PERFORMANCE AUDIT REPORT 4 June 2024

Responding to and recovering from cyber attacks

Report 12: 2023–24

Queensland Audit Office
Better public services

As the independent auditor of the Queensland public sector, including local governments, the Queensland Audit Office:

- provides professional audit services, which include our audit opinions on the accuracy and reliability of the financial statements of public sector entities
- provides entities with insights on their financial performance, risk, and internal controls; and on the efficiency, effectiveness, and economy of public service delivery
- produces reports to parliament on the results of our audit work, our insights and advice, and recommendations for improvement
- supports our reports with graphics, tables, and other visualisations, which connect our insights to regions and communities
- conducts investigations into claims of financial waste and mismanagement raised by elected members, state and local government employees, and the public
- shares wider learnings and best practice from our work with state and local government entities, our professional networks, industry, and peers.

We conduct all our audits and reports to parliament under the *Auditor-General Act 2009* (the Act). Our work complies with the *Auditor-General Auditing Standards* and the Australian standards relevant to assurance engagements.

- Financial audit reports summarise the results of our audits of over 400 state and local government entities.
- Performance audit reports cover our evaluation of some, or all, of the entities' efficiency, effectiveness, and economy in providing public services.

Learn more about our publications on our website at www.qao.qld.gov.au/reports-resources/fact-sheets.

The Honourable C Pitt MP
Speaker of the Legislative Assembly
Parliament House
BRISBANE QLD 4000

4 June 2024

This report is prepared under Part 3 Division 3 of the *Auditor-General Act 2009*.

Brendan Worrall
Auditor-General

ISSN 1834-1128

Contents

Report on a page **1**

1. Audit conclusions **2**

2. Recommendations **3**

3. Managing cyber incidents **6**

4. The role of public sector entities in managing cyber incidents **11**

5. The role of expert and lead entities in managing cyber incidents **21**

Appendices **30**

A. Entity responses 31

B. Audit scope and methods 36

C. Better practice frameworks 38

D. Other legislative requirements 39

E. Cyber response and recovery governance checklist 41

F. Role capability checklist 43

G. Glossary 46

Acknowledgement

The Queensland Audit Office acknowledges the Traditional and Cultural Custodians of the lands, waters, and seas across Queensland. We pay our respects to Elders past, present, and emerging.

Report on a page

Cyber incidents are unwanted or unexpected events that could compromise computer and information systems and business operations. They can cause significant disruption and are happening more often, according to the Australian Cyber Security Centre (ACSC). Across Australia, nearly 94,000 cyber crime reports were made to the ACSC in 2022–23 – a 23 per cent increase in one year. Queensland accounted for 30 per cent of these reports, which is disproportionate to its population size, and one in 8 reports nationally related to state or local government entities. Cyber risks are continuing to evolve, and new technologies such as artificial intelligence increase the risk.

In this report we discuss how prepared Queensland public sector entities, including local governments, are to deal with cyber security incidents. We examined 2 lead agencies with responsibility for guiding cyber security, and we audited 3 other entities with varying levels of resources and capability. We have not named them, to avoid publicly identifying any security vulnerabilities.

The current picture

Since we produced *Managing cyber security risks* (Report 3: 2019–20), the Queensland public sector has invested in building its cyber resilience. The Cyber Security Unit (CSU – Department of Transport and Main Roads) has worked with entities to improve their information security management systems (their policies and procedures for managing sensitive data). The government has made additional investments to provide support, share cyber intelligence, and assist government owned corporations and local governments.

Despite this, public sector entities are not as prepared as they have to be. Just having plans is not enough. They need to test their plans and readiness. They need to identify and address any skills gaps they have for dealing with cyber incidents. Also, some entities do not yet know about the services CSU provides, and CSU does not know which entities most need its help and expertise.

What entities need to do

The entities we audited had plans for managing cyber incidents, but all had room to improve. Their plans were not always well integrated with their risk management strategies, did not incorporate cyber insurance requirements, and were not designed to respond to a wide range of threats. One entity had struggled to integrate its plans due to consistent machinery of government changes (restructures of government functions). Some entities also needed to be clearer on roles and responsibilities and on how to escalate their responses to cyber incidents. Only one entity had tested its incident response plan, and all entities needed to do more to ensure they can effectively communicate in a cyber crisis. Some entities did not have an up-to-date and complete understanding of their critical systems and information assets – an essential starting point for cyber security.

Entities relied heavily on third parties or other government entities when dealing with responses to cyber incidents, and were not always clear on accountability requirements. None had tested how these third parties would perform in a crisis. This means they could not be confident the third parties would be available or have the expertise to deal with a real incident in an effective and timely manner.

What expert and lead agencies need to do

CSU needs to continue working with entities to improve their information security management systems. It also needs to help entities to assess their individual needs, which would assist it in deciding where to focus its support and training. CSU should also start helping entities test their incident response processes. Again, this will benefit CSU, because it will familiarise its external experts with public sector requirements.

The Department of Housing, Local Government, Planning and Public Works needs to ensure councils are aware of the cyber-related skills available through CSU and encourage them to use them.

1. Audit conclusions

The public sector entities we audited were not as prepared as they need to be. All had response and recovery plans in place, but they were not as effective or complete as they need to be to deal with the complications and risks associated with cyber attacks.

Entities' capability and confidence in managing cyber incidents varied. We found that those who continually plan, rehearse, and test their people, processes, and technology were more likely to respond and recover effectively.

All of those we audited were reliant on parties outside of their entities for technical expertise and action on cyber incidents. None of them had tested these arrangements to ensure they would work, or to confirm that the third-party experts would provide timely responses in a cyber crisis.

Public sector entities cannot delegate responsibility for managing their cyber risks to an external organisation. Those charged with governance (such as executive management, boards, and councillors) must be satisfied that their entity has plans in place that are fit for purpose and have been thoroughly tested. Only one of the 3 entities we examined in detail had tested its plans. When we ran cyber security simulation exercises, it performed the best.

Entities also do not currently have all the capabilities they need to manage cyber incidents. This relates to technical cyber skills and capabilities, as well as supporting tools. They can access frameworks to guide them in understanding and developing capabilities, and the Cyber Security Unit (CSU – located within the Department of Transport and Main Roads) can help in selecting the appropriate framework and in assessing and developing capabilities.

The expertise of CSU is of great potential value to public sector entities, but not all the entities were aware of the breadth of services it offers, including its 'communities of practice', which share intelligence and learnings about cyber threats. CSU needs to address this by publishing a strategic plan and by increasing awareness of its services.

CSU has recently provided services to local governments. These entities – particularly the regional, rural, and remote councils – could benefit from accessing these to help protect themselves against cyber threats. This would help them be more aware of the risks they are facing and of the training, guidance, and resources they can access to help them deal with cyber threats.

The Queensland Government has increased its investment in cyber security, and much is now available to help entities protect themselves. Based on this audit, the lead and expert agencies, and the entities, now need to make a concerted effort to assess the threats; prepare their defences; and take full advantage of the expertise, resources, and intelligence at their disposal.

2. Recommendations

We gave specific recommendations to each of the 3 entities we examined in detail. All public sector entities – big or small – are a target for cyber criminals because of what they do and the information they hold. Cyber attacks are continuing to increase, and all entities need to ensure they are prepared to identify and respond to an incident. Accordingly, we provide the following recommendations, drawn from the learnings of this audit, for the benefit of all public sector entities.

We have also created a checklist of key questions (Appendix E) for those charged with the governance of public sector entities to consider when planning how they respond to and recover from cyber security incidents.

We recognise that implementing effective controls for cyber incident response should be performed on a cost-benefit and risk basis. Entities should decide, based on their individual organisational needs, the extent to which they can and should act on each of the following recommendations.

Chapter 4: The role of public sector entities in managing cyber incidents

We recommend all public sector entities:

1. protect their systems and sensitive information by
   - maintaining a register of all systems and information assets and resources that are critical to their operations
   - updating the register annually and whenever significant changes occur – either to their technology or to their organisational structure (for example, through machinery of government changes)
   - identifying any 'entry points' or weaknesses through which threat actors (those who attack systems) could access information or disrupt services
   - conducting regular risk assessments of all critical systems to identify security concerns
   - considering the risks, and clearly specifying expectations and requirements, when setting up or extending contracts for cyber-related services with external organisations
2. formally recognise in key governance documents that responsibility for cyber security rests with the chief executive, or equivalent
3. improve and test incident response plans by
   - reviewing their incident response plans (which are for identifying, eliminating, and responding to cyber incidents) annually against better practice frameworks and guidelines
   - ensuring incident response plans integrate with other risk management strategies and plans (such as business continuity plans – which entities use to ensure they can continue to operate in the face of major business disruptions)
   - producing playbooks (sets of procedures for responding to particular incidents) for a variety of risks and cyber incident scenarios
   - ensuring they understand the conditions and requirements of any insurance they take out to protect themselves against cyber incidents. These should be incorporated into their plans
   - testing their incident response and business continuity plans regularly against a range of cyber incident scenarios. This should include testing any external capabilities they plan to rely upon
4. improve their crisis communication plans and templates by
   - ensuring crisis communication plans (which outline processes, steps, and roles for communicating with stakeholders during a crisis) include thresholds for contacting key stakeholders and escalating communications to other parties (such as ministers and other government entities)
   - developing templates for a variety of scenarios to support the quality and consistency of internal and external communications during times of crisis

5. gain access to the technical skills required to respond to and recover from cyber incidents by
   - assessing their cyber capabilities (both those in-house and through external arrangements)
   - developing training plans to address gaps, or obtaining access to specialist technical skillsets externally where required (through either the Cyber Security Unit – CSU – or other external providers)

6. share cyber threat intelligence and lessons learnt with CSU and other public sector entities as quickly as possible.

