategies recommended by the ACSC
- escalating cyber readiness attestation to agency CEOs via agency risk committees
- implementing mandatory cyber incident reporting
- enhancing operational governance and threat intelligence sharing.

Queensland Protective Security Framework

The Queensland Government recognises that good security culture forms the basis for protecting people, information, and assets.

Queensland has developed and is progressively implementing the Queensland Protective Security Framework (QPSF). The QPSF builds on the Commonwealth Government Protective Security Policy Framework (PSPF) and aims to provide Queensland Government agencies with the mandate and supporting guidance in the Queensland context to implement and maintain effective protective security processes and procedures.

The QPSF integrates with, and builds on existing security practices and policies by establishing requirements across the following outcomes:

- security governance
- personnel security
- physical security
- information security (integrating and building on existing practices established by IS18).

Intelligence and Information Sharing

National Cyber Security Threat Level

The National Cyber Security Threat Level (NCSTL) sets out the likelihood of a cyber security threat occurring in Australia, with consideration to the potential impact if a threat is realised. The NCSTL takes a risk-based approach to assist state and territory governments in flexibly addressing a set of principles set under a guided tier system.

The NCSTL is separate to the national incident levels identified in the CIMA which are modified/ increased once a cyber threat is realised. As a result of a change in the NCSTL, Queensland may be asked to implement specific mitigations in response to specific threats.

National, Interjurisdictional, and Industry Cooperation

Queensland Government agencies work closely with the Australian Government, other States and Territories and the private sector to maximise information sharing, increase the awareness of threats and risks, and develop solutions to common security and resilience challenges through mechanisms such as the Australian Government's Trusted Information Sharing Network.

Australian Cyber Security Centre (ACSC)

The ACSC leads the Australian Government's operational cyber security efforts. It monitors cyber threats across the globe, 24 hours a day, seven days a week, to alert Australians to new and emerging cyber risks.

The ACSC shares intelligence with the Queensland Government in response to significant threats and cyber incidents. The ACSC also facilitates briefings with the Queensland Government, as required, in response to a change of threat level under the CIMA.

In addition to the Queensland Government's threat sharing capabilities, the ACSC Partnership Program enables a wide range of organisations to engage with the ACSC and fellow partners, drawing on collective understanding, experience, skills, and capability to lift cyber resilience across the Australian economy.

The ACSC's Joint Cyber Security Centre (JCSC) acts as a local conduit in Queensland for liaison and serves to assist operators of critical infrastructure and industries in Queensland to respond to cyber incidents and threats.

The Queensland Government strongly encourage all entities to visit the ACSC website and utilise its expert guidance and services.

Preparedness

Preparedness is a critical element in minimising the consequences of a cyber incident on Queensland communities and ensuring effective response and recovery (facilitating resilience). Preparedness builds on existing awareness of risk and participation in activities that enhance resilience.

Planning

Strategic planning at the state level is the responsibility of DTMR, which develops and maintains the QGCSA.

All Queensland Government departments are required to have approved agency specific plans (including ICT disaster recovery and business continuity plans under the *Financial Accountability Act 2009*), comprising procedures and arrangements that effectively manage the cyber security hazard and enable ongoing government function during a cyber incident. These plans are required to align with the strategic arrangements in this plan, and the accompanying QGCSA.

Queensland Government departments strongly encourage all portfolio stakeholders to develop and maintain approved capability, planning and continuity arrangements that consider the cyber security hazard. As a part of this planning, entities that do not have access to cyber incident response specialists are encouraged to have a standing arrangement with a third-party provider to ensure access to such resources in a timely manner.

Queensland Disaster Management Integration

The Queensland Disaster Management Arrangements (QDMA) typically enable the progressive escalation of requests for support and assistance in a 'bottom up' approach starting at the local government level. Disaster management groups operating at local, district and state levels are responsible for the planning, organisation, coordination, and implementation of all measures to mitigate/prevent, prepare for, respond to, and recover from disaster situations.

For cyber incidents, most planning and response activities (that accompany and support the incident response activities of individual entities) are coordinated at the national and state level in a 'top down' approach where national or state authorities pass directions or guidance from the top tier to the bottom. A top down approach enables faster decision making and information sharing which is necessary as cyber incidents can escalate rapidly. A centralised management process aligns strategy and focus.

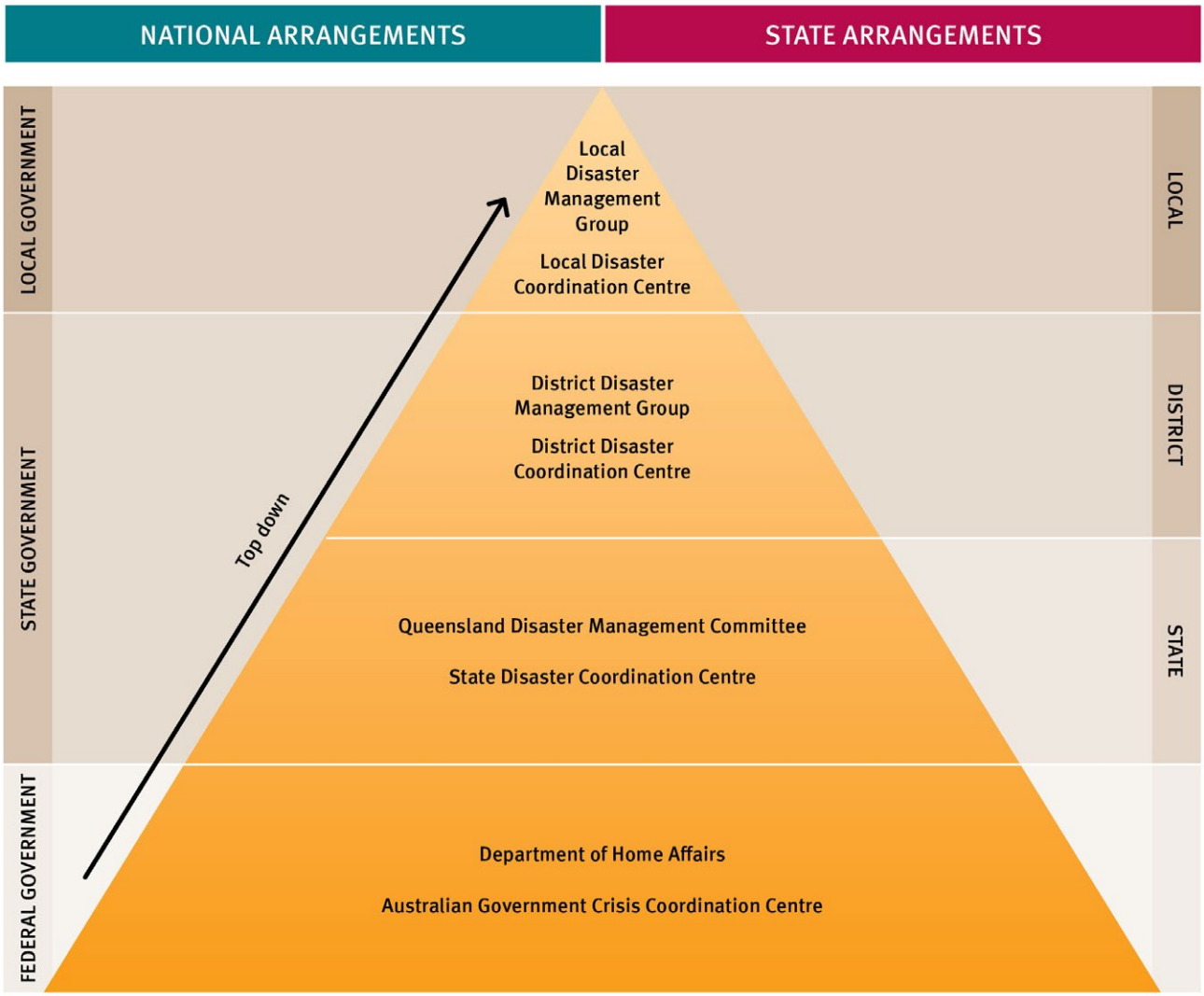


Figure 1: QDMA Overview

The QDMA focus on the consequence management aspects of a cyber incident, and the QGCSA focus on the management of a cyber incident. The QDMA and QGCSA may be activated at the same time in response to a cyber incident. If activated concurrently, both will work towards the one goal of responding to the incident by addressing both the cyber security and disaster management aspects.

