Queensland Government
Cyber Security Hazard Plan

DELIVERING
FOR QUEENSLAND

Queensland
Government

This publication has been compiled by the Data and Digital Government Division, Department of Customer Services, Open Data, and Small and Family Business.

© State of Queensland, 2025

The Queensland Government supports and encourages the dissemination and exchange of its information. The copyright in this publication is licensed under a Creative Commons Attribution 4.0 International (CC BY 4.0) licence.

Under this licence you are free, without having to seek our permission, to use this publication in accordance with the licence terms.

You must keep intact the copyright notice and attribute the State of Queensland as the source of the publication.

Note: Some content in this publication may have different licence terms as indicated.

For more information on this licence, visit https://creativecommons.org/licenses/by/4.0/.

The information contained herein is subject to change without notice. The Queensland Government shall not be liable for technical or other errors or omissions contained herein. The reader/user accepts all risks and responsibility for losses, damages, costs and other consequences resulting directly or indirectly from using this information.

Contents

Authorisation statement

Queensland is a leader in crisis and disaster management. In addition to natural disasters, pandemics and biosecurity incidents, the state also faces increasingly complex threats to cyber security.

Queensland uses an all-hazards approach to disaster management, with sub-plans to address some hazards, including cyber security, which require extra coordination and special actions.

The Queensland Government Cyber Security Hazard Plan (the Plan) is issued under the authority of the Director-General, Department of Customer Services, Open Data and Small and Family Business (CDSB). The Plan outlines the response and escalation pathway for cyber incidents with statewide or national consequences or security implications, in support of CDSB as the lead agency. In the event that a threat or incident requires a coordinated response, the Plan outlines how the Queensland Government will work with partners and agencies to protect Queenslanders and digital services.

The Plan is hereby approved and recommended for distribution.

Chris Lamont

Chris Lamont

Director-General

Department of Customer Services, Open Data, and Small and Family Business

18/08/2025

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 consequences or security implications. The Department of Customer Services, Open Data and Small and Family Business (CDSB) is the lead agency responsible for the development and implementation of the Plan.

Aim

The Plan outlines Queensland's role in preventing, preparing, responding to, and recovering from cyber incidents. It describes the interaction between the cyber security community, law enforcement and security agencies, business continuity personnel, the emergency management sector, and inter-jurisdictional partners 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 consequences or security implications 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 consequences or security implications
- outline Queensland's role in supporting the Australian Government's *Australian Cyber Incident Response Plan* (AUSCYBERPLAN) and the *Cyber Incident Management Arrangements for Australian Governments* (CIMA) as the applicable national response frameworks for cyber incidents under the *Australian Government Crisis Management Framework* (AGCMF).

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 Operations Plan which outlines Queensland's operational cyber incident response
- aligns with Queensland Police Service (QPS) planning for the management of confined, serious and significant security incidents
- aligns with the Australian Government's AUSCYBERPLAN and CIMA, which provide guidance on governmental collaboration on response 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 prevent, 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 or security implications occurring
- annual planned exercise evaluations demonstrating a need for review.

Context

Hazard definition

As defined by the (AGCMF), a cyber incident is a single or series of unwanted or unexpected event(s) that have the potential to impact the confidentiality, integrity or availability of a network or system or the information that it stores, processes or communicates.

This may disrupt government operations, essential services, or critical infrastructure and require a coordinated response. This may include unauthorised or malicious sharing of data, manipulation or destruction of critical data and software, disruptions to ICT networks or systems, and exploitation of networks to cause a physical effect.

Not all cyber incidents are caused by the unlawful acts of a threat actor.

In Queensland, a response to a cyber incident may be led by an individual organisation or agency, or may require coordination under this plan and/or the AGCMF when considering technical aspects or broader consequences of the incident.

The importance of cyber security

In today's digital economy, all sectors of government, society and industry rely on 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.

Relying more on digital technology has its benefits, but it also brings extra risks, especially for security. Cyber criminals take advantage of digital connectivity for criminal activities. The term 'cybercrime' describes a broad range of criminal offences that rely on or involve the use of computers or electronic devices.

The actions of cyber criminals pose a critical business risk to the Queensland community. Any organisation that operates in the online space could be affected. No one is completely safe from cyber security risks, and the impact of an incident depends on how effective the hazard mitigation and risk management strategies are.

Critical assets and systems are subject to a range of ownership and governance structures. Effective cyber security and incident response depend on clearly defining the roles and responsibilities of government bodies, corporations, and private businesses.

The digital security environment

The digital security environment is rapidly deteriorating, leading to more frequent, larger, and more complex cyber security incidents. Threat actors are advancing faster than cyber defenders can keep up, making cyber incidents a regular occurrence rather than a rare event.

In 2023–2024 the Australian Signals Directorate's (ASD) Australian Cyber Security Centre (ACSC) Annual Cyber Threat Report noted[1]:

- One new cybercrime report was made approximately every six minutes
- More than 87,400 cybercrime reports were made to ReportCyber
- 30 per cent (approximately 26,220) of these reports were attributed to Queensland (Queensland reports disproportionately higher rates of cybercrime relative to the population)
- The average self-reported cost of cybercrime for medium-sized businesses was $62,600.

Malicious cyber activity poses a significant risk to Australian networks and systems. Threat actors are continuing to target every sector of the Australian economy, including an increasing number of attacks on critical infrastructure. Basic attack techniques continue to be effective, identifying the need to collectively uplift cyber maturity.

The deteriorating of the digital security environment is spurred further by geopolitical tensions, conflict and global economic conditions. Central incident caseloads as tracked by the Australian Government continue to increase. Looking forward to 2030, the Australian Security Intelligence Organisation (ASIO) predicts a 'dynamic security environment with an unprecedented number of challenges and a cumulative level of potential harm.'

In 2024, the national terrorism threat level was raised, highlighting the digital environment as a key catalyst for concerning security behaviour in the physical environment. This is because information online spreads quickly and far, with little moderation, and vulnerable cohorts who engage with online content.

While threat actor groups have different motivations, their skills are improving, and they are quickly taking advantage of unpatched vulnerabilities. Even with strong defences, supply chain cyber incidents are becoming more common and effective. This has prompted governments and industry to focus on incorporating cyber risk management procedures into contracts.

While the capacity and capability of cybercriminals is increasing, security and intelligence agencies have continued to identify that authoritarian regimes are growing more willing to disrupt or destroy critical infrastructure to further their strategic interests. Recent attribution activity by the Australian Government identifies that nation state threat actors are trying to explore and exploit Australia's important networks, almost certainly mapping systems so they can lay down malware or maintain access in the future.

Operational Technology (OT) and Internet of Things (IoT) devices are increasingly targeted by skilled cyber actors more frequently. These devices are used as entry points before attackers pivot to target IT systems and data. OT systems often have outdated or unsupported software that can't be patched, making them vulnerable. Since OT is common in critical infrastructure, patching these systems is done carefully to avoid causing disruptions to service delivery.

[1] ASD Annual Cyber Threat Report 2023-2024.

Prevention

Cyber incidents cannot be completely avoided, so the focus is on understanding and reducing the risk and minimising impact. Prevention activities for cyber security are now business-as-usual practice, underpinned by systematic risk management. Cyber security is no longer an ICT problem, but a business risk.

CDSB is responsible for strengthening and expanding the cyber security capabilities and capacity of Queensland Government to maintain pace with the dynamic digital security environment.

CDSB helps by providing:

- cyber security leadership and direction
- guidance on governance, policy, and standards
- cyber security fund allocation and delivery
- a coordinated response to cyber incidents
- cyber security capability uplift and awareness
- cyber security products and services.

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

Queensland Government Information Security Policy

The *Queensland Government Information and Cyber Security Policy* (IS18) ensures the Queensland Government applies a consistent, risk-based approach to the implementation of information security.

Under IS18, Queensland Government agencies (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, IS18 sees applicable agencies:

- aligning to international best practice cyber-governance based on ISO27001 standards
- continuously maturing and reporting on the implementation of the Essential Eight mitigation strategies recommended by the ASD's 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 Australian Government's Protective Security Policy Framework and aims to provide Queensland Government agencies with the mandate and supporting guidance in the Queensland context to implement and maintain effective 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 and cyber security (integrating and building on existing practices established by IS18).

Intelligence and information sharing

National, interjurisdictional, and industry cooperation

The Queensland Government works closely with Australian Government agencies, 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. This is done through mechanisms such as the National Cyber Security Committee (NCSC) and the Australian Government's Trusted Information Sharing Network.

National Cyber Security Committee

The NCSC is the mechanism for inter-jurisdictional coordination for cyber security incident response. The NCSC members include:

- the Head of the ASD's ACSC
- the National Cyber Security Coordinator
- cyber security leads from each jurisdiction

- representatives from the Department of Home Affairs (DOHA), the National Emergency Management Agency (NEMA), the Australian Federal Police (AFP), and the Department of Prime Minister and Cabinet.