Chapter 5: The role of expert and lead entities in managing cyber incidents

We recommend the Department of Transport and Main Roads – Cyber Security Unit:

7. improves awareness of its products and services and enhances its guidance for developing incident response plans by
   - developing and publishing its strategic plan
   - creating greater awareness of its role and responsibilities and the services it offers
   - refreshing its incident management guideline to reflect current better practice frameworks and guidelines, and enhancing it with practical examples (such as playbooks) for a range of common cyber incident scenarios

8. assists public sector entities in conducting cyber simulations by
   - supporting them in testing their incident response plans
   - where practical, involving external experts, to ensure they become sufficiently familiar with the information and communication technology (ICT) in public sector entities

9. increases public sector cyber skills and capabilities through
   - developing or adopting a cyber security capability framework that public sector entities can apply
   - developing or adopting tools to assist public sector entities in understanding their capability gaps
   - coordinating delivery of a training program that addresses identified capability gaps

10. improves the maturity of information security management systems by
    - working to understand root causes and challenges preventing entities from progressing and improving their information security management systems
    - amending policy requirements to require public sector entities to test their incident responses through cyber security simulations
    - continuing to encourage all public sector entities' application of the Queensland Government Information Security Policy (IS18:2018) or an equivalent better practice framework.

We recommend that all statutory bodies:

11. document their assessment as to whether IS18:2018 is applicable to their circumstances, and report this information to CSU. If applicable, statutory bodies should apply and adopt IS18 requirements.

We recommend that all government owned corporations and local governments:

12. document whether IS18:2018 is appropriate for their environments, and if not, which frameworks are being applied to manage information security risks.

We recommend the Department of Transport and Main Roads – Cyber Security Unit:

13. shares cyber threat intelligence and lessons learnt by
    - developing and distributing a process for entities to share cyber threat intelligence from incidents, in a consistent format
    - engaging with public sector entities (including statutory bodies, government owned corporations, and local governments) to raise awareness of communities of practice and to promote sharing of cyber threat intelligence
    - using its unique position to compile and share examples of better practice templates and guidance, such as playbooks.

We recommend the Department of Housing, Local Government, Planning and Public Works:

14. increases local governments' knowledge of available support by partnering with CSU to
    - increase local governments' awareness of CSU's services and communities of practice (for sharing cyber threat intelligence) through its existing channels
    - increase local governments' awareness of CSU's incident response capabilities and services in the event of a cyber incident
    - encourage local governments to establish agreements with neighbouring councils to increase access to the required capabilities in the event of a cyber-related crisis.

Reference to comments

In accordance with s. 64 of the *Auditor-General Act 2009*, we provided a copy of this report to relevant entities. In reaching our conclusions, we considered their views and represented them to the extent we deemed relevant and warranted. Any formal responses from the entities are at Appendix A.

Technical language

Cyber security is a complex field, and the language about it reflects this. It is necessary to use some of this language to be precise, but we have explained and simplified it in this report and provided definitions when necessary. We have provided extra details on many of the terms in the glossary (Appendix G).

3. Managing cyber incidents

A cyber incident is an unwanted or unexpected event that is likely to compromise computer and information systems and business operations.

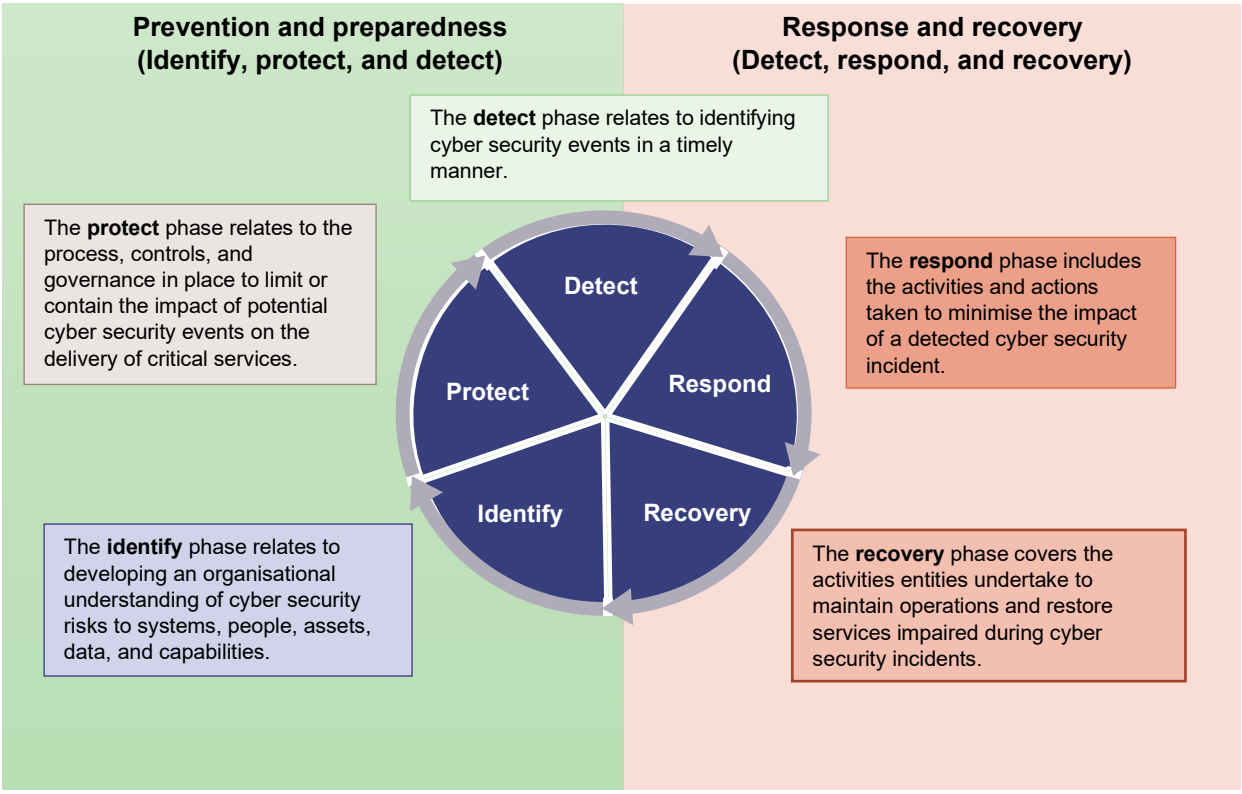
The economic and social impacts of cyber incidents can be significant and long lasting, so entities must be proactive in managing their cyber security risks. The Australian Cyber Security Centre (ACSC – part of the Australian Signals Directorate) states that the most effective way to defend against cyber incidents is to implement appropriate preventative strategies. We covered some of these strategies in *Managing cyber security risks* (Report 3: 2019–20). If entities adopt them, they can reduce, and in some cases, prevent cyber threats.

The changing nature of technology means that cyber security threats evolve rapidly. This is compounded by the development of new technologies such as artificial intelligence and machine learning. For a measure of how damaging cyber security incidents can be, we only have to look at recent events at organisations such as Medibank and Optus.

Even the best prepared organisations can be susceptible, so all entities need to have effective plans in place to minimise potential damage. They need to be informed about the risks, and ready and able to manage them.

Figure 3A shows the cyber security life cycle focus of our 2 reports. In *Managing cyber security risks* (Report 3: 2019–20), we mainly concentrated on prevention and preparedness (shown on the left-hand side of Figure 3A). This report examines response and recovery (right-hand side).

Figure 3A
Cyber security life cycle



Source: Compiled by the Queensland Audit Office using information from the National Institute of Standards and Technology (NIST) Cyber Security Framework 2.0.

Cyber incidents in Queensland and Australia

The ACSC reported that in 2022–23, cyber incidents, including those impacting government entities, have increased in frequency and severity.

Figure 3B
Key trends in cyber incidents

Source: Compiled by the Queensland Audit Office using information from the Annual Cyber Threat Report, July 2022 to June 2023 – Australian Signals Directorate.

Roles, responsibilities, and requirements for responding to and recovering from cyber incidents

Figure 3C shows how roles, accountabilities, and responsibilities for cyber response and recovery activities within Queensland state and local governments are split between expert government agencies and individual entities.

Figure 3C
Key roles, accountabilities, and responsibilities in Queensland

Public sector entities	Department of Transport and Main Roads	
	Queensland Government Cyber Security Unit (CSU)	CITEC**
Manage cyber risks, information assets, and systems as per applicable legislation*. Maintain minimum security requirements in line with relevant Queensland Government policies (departments and some statutory bodies only). Report on and attest to the operation of an information security management system (ISMS – policies and procedures for managing sensitive data) based on ISO 27001 (departments and some statutory bodies only).	Maintains cyber policies, standards, and guidance. Provides cyber threat intelligence updates on cyber security risks and incidents. Provides a coordination role during incident responses (if entities escalate the issue to it). Monitors compliance of departments and some statutory bodies, in line with Queensland Government policies (see later in chapter for further detail). Provides whole-of-government access to training in cyber security and information technology. Negotiates and provides access to technical skills for cyber security prevention, response, and recovery.	Maintains whole-of-government security monitoring services on behalf of entities that have activated it. Maintains the Queensland Government internet service provider and associated gateways and firewalls. Provides access to additional technical and operational skills through the Queensland Government Cyber Defence Centre (CDC).