Any type of specific assistance required through the QDMA will be identified by DTMR as the lead and requested by the Department of the Premier and Cabinet (DPC) (outside of an existing QDMA activation) or via the State Coordination Group (when the QDMA are already activated) who will then coordinate with the relevant entities.

Decision Making in a Crisis

Strategic decision making and policy for cyber security at the Cabinet and Ministerial level can fall within the scope of both the Queensland Disaster Management Committee (QDMC), and Queensland Security Cabinet Committee (QSCC).

The QDMC will be the primary forum for whole-of-government coordination and leadership if the consequences of an incident lead to a disaster that will invoke the various levels of the QDMA. The QDMA focus on the consequence management aspects of an incident, whereas the QGCSA focus on assessing and then managing the cyber event itself.

For significant security incidents, the QSCC may be convened to provide strategic decision making and guidance, including deciding community leadership messaging, and strategic direction on the management of the relationship with the Australian Government and other state and territory governments during the incident.

If both committee systems are convened concurrently to respond to a cyber incident, they will work jointly to address both the disaster management and security aspects. If the QGCSA escalate to a Level 1 or Level 2 incident, the State Disaster Coordination Group (SDCG), may be activated by the QDMC or QSCC.

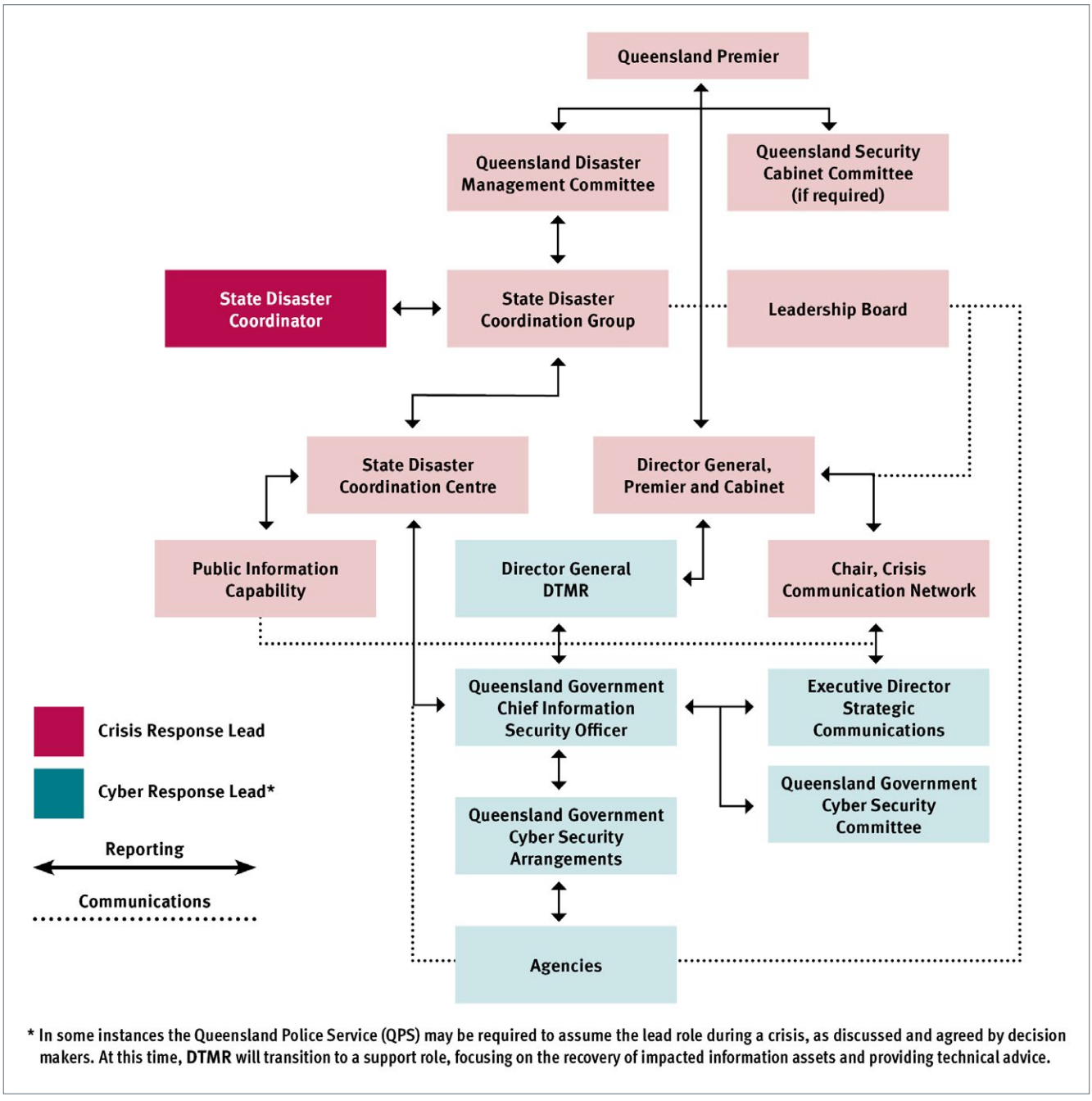


Figure 2: State Cyber Crisis Integration

Roles and Responsibilities

State Strategic

Group / Position	Roles and Responsibilities
Queensland Disaster Management Committee (QDMC)	• Chaired by the Premier of Queensland; core membership comprised of applicable Ministers. • Provides senior strategic leadership and decision making in relation to disaster management during a cyber incident (consequence management).
Queensland Security Cabinet Committee (QSCC)	• Chaired by the Premier of Queensland; core membership comprised of applicable Ministers. • Provides senior strategic leadership and decision making in relation to a significant security incident (e.g., cyber incident, terrorism, or major crime).
Leadership Board	• Chaired by the Director-General, Department of the Premier and Cabinet (DPC). • Leadership Board meetings (comprised of all relevant Directors-General) are convened from time to time to specifically coordinate and provide strategic leadership across Government and to relevant Ministerial bodies.
Crisis Communication Network (CCN)	• Chaired by the Assistant Director-General, Reform and Delivery, DPC. • Provides direction and support to the lead agency throughout the life of the major issue or crisis. • With representatives of the lead agency, participates in relevant meetings to report on public information matters. • Provides CCN members (department and agency Heads of Communication) with advice about the key themes and strategic messages to build into the public information products of each agency. • Provides direction to CCN members about the development of talking points, media releases, promotional resources, and advertising.

State Operational

Group / Position	Roles and Responsibilities
State Disaster Coordinator (SDC)	• Coordinates the disaster response operations for QDMC. • Reports regularly about such operations and ensures that any strategic decisions by QDMC for disaster response operations are implemented.
Queensland Government Chief Information Security Officer (QGCISO)	• Provides leadership and coordinates the technical response for a cyber incident impacting multiple government entities. • Provides advice to senior decision makers on the potential for further impacts through escalation of a cyber incident and the approach to the technical recovery.
State Disaster Coordination Group (SDCG)	• Supports the SDC and Leadership Board in areas such as coordinating disaster response operations for the QDMC and QSCC. • Helps ensure, as far as reasonably practicable, that any strategic decisions by these committees about disaster response or security operations are implemented.
State Disaster Coordination Centre (SDCC)	• Supports the QDMC, QSCC, SDCG and SDC through the coordination of the state-level operational response during disaster operations. • Ensures information about an event and associated disaster operations is disseminated to all levels of the QDMA (local and district tiers).
Queensland Government Cyber Security Committee (QGCSC)	• Chaired by the QGCISO. • Comprised of Chief Information Officers (or equivalent) and Agency Security Executives) from Queensland Government Departments. • May also include the investigations arm of the Queensland Police Service (QPS). • Provides a collective forum to aid agencies in providing advice and support to QDMC and QSCC through Ministers and SDCG representatives. • Supports the management of response and communication activities during a state cyber incident or crisis.

Other

Group / Position	Roles and Responsibilities
Government entities	• Responsible for individual cyber incident responses (including reporting), business continuity and disaster management planning. • Required to operate in accordance with legislation and codes of practice and manage cyber security as a business risk. • Some government-owned entities conduct activities and provide essential services in a commercially orientated and competitive manner. • Some government-owned entities also have emergency support functions, roles and responsibilities listed in the QSDMP, but for the purposes of disaster management are coordinated by their relevant government agency.
Private sector	• Responsible for individual cyber incident responses, (including reporting), business continuity and disaster management planning. • Required to operate in accordance with legislation and codes of practice and manage cyber security as a business risk.