The NCSC coordinates national efforts to prevent, prepare for, and respond to cyber security incidents. Its members lead their jurisdictions response during a national cyber security event.

Australian Signals Directorate's Australian Cyber Security Centre

The ASD's ACSC leads the Australian Government's operational cyber security efforts. It monitors cyber threats globally at all times to alert Australians to new and emerging cyber risks.

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

The ACSC Partnership Program enables organisations to engage with the ACSC and fellow partners, drawing on collective skills and capability to lift cyber resilience across the Australian economy.

The ACSC's Joint Cyber Security Centre (JCSC) in Queensland helps local operators of critical infrastructure and industries 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.

National Office of Cyber Security

The National Office of Cyber Security (NOCS) supports the National Cyber Security Coordinator to deliver their functions under the AGCMF. The Coordinator manages responses to cyber security incidents of national significance or interest and is accountable to the Australian Government Minister for Cyber Security.

The NOCS serves as a key contact point for affected organisations, working with Australian state and territory governments to manage the broader impacts of cyber incidents. These impacts, known as consequence management, relate to the second and subsequent order effects from cyber security incidents.

The NOCS helps government and industry work together to identify and mitigate the secondary harms, which in serious cases could include 'real world' impacts. This may require activating emergency management arrangements such as the National Coordination Mechanism.

Department of Home Affairs

The Department of Home Affairs (DOHA) is responsible for central coordination, strategy and policy leadership in relation to:

- cyber and critical infrastructure resilience and security
- immigration
- border security and management
- counterterrorism
- the protection of Australian sovereignty
- citizenship and social cohesion.

The DOHA implement a strategically coordinated approach to the cyber security and resilience of all Australians. This includes enabling rapid responses to threats of foreign interference and supporting development of cyber security policy for the Australian Government, including implementation of *2023-2030 Australian Cyber Security Strategy*. DOHA work on cyber security threats and opportunities in Australia and overseas, including the security of critical and emerging technology.

Australian Federal Police

The AFP investigate serious and organised cybercrime against:

- the Australian Government
- critical infrastructure and systems
- the Australian economy.

This involves working with other government bodies and partnering with international agencies. The AFP lead the Joint Policing Cybercrime Coordination Centre (JPC3), which is based at a purpose-built facility in Sydney.

The JPC3 brings together all Australian policing jurisdictions. It ensures maximum impact on high-harm, high-volume cybercrime affecting the Australian community.

Trusted Information Sharing Network

The Trusted Information Sharing Network (TISN) is the primary forum where industry and all levels of government work together to improve the security and resilience of critical infrastructure (CI). Through the TISN, members collaborate to strengthen their organisations and industry sectors against all hazards. TISN members collaborate to identify and manage CI risks, address security gaps, implement mitigation strategies, inform policy development and achieve the objectives of the *Critical Infrastructure Resilience Strategy*.

Preparedness

Preparedness is essential to minimise the consequences of a cyber incident on Queensland communities by enabling effective response and recovery (facilitating resilience). Being prepared builds on understanding risk and participating in activities that strengthen resilience.

Planning

Strategic planning at the state level is the responsibility of CDSB, which develops and maintains whole-of-government cyber incident planning.

All Queensland Government agencies must have approved plans with procedures and arrangements to manage cyber security hazards to ensure that government services continue during a cyber incident. These plans are required to align with the strategic arrangements and operational arrangements outlined in this plan.

They should include, but are not limited to, incident response plans, ICT disaster recovery and business continuity plans.

Queensland Government agencies strongly encourage all portfolio stakeholders to develop and maintain plans and continuity arrangements that consider cyber security hazards. 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 quick access when needed.

Queensland Disaster Management Integration

The Queensland Disaster Management Arrangements (QDMA) typically follow 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 prevent, prepare for, respond to, and recover from disasters.

For cyber incidents, a 'top down' approach is used. National and state authorities lead the response, providing guidance and direction to the lower levels. This enables faster decision making and information sharing which is necessary as cyber incidents can escalate rapidly. A centralised management process aligns strategy and focus.

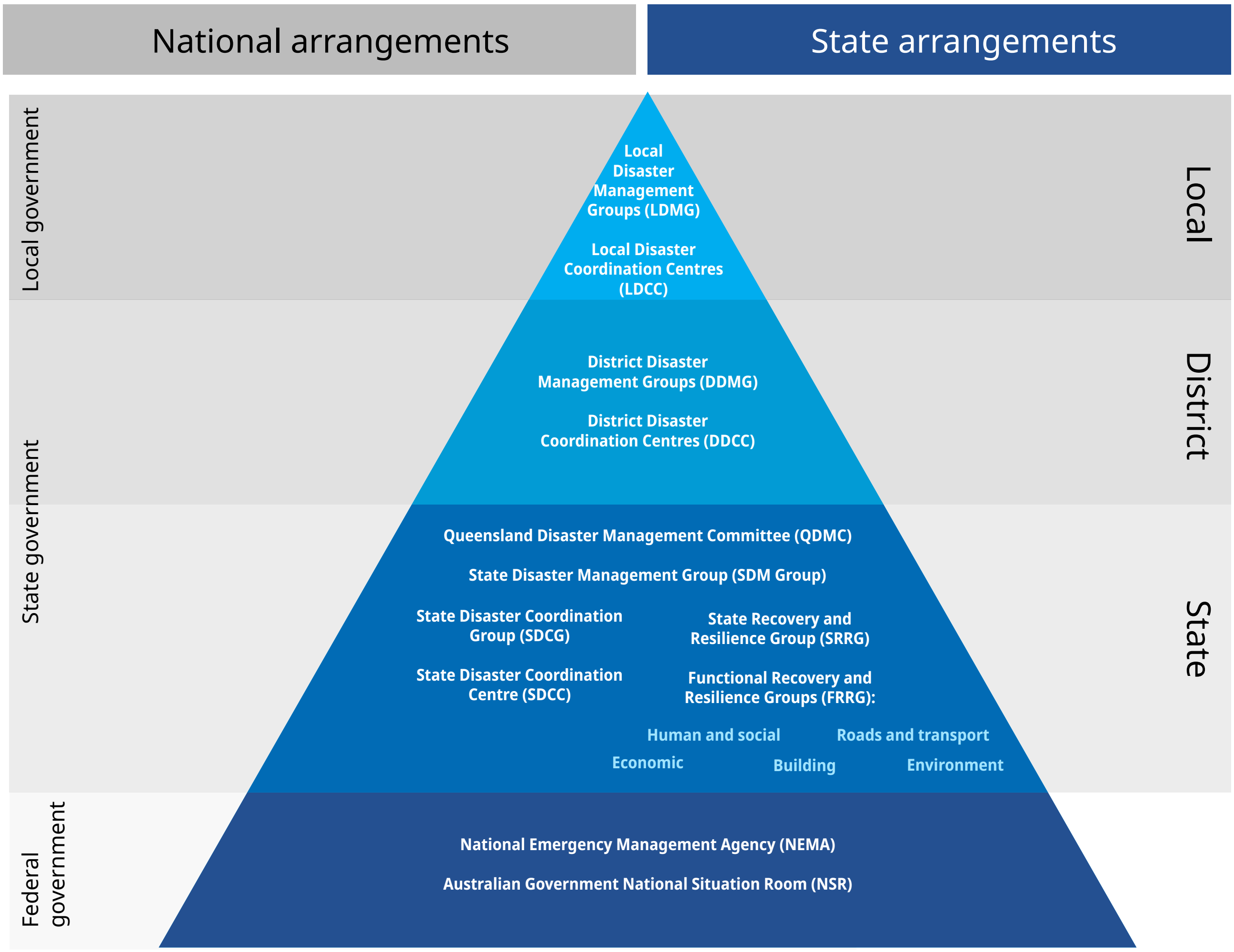

National arrangements
State arrangements
Local government
State government
Federal government
Local
District
State
Local Disaster Management Groups (LDMG)
Local Disaster Coordination Centres (LDCC)
District Disaster Management Groups (DDMG)
District Disaster Coordination Centres (DDCC)
Queensland Disaster Management Committee (QDMC)
State Disaster Management Group (SDM Group)
State Disaster Coordination Group (SDCG)
State Recovery and Resilience Group (SRRG)
State Disaster Coordination Centre (SDCC)
Functional Recovery and Resilience Groups (FRRG):
Human and social
Roads and transport
Economic
Building
Environment
National Emergency Management Agency (NEMA)
Australian Government National Situation Room (NSR)

Figure 1: QDMA Overview

The QDMA focus on the consequence management of a cyber incident, whereas this hazard plan focuses on the management of a cyber incident. Both may be activated at the same time in response to a cyber incident, working towards the one goal of responding to the incident by addressing both the cyber security and disaster management aspects.