Notes:

* Financial and Performance Management Standard 2019 for departments and statutory bodies, *Corporations Act 2001* for government owned corporations, and Local Government Regulation 2012 and City of Brisbane Regulation 2012 for local governments. Public sector entities may have further legislative requirements depending on the nature of their operations. Refer to Appendix D for further information and relevant Acts.

** CITEC is the Queensland Government's shared corporate service provider for information and communication technology services.

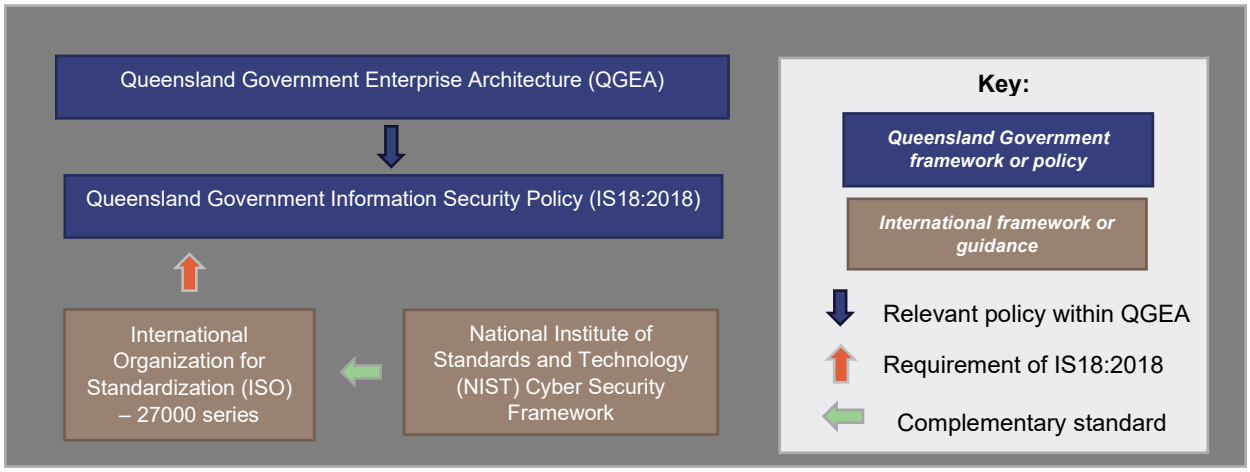
Source: Queensland Audit Office from Queensland Government website.

Better practice frameworks and Queensland guidance

Appendix C lists different international, national, and state frameworks, policies, and guidance, which we refer to collectively as 'better practice frameworks'.

Entities can access a variety of national and international frameworks to help them in managing cyber risks. Figure 3D shows the overall Queensland Government approach, which includes the overarching Queensland Government Enterprise Architecture (QGEA), the Queensland Government Information Security Policy (IS18:2018), and related standards and frameworks.

Figure 3D
Queensland Government cyber policy and frameworks



Source: Queensland Audit Office.

DEFINITION

The **Queensland Government Enterprise Architecture** is a collection of publications such as digital and information and communication technology (ICT) strategies, frameworks, policies, and other guidance materials. These publications aim to support the efficient and effective use of digital and ICT resources across government.

The **Queensland Government Information Security Policy** (**IS18:2018**) aims to ensure all departments apply a consistent, risk-based approach to information security to maintain confidentiality, integrity, and availability. While IS18:2018 only applies to departments defined under the *Public Sector Act 2022*, all Queensland public sector entities, including local governments, should consider the policy.

The **ISO 27000 series** is a set of standards for establishing an information security management system and underlying controls. It includes a library of technical controls and requires entities to conduct training and awareness activities. To be compliant, entities must conduct a risk assessment and design and implement security controls, and regularly review their effectiveness.

The **National Institute of Standards and Technology** (**NIST**) **Cyber Security Framework** is a risk-based approach to managing cyber security risk. It reinforces the relationship between cyber security activities and the business operations of an entity.

All public sector entities are responsible for managing their cyber security risks and being prepared to respond and recover when cyber events occur. However, policy requirements differ between different types of public sector entities, as outlined in Figure 3E.

Figure 3E
Cyber policy and framework requirements for public sector entities

Public sector entity	Relevant requirements
Departments	All departments must apply the policy requirements in IS18:2018 to all information, applications, and technology assets. This includes the requirement to comply with ISO 27001. Departments may apply other frameworks in addition to this if they consider them suitable to their needs.
Statutory bodies	All statutory bodies must have regard to the QGEA, including IS18:2018 and ISO 27001. This means that they must consider and document whether the framework applies to their circumstances in setting their own internal controls and policies. Statutory bodies may also adopt other frameworks they consider suitable for their needs. Some statutory bodies may be directed to comply with IS18:2018 by their minister or chief executive.
Government owned corporations	Government owned corporations (GOCs) do not have to comply with QGEA or IS18:2018 requirements. However, in accordance with the *Corporations Act 2001*, GOC boards are responsible for ensuring appropriate controls and processes are in place to address identified risks (which includes cyber-related risks).
Local governments	Local government entities do not have to comply with QGEA or IS18:2018 requirements. However, in accordance with risk management requirements in their regulations, they are required to develop and implement fit-for-purpose strategies to address identified risks (which includes cyber-related risks).

Source: Queensland Audit Office.

Other legislative requirements

Public sector entities may have additional legislative obligations relating to cyber incidents. These obligations are dependent on the nature of their business and operations. For example, many public sector entities will hold personal information and may have reporting obligations under relevant privacy legislation, while those entities who own or operate critical infrastructure (services that are essential for everyday life, such as energy, communications, water, transport, and health) will have additional obligations under the *Security of Critical Infrastructure Act 2018* (Commonwealth). We provide further detail on these obligations in Appendix D.

What we audited

In this audit, we assessed the role of lead agencies, and the preparedness of 3 public sector entities to respond to and recover from cyber security incidents. The entities have different levels of resourcing and capability for managing cyber security risks. We do not want to compromise the security of these entities by publicly identifying their security vulnerabilities, so we have not named them in this report.

Appendix B provides greater detail on our audit scope and methodology.

We use the term ‘entities’ in this report to refer broadly to all Queensland public sector entities (departments, statutory bodies, and government owned corporations) and local governments.

4. The role of public sector entities in managing cyber incidents

In this chapter, we report on how prepared the 3 entities we audited were in relation to responding to and recovering from cyber incidents. They may not be representative of all public sector entities in Queensland, and results cannot be extrapolated. However, all public sector entities should consider our findings and recommendations to determine if they are relevant to their own organisations and risks.

We identified a range of gaps and improvement opportunities in the audited entities' approaches to cyber response and recovery. Figure 4A summarises the gaps across the areas we audited, which were:

- risk assessment
- incident response plans
- capability and sharing cyber threat intelligence (and lessons learnt).

Figure 4A
Key areas of improvement for cyber response and recovery

Area	What we expected to see	Entity 1	Entity 2	Entity 3
Risk assessment	Up-to-date system and information asset registers and cyber security risk assessments	☑	☒	⊟
Incident response plans	Incident response plans aligned to better practice frameworks	⊟	⊟	⊟
	Tests of the adequacy of cyber incident response strategies and plans	☑	☒	☒
	Clear cyber incident response communication strategies, plans, and escalation points	⊟	⊟	☒
Capability and sharing cyber threat intelligence	Access to enough technical and non-technical capabilities to respond to and recover from a cyber incident	⊟	⊟	⊟
	The capturing, recording, and sharing of cyber threat intelligence and lessons learnt	⊟	⊟	⊟

Key:

☑ No gaps identified ⊟ Improvement opportunities identified ☒ Gaps noted

Source: Queensland Audit Office.

Understanding cyber risks in system and information assets

Public sector entities must understand the systems they have and the information assets contained within them. This is essential if they are to effectively identify all potential risks that may be exploited by threat actors. They should periodically undertake cyber security risk assessments of key systems and those information assets that increase risk because of the desirability of the data they contain. These assessments should consider all possible points of system access by threat actors.

Of the 3 public sector entities we audited, 2 did not have an up-to-date or complete listing of the systems and information assets they held, and their risk assessment activities were not up to date. These entities did not have the information they needed to identify key risks and assess the potential business impacts on their operations.

DEFINITION

A **threat actor** (also commonly referred to as a cyber criminal) is any person or organisation that intentionally exploits weaknesses in computers, networks, and systems for gain or to disrupt individuals or services.

Managing cyber risks from third-party systems

Not all entities manage their risks themselves. Some have contracts with other organisations to provide access to the necessary expertise and resources, including systems. In this report, we refer to these as ‘third parties’.

Not all the entities we examined had considered risks for critical systems and information assets managed by third parties. This means they were unaware of potential risks, and were therefore not actively managing these risks.

It is important for all public sector entities to consider cyber security risks relating to third-party arrangements. They should ideally do this prior to setting up or extending contracts. In this way, they can ensure appropriate arrangements (such as the provision of assurance certificates, which outline effectiveness of system controls and processes) are in place through contractual obligations.

We plan to conduct an audit on managing third-party cyber security risks in 2025–26.

Impact of machinery of government changes on cyber risks

Machinery of government changes (restructures of government functions) can cause disruption to public sector entities.