Queensland Government Cyber Security Committee (QGCSC)

Overview	
Formation	Established by the QGCISO under the Queensland Government Cyber Security Hazard Plan.
Area of responsibility	State of Queensland.
Members	• Chaired by the QGCISO. • Membership consists of representatives from each Queensland Government agency. – Primary member is agency security/business impact lead – Secondary member is the agency CISO, Chief Information Officer, or equivalent. – The QPS may also extend membership to applicable staff from the Cybercrime Squad and Financial and Cybercrime Group (investigations arm). – Attendance for statutory authorities and critical infrastructure providers will be considered on a needs basis, or information will be shared to these entities through the applicable portfolio agency.
Functions	• Provides a collective forum to aid agencies in providing advice and support to QDMC and QSCC through Ministers and SDCG representatives. • May support the management of response and communication activities during a cyber incident. – Activate or de-escalate the QGCSA. – Aggregate information and facilitate briefing and awareness. – Consult with and share expertise and resources among Queensland Government agencies. – Develop and share key messages. • Assists DTMR to facilitate coordinated prevention, preparedness, response, and recovery for cyber incidents in Queensland. • Provides input into the development of cyber security exercises, and reviews reports, recommendations, and proposed actions from the same. • Establishes teams or sub-groups as required and endorsed by the QGCSC (e.g., convene CIOs to assist in the technical management of a cyber incident). • Monitors and reports on work led by teams or sub-groups. • Shares information on emergency management as it relates to cyber security. • Identifies areas where the QGCSA could be improved. • Annually reviews operational procedures under the QGCSA
Communications	• The QGCSC may be convened by the QGCISO to identify strategic priorities and provide direction or guidance during a cyber incident. • Through the QGCISO and agency representation, the QGCSC provides reports, advice, and recommendations to decision makers: – QDMC/QSCC • State Disaster Coordination Group – Leadership Board – Agency Ministers and executives

Table 2: Overview of the Queensland Government Cyber Security Committee

Queensland Capability

Exercises

Exercises determine the effectiveness of capability, planning actions, and provide assurance of readiness. The DTMR CSU will exercise the Plan, accompanying QGCSA, and general preparedness at least annually, and strongly encourage that all entities also test their cyber security arrangements on a regular basis.

Lessons Management

The DTMR CSU utilises a lessons management framework to continually enhance processes and activities, future service delivery planning, and performance in managing the cyber security hazard. The framework aligns with guidance from the Queensland Inspector-General Emergency Management and the Australian Institute of Disaster Resilience.

Through this framework, the CSU captures and analyses observations to ensure that implemented changes to the QGCSA are:

- evidence based
- integrated
- consistent
- continuous
- meaningful.

Intelligence and Capability Integration

The ACSC maintains national daily cyber information and intelligence monitoring capabilities to identify potential threats to Australia. The Queensland Government is an active member of the ACSC Partnership Program. This membership aids lifting cyber resilience by enabling the sharing of threat intelligence and insights and collaborating on mitigating controls.

Capability Integration and Resources

In addition to the 24/7 cyber information and intelligence monitoring capabilities of the ACSC, the Queensland Government has additional cyber information and intelligence monitoring capabilities to identify potential threats in the Queensland context.

- The Queensland Government Cyber Defence Centre (CDC) operated by CITEC provides Security Operations Centre services on a year-round, 24/7 basis. The CDC communicates to SDCC through the DTMR CSU.
- An incident response tender allows for the DTMR CSU to help smaller agencies without dedicated cyber incident response arrangements access expert support.

Detection

At a state level, the DTMR CSU facilitates and supports cyber information and intelligence monitoring capabilities to identify potential threats to Queensland Government entities. DTMR CSU also shares information with the ACSC and other states and territories.

The Queensland Government has various capabilities to produce and share cyber threat intelligence and information. This aids the early detection of cyber incidents as a key response priority, and all stakeholders have a responsibility to report cyber incidents. Early notification provides more time to effectively contain and mitigate cyber incidents before they can escalate into something more serious, costly and disruptive.

Queensland Government Agency Notification

In accordance with the mandatory reporting requirements outlined under the Information Security Policy (IS18) and the incident reporting standard, Queensland Government agencies who have committed to implementing IS18 are required to report:

- immediately for security incidents affecting a single system with a business impact level of ‘Medium’ or above
- immediately for security incidents affecting multiple systems / agencies.

Reports are to be made to the Queensland Government Information Security Virtual Response Team (QGISVRT) on 07 3215 3951 and QGISVRT@qld.gov.au. Agencies should also notify, and brief all required internal parties for any incident with an immediate reporting requirement.

Industry Notification

Organisations (private business, and Queensland Government entities not utilising IS18) should report all cyber incidents and emergencies to the ACSC on 1300 CYBER1 (1300 292 371) (24/7). Notifications should also be made by the entity to the relevant Queensland Government portfolio department, who will advise DTMR if required.

Notification Requirements for Critical Infrastructure

In addition to the above, it should be noted that owners and operators of critical infrastructure captured by the SOCI Act are subject to mandatory cyber incident reporting to the ACSC for critical infrastructure assets.

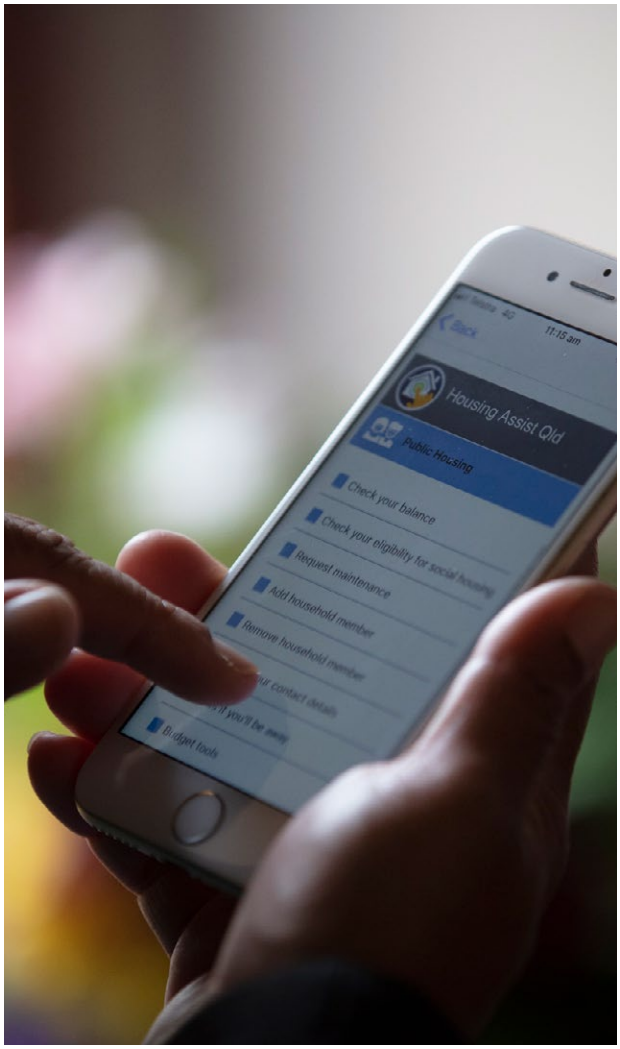
- Critical cyber incidents must be reported within 12 hours of becoming aware of the incident.
  - Verbal reports must be supported by a written record within 48 hours of a verbal notification.
- Other cyber incidents must be reported within 72 hours of becoming aware of the incident.
  - Verbal reports must be supported by a written record within 48 hours of a verbal notification.

Support

While Queensland Government entities are responsible for maintaining daily cyber information and intelligence monitoring capabilities to identify, respond to, and escalate potential system threats, the DTMR CSU can provide direct technical support and advice to an entity affected by a cyber incident. When multiple entities are affected, the DTMR CSU can provide prioritised technical support, as well as indirect support, advice, and community messaging.

Private Industry Support

The DTMR CSU has no legal authority to shape the way private industry act in preparation for, or response to, cyber incidents. If required or requested, the DTMR CSU can work in partnership with the applicable portfolio department to offer expert advice to support private industry in managing cyber security risks.