Assistance required through the QDMA will be identified by CSDB as the lead agency requested (outside of an existing QDMA activation) or will be raised by CDSB via the State Disaster Coordination Group (SDCG) (when the QDMA are already activated) who will then coordinate with the relevant entities.

Decision making in a crisis

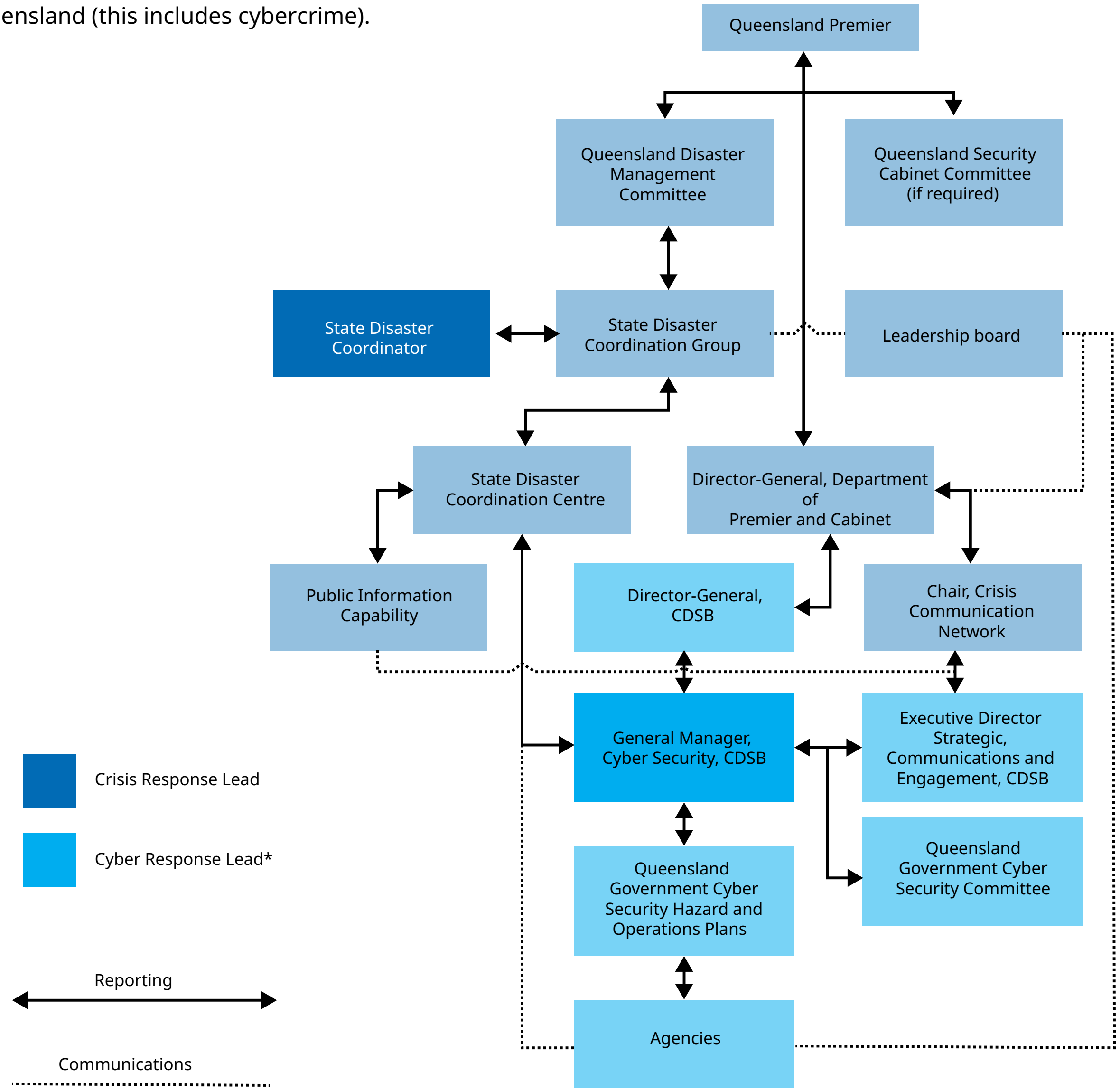
Strategic decision making and policy for cyber security at the Cabinet and Ministerial level may fall within the scope of either the Queensland Disaster Management Committee (QDMC) or the Queensland Security Cabinet Committee (QSCC).

The QDMC is the primary forum for coordinated whole-of-government consequence management and leadership. It provides strategic leadership and decision making, coordinates State and Commonwealth assistance, and identifies resources to support disaster management and disaster operations. If this plan is escalated to a Level 1 or Level 2 incident, the State Disaster Coordination Group, may be activated by the QDMC or QSCC.

The QSCC is responsible for senior strategic leadership on security and counter-terrorism preparedness arrangements and managing significant security or terrorist incidents in Queensland (this includes cybercrime).

The Committee stays across the security environment internationally, nationally and within Queensland. In the case that a cyber incident is determined to be a security incident motivated by terrorism, major crime action, or a geo-political security threat, the QSCC may be convened to provide guidance, including deciding community leadership messaging and strategic direction on managing the relationship with the Australian Government and other state and territory governments.

A situation may occur where both bodies are required to manage a cyber security incident. In this situation the QSCC will oversee the security threat response, while the QDMC will coordinate consequence management and recovery.


Queensland Premier
Queensland Disaster Management Committee
Queensland Security Cabinet Committee (if required)
State Disaster Coordinator
State Disaster Coordination Group
Leadership board
State Disaster Coordination Centre
Director-General, Department of Premier and Cabinet
Public Information Capability
Director-General, CDSB
Chair, Crisis Communication Network
General Manager, Cyber Security, CDSB
Executive Director Strategic, Communications and Engagement, CDSB
Queensland Government Cyber Security Hazard and Operations Plans
Queensland Government Cyber Security Committee
Agencies
Crisis Response Lead
Cyber Response Lead*
Reporting
Communications

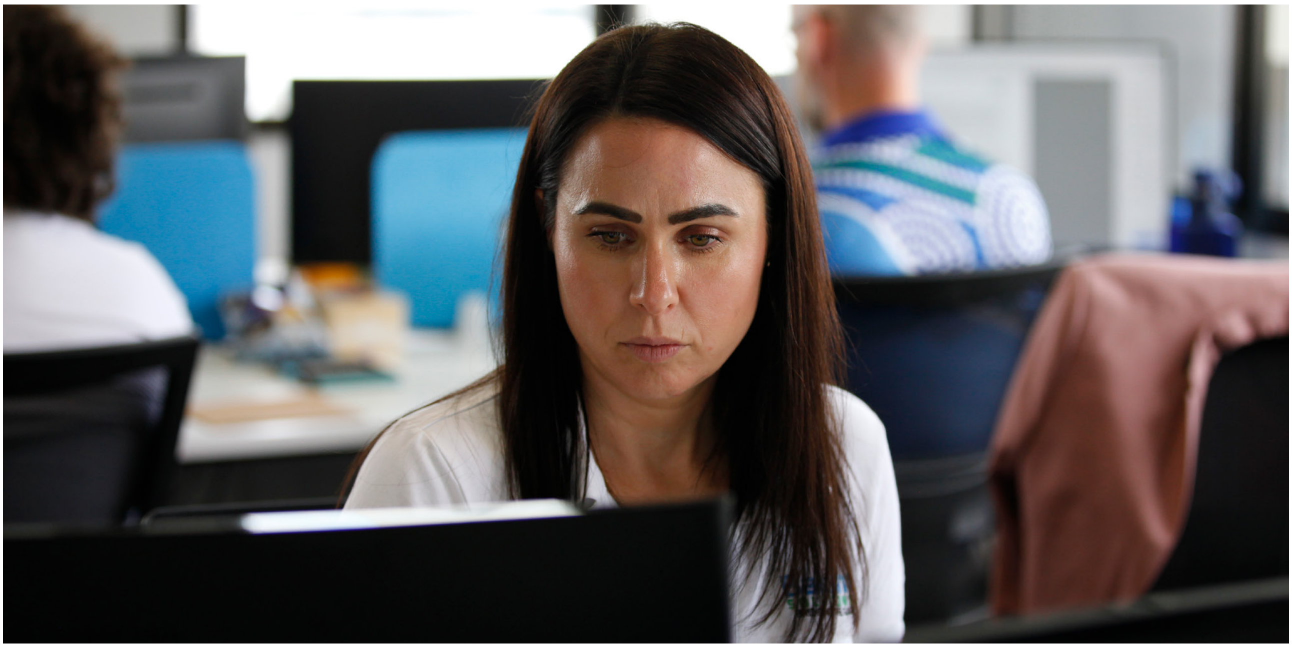
*In some instances the QPS may be required to assume the lead role during a crisis, as discussed and agreed by decision makers. At this time, CDSB will transition to a co-lead or support role, focusing on the recovery of impacted information assets and providing technical advice.