One of the entities we audited had been through various machinery of government changes over the last 5 years. As a result, it was using and relying on several systems managed by other government entities. This adds to the complexity of managing and responding to risks of a cyber incident. The entity did not have a well-integrated incident response plan and recovery plans to guide it in the event of a cyber incident.

It is important for any entity impacted by a machinery of government change to identify and understand its new critical systems in a timely manner, so it can manage its risks. Entities also need to clarify the roles and responsibilities for managing cyber incident responses across the new structure.

We have previously produced a guide – *Checklist for managing machinery of government (MoG) changes* – to assist entities to identify, manage, and monitor the associated operational and strategic risks.

Recommendation 1

We recommend all public sector entities protect their systems and sensitive information by:

- maintaining a register of all systems and information assets and resources that are critical to their operations
- updating the register annually and whenever significant changes occur – either to their technology or to their organisational structure (for example, through machinery of government changes)
- identifying any 'entry points' or weaknesses through which threat actors (those who attack systems) could access information or disrupt services
- conducting regular risk assessments of all critical systems to identify security concerns
- considering the risks, and clearly specifying expectations and requirements, when setting up or extending contracts for cyber-related services with external organisations.

Improving incident response plans

An incident response plan (IRP) is critical to incident response and recovery. It supports a swift and effective response to cyber incidents, in line with an entity's security and risk management strategies and plans.

Alignment to better practice

All entities we examined had an IRP. Figure 4B provides a summary of the strengths and weaknesses we found when comparing these plans to better practice frameworks.

Figure 4B
Improvement areas for incident response plans

What we expected to see	Entity 1	Entity 2	Entity 3
An IRP that included: • clear roles, responsibilities, and thresholds (such as who has the authority to shut down systems, and at what point) • when and how the plan would be tested, for example, through an exercise such as a cyber simulation • regular review points.	⊟	⊟	⊟
An IRP that fulfilled IS18:2018 or equivalent requirements, including procedures for annual reporting requirements to CSU.	**Not mandated for the entity**	**Not mandated for the entity**	⊟
An IRP that integrated with the entity's risk management strategies and procedures and that included: • risk appetites (the level of risk that an entity is prepared to accept in pursuit of its objectives) that match the expectations of those charged with governance (such as executive management, boards, and councillors) • a complete view of exploitation risks across networks, systems, and information assets • periodic risk assessments which enable timely decision-making.	☑	☒	☒
An IRP that outlined: • a range of strategies for managing different types of cyber risks, including playbooks (incident response procedures) for several different types of disruptive cyber scenarios • any insurance policies and exclusions.	⊟	⊟	⊟

Key:		
☑ No gaps identified	⊟ Improvement opportunities identified	☒ Gaps noted

Source: Queensland Audit Office.

All public sector entities should continually improve their IRPs, particularly the playbooks they produce for managing different types of cyber risks.

Being fully compliant with better practice frameworks can require significant investment. Accordingly, entities have to decide and document the extent to which they are prepared and can afford to align to better practice frameworks, in line with their resources and risk appetites.

Entities told us that they would benefit from more guidance on how to effectively respond to common cyber risks and incident types. Common incident types include:

- ransomware (demanding payment to let entities into their own files)
- insider privilege abuse (by current or former employees with access to the system)
- social engineering (manipulating employees into giving up information)
- denial of service attacks (flooding a network to disrupt operations)
- malware (gaining access to a system via software)
- phishing (enticing users to share confidential information).

Appendix G provides more details on each of these incident types.

Better practice approaches

An effective incident response plan:

- aligns with a framework such as ISO 27035 (part of the ISO 27000 series)
- is integrated with the entity's risk management systems
- identifies, assesses, and treats cyber security risks for critical systems, information systems, and business continuity
- provides guidance on the steps required to respond to a range of cyber incidents
- outlines the roles, responsibilities, accountabilities, and authorities of personnel and teams required to manage responses to cyber incidents
- identifies legal and regulatory compliance requirements for cyber incidents
- links to internal and external communication processes when responding to cyber incidents
- provides guidance on post-incident activities to support continuous improvement.

An effective IRP must be a 'living document', meaning it is continually rehearsed, tested, improved, and supported with training and a culture that promotes cyber resilience.

Understanding insurance arrangements

Having effective strategies and plans does not eliminate the risk of a cyber incident. Entities need to consider how they manage that residual risk. Many use cyber insurance arrangements to do this, as this can be an effective way to protect entities from financial impacts and losses. Those entities who do this need to fully understand their coverage and requirements and integrate them into their incident response planning.

Some of the entities we audited did not fully understand specific clauses and escalation points in their insurance arrangements. This could have meant that their insurance coverage was at risk in the event of a cyber incident.

Accountability for cyber risks

Some of the entities we audited had not clearly defined incident response roles, responsibilities, and accountabilities. One entity had assigned, through a memorandum of understanding, most information and communication technology (ICT) accountabilities to CITEC (a Queensland Government shared corporate service provider for ICT), including most cyber security monitoring and response.

Ultimately, the responsibility for cyber risks (as with all risks) rests solely with the accountable officer and they *cannot* assign it to external entities, including other government bodies. The accountable officer must be satisfied that third-party arrangements adequately reduce risks to an acceptable level. We discuss testing of third-party arrangements later in this chapter.

Testing cyber incident response strategies and plans

As entities are ultimately responsible for their own systems and information assets, they should regularly test their IRP and business continuity plans (plans which entities use to ensure they can continue to operate in the face of major business disruptions) to make sure they can adapt to the ever-evolving threat of cyber attacks. Those entities who regularly test their processes, people, and technology for a variety of cyber security incidents should have an increased chance of success.

Only one of the 3 entities we audited had previously tested its IRP through an entity-level cyber security simulation (one it conducted itself, of its own processes) to ensure that it was fit for purpose. This entity performed the best in our simulations.

DEFINITION

Cyber security simulations are workshops to test how key incident response personnel (both technical and non-technical) respond to a cyber incident within their information systems or networks. Simulations can help identify vulnerabilities, assess risks, and improve security measures.

Testing third-party arrangements through simulations

All 3 entities were reliant on third-party capabilities as a part of their incident response plans, but none had ever tested these arrangements.

It is important to use simulations to test any third-party arrangements. They give entities insights into whether they will deliver the services and expertise needed in the event of an actual incident. Public sector entities should not be testing these arrangements for the first time during an incident.

For third parties to be effective and respond promptly to incidents, they need to become familiar with public sector systems and environments. The greater the reliance entities place on these arrangements, the more time and effort they need to invest in familiarising the third parties.

Lessons from our cyber simulations

All audited entities participated in our cyber simulations. These identified valuable lessons and opportunities to improve for each of the entities. Some examples we noted were:

- Entities that took a business-led approach (as opposed to a technical approach) to incident response were more effective in coordinating the incident response. A business-led approach focuses on the broader organisational impacts of a cyber incident rather than just the technical cyber and systems elements.
- Those entities who documented key information through the simulations performed better. This included facts relating to the incident, questions requiring further investigation, key decisions, and key times and milestones.
- Entities benefit from having key plans and documents available and easily accessible in hard copy. During the simulations, some key documents (including key strategies, plans, playbooks, and contact listings) were no longer available electronically due to the cyber attack.
- Entities need to make manual forms (for maintaining business operations and services) available for use during prolonged disruptions.
- When services are disrupted, entities need to ensure internal and external communication is consistent, to not breach the trust of employees, customers, stakeholders, and the public.
- Entities need to clearly document thresholds for decision-making and communication protocols to ensure escalation of an incident at appropriate intervals.

The following case study shows the importance of a quick response in the event of a cyber incident.

Figure 4C
Case study 1: The importance of a timely response

Maersk NotPetya cyber incident

The Maersk NotPetya cyber incident, which occurred in June 2017, escalated rapidly, causing widespread disruptions and significant damage to Maersk, one of the world's largest shipping companies. The following timeline highlights the key events and escalation of the incident:

Day 0

27 June 2017:
- The NotPetya ransomware attack begins by exploiting a software update from a Ukrainian accounting software.
- Maersk's information technology (IT) systems are infected with the malware.

Within 24 hours

Within 24 hours:
- NotPetya spreads rapidly through Maersk's global network, affecting various subsidiaries and offices worldwide.
- Maersk's IT systems begin to experience widespread disruptions and become inaccessible.
- Maersk is forced to shut down multiple systems, including email, order processing, and container booking, to contain the infection. This causes operational disruptions across its global operations.
- Maersk's operations at several ports, including the Port of Los Angeles, Port of New York and New Jersey, and Port of Rotterdam, are severely affected due to the inability to process cargo.
- Maersk confirms in a statement that the company is dealing with a widespread cyber incident and that it is working tirelessly to mitigate the impact.

10 days

After 10 days:
After a monumental effort, Maersk reinstalled its entire infrastructure including 4,000 new servers; 45,000 new PCs; and 2,500 applications over 10 days to reinstate operations. This feat would normally take several months but came at great cost.

After 2 months

After 2 months:
Full global recovery of operations after the cyber incident. Maersk suffered a huge loss of data and estimated the impact at US$250 to US$300 million.

Source: Queensland Audit Office, compiled from various news articles, podcasts, and journals.

Whole-of-government cyber security simulations

The CSU has conducted annual whole-of-government incident response simulations for the past 3 years. These simulations have had good participation rates from Queensland Government departments.