Response

Response involves taking appropriate measures to respond to an incident, which includes actions taken and measures planned before, during and after a cyber incident to ensure that its effects are minimised, and persons affected by the event are given immediate relief and support.

The Queensland Government and its agencies are responsible for the WoQG response to a cyber incident affecting Queensland Government services and systems.

Priorities

- Public Safety
- Delivery of essential services
- National security
- Trust in the Queensland Government's digital systems and the digital economy more broadly.

While there may be competing priorities and actions during a cyber incident, public safety is to be the highest priority when undertaking decision making.

Decision making is underpinned by authority, event management and reporting.

Control and Coordination

Upon notification of a potential threat or actual cyber incident (through agency, organisation or ACSC reporting), the QGCISO, DTMR CSU, and QPS Cybercrime Squad will work with agencies and use reported information to perform an assessment of the severity of an incident using the QGCSA. This helps ensure that the appropriate notifications are made, and that any required response resources are allocated, or support provided with a view to potentially neutralising or reducing the impacts of any cyber incident.

As soon as there is justification that any incident pertains to multiple Queensland Government agencies or systems, multiple critical infrastructure entities, or a large-scale data breach, DTMR may be required to support response efforts and/or assume control as lead agency.

If DTMR is required to assume the lead agency role, the QGCISO and the DTMR CSU will be responsible for coordinating the incident response and will exercise control over, and share relevant information with, any applicable stakeholders and other responding agencies

If WoQG information sharing, response and/or resource coordination is required to support the assessment, response, and escalation of a cyber threat or incident, the QGCISO may convene the QGCSC. This forum is designed to be used for briefing and/or formal activation purposes to support situational awareness, response coordination, and decision making among agencies.

Where required, the QGCISO will consider the need to provide early advice to relevant agencies involved in managing the consequences of an incident to ensure timely notification and activation of support mechanisms. Should a state cyber incident or crisis occur or is justified, the QGCISO will advise the Director-General, DTMR, who will advise the Director-General, DPC, of the incident. This will include initial advice about the severity of the incident and the current response.

Levels of Cyber Incidents

In Queensland, cyber incidents are classified into five levels on increasing severity. The determination of the emergency level by threat and risk characteristics provides an indication of the extent of response and coordination that will be required to manage an incident. These levels (outlined in Table 3) align with the Australian Government's CIMA and the QGCSA. They can also be used alongside the publicly available ACSC cyber incident categorisation matrix.

CIMA Level	QGCSA Level	Authority to Declare	Characteristics that inform key activities (not exhaustive)	QDMA Level
5	5	N/A	**Business as usual** • Threats with potential to breach security controls and incidents with a low business impact may be detected and resolved with existing business processes/capability/capacity.	Stand Down
4	4	QGCISO	**Potential Cyber Incident** • Potential suspected or unconfirmed cyber incident of medium or high business impact. • Watching brief - enhanced monitoring, analysis, and engagement to manage.	Alert
3	3	QGCISO	**Cyber Incident** • Breach of security controls is causing minor to moderate impacts to services, information, assets, reputation, relationships. • Requires response action in a single entity, with others on alert and/or assisting	
2	2	DG DPC and DG DTMR*	**State Cyber Incident** • Breach of security controls is causing moderate to major impacts to services, information, assets, reputation, relationships. • Involves more than one critical infrastructure asset or government organization or is a significant data breach that requires a coordinated response. • Immediate inter-departmental response, QDMC may activate for preparedness	Lean Forward
1	1	Leadership Board or DG DPC / DG DTMR* or QDMC	**State Cyber Crisis** • Breach of security controls with extenuating or particularly severe impacts to services, information, assets, reputation, relationships, or Queensland communities. • Potential to cause, or is actively causing significant harm to people, property, or the environment. • Collective strategic approach to response, requirement for WoQG crisis management. If already activated, QDMC may give authority to declare a state of emergency.	Stand Up

Table 3: QGCSA levels and alignment

*A state cyber incident or crisis will be declared by the Director-General DPC in consultation with DG DTMR, acting on advice from the QGCISO and affected Queensland Government agencies and/or stakeholders

Crisis Escalation

Should any notification be received and assessed by the QGCISO as likely to meet the threshold of a state cyber incident (QGCSA Level 2) or crisis (QGCSA Level 1), the QGCISO will work with the Director-General of DTMR to brief the Director-General of DPC, who will determine which of the Government's strategic crisis management arrangements may need to be activated.

Concurrent with these actions, the QGCISO and DTMR CSU will work with DTMR strategic communications to aid awareness and help ensure any early link in with the Chair of the Crisis Communication Network (CCN).

A state cyber incident or crisis may then be collectively declared by the Leadership Board or the Director-General of DPC in consultation with the Director-General of DTMR, acting on advice from affected Queensland Government agencies and/or stakeholders.

As a result, the QDMC and/or QSCC may convene at the direction of the Premier on the advice of the Director- General of DPC.

- The QDMC may be utilised to take responsibility of a cyber incident requiring significant consequence management.
- The QSCC may be utilised to provide strategic decision making and guidance in the event of a significant security incident.

The SDCC will also be informed of any state cyber incident (QGCSA Level 2) or crisis (QGCSA Level 1) that poses a potential or actual risk to people, property, or the environment.

- The Executive Director, Law and Justice Policy, DPC, will contact the Australian Government National Situation Room to advise that Queensland's Crisis Management Arrangements have been activated.

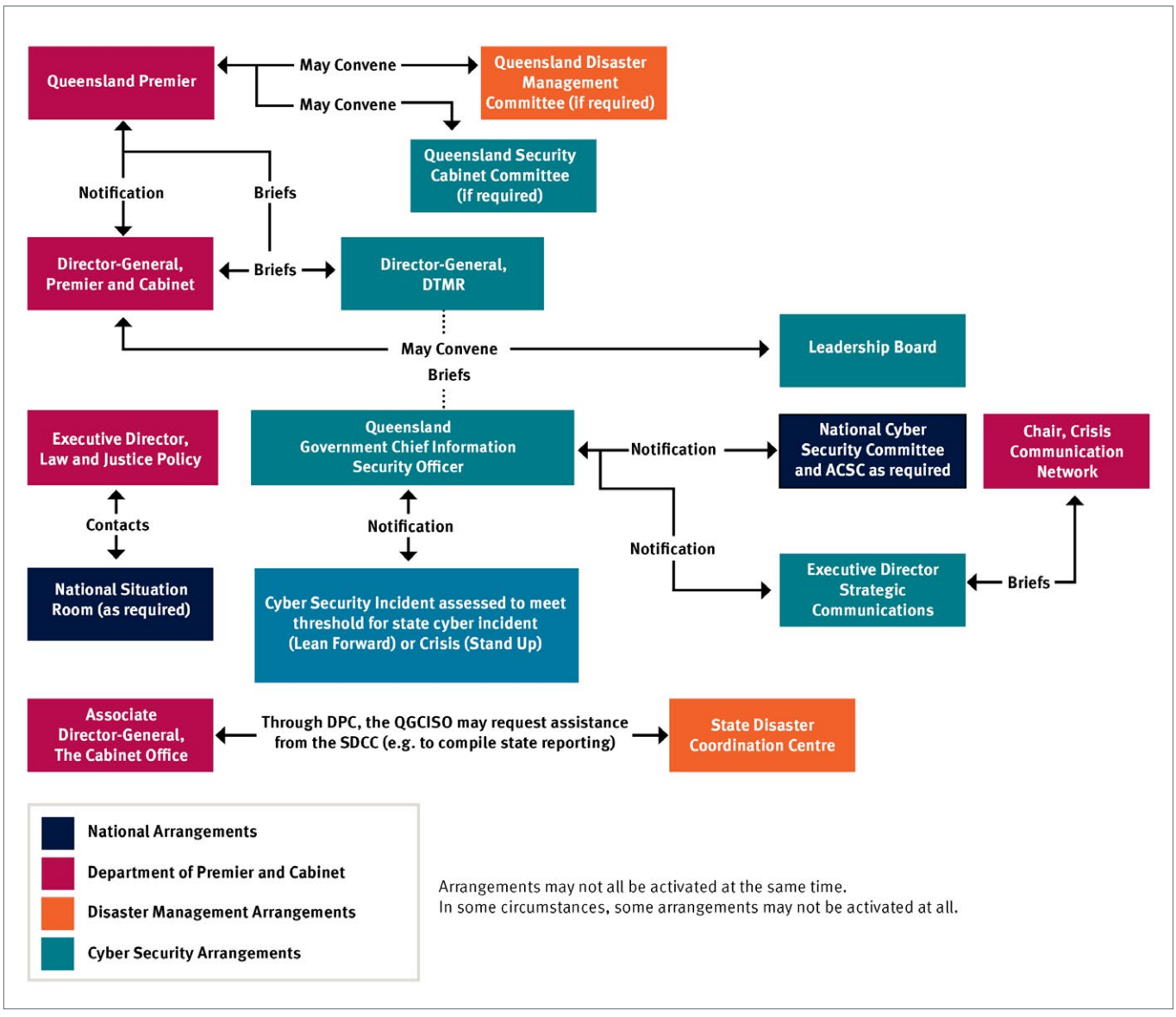


Figure 3: Escalation Pathway for a State Cyber Incident or Crisis

De-escalation

If declared, de-escalation of a state cyber incident will be authorised by the Director-General DPC in consultation with DG DTMR, acting on advice from the QGCISO and affected Queensland Government agencies and/or stakeholders.