Figure 2: State cyber incident control structure

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 security incident (consequence management).
Queensland Security Cabinet Committee (QSCC)	• Chaired by the Premier of Queensland; core membership comprised of the Premier, Deputy Premier, Attorney-General and Minister for Police. • 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, 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 Deputy Director-General, Strategic Communication, 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.
General Manager Cyber Security (GMCS)	• 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 any 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 GMCS. • Comprised of Chief Information Officers, Chief Information Security Officers (or equivalent) and Agency Security Executives from Queensland Government agencies. • May also include the investigations arm of the 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.

Table 1: Roles and responsibilities of key governance groups

Queensland Government Cyber Security Committee

Overview	
Formation	Established by the GMCS under the Queensland Government Cyber Security Hazard Plan.
Area of responsibility	State of Queensland.
Members	• Chaired by the GMCS. • Membership consists of representatives from each Queensland Government agency: – Primary member is Agency Security Executive. – Secondary member is the agency Chief Information Officer, Chief Information Security 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 need's 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 this hazard plan. – Aggregate information and facilitate briefing and awareness. – Consult with and share expertise and resources among Queensland Government agencies – Develop and share key messages. • Assists CDSB 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 Queensland Government Cyber Security Committee (QGCSC) (e.g., convene 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 plans could be improved. • Annually reviews operational procedures under the plans.
Communications	• The QGCSC may be convened by the GMCS to identify strategic priorities and provide direction or guidance during a cyber incident. • Through the GMCS 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. CDSB will exercise the Plan, accompanying Operations Plan, and general preparedness at least annually, and strongly encourage all entities to test their cyber security arrangements on a regular basis.

CDSB offers an exercise program to Queensland Government agencies, including templates and resources, specialised training and support to exercise planning, facilitation and evaluation.

The exercise program includes:

- an Exercising Community of Practice (CoP) for government staff to learn, share insights and create a support network for cyber security exercising
- an Exercise Toolkit and Scenario Library to support agencies to independently conduct exercises
- an Exercise Practitioner Program so organisations can independently design, deliver and evaluate cyber security exercises using the Toolkit and Scenario Library
- an Exercise On-Demand service to design and deliver cyber exercises that meet their unique needs
- whole-of-government exercises to provide an opportunity for exercising complex incidents that may impact multiple agencies, or agency exercising at scale.

Lessons management

These activities are supported by a lessons management framework to continuously improve planning, processes and activities, future service delivery, 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, CDSB captures and analyses observations to ensure that implemented changes for cyber security arrangements are:

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

Intelligence and capability integration

ASD's ACSC maintains national daily cyber information and intelligence monitoring to identify potential threats to Australia. The Queensland Government is an active member of the ASD's ACSC Partnership Program. This membership helps improve cyber resilience through sharing threat intelligence, insights, and working together on protective measures.

Capability integration and resources

The Queensland Government has additional cyber information and intelligence monitoring capabilities to identify potential threats in the Queensland context:

- CDSB provide Security Operations Centre, assurance and cyber threat intelligence services on a year-round, 24/7 basis.
- An incident response tender allows for CDSB to help smaller agencies without dedicated cyber incident response arrangements to access expert support.

Detection

CDSB facilitates and supports cyber information and intelligence monitoring capabilities to identify potential threats to Queensland Government entities. CDSB shares information with the ASD's ACSC and other states and territories.

The Queensland Government has various capabilities to produce and share cyber threat intelligence to help detect incidents early. All stakeholders must report cyber incidents promptly, as early notification allows for quicker containment and mitigation to prevent serious, costly disruptions.

Queensland Government agency notification

In accordance with the *Information and Cyber Security Policy* (IS18) and the Information Security Incident Reporting Standard, Queensland Government agencies who have committed to implementing IS18 are required to report:

- immediately for information security incidents affecting information / a system with an assessed business impact level (BIL) of medium or high
- immediately for information security incidents affecting multiple systems / agencies
- within five days for information security incidents affecting information / a system with an assessed BIL of low or none.

Reports are to be made to CDSB using the Information Security Incident Reporting Portal. Reporting agencies can also email a manual incident report form to CyberDefenceCentre@cyber.qld.gov.au or calling on 07 3215 3951. Agencies should also brief all required internal parties for any incident with an immediate reporting requirement.

Industry notification

All organisations (including private businesses and Queensland Government entities not utilising IS18) should report all cyber incidents and emergencies to the ASD's ACSC on 1300 CYBER1 (1300 292 371) (24/7). CDSB and the relevant Queensland Government portfolio department should also be notified.

Notification requirements for critical infrastructure

In addition to the above, owners and operators of critical infrastructure captured by the *Security of Critical Infrastructure Act 2018 (Cth)* (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

Queensland Government agencies are responsible for maintaining daily cyber information and intelligence monitoring capabilities to identify, respond to and escalate potential system threats. If a cyber incident occurs, CDSB or their retained response partners can offer technical support and advice to the affected agency.

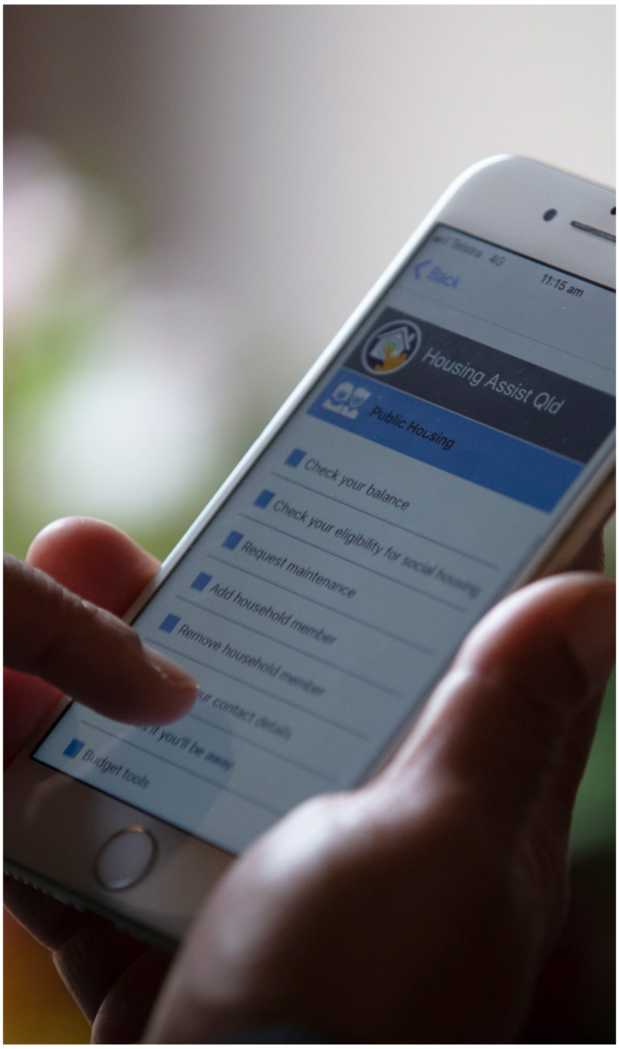
When multiple agencies are affected, CDSB will engage with agencies to provide prioritised technical support. CDSB can also provide support and guidance to coordinate consequence management, reporting, and internal and external communication activities.

Private industry support

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

Mandatory notification of data breach

The Office of the Information Commissioner (OIC) is an independent statutory body that assists Queensland Government agencies to fulfill their obligations under the *Information Privacy Act 2009*. OIC is also responsible for managing the Mandatory Notification of Data Breach Scheme. When an entity that is covered by the Act suffers a data breach that is likely to result in serious harm, they are required to notify the OIC. An entity may take up to 30 days to assess if the breach is a notifiable data breach.



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 are given immediate relief and support.

The Queensland Government and its agencies are responsible for responding 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 or actual cyber incident (through agency, organisation or ASD's ACSC reporting), the GMCS, CDSB, and QPS will work with agencies to assess the incident's severity using this Cyber Security Hazard Plan and underlying Operations Plan. This helps ensure appropriate notifications, and that resources are allocated or support provided with a view to reducing or eliminating the impacts of any cyber security incident.

If an incident affects multiple Queensland Government agencies, critical infrastructure, or involves a large-scale data breach, CDSB may step in to support the response or assume control as the lead agency.

If CDSB is required to assume the lead agency role, the GMCS will be responsible for coordinating the response, manage information sharing, and work with stakeholders and other responding agencies.