The main objective of these simulations has been to test the *Queensland Government Cyber Security Operations Plan*. The plan aims to detail the whole-of-government coordination and communication response to cyber incidents.

These simulations are important and should continue to be held at regular intervals. They test different events and scenarios to continue building resilience at a whole-of-government level. However, the simulations have not been designed to assess the preparedness of individual entities to respond to or recover from a cyber security incident.

During our audit, one entity was under the misconception that its participation in CSU's whole-of-government simulations was evidence that its incident response plans and approach were effective. CSU should take steps to fully educate entities participating in its whole-of-government simulations on the limitations of what these simulations mean for them. We discuss this further in Chapter 5.

Recommendation 2

We recommend all public sector entities formally recognise in key governance documents that responsibility for cyber security rests with the chief executive, or equivalent.

Recommendation 3

We recommend all public sector entities improve and test incident response plans by:

- reviewing their incident response plans (which are for identifying, eliminating, and responding to cyber incidents) annually against better practice frameworks and guidelines
- ensuring incident response plans integrate with other risk management strategies and plans (such as business continuity plans – which entities use to ensure they can continue to operate in the face of major business disruptions)
- producing playbooks (sets of procedures for responding to particular incidents) for a variety of risks and cyber incident scenarios
- ensuring they understand the conditions and requirements of any insurance they take out to protect themselves against cyber incidents. These should be incorporated into their plans
- testing their incident response and business continuity plans regularly against a range of cyber incident scenarios. This should include testing any external capabilities they plan to rely upon.

Planning communication strategies and escalation points

In a time of crisis, trust erodes when the public, employees, and customers are not provided with timely, consistent, or informative communication. In accordance with better practice frameworks, we expected entities to have clear, consistent, and endorsed communication plans, protocols, and templates to guide their communication in the event of a crisis. Not all did.

For those that did have communication plans and templates, most of the documents were in draft and incomplete. The cyber crisis communication plans were commonly missing clear processes and thresholds for:

- contacting those charged with governance, relevant ministers, the Department of the Premier and Cabinet, and CSU
- contacting key stakeholders (such as employees, insurers, Office of the Information Commissioner, and the public)
- escalating communication to other agencies.

Entities showed a lack of consistent content and messaging in internal and external communications during the cyber security simulations. This inconsistency could result in a lack of trust if internal messaging is found to be inconsistent with external messaging.

Recommendation 4

We recommend all public sector entities improve their crisis communication plans and templates by:

- ensuring crisis communication plans (which outline processes, steps, and roles for communicating with stakeholders during a crisis) include thresholds for contacting key stakeholders and escalating communications to other parties (such as ministers and other government entities)
- developing templates for a variety of scenarios to support the quality and consistency of internal and external communications during times of crisis.

Capabilities for incident response and recovery

Entities may require access to a broad range of skills, capabilities, and tools to effectively navigate a cyber incident. These span:

- technical areas such as digital forensics (the ability to assess the source and extent of a breach) and a security operations centre (which is the focal point for network security operations)
- non-technical areas (such as crisis management and communication)
- general ICT areas (such as system applications and networks).

We refer to these collectively as 'capabilities' within this report. These may be sourced through a combination of in-house and third-party resources.

While all 3 chief information officers (or equivalent) were aware of limitations in their own entities' cyber technical skills, none of the entities had formally assessed their capability. They need to do so, in detail, to ensure they understand and can address any gaps.

Public sector entities can consider several models in formalising a skills and capability assessment. In Appendix F, we provide an example framework that details the key technical and non-technical capabilities required for cyber incident response and recovery. It can be used by entities to assess their capabilities.

We discuss broader capability building across Queensland public sector entities further in Chapter 5. Appendix G – Glossary, provides more detailed explanation of the various capabilities needed to manage a cyber incident.

Recommendation 5

We recommend all public sector entities gain access to the technical skills required to respond to and recover from cyber incidents by:

- assessing their cyber capabilities (both those in-house and through external arrangements)
- developing training plans to address gaps, or obtaining access to specialist technical skillsets externally where required (through either the Cyber Security Unit – CSU – or other external providers).

Capturing, recording, and sharing cyber threat intelligence

All audited entities demonstrated an understanding of the importance of sharing cyber threat intelligence (CTI). However, for each entity, weaknesses were identified in the processes put in place to capture and share learnings. Gaps were identified in relation to:

- processes on where and how to capture lessons learned, and how to conduct assessments of incidents
- the tracking and monitoring of actions and/or recommendations arising from lessons learned exercises
- identification of external stakeholders to share information with, and the correct medium for sharing.

This could lead to a missed opportunity for the sector to build cyber resilience.

DEFINITION

Cyber threat intelligence is information that helps entities better protect against cyber incidents by increasing their understanding of current and emerging threats and vulnerabilities. It can incorporate recent threat actor behaviours and successful remedial procedures, tools, and techniques.

Better practice approaches

All public sector entities can strengthen their cyber resilience by:

- creating greater awareness of cyber risks and incidents
- gathering and sharing intelligence
- ensuring effective cooperation between entities in relation to incident preparedness and response.

CTI can come from a variety of sources. The Australian Cyber Security Centre and CSU both produce CTI reports and alerts for their subscribers. These contain critical information about vulnerabilities and how to prevent, contain, and strengthen controls.

The most effective collection of CTI is through reporting of actual incidents that occur at individual entities. Many entities use the same products, networks, hardware, systems, and applications. As such, it is likely that if one entity has a vulnerability, another will also have the same entry point. Better practice frameworks recognise the potential for reoccurrences of an incident as an opportunity to learn.

Recommendation 6

We recommend all public sector entities share cyber threat intelligence and lessons learnt with CSU and other public sector entities as quickly as possible.

5. The role of expert and lead entities in managing cyber incidents

In this chapter, we report on the effectiveness of lead and expert agency strategies for supporting state and local government entities in managing cyber incidents.

The role of the Queensland Government Cyber Security Unit

The Queensland Government Cyber Security Unit (CSU), within the Department of Transport and Main Roads, is the lead agency for Queensland cyber security operations and management.

CSU sets cyber security policy and guidance for Queensland Government departments and statutory bodies, providing:

- cyber security leadership
- governance, policy, and standards
- coordinated responses to cyber security incidents
- development of cyber security capability across government
- greater cyber security awareness.

CSU also provides assistance to local governments and government owned corporations.

Promotion and awareness of CSU's products and services

CSU plays a critical role in supporting public sector entities across Queensland in the management of cyber security. In June 2023, the Queensland Government committed $73.5 million in additional funding to CSU over 4 years (from 2023–24 to 2026–27) and $17.8 million ongoing (from 2027–28). This was to expand and improve the services CSU provides.

CSU needs to do more to increase awareness of its services and increase its engagement with entities. Its services, such as access to specialist skillsets to assist entities during a cyber incident, can assist in the management of risks and in building capabilities within entities. However, it currently provides limited documentation outlining what products and services are available and the benefits of using them.

It has put initiatives in place, such as communities of practice, to help build awareness, but more is needed to capitalise on the investment the Queensland Government has made. Not all entities we audited had awareness of CSU's products and services specific to managing and coordinating cyber security response and recovery.

DEFINITION

CSU's **communities of practice** aim to raise awareness of information security and develop and share information, methods, and tools to create a knowledge base for public sector entities. They also provide opportunities to meet other practitioners and share cyber threat intelligence across the government. Membership of the communities of practice is voluntary and is open to all state government and local government employees.

Publishing a strategic plan

While CSU has a vision, it does not have a strategic plan. It also does not have supporting plans in place to implement its vision – which is important to address areas such as key person risk. We would expect to see a strategic plan that covers, at a minimum:

- the vision, purpose, mission statement, and role of CSU in managing cyber risks across the state
- strategic objectives that will drive the vision
- current challenges and services of CSU
- key threats in the current Queensland environment
- key performance indicators or performance targets to measure effectiveness.

CSU has drafted the *Queensland Government Cyber Security Operations Plan*, which has been circulated for consultation. The objective of the plan is to facilitate coordinated and cooperative escalation and response during a cyber incident.

It is designed to acquit CSU's responsibilities for responding to a whole-of-government cyber incident under the disaster management arrangements. It does not cover CSU's broader role, responsibilities, or services.

The New South Wales and Victorian governments' equivalent cyber security units have published their strategies and plans across their jurisdictions.

Leading the public sector in increasing cyber resilience

Guidance materials to better support entities

CSU provides public sector entities with access to a variety of guidance and materials to support the management of cyber risk. In September 2018, it issued the *Incident Management Guideline*. The guideline provides information for Queensland Government departments on the recommended practices for establishing and implementing an information security incident management policy and a planned, systematic approach to handling an incident.

It appropriately references the relevant framework, ISO 27000 incident management standard (ISO 27035). It also provides entities with an example playbook (incident response procedures) on phishing (tricking entities and individuals into providing access to data and information, often through fraudulent emails or texts).

On its website, CSU also provides links to more guidance including:

- Australian Cyber Security Centre resources
- other ISO standards
- both the Australian and Queensland Information Commissioner websites, given their roles in information management
- various other legislation, policies, and guidance, and other resources.

CSU's guideline could be enhanced by:

- including updates for the most recent release of the ISO 27035 (2023)
- developing and sharing practical examples for a range of common cyber scenarios.

All 3 of the entities we audited stated that they would appreciate more guidance from CSU on how to improve their incident response plans and promote a culture of continuous improvement, to help them stay across the rapidly changing cyber risks facing the public sector.