If declared, the de-escalation of a state cyber crisis and any transition to recovery will be authorised by the QDMC, acting on advice from affected Queensland Government agencies and/or stakeholders.

De-escalation from QGCSA Levels 4 and 3 will be authorised by the QGCISO.

Event Coordination

State cyber incidents or crises may occur alongside other major emergencies. Several sector specific coordination arrangements exist at the state and national level to manage cyber incidents.

As a result, DTMR (as led by the QGCISO or delegate) may need to coordinate with other Queensland Government agencies who also have a direct responsibility to manage a cyber incident under legislation or policy. This will ensure an integrated operational response.

During a State Cyber Crisis, the State Disaster Coordinator will work with relevant departments to prioritise response roles according to the QSDMP and agreed management priorities.

Situation Reporting

The nature and severity of a cyber incident will influence the activation of information sharing mechanisms used. Mechanisms which allow for the flow of information and collaboration between centres and agencies may include secure and non-secure information systems (including teleconference/videoconference/email facilities), or the convening of committees. Verbal information or written information (including information requests and official reports) will be exchanged through these mechanisms on a regular basis.

Where required, the QGCISO and DTMR CSU will work with affected agencies and/or stakeholders to request approved information for inclusion in WoQG situation reporting. Situation reporting is separate to incident reporting and management – it focuses on the business/community impact and consequences of a cyber incident on an agencies area of responsibility, identifying any current or emerging issues and actions to resolve the same. While not exhaustive, situation reporting may be required for the National Situation Room, the Leadership Board, QDMC, and QSCC to form a common operating picture and inform decision making.

If required at QGCSA Levels 2 and 1, the QGCISO will work with DPC to request that the SDCC help with the compilation of a State Update and Executive Summary using the Emergency Management System. The QGCSA also provide situation reporting templates to agencies for this purpose that are flexible and can be adapted to suit any incident. It also allows for agencies to attach more detailed technical advice.

National Arrangements

The Australian Government leads national coordination and collaboration for cyber incidents on a large or multi-jurisdictional scale that require a coordinated inter jurisdictional response or have national or international consequences. National coordination efforts are designed to support, but not replace, cyber incident management arrangements in each Australian state or territory.

The Australian Government's Cyber Incident Management Arrangements for Australian Governments (CIMA) provide a national framework to reduce the scope, impact, and severity of a national cyber incident through interjurisdictional cooperation and collaboration. The CIMA links to the Australian Government Crisis Management Framework (AGCMF) and establishes requirements for states and territories to:

- control their own response to a cyber incident
- maintain government cyber security planning and policies that align with the CIMA to promote interoperability and consistency, including within individual agencies
- provide coordinated and consistent public communication about a cyber incident and liaise with local government as necessary
- provide the ACSC with information on cyber threats, vulnerabilities, and mitigation strategies for sharing nationally by the ACSC
- liaise with law enforcement agencies to assist with any criminal investigation into a national cyber incident.

The CIMA is owned and maintained by the National Cyber Security Committee (NCSC). The NCSC is the authoritative cyber security coordination body, comprised of Commonwealth representatives and representatives from all states and territories. Queensland is represented at the NCSC by the QGCISO.

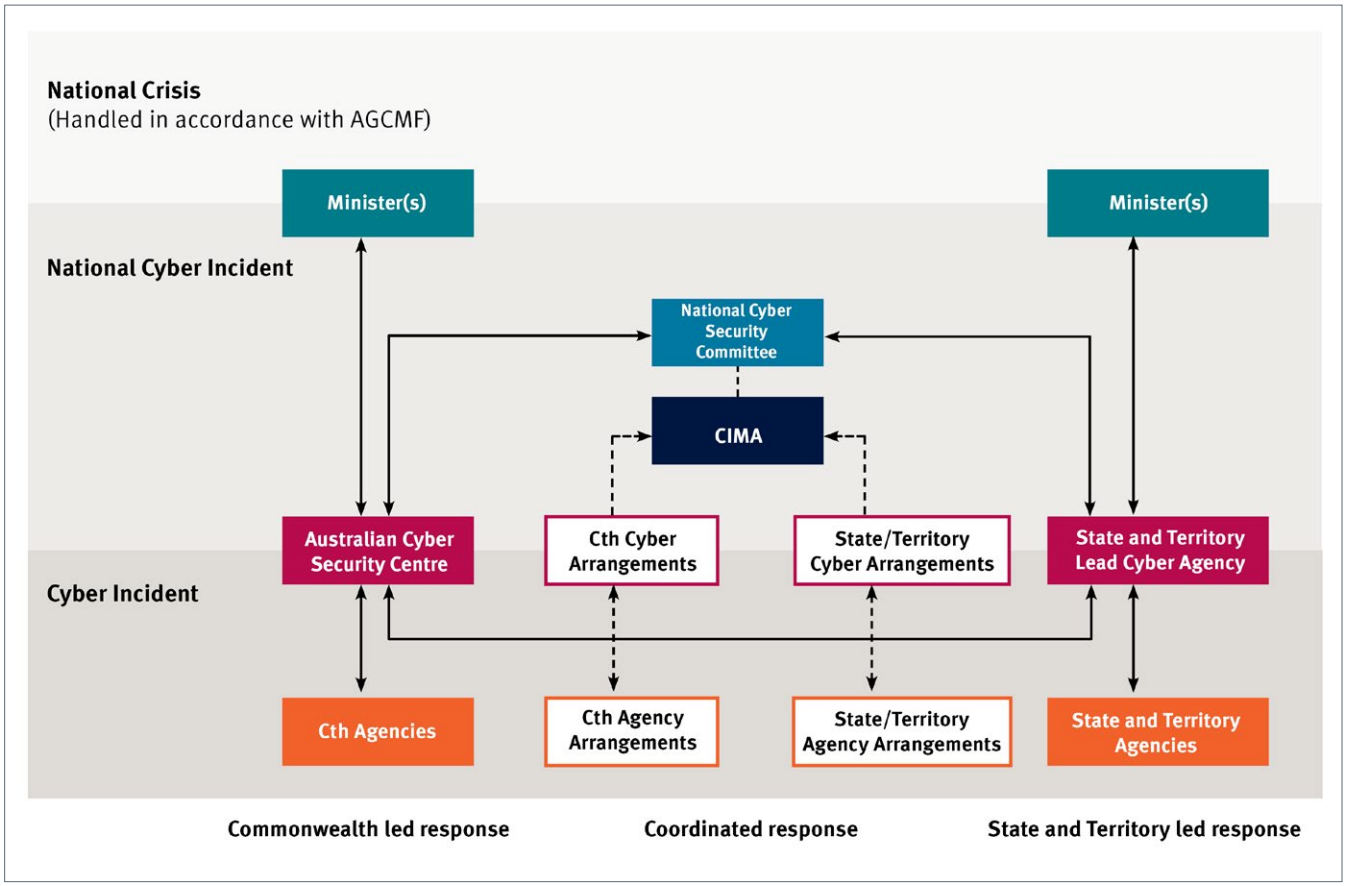


Figure 4: Current CIMA Integration Overview (undergoing National review)

The ACSC leads the bulk of operational response efforts for cyber security at the national level, supported by the Department of Home Affairs (DHA). As the co-chair of the NCSC and the primary Australian operational response lead, the ACSC is the authoritative body for the purposes of declaring a national cyber incident in consultation with the NCSC representatives in affected jurisdictions. State and territory government NCSC representatives advise the ACSC on matters pertaining to their jurisdiction and can also request that the ACSC declare a National Cyber Incident. The Australian Government may also provide, as required, other operational support or guidance from agencies such as the ACSC, Australian Signals Directorate, Australian Security Intelligence Organisation, Australian Federal Police, or the Department of Home Affairs. The need for Australian Government and/or inter-jurisdictional resources and assistance will be determined and communicated by the QGCISO in partnership with agencies (utilising existing relationships where appropriate). Where necessary, requests may also be coordinated by the SDCG and/or DPC.