If WoQG information sharing, response and/or resource coordination is needed for a cyber threat or incident, the GMCS may convene the QGCSC, fully or partially. This forum helps with briefings, coordination, and decision-making to manage the situation effectively.

Where required, the GMCS will quickly inform agencies managing an incident to ensure timely support. If a state cyber incident or crisis happens or is likely, the GMCS will notify the Director-General, CDSB, who will then inform the Director-General, DPC, including details on the incident's severity and the response so far.

Levels of cyber incidents

In Queensland, cyber incidents are classified into five levels based on escalating severity. The level is determined by the threat and risk characteristics, which helps indicate the response and coordination needed to manage the incident. These levels (outlined in Table 3) align with the Australian Government's CIMA, the QSDMP, and the AGCMF. They can be used alongside the ASD's ACSC cyber incident categorisation matrix, which is publically available.

Plan level	Authority to declare	Characteristics that inform key activities (not exhaustive)	QDMA level	AGCMF tier
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	N/A
4	GMCS	**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	GMCS	**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		May reach Tier 1
2	DG DPC and DG CDSB*	**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 Queensland Government data breach that requires a coordinated response. Immediate inter-agency response, QDMC may activate for preparedness	Lean Forward	Tier 1 or Higher
1	Leadership Board or DG DPC / DG CDSB* 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: Hazard Plan levels and alignment

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

Crisis escalation

If the GMCS assesses a notification as likely to meet the threshold of a state cyber incident (Hazard Plan Level 2) or crisis (Hazard Plan Level 1), they will work with the Director-General, CDSB to brief the Director-General, DPC, who will decide which strategic crisis management arrangements to activate.

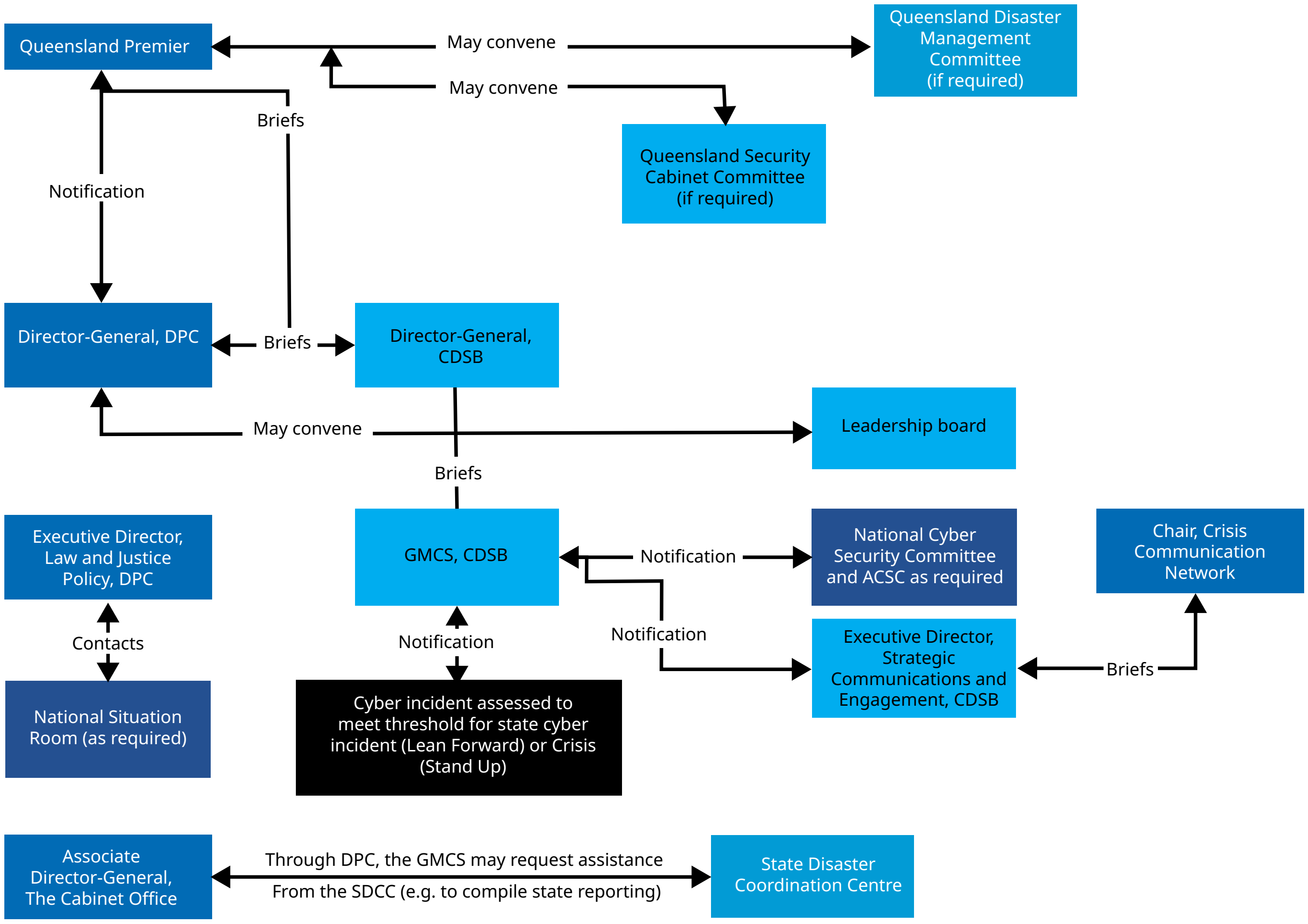
At the same time, the GMCS will work with the CDSB Strategic Communication and Engagement team and link in with the Chair of the CCN.

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

- The QDMC may manage cyber incidents with significant impacts.
- The QSCC may provide strategic decision making and guidance during significant security incidents (whether confined, serious, or significant).

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.

As part of operational notification activity, the SDCC and State Policing Operations Centre will also be informed of any changes to the posture of the Queensland Government Cyber Security Hazard Plan.


Queensland Premier
May convene
Queensland Disaster Management Committee (if required)
May convene
Briefs
Queensland Security Cabinet Committee (if required)
Notification
Director-General, DPC
Briefs
Director-General, CDSB
May convene
Leadership board
Briefs
Executive Director, Law and Justice Policy, DPC
GMCS, CDSB
Notification
National Cyber Security Committee and ACSC as required
Chair, Crisis Communication Network
Contacts
Notification
Notification
Executive Director, Strategic Communications and Engagement, CDSB
Briefs
National Situation Room (as required)
Cyber incident assessed to meet threshold for state cyber incident (Lean Forward) or Crisis (Stand Up)
Associate Director-General, The Cabinet Office
Through DPC, the GMCS may request assistance
From the SDCC (e.g. to compile state reporting)
State Disaster Coordination Centre

■ National Arrangements

■ Department of Premier and Cabinet

■ Disaster Management Arrangements

■ Cyber Security Arrangements

Figure 3: Escalation pathway for a state cyber incident or crisis

De-escalation

If declared, the Director-General, DPC, with advice from the GMCS, Director-General, CDSB, and affected agencies and stakeholders, will authorise the de-escalation of a state cyber incident.

For a state cyber crisis, the QDMC and/or QSCC, acting on advice from GMCS, affected agencies and stakeholders will authorise de-escalation and recovery.

De-escalation from Hazard Plan Levels 4 and 3 will be authorised by the GMCS.

Event coordination

Cyber incidents 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, CDSB (as led by the GMCS 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 agencies to prioritise response roles according to the QSDMP and agreed management priorities.

Activation of the State Policing Operations Centre occurs under a separate concept of operations.

Situation reporting

The nature and severity of a cyber incident will influence how information is shared. This 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 regularly shared through these channels.

The GMCS 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 and focuses on providing situational awareness and identifying current or emerging issues and actions to resolve the same. They 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 during a state cyber incident or crisis, the GMCS will work with DPC and/or QPS to request help from the SDCC and/or SPOC in preparing a State Update and Executive Summary using the Emergency Management System. CDSB also provides adaptable situation reporting templates to agencies, which can include technical advice if needed.

National arrangements

The Australian Government leads national coordination for cyber security incidents on a large or multi-jurisdictional scale that require a coordinated inter-jurisdictional response or have national or international consequencesaffecting multiple areas or with national or international impacts. National efforts support, but do not replace, cyber incident management arrangements in each Australian state or territory.

Australian Cyber Response Plan

The AUSCYBERPLAN outlines the Australian Government's response coordination arrangements to cyber incidents. It provides an overview of the Australian Government's response coordination arrangements, describes activities covered by those arrangements and identifies the departments and agencies.