Recommendation 7

We recommend that the Department of Transport and Main Roads – Cyber Security Unit improves awareness of its products and services and enhances its guidance for developing incident response plans by:

- developing and publishing its strategic plan
- creating greater awareness of its role and responsibilities and the services it offers
- refreshing its incident management guideline to reflect current better practice frameworks and guidelines, and enhancing it with practical examples (such as playbooks) for a range of common cyber incident scenarios.

Helping public sector entities test their incident response plans

As detailed in Chapter 4, CSU conducts cyber simulations that test the response to cyber incidents at the whole-of-government level. While this is an important exercise, public sector entities must also regularly test their individual readiness to respond to a cyber incident. To date, CSU has not assisted entities in coordinating or running individual simulations.

The investment made in CSU to provide public sector entities with access to incident response capabilities has been an important step. This work is undertaken through CSU by a panel of third-party incident response providers. It is expected that many public sector entities will use CSU's incident response capabilities, but these capabilities must be tested within entities' environments.

For CSU to be fully effective and able to deliver timely incident response services, its external providers must understand the systems and environments they are working with. Being involved in cyber simulations at individual entities presents CSU with an opportunity to assist the entities with their own readiness, and to ensure that its incident response providers build the necessary understanding of public sector entities.

Recommendation 8

We recommend the Department of Transport and Main Roads – Cyber Security Unit assists public sector entities in conducting cyber simulations by:

- supporting them in testing their incident response plans
- where practical, involving external experts, to ensure they become sufficiently familiar with the information and communication technology (ICT) in public sector entities.

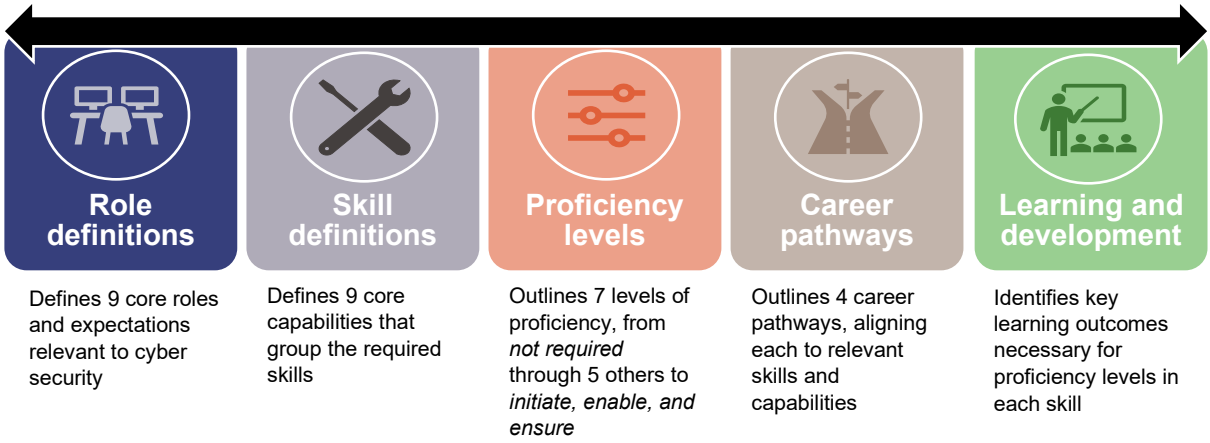
Understanding the current state of public sector cyber capability

CSU is responsible for supporting the development of the Queensland Government's cyber security workforce. As with many professions, experienced and qualified cyber security consultants are in high demand.

At present, CSU does not fully understand the level of capability within public sector entities. It has not assessed entity-level capabilities or (as previously discussed) provided support to public sector entities in assessing them. Doing so would enable it to better target its investment in building cyber resilience by directing resources and training to the most significant gaps.

Numerous frameworks are available to assist in identifying and developing cyber skills and capabilities. One such example is the Australian Signals Directorate (ASD) *Cyber Skills Framework*. The skills framework (Figure 5A) helps users map and develop skills using 9 cyber role definitions, 9 capability and skill definitions, 7 proficiency levels, 4 career pathways, and a learning and development pathway.

Figure 5A
Australian Signals Directorate Cyber Skills Framework



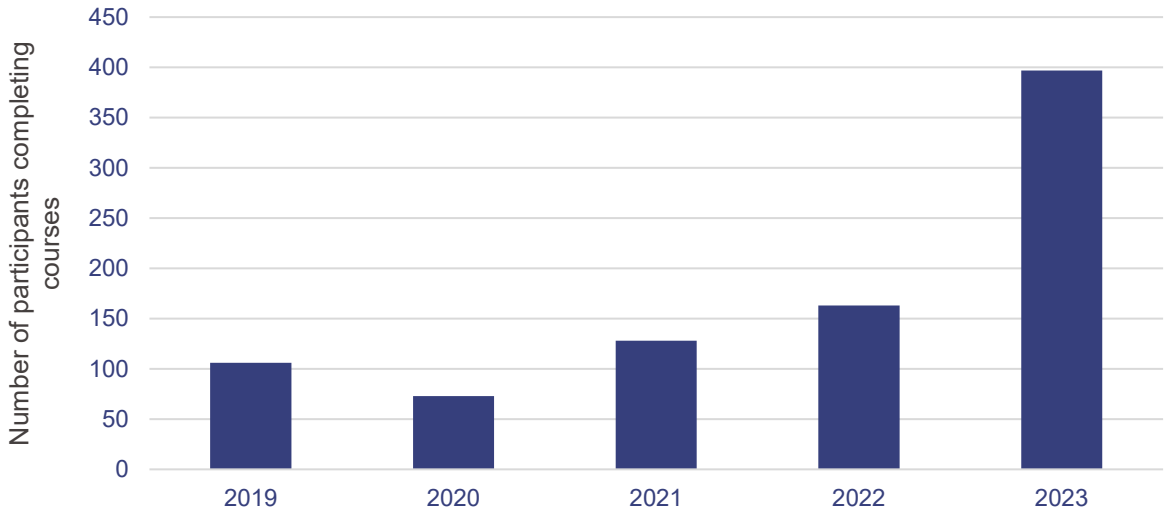
Source: Queensland Audit Office from Australian Signals Directorate's Cyber Skills Framework.

Providing cyber security and technology training

CSU provides training courses ranging from basic computer operations to full cyber security certificates. These courses are offered to public sector employees at cost, or subsidised depending on the course and the type of public sector entity. They are not targeted to specific roles or agencies.

Figure 5B shows an increase in training uptake since 2020, when the training opportunities were reduced during COVID-19. CSU has engaged external providers to offer a variety of courses in the last 5 years (January 2019 to December 2023). This has increased from 2 courses in 2019, to 22 courses in 2023, with a total of 867 participants completing courses over this period.

Figure 5B
Number of Cyber Security Unit courses completed: 2019–2023



Source: Queensland Audit Office from Department of Transport and Main Roads – Cyber Security Unit data.

While the delivery of training has increased, CSU's current training offerings may not be meeting the needs of the Queensland public sector. CSU performs limited analysis on training data. It is not aware of whether the courses are being undertaken by the public sector entities and employees who have capability gaps. It needs to examine its funded courses – by entities, attendees' positions, and whether they completed all the content – to build this understanding.

CSU also needs to be more targeted in its training offerings. It could better align them to the needs of entities and their staffs' development needs to ensure that significant capability gaps are addressed. CSU's lack of understanding of current capability gaps across the sector has prevented it from doing this.

Recommendation 9

We recommend the Department of Transport and Main Roads – Cyber Security Unit increases public sector cyber skills and capabilities through:

- developing or adopting a cyber security capability framework that public sector entities can apply
- developing or adopting tools to assist public sector entities in understanding their capability gaps
- coordinating delivery of a training program that addresses identified capability gaps.

Improving information security management systems

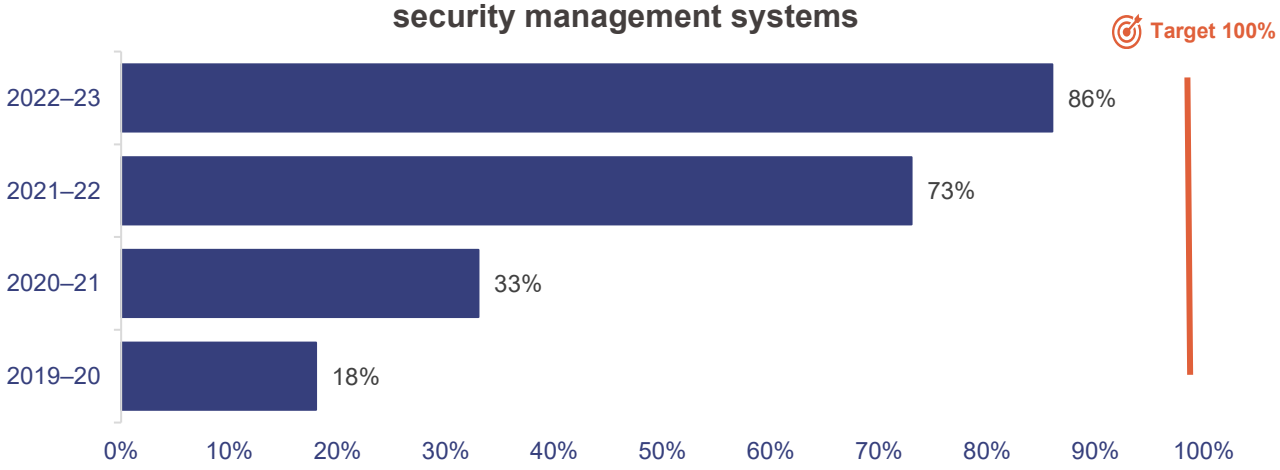
Chief executives of departments and some statutory bodies (those who have been directed to comply with IS18:2018 and its annual return requirements, refer to Chapter 3) must attest to the appropriateness of their information security under IS18:2018 (the Queensland Government's information security policy). This includes providing an information security annual return by 30 September each year. A third party must conduct periodic reviews of the annual returns to assess the entity's information security management system (ISMS) to conclude:

- if it is fully operational
- if it aligns with ISO 27001
- its overall effectiveness.