National Cyber Incident

If a national cyber incident is agreed and declared, the NCSC will activate to support national collaboration and coordination of response efforts. The ACSC will coordinate media, Federal Government, and national public communications for a Level 2 or 1 incident under the CIMA. For a national cyber incident, Queensland will align any messaging to national talking points provided by the ACSC and provide updates on any Queensland impacts, response, or recovery actions. Media and public queries will be referred by Queensland to the ACSC or for response.

National Coordination Mechanism

In the event of a national cyber incident declaration by the ACSC, national crisis management arrangements may be activated. Under the Australian Government Crisis Management Framework, the National Coordination Mechanism (NCM) within the National Emergency Management Agency operates through the Department of Home Affairs. If required, the NCM will be utilised to work with jurisdictions and coordinate the whole-of-government response to address specific impacts of a national cyber crisis.

Depending on an event's scale, nature, and duration, not all national cyber incidents will require the activation of the NCM to respond. The NCM may make a recommendation for consideration by the Prime Minister and First Minister of the directly affected jurisdiction(s). If a national cyber incident is declared (including any subsequent NCM activation), Queensland (via the DTMR CSU) will remain responsible for management of the response within Queensland. This includes the briefing of respective Ministers and officials using key messages and talking points provided by the ACSC.

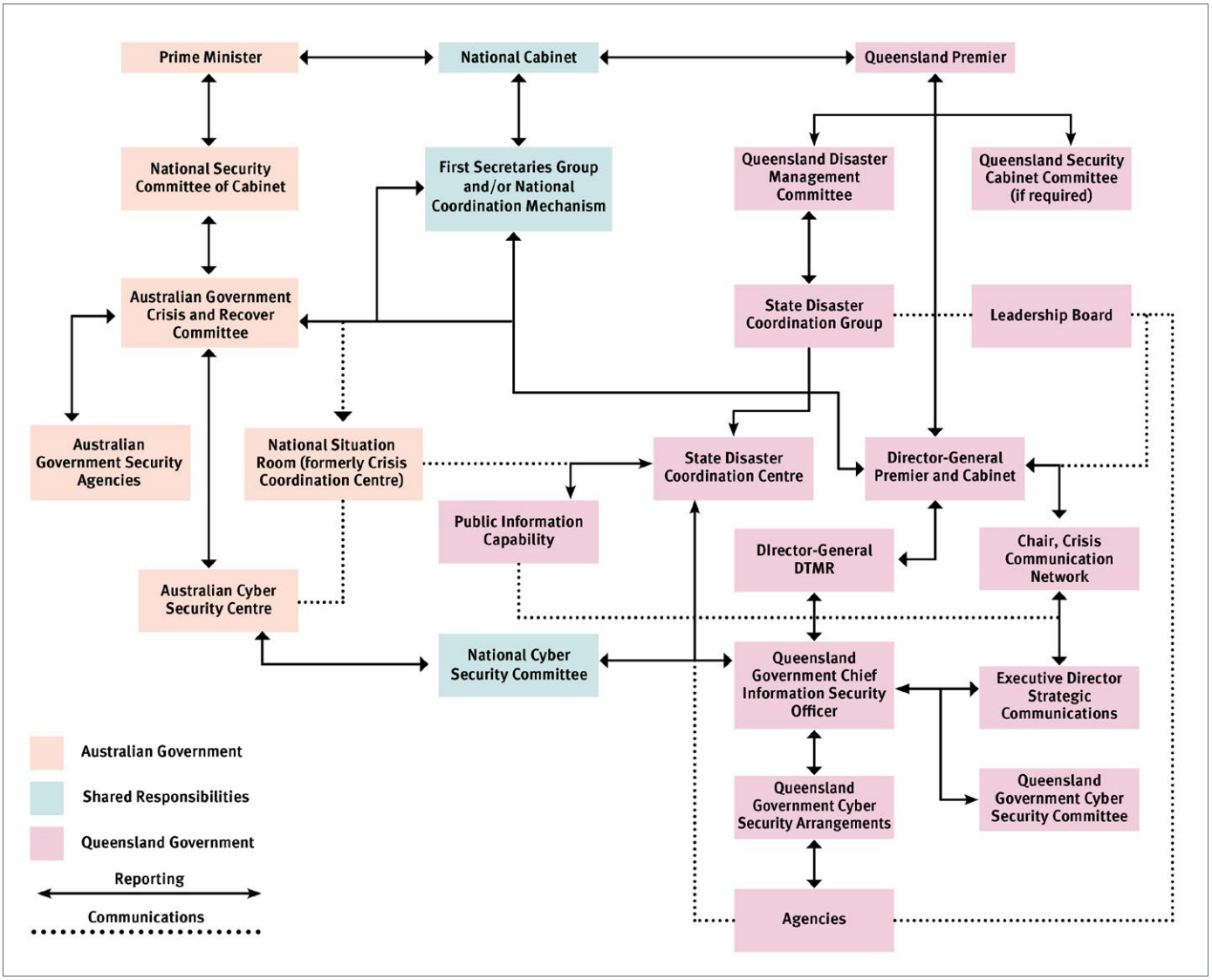


Figure 5: National and State Crisis Response Integration

Media and Communications

Public information in the event of a state cyber incident or crisis will be managed in accordance with the Queensland Government's Crisis Communication Plan. This Plan outlines the actions to be taken by the government in response to an issue or crisis that has a high impact to Queensland, impacts a significant portion of the state's population, or has the potential to negatively impact the reputation of the Queensland Government.