AUSCYBERPLAN is the national plan for cyber incident hazards categorised as crises under the AGCMF. The AGCMF defines cyber incidents and designates the Minister for Cyber Security as the Lead Minister, with the National Cyber Security Coordinator (the Coordinator) and the NOCS in the DOHA as the Lead Coordinating Senior Official and the Australian Government Coordinating Agency respectively for coordinating responses to cyber incidents.

AUSCYBERPLAN is also complementary to the *2023-2030 Australian Cyber Security Strategy* and the CIMA.

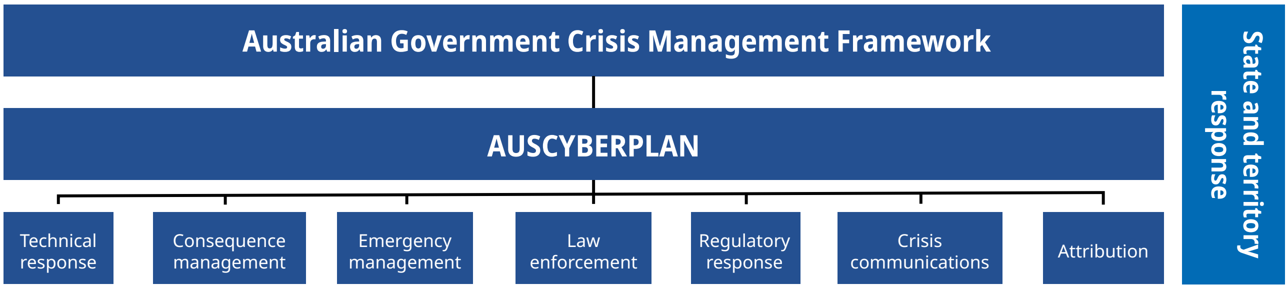


Figure 4: AUSCYBERPLAN integration overview

Cyber incident management arrangements

The CIMA is the national technical response arrangement. It provides Australian and state and territory governments with guidance on how to collaborate technical activities in response to, and reduce the harm associated with, national cyber security incidents. The CIMA is not an operational incident management protocol. It outlines the inter-jurisdictional coordination arrangements, roles and responsibilities, and principles for the Australian Government's cooperation with states and territories in technical response to national cyber security incidents.

The CIMA is endorsed by the First Secretaries Committee and implemented by the NCSC. Queensland is represented at the NCSC by the GMCS, alongside other state and territory cyber security leads, the ASD's ACSC, NOCS, DOHA, NEMA, and AFP.

NCSC members assess and report cyber security incidents considering the scope, impact and severity of an incident and its potential to harm Australia or relevant jurisdictions. If an incident meets thresholds, the NCSC Co-Chairs may declare a national cyber security incident or crisis in consultation with members.

In a national cyber security incident or crisis, the CIMA will support state, territory and national crisis management as outlined by the AGCMF.

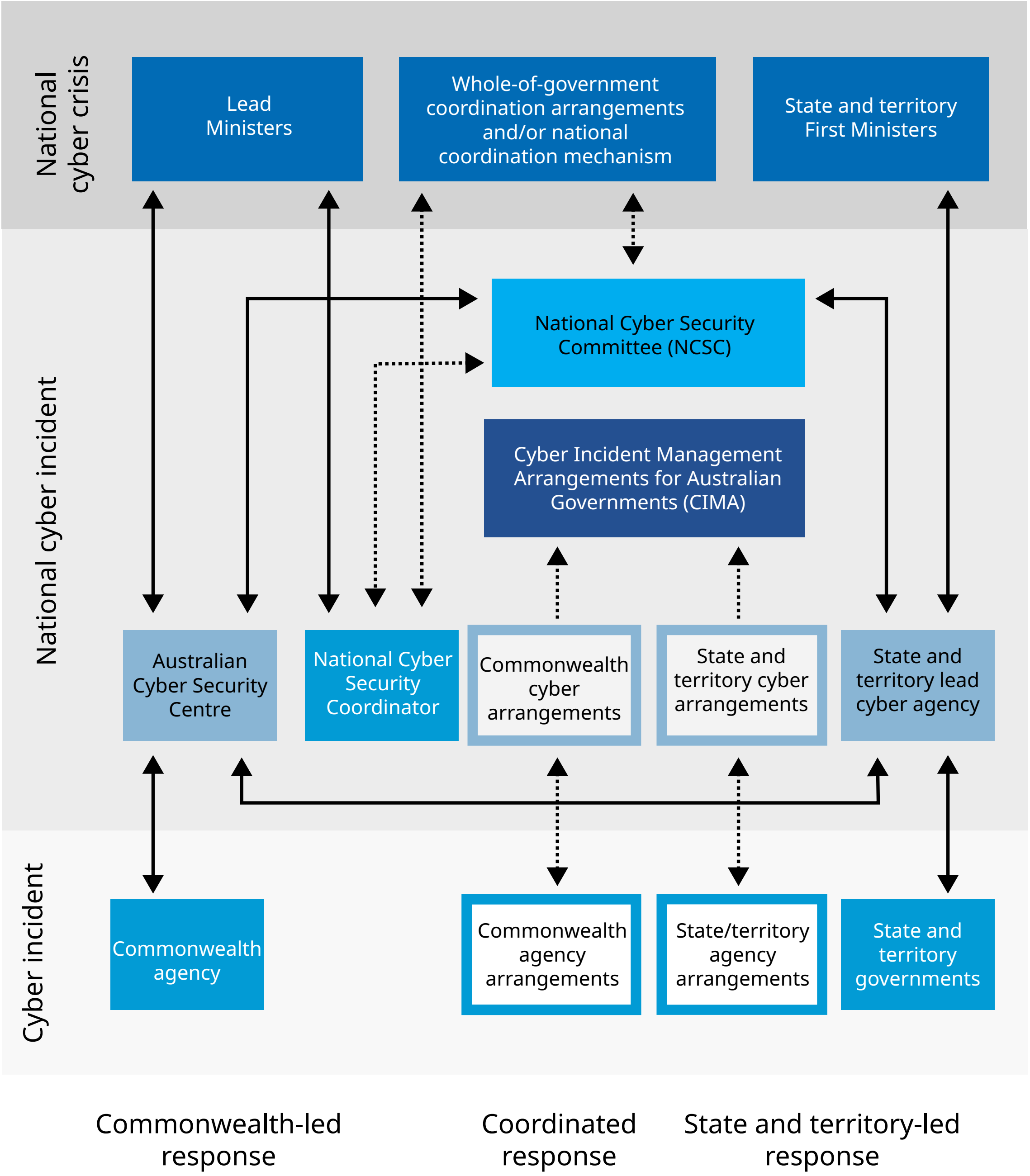

National cyber crisis
Lead Ministers
Whole-of-government coordination arrangements and/or national coordination mechanism
State and territory First Ministers
National cyber incident
National Cyber Security Committee (NCSC)
Cyber Incident Management Arrangements for Australian Governments (CIMA)
Australian Cyber Security Centre
National Cyber Security Coordinator
Commonwealth cyber arrangements
State and territory cyber arrangements
State and territory lead cyber agency
Cyber incident
Commonwealth agency
Commonwealth agency arrangements
State/territory agency arrangements
State and territory governments
Commonwealth-led response
Coordinated response
State and territory-led response

Figure 5: CIMA integration overview

The GMCS, working with agencies, will decide if extra Australian Government or inter-jurisdictional support is needed and communicate this in partnership with agencies (utilising existing relationships where appropriate). Where necessary, requests may also be coordinated by the SDCG and/or DPC.

National cyber incidents and crises

If a national cyber incident or crisis is agreed and declared, the NCSC will activate to coordinate the national response.

Queensland (via the GMCS in CDSB) will manage the response within the state, brief Ministers and officials using key messages from the NOCS or NEMA, and provide updates on Queensland's actions. Media and public queries may be referred by Queensland to the appropriate federal agency for response.

The Australian Government uses a four-tiered approach to guide and support appropriate and consistent levels of coordination in response to crises. The tiers of crisis coordination are shown on Figure 6, and refer to the scale of Australian Government coordination required rather than the scope and impact of the incident.