Entities must publish the results in their annual report.

CSU consolidates returns and reports outcomes to chief executives. Since our last audit on cyber security in 2019–20, CSU has assisted in-scope entities to improve their ISMSs, increasing overall compliance with IS18:2018 (Figure 5C). In 2019–20, only 18 per cent of departments had appropriately designed and implemented an ISMS. By 2022–23, 86 per cent had one.

Figure 5C
Percentage of departments with operational information security management systems



Source: Queensland Audit Office from Department of Transport and Main Roads – Cyber Security Unit ISMS report.

ISMS compliance reviews are only required for departments and some statutory bodies that fall under IS18:2018 requirements. Other public sector entities are not required to review their ISMS, but are encouraged to do so. This restricts CSU's ability to monitor risks and capabilities at the entity level, outside of departments and those statutory bodies who comply. The policy states that all statutory bodies must *have regard* to IS18:2018. This means that they must consider and document whether the framework applies to their circumstances in setting their own internal controls and policies. It is unclear whether all statutory bodies have undertaken and documented this assessment. One of the entities we audited had considered this and adopted the principles of IS18:2018, but this was not documented or shared with CSU. For government owned corporations and local governments, there is no requirement to do this.

Also, current IS18:2018 requirements do not explicitly address incident management readiness, which can only be tested through cyber security simulations. Testing of incident management plans is critical to improving the effectiveness of cyber responses.

Recommendation 10

We recommend the Department of Transport and Main Roads – Cyber Security Unit improves the maturity of information security management systems by:

- working to understand root causes and challenges preventing entities from progressing and improving their information security management systems
- amending requirements to require public sector entities to test their incident responses through cyber security simulations
- continuing to encourage all public sector entities' application of the Queensland Government Information Security Policy (IS18:2018) or an equivalent better practice framework.

Recommendation 11

We recommend that all statutory bodies document their assessment as to whether IS18:2018 is applicable to their circumstances, and report this information to CSU. If applicable, statutory bodies should apply and adopt IS18 requirements.

Recommendation 12

We recommend that all government owned corporations and local governments document whether IS18:2018 is appropriate for their environments, and if not, which frameworks are being applied to manage information security risks.

Increasing cyber threat intelligence and transferring knowledge

CSU runs communities of practice with technical and security leads from across the Queensland public sector. These forums are used to share cyber threat intelligence, provide updates, advocate for learning or training opportunities, and share ideas.

The following case study demonstrates the value of acting promptly on shared intelligence.

Figure 5D
Case study 2: Proactive sharing of cyber threat intelligence

Cyber Security Unit amber alert
In December 2021, following a public sector entity reporting a phishing incident, CSU provided an amber alert to entities. Within 2 hours, one of the entities we audited was able to alert its employees of the potential phishing and begin reviewing its system applications. Within a day, it had removed the vulnerabilities from its environment and contacted all its service providers to patch the vulnerabilities.

Source: Queensland Audit Office from departmental records.

This case study shows the value in CSU promptly sharing cyber threat intelligence through alerts to entities. However, 2 of the 3 entities we audited were not aware of the community of practice forums. CSU needs to improve awareness of its activities.

All 3 entities had ideas for additional guidance and better practice frameworks for CSU to share through its communities of practice. A key example was generic playbooks for various cyber scenarios – for entities to customise to their needs and circumstances.

Recommendation 13

We recommend the Department of Transport and Main Roads – Cyber Security Unit shares cyber threat intelligence and lessons learnt by:

- developing and distributing a process for entities to share cyber threat intelligence from incidents, in a consistent format
- engaging with public sector entities (including statutory bodies, government owned corporations, and local governments) to raise awareness of communities of practice and to promote sharing of cyber threat intelligence
- using its unique position to compile and share examples of better practice templates and guidance, such as playbooks.

Increasing cyber resilience in the local government sector

Local governments deliver a range of critical services to the public, such as water and sewerage services. They must be as prepared as possible to manage a cyber incident. The following case study demonstrates the prolonged and costly consequences cyber incidents can have on local governments if they are not able to access the required cyber incident response skills in a timely manner. It includes 3 examples which impacted councils since 2020. These councils included regional councils, and those with both small and large populations.

Figure 5E
Case study 3: The importance of cyber resilience in local government

Impact of cyber attacks on councils

Example 1

In 2023, a Queensland council became a victim of a cyber attack that used ransomware (where a threat actor locks electronic files through encryption and demands a payment to unlock them). The incident occurred on a Saturday morning before systems were switched off over the weekend. The council had to access cyber security expertise from a third party who was flown in 2 days after the initial event.

Twelve days into the incident, the council identified, with the help of third-party digital forensics skills, the potential entry points for the ransomware. The likely scenario was through a phishing email and a council worker clicking a malicious link. Council did not pay a ransom to access its locked data.

The continued disruption meant the postponement of an important oversight committee – council's April 2023 Standing Committee meeting. It also meant phone connections could not be restored until May 2023.

Example 2

In 2022, a Queensland council was subject to a ransomware attack on a network responsible for operating public infrastructure. The impact to the business was significant and included access to assets, systems, and services which were used by the council, external government bodies, and the public.

The time between the initial identification of the incident to recovery attempts took approximately 2 days before the decision was made to shut down the network containing those services. The recovery process from this attack took a further 24 days, with permanent corrective actions taking a further 12 months to complete.

This incident was reported to the Australian Cyber Security Centre (ACSC) and the Queensland Government CSU.

Example 3

In 2020, one regional council was subject to a ransomware attack. The cyber attacker gained access to all council systems, including the backup data that was stored on the council's network.

The impacts of this attack were that:

- the council was unable to access systems and information, with full restoration taking an extended period (for example, payroll and creditors had to be paid manually for 5 weeks)
- normal activities could not be performed or were delayed (for example, the council was unable to prepare monthly financial management reports)
- key staff, including information technology staff and contractors, needed to work extended hours to resolve the situation
- significant time was spent by council staff in dealing with various parties and investigating the source of the data breach.

This incident was reported to the CSU.

Source: Queensland Audit Office.

Local governments do not have to comply with or have regard to Queensland Government policies and requirements, including IS18:2018. They can choose a cyber security incident response framework that best suits them.

There are no central strategies, policies, or procedures for managing and coordinating cyber response and recovery capabilities specific to local governments. However, CSU has been funded to provide them with essential cyber advice and services. Given the large variability in capabilities and resources available across the local government sector, this presents both a challenge and an opportunity.

One of the entities we examined in detail in this audit was a local government, which was not aware of the CSU's support offerings prior to the audit but has since started engaging more frequently with it.

The role of the Department of Housing, Local Government, Planning and Public Works and the councils themselves

As the lead department for local governments, the Department of Housing, Local Government, Planning and Public Works (the department), has a role in providing advice to councils on managing risks – to ensure they comply with the requirements of the *Local Government Act 2009* (or equivalent) and associated regulations. These include cyber security risks, but the department does not have the requisite skills to provide specialist advice to councils regarding cyber response and recovery. It can do more to raise awareness and connect the councils with CSU.

Local governments could also consider establishing agreements with neighbouring councils to increase their access to expertise in the event of a cyber-related crisis. This can be a cost-effective solution for smaller, regional, or remote councils that cannot afford to have in-house cyber security expertise or access it externally.

Recommendation 14

We recommend the Department of Housing, Local Government, Planning and Public Works increases local governments' knowledge of available support by partnering with CSU to:

- increase local governments' awareness of CSU's services and communities of practice (for sharing cyber threat intelligence) through its existing channels
- increase local governments' awareness of CSU's incident response capabilities and services in the event of a cyber incident
- encourage local governments to establish agreements with neighbouring councils to increase access to the required capabilities in the event of a cyber-related crisis.

Appendices

A.	Entity responses	31
B.	Audit scope and methods	36
C.	Better practice frameworks	38
D.	Other legislative requirements	39
E.	Cyber response and recovery governance checklist	41
F.	Role capability checklist	43
G.	Glossary	46

A. Entity responses

As mandated in Section 64 of the *Auditor-General Act 2009*, the Queensland Audit Office gave a copy of this report with a request for comments to:

- the Queensland Government Cyber Security Unit within the Department of Transport and Main Roads
- the Department of Housing, Local Government, Planning and Public Works.

Excerpts of relevant sections were provided to the 3 public sector entities we audited. Due to the sensitivity of the findings and possible security implications, these entities were not named in this report.

This appendix contains the responses we received.

The heads of these entities are responsible for the accuracy, fairness, and balance of their comments.