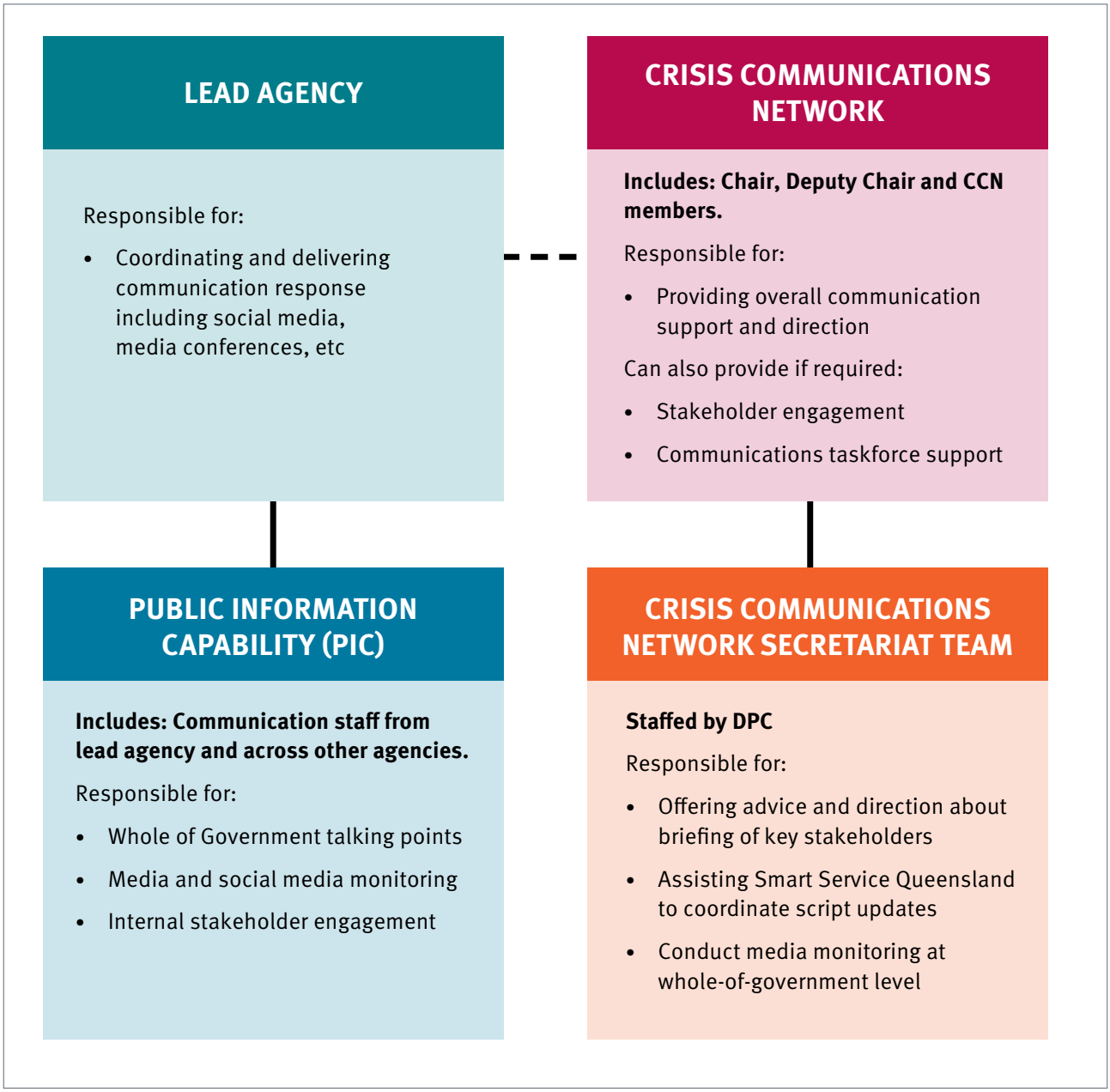


Figure 6: Overview of Queensland Government Crisis Communication Arrangements

Recovery

Cyber incidents often have a long and unpredictable tail, which can make recovery complex. Often, the initial business or system impact of a cyber incident may be followed by unexpected data exfiltration months from the initial detection of a breach, and accompanied by financial losses, and reputational damage.

Recovery in the aftermath of a cyber crisis in Queensland will be undertaken in accordance with the arrangements set out in the Queensland Recovery Plan, maintained by the Queensland Reconstruction Authority (QRA) on behalf of the QDMC.

The Queensland Recovery Plan outlines the recovery governance arrangements in Queensland, focusing on collaboration between agencies, stakeholders and resources for planning and coordinating the delivery of recovery operations.

Responsibility

The QRA is responsible for the coordination of the state's recovery operations following a cyber crisis and is supported by Functional Recovery Groups (FRGs).

Dependant on the nature of a cyber crisis, a State Recovery Coordinator may be appointed who:

- coordinates the recovery and reconstruction efforts of government and non-government entities in the affected areas to support local recovery objectives
- ensures, as far as reasonably practicable, that any strategic decisions about disaster recovery operations made by the QDMC are implemented
- provides strategic advice on disaster recovery operations to Queensland Government entities performing these operations
- escalates risks and issues to FRGs and Leadership Board sub-committee (Recovery) where appropriate
- reports regularly to the Leadership Board sub-committee (Recovery) on progress of recovery operations.

Following a cyber crisis, individual Government entities affected are responsible for consequence management and subsequent recovery operations internally, participating in or providing input to QRA or FRG recovery operations as required to ensure a coordinated approach.

During, or in the aftermath of a cyber crisis, DTMR may work with the QRA and other Queensland Government agencies to identify and/or advise on assistance actions to provide support or relief to Queensland communities

Recovery priorities may include:

- restoring essential services, networks, or information systems
- communicating and providing support to affected communities or persons.

Debriefing and Post Incident Review

The DTMR CSU will coordinate a formal post incident review following the declaration of a state cyber incident or crisis. This review will be conducted in alignment with the DTMR CSU lessons management framework and will collect and utilise observations from all involved parties to drive evidence-based continuous improvement to the QGCSA. Review reports for each incident will be provided to key Queensland Government cyber governance bodies as appropriate.

Appendix 1 – Reference Documents and Legislation

Commonwealth Legislation

Terrorism	*Terrorism (Commonwealth Powers) Act 2002* • The Act refers certain matters relating to terrorist acts to the Parliament of the Commonwealth.
Crime	*Commonwealth Criminal Code Act 1995* • The Act codifies the general principles of criminal responsibility under laws of the Commonwealth.
	Crimes Act 1914 • The Act sets out Commonwealth powers, authorities and obligations for dealing with Commonwealth criminal offences and related matters.
Critical Infrastructure	*Security of Critical Infrastructure Act 2018* • The Act seeks to better risk management and manage complex and evolving national security risks of sabotage, espionage, and coercion posed by foreign involvement in Australian critical infrastructure (e.g., cyber security)
Information	*My Health Records Act 2012* • The Act enables establishment and operation of a voluntary national system for the provision of access to health information relating to recipients of healthcare.
	National Security Information (Criminal and Civil Proceedings) Act 2004 • The Act provides a framework for how National security information is disclosed and protected in criminal and civil proceedings.
	Privacy Act 1988 • The Act promotes and protects the privacy of individuals and to regulate how Australian Government agencies and applicable organisations, and some other organisations, handle personal information.
Disaster Management	*National Emergency Declaration Act 2020* • The Act recognises and enhances the role of the Commonwealth in preparing for, responding to and recovering from emergencies that cause, or are likely to cause, nationally significant harm.

Queensland Legislation

Disaster Management	*Disaster Management Act 2003* The main objects of this Act include: • helping communities mitigate the potential adverse effects of an event, prepare for managing the effects of an event, and effectively respond to, and recover from, a disaster or an emergency • providing for effective disaster management for the State • establishing a framework for the management of the State Emergency Service and emergency service units to ensure the effective performance of their functions.
Public Safety	*Public Safety Preservation Act 1986* • The main object of this Act is to providing protection for members of the public in terrorist, chemical, biological, radiological, or other emergencies that create or may create danger of death, injury, or distress to any person, loss or damage of property, or pollution of the environment and for related purposes.

Queensland Legislation

Public Safety

Police Powers and Responsibilities Act 2000

The main objects of this Act include:

- consolidate and rationalise powers and responsibilities police officers have for investigating offices and enforcing the law
- provide powers necessary for effective modern policing and law enforcement
- provide consistency in the nature and extent of police powers/responsibilities
- standardise the way powers/responsibilities are exercised
- ensure fairness to and protect the rights of persons against whom police officers exercise powers under the Act.

Terrorism

Terrorism (Preventative Detention) Act 2005

- The Act enables a person to be detained for a short time to prevent a terrorist attack from occurring in the near future or to preserve evidence relating to a recent terrorism act.

Information Privacy

Information Privacy Act 2009

The main objects of this Act include:

- the fair collection and handling of information in the public sector environment
- right of access to, and amendment of, personal information in the government's procession or under the Government's control unless, on balance, it is contrary to the public interest to give the access or allow the information to be amended.

Public Records Act 2002

The main objects of this Act include:

- ensuring the public records of Queensland are made, managed, kept, and if appropriate preserves in a useable form for the benefit of present and future generations
- ensuring public access to records is consistent with the principles of the *Right to Information Act 2009* and the *Information Privacy Act 2009*.

Other

Coroners Act 2003

The main objects of this Act include:

- reporting of particular deaths
- establishing procedures for investigations into particular deaths
- helping prevent deaths from similar causes happening in the future by allowing coroners to comment on matters connected with the deaths, including public safety matters or the administration of justice.

Transport Security (Counter Terrorism) Act 2008

- The Act implements a system for identifying surface transport operations at an elevated risk of terrorist attack and ensures they conduct risk assessments, develop security plans, and implement and review security measures.

Ambulance Service Act 1991

- The Act establishes Queensland Ambulance Service and its functions.

Crime and Corruption Act 2001

- The Act defines corrupt conduct and sets out the functions for the Crime and Corruption Commission and its powers.