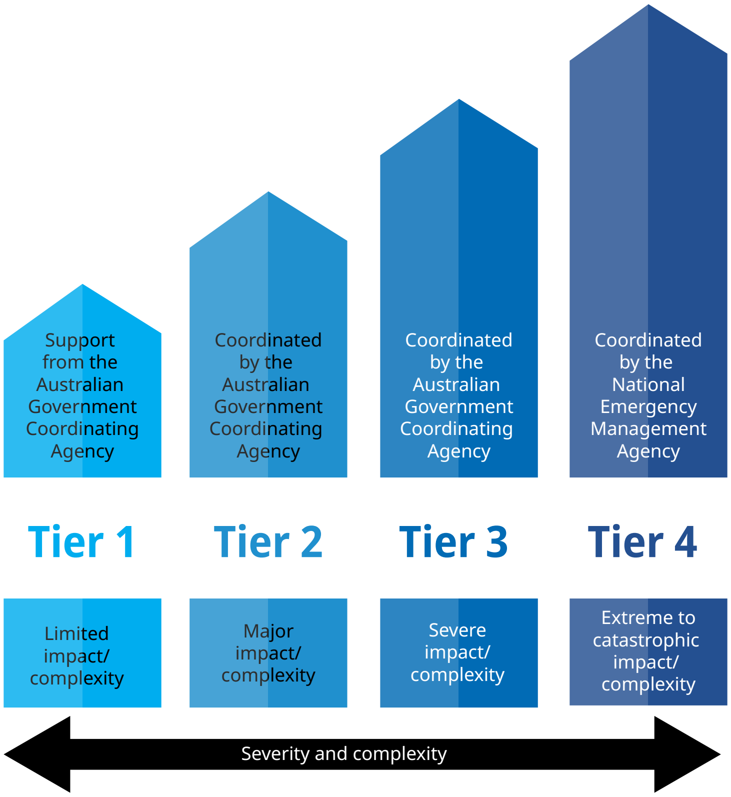

Support from the Australian Government Coordinating Agency
Coordinated by the Australian Government Coordinating Agency
Coordinated by the Australian Government Coordinating Agency
Coordinated by the National Emergency Management Agency
Tier 1
Tier 2
Tier 3
Tier 4
Limited impact/ complexity
Major impact/ complexity
Severe impact/ complexity
Extreme to catastrophic impact/ complexity
Severity and complexity

Figure 6: The Australian Government's 4-tier crisis coordination model

Under the AGCMF, the National Coordination Mechanism (NCM) within the NEMA operates through the DOHA. If required, the NCM will be utilised to work with jurisdictions and non-government organisations to coordinate the whole-of-government response to address specific impacts of a national cyber crisis.

Whether the NCM is activated depends on scale, nature and duration. The NCM may make a recommendation for consideration by the Prime Minister and First Minister of the directly affected jurisdiction(s).

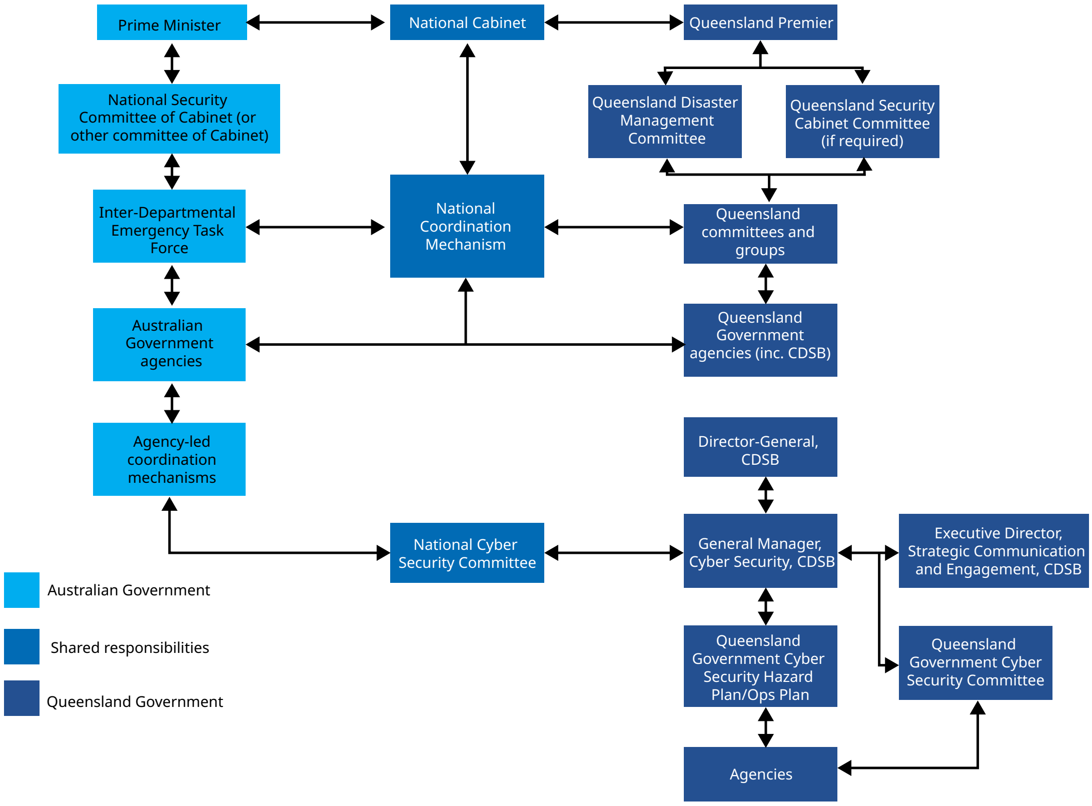
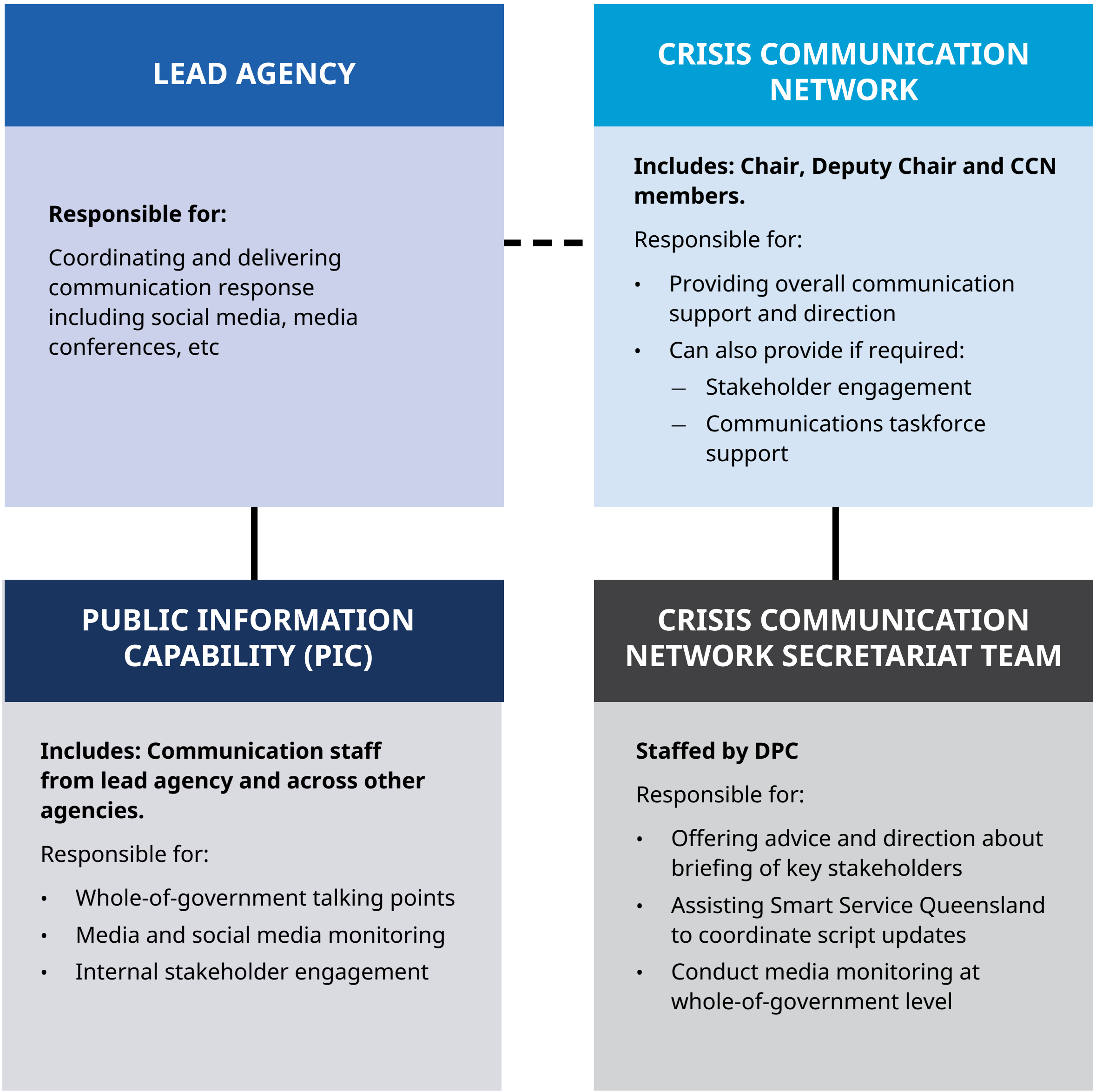

Prime Minister
National Cabinet
Queensland Premier
National Security Committee of Cabinet (or other committee of Cabinet)
Queensland Disaster Management Committee
Queensland Security Cabinet Committee (if required)
Inter-Departmental Emergency Task Force
National Coordination Mechanism
Queensland committees and groups
Australian Government agencies
Queensland Government agencies (inc. CDSB)
Agency-led coordination mechanisms
Director-General, CDSB
National Cyber Security Committee
General Manager, Cyber Security, CDSB
Executive Director, Strategic Communication and Engagement, CDSB
Queensland Government Cyber Security Hazard Plan/Ops Plan
Queensland Government Cyber Security Committee
Agencies
Australian Government
Shared responsibilities
Queensland Government

Figure 7: National and state crisis response integration (cyber incident)

Media and communications

In the event of a state cyber security incident or crisis, public information will be managed in accordance with the Queensland Government's crisis communication plan. This Plan outlines the government's response to issues or crises that heavily affect Queensland, a large part of its population, or the government's reputation.