Comments received from Director-General, Department of Transport and Main Roads

Queensland Government

Office of the
Director-General

Department of
Transport and Main Roads

Our ref: DG46179

Your ref: PRJ03885

26 April 2024

Mr Brendan Worrall
Auditor-General
Queensland Audit Office
qao@qao.qld.gov.au

Dear Mr Worrall

Thank you for your email of 15 April 2024 about the proposed report to parliament, 'Responding to and recovering from cyber attacks'.

The Department of Transport and Main Roads (TMR) acknowledges the recommendations raised in the report and has agreed to all recommendations, providing responses focused on opportunities to raise core preparedness and response capabilities sector wide.

TMR appreciates the opportunity provided to comment on this proposed report; enclosed is the document with the comments.

If you require further information, please contact

Yours sincerely

Sally Stannard
Director-General
Department of Transport and Main Roads

Enc (1)

1 William Street Brisbane
GPO Box 1549 Brisbane
Queensland 4001 Australia

Telephone +61 7 3066 7316
Website www.tmr.qld.gov.au
ABN 39 407 690 291

Responses to recommendations

Queensland Audit Office
Better public services

Department of Transport and Main Roads

Responding to and recovering from cyber attacks

Response to recommendations provided by CSU on 19/04/2024

Recommendation	Agree/ Disagree	Timeframe for implementation (Quarter and financial year)	Additional comments
We recommend that the Department of Transport and Main Roads – Cyber Security Unit:	Agree	Q2 2024/5	CSU will develop and publish a Cyber Security strategy.
7. improves awareness of its products and services and enhances its guidance for developing incident response plans by • developing and publishing its strategic plan • creating greater awareness of its role and responsibilities and the services it offers • refreshing its incident management guideline to reflect current better practice frameworks and guidelines and enhancing it with practical examples (such as playbooks) for a range of common cyber incident scenarios.			CSU will enhance management of its product portfolio to improve awareness of our services amongst key stakeholders. CSU will refresh the IM guideline as part of the IS18 Information Security Policy review currently underway.
8. assists public sector entities in conducting cyber simulations by • supporting them in testing their incident response plans • where practical, involving external experts, to ensure they become sufficiently familiar with the information and communication technology (ICT) in public sector entities.	Agree	Q2 2024/5	CSU will enhance its current exercising capability to facilitate individual entity testing of Incident Response plans. CSU will where appropriate, include Government's external Incident Response partners in exercises.
9. increases public sector cyber skills and capabilities through • developing or adopting a cyber security capability framework that public sector entities can apply • developing or adopting tools to assist public sector entities in understanding their capability gaps • coordinating delivery of a training program that addresses identified capability gaps.	Agree	Q4 2024/5	CSU will develop a workforce strategy that will outline the approach for adoption of a holistic core cyber skills matrix and promote analysis of cyber skill gaps within agencies. CSU will continue to source training for gaps where **common requirement exist.**

1

Queensland Audit Office
Better public services

Recommendation	Agree/ Disagree	Timeframe for implementation (Quarter and financial year)	Additional comments
10. improves the maturity of information security management systems by • working to understand root causes and challenges preventing entities from progressing and improving their information security management systems • amending policy requirements to require public sector entities to test their incident responses through cyber security simulations • continuing to encourage all public sector entities' application of the Queensland Government Information Security Policy (IS18:2018) or an equivalent better practice framework.	Agree	Q4 2024/5	CSU will continue to support maturity improvement in ISMS implementation in the public sector entities, including promotion of an active risk management approach, and pathways to ISO 27001 certification for critical business systems where it is deemed appropriate. The IS18 review will consider incorporating measures for the effectiveness of incident response and the role that cyber security simulations play. CSU will continue to promote best practice governance to all stakeholders including increasing the visibility of current and future guidance through the review of the IS18 policy.
13. shares cyber threat intelligence and lessons learnt by • developing and distributing a process for entities to share cyber threat intelligence from incidents, in a consistent format • engaging with public sector entities (including statutory bodies, government owned corporations, and local governments) to raise awareness of communities of practice and to promote sharing of cyber threat intelligence • using its unique position to compile and share examples of better practice templates and guidance, such as playbooks.	Agree	Q4 2024/5	CSU will enhance where necessary, its existing Cyber Threat Intelligence and Incident Response capabilities to ensure proactive quality intelligence sharing. CSU will continue to promote the benefits of threat intelligence sharing across all stakeholder engagement channels including communities of practice. The IS18 review will consider options for sharing better practice guidance including appropriate access to operational playbooks and Post Incident Reviews for **high severity incidents.**

2

Comments received from Director-General, Department of Housing, Local Government, Planning and Public Works

Your reference: PRJ03885
Our reference: MN04722-2024

Queensland Government

7 May 2024

Office of the
Director-General

Department of
Housing, Local Government, Planning and Public Works

Mr Brendan Worrall
Auditor-General
Queensland Audit Office
qao@qao.qld.gov.au

Dear Auditor-General

Thank you for your correspondence of 15 April 2024 regarding the draft report titled *Responding to and recovery from cyber attacks*, and for providing the Department of Housing, Local Government, Planning and Public Works (the department) with an opportunity to review the report.

I acknowledge the importance of ensuring that all public sector entities, including Queensland's councils, are as well prepared as possible to prevent, respond to and recover from cyber security attacks.

I note the report makes 14 recommendations with Recommendation 1-6 relating to all public sector entities and one recommendation specifically for the department (Recommendation 14), which is focused on the department's role in increasing the knowledge and awareness of the support councils can access regarding cyber attack prevention and response.

I confirm that the department supports all relevant recommendations in the draft report.

The department is currently undertaking a number of activities related to the relevant recommendations and specifically regarding Recommendation 14, and will engage with the Cyber Security Unit in the Department of Transport and Main Roads during 2024-25 to identify further opportunities to collaborate to support council awareness.

If you require further information or assistance in relation to this matter, Department of Housing, Local Government, Planning and Public Works can be contacted on

Yours sincerely

Mark Cridland
Director-General

1 William Street
Brisbane Queensland 4000
GPO Box 806 Brisbane
Queensland 4001 Australia

B. Audit scope and methods

Performance engagement

This audit has been performed in accordance with the *Auditor-General Auditing Standards*, incorporating, where relevant, the standards on assurance engagements issued by the Auditing and Assurance Standards Board. This includes the Standard on Assurance Engagements ASAE 3500 *Performance Engagements*. This standard establishes mandatory requirements, and provides explanatory guidance for undertaking and reporting on performance engagements.

Audit objective and scope

The objective of the audit was to assess public sector entities' preparedness to respond to and recover from cyber security incidents.

The audit addressed the objectives through the following sub-objectives and criteria:

Sub-objective 1:	**To evaluate the effectiveness of strategies and guidance supporting the management and coordination of cyber security response and recovery capabilities across state and local government.**
Criteria 1.1	Lead agencies establish strategies and procedures that enable and support entities to effectively manage and coordinate cyber security response and recovery capabilities.
Sub-objective 2:	**To evaluate selected entities' level of preparedness to respond to and recover from cyber security incidents.**
Criteria 2.1	Entities develop, implement, and maintain risk-based strategies and plans to effectively identify and respond to cyber security incidents.
Criteria 2.2	Entities can effectively isolate cyber security incidents to restore capabilities or services that were impaired, capturing lessons learnt through reporting.

The entities we audited

The entities subject to this audit included:

- the Department of Transport and Main Roads, specifically the Cyber Security Unit (formerly within the Department of Communities, Housing and Digital Economy) – is responsible for setting cyber security policy and guidance for Queensland Government departments and statutory bodies, and providing assistance to government owned corporations and local governments
- the Department of Housing, Local Government, Planning and Public Works (Local Government was formerly within the Department of State Development, Infrastructure, Local Government and Planning) – regulates the local government sector, including councils' corporate governance, and administers the local government legislation and the sector's funding program. It aims to build council capability and grow a positive council culture of strong, accountable decision-making and financial management.

We also audited 3 public sector entities (state and local government entities). We do not want to compromise the security of these 3 entities by publicly identifying their security vulnerabilities, so we have not named them in this report.

We acknowledge the 3 entities have different levels of resourcing and capability for managing cyber security risks. We use the term 'entities' in this report to refer broadly to all Queensland public sector entities (departments, statutory bodies, and government owned corporations) and local governments.

Exclusions from the scope of the audit

As part of the audit, we did not:

- assess prevention of cyber security incidents
- undertake exhaustive technical analysis on the adequacy of detailed processes used to detect and respond to cyber incidents
- assess the quality of technical advice provided to entities in the event of an incident.

Audit methods and approach

The audit was conducted from May 2023 to January 2024 and consisted of:

- field interviews and site visits
- documentation analysis
- data analysis
- cyber security simulations led by our subject matter experts.

Field interviews and site visits

We conducted interviews with key officials, staff, and stakeholders from:

- the Department of Transport and Main Roads, specifically the Cyber Security Unit (formerly within the Department of Communities, Housing and Digital Economy)
- the Department of Housing, Local Government, Planning and Public Works (Local Government was formerly within the Department of State Development, Infrastructure, Local Government and Planning)
- 3 additional public sector entities.

Document review

We obtained and reviewed relevant documents from the entities involved in the audit. This included legislation, strategic plans, annual plans, guidelines, correspondence, performance reports, reviews, and evaluations. We also considered research from other jurisdictions and academia.

Data analysis

We analysed data from:

- the Cyber Security Unit's training attendance records
- audited entities' incident reporting systems.

Subject matter experts

We engaged a team of subject matter experts in cyber incident response to assist in the audit. The team provided advice to the Queensland Audit Office on