National non-legislative policy drivers, agreements and planning

Cyber Security	Cyber Incident Management Arrangements • If a national cyber incident reaches a crisis level, the CIMA will operate in support of jurisdictions' respective crisis management arrangements.
	Notifiable Data Breaches Scheme • Under the Notifiable Data Breaches scheme any organisation or agency the *Privacy Act 1988* covers must notify affected individuals and the OAIC when a data breach is likely to result in serious harm to an individual whose personal information is involved.
	Australian Privacy Principles • The Australian Privacy Principles are the cornerstone of the privacy protection framework in the *Privacy Act 1988* (Cth). They apply to any organisation or agency the Privacy Act covers.
Protective Security	Protective Security Policy Framework (PSPF) • The PSPF assists Australian Government entities to protect their people, information and assets, both at home and overseas.
Disaster Management	Australian Government Crisis Management Framework (AGCMF) and associated response plans and resilience policy. • The AGCMF underpins other crisis plans.
	Australian Institute of Disaster Resilience Lessons Management Handbook • The Lessons Management Handbook identifies core principles and suggests frameworks and processes to support the successful implementation of lessons management, which is integral to learning, resilience and continual improvement.

State non-legislative policy drivers and planning

Cyber Security	Cyber Security Operations Plan • The plan supports the governance arrangements as outlined in the plan, and describes the response actions and incident management responsibilities for cyber incidents at all levels, including a cyber security crisis.
Information Security	Information Security Policy (IS18) • The policy seeks to ensure all departments apply a consistent, risk-based approach, to the implementation of information security to maintain confidentiality, integrity, and availability.
Protective Security	Queensland Protective Security Framework (QPSF) • The QPSF assists Queensland Government entities to protect their people, information and assets.
	Crisis Communication Plan • The Crisis Communication Plan outlines the actions to be taken by the government in response to an issue or crisis that has a high impact to Queensland, impacts a significant portion of the state's population, or has the potential to negatively impact the reputation of the Queensland Government.

State non-legislative policy drivers and planning

Disaster Management

Queensland State Disaster Management Plan (QSDMP)

- The QSDMP enables Queensland to mitigate the effects of, prepare for, respond to, recover from, and build resilience to disaster events.

Queensland Disaster Management Strategic Policy Statement

- The statement informs the Queensland Government's strategic approach to keeping people safe and making communities more resilient to disaster risks and impacts.

Queensland Prevention, Preparedness, Response, and Recovery Disaster Management Guideline

- The guideline informs the Queensland Government's strategic approach to keeping people safe and making communities more resilient to disaster risks and impacts.

Queensland Disaster Management Lessons Management Framework

- The framework enables interoperability and leverages the internal processes currently applied across all levels of the disaster management arrangements in Queensland to drive system level improvements.

Queensland Recovery Plan (QRA)

- The QRA outlines the recovery governance arrangements in Queensland. It focuses on collaboration between agencies, stakeholders and resources for planning and coordinating the delivery of recovery operations.

DTMR Disaster Management Framework

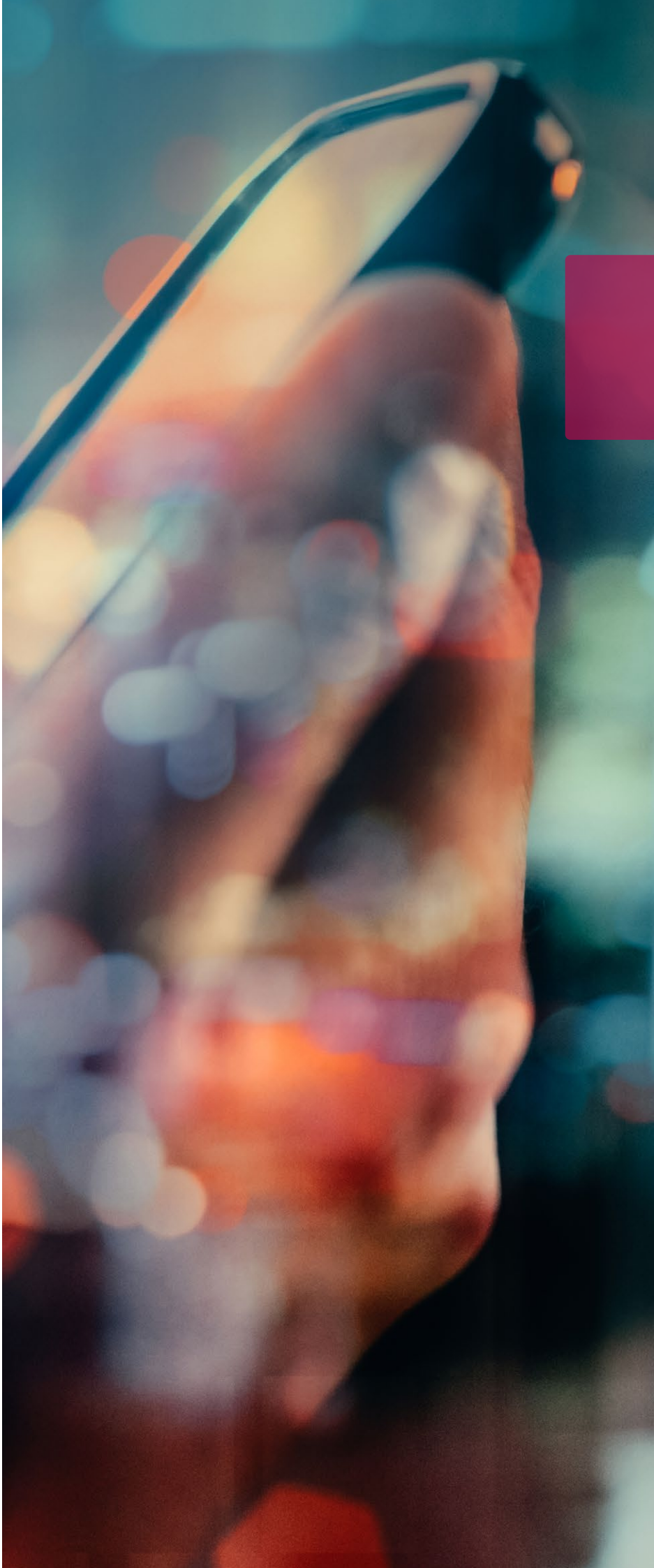
- The framework relates to strategic and operational disaster management planning necessary for DTMR to fulfil roles and responsibilities defined in the QSDMP and other legislation/policy.

Crisis Communication Plan

- The Crisis Communication Plan outlines the actions to be taken by the government in response to an issue or crisis that has a high impact to Queensland, impacts a significant portion of the state's population, or has the potential to negatively impact the reputation of the Queensland Government.

Appendix 2 – Glossary

Abbreviation	Name
ACSC	Australian Cyber Security Centre
AGNSR	Australian Government National Situation Room
ASD	Australian Signals Directorate
CCN	Crisis Communication Network
CCT	Crisis Communications Taskforce
CDC	Cyber Defence Centre
CERT	Computer Emergency Response Team
CIMA	Cyber Incident Management Arrangements for Australian Governments
CSU	Cyber Security Unit
DTMR	Department of Transport and Main Roads
DG	Director-General
DPC	Department of the Premier and Cabinet
EMS	Emergency Management System
FRG	Functional Recovery Group
GOC	Government-Owned Corporation
ICT	Information and Communications Technology
IS18	Information Security Policy (IS18:2018)
ISMS	Information Security Management System
JCSC	Joint Cyber Security Centre
NCC	National Crisis Committee
NCM	National Coordination Mechanism
NCSA	National Cyber Security Arrangements
NCSC	National Cyber Security Committee
NCSTL	National Cyber Security Threat Level
NEMA	National Emergency Management Agency
PIC	Public Information Capability
PPRR	Prevention, Preparedness, Response, Recovery
QDMA	Queensland Disaster Management Arrangements
QDMC	Queensland Disaster Management Committee
QGCISO	Queensland Government Chief Information Security Officer
QGCSA	Queensland Government Cyber Security Arrangements
QGCSC	Queensland Government Cyber Security Committee
QGISVRT	Queensland Government Information Security Virtual Response Team
QPS	Queensland Police Service
QPSF	Queensland Protective Security Framework
QRA	Queensland Reconstruction Authority
QSCTC	Queensland Security and Counter Terrorism Committee
QSCC	Queensland Security Cabinet Committee
QSDMP	Queensland State Disaster Management Plan
SCADA	Supervisory Control and Data Acquisition
SDC	State Disaster Coordinator
SDCC	State Disaster Coordination Centre
SDCG	State Disaster Coordination Group
SOCI	Security of Critical Infrastructure Act 2018 (Cth)
SSQ	Smart Service Queensland
WoQG	Whole of Queensland Government



Queensland Government