LEAD AGENCY

Responsible for:

Coordinating and delivering communication response including social media, media conferences, etc

CRISIS COMMUNICATION NETWORK

Includes: Chair, Deputy Chair and CCN members.

Responsible for:

- Providing overall communication support and direction
- Can also provide if required:
  - Stakeholder engagement
  - Communications taskforce support

PUBLIC INFORMATION CAPABILITY (PIC)

Includes: Communication staff from lead agency and across other agencies.

Responsible for:

- Whole-of-government talking points
- Media and social media monitoring
- Internal stakeholder engagement

CRISIS COMMUNICATION NETWORK SECRETARIAT TEAM

Staffed by DPC

Responsible for:

- Offering advice and direction about briefing of key stakeholders
- Assisting Smart Service Queensland to coordinate script updates
- Conduct media monitoring at whole-of-government level

Figure 8: 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 theft months from the initial detection of a breach, financial losses and reputational damage.

If not led by CDSB (pending the nature of consequences to be managed and recovery needs), recovery in the aftermath of a declared cyber crisis in Queensland may fall under 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 any declared 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 incident (whether a declared cyber crisis or otherwise), those affected manage their own recovery and consequences. They also work with CDSB, QRA or FRG recovery operations as required to ensure a coordinated approach.

During, or after a cyber crisis, CDSB may work with the QRA and other Queensland Government agencies to identify and/or advise 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

Following any escalation of the Plan, CDSB will coordinate a formal post incident review. This will follow the lessons management framework using feedback from all involved parties to drive evidence-based continuous improvement to Queensland’s cyber planning. Incident review reports 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.
	Commonwealth Criminal Code Act 1995 • The Act codifies the general principles of criminal responsibility under laws of the Commonwealth.
Critical infrastructure	*Security of Critical Infrastructure Act 2018* • The Act seeks to better manage risk and complex and evolving national security risks of sabotage, espionage, and coercion posed by foreign involvement in Australian critical infrastructure (e.g., cyber security).
Information	*Privacy Act 1988* The main objectives of this Act include: • promoting protection of privacy of individuals • balancing protecting privacy with interests of entities carrying out functions or activities • providing a base of nationally consistent regulation of privacy and handling of personal information • facilitating efficient credit reporting that respects privacy • facilitating free flow of information while respecting privacy • implementing Australia's international obligation in relation to privacy.
	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.
	Intelligence Services Act 2001 • The Act establishes the legal foundation of the ASD as Australia's Signal Intelligence service. • Outlines a 'limited use' obligation that restricts how cyber security information voluntarily provided to ASD can be used and disclosed.
	Cyber Security Act 2024 The Act addressed legislative gaps to bring Australia in line with international best practice. Key measures of this Act include: • mandated minimum cyber security standards for smart devices • mandatory ransomware and cyber extortion reporting obligations for certain businesses to report ransom payments • the introduction of a 'limited use' obligation to encourage industry engagement with government following cyber incidents • establishing a Cyber Incident Review Board.

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 objective of this Act is to provide 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. *Police Powers and Responsibilities Act 2000* The main objects of this Act include: • consolidating and rationalising powers and responsibilities police officers have for investigating offences and enforcing the law • providing powers necessary for effective modern policing and law enforcement • providing consistency in the nature and extent of police powers/responsibilities • standardising the way powers/responsibilities are exercise • ensuring 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.

Queensland Legislation	
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 • the 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 • introducing a Mandatory Notification of Data Breach Scheme applicable to all Queensland Government agencies from 1 July 2025. This scheme applies to local government from 1 July 2026.
	Public Records Act 2002 The main objects of this Act include: • ensuring the public records of Queensland are made, managed, kept, and if appropriate preserved 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*.
	Right to Information Act 2009 The main objectives of this Act include: • providing individuals with the legal right to access information held by Queensland Government agencies • outlining the principles of transparency, how to access information and seek to balance security with privacy.
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.
	Fire Services Act 1990 • The main objectives of this Act include providing for the prevention of, and responses to, fires and other emergency incidents.
	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 the conduct of risk assessments, development of security plans, and implementation and review of 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* • National technical response and cooperation arrangements.
Information security	*Notifiable Data Breaches Scheme* • Under the *Notifiable Data Breaches Scheme* any organisation or agency the *Privacy Act 1988* (Cth) covers must notify affected individuals and the Office of the Australian Information Commissioner 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* • The framework assists Australian Government entities to protect their people, information and assets, both at home and overseas.
Disaster management	*Australian Government Crisis Management Framework* and associated response plans and resilience policy. • The framework underpins other crisis plans.
	Australian Cyber Response Plan • The plan outlines the Australian Government's cyber incident response coordination arrangements to cyber incidents.

State non-legislative policy drivers and planning	
Cyber security	Cyber Security Operations Plan • The plan supports the governance arrangements as outlined in this plan and describes the response actions and incident management responsibilities for cyber security incidents at all levels, including a cyber security crisis. Cyber Security Communications Plan • The communications plan includes plans for internal and external communications during an incident. This enables the Queensland Government to convey accurate and timely messages to desired audiences during an incident.
Information security	*Information and Cyber Security Policy* (IS18) • The policy seeks to ensure all agencies apply a consistent, risk-based approach, to the implementation of information security to maintain confidentially, integrity and availability.
Protective security	*Queensland Protective Security Framework* • Currently in pilot implementation, the framework assists Queensland Government entities to protect their people, information and assets.
Disaster management	*Interim Queensland State Disaster Management Plan 2024-2025* • The plan 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 Recovery Plan • The plan 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.
	CDSB Disaster Management Framework • The framework relates to strategic and operational disaster management planning necessary for CDSB to fulfil roles and responsibilities defined in the QSDMP and other legislation/policy.

Appendix 2 – Glossary

Abbreviation	Name
AFP	Australian Federal Police
AGCMF	Australian Government Crisis Management Framework
ASD’s ACSC	Australian Signals Directorate’s Australian Cyber Security Centre
ASIO	Australian Security Intelligence Agency
AUSCYBERPLAN	Australian Cyber Response Plan
CCN	Crisis Communication Network
CDSB	Department of Customer Services, Open Data and Small and Family Business
CI	Critical Infrastructure
CIMA	Cyber Incident Management Arrangements for Australian Governments
CoP	Community of Practice
DG	Director-General
DOHA	Department of Home Affairs
DPC	Department of the Premier and Cabinet
EMS	Emergency Management System
FRG	Functional Recovery Group
GMCS	General Manager, Cyber Security (CDSB)
ICT	Information and Communications Technology
IoT	Internet of Things
IS18	Information and Cyber Security Policy (IS18:2018)
JCSC	Joint Cyber Security Centre
JPC3	Joint Policing Cybercrime Coordination Centre
NCM	National Coordination Mechanism
NCSC	National Cyber Security Committee
NEMA	National Emergency Management Agency
NOCS	National Office of Cyber Security
OAIC	Office of the Australian Information Commissioner
OIC	Office of the Information Commissioner (Queensland)
OT	Operational Technology
PIC	Public Information Capability
QDMA	Queensland Disaster Management Arrangements
QDMC	Queensland Disaster Management Committee
QGCSC	Queensland Government Cyber Security Committee
QPS	Queensland Police Service
QPSF	Queensland Protective Security Framework
QRA	Queensland Reconstruction Authority
QSCC	Queensland Security Cabinet Committee
QSDMP	Queensland State Disaster Management Plan

Abbreviation	Name
SDC	State Disaster Coordinator
SDCC	State Disaster Coordination Centre
SDCG	State Disaster Coordination Group
SOCI	Security of Critical Infrastructure Act 2018 (Cth)
SPOC	State Policing Operations Centre
TISN	Trusted Information Sharing Network
WoQG	Whole of Queensland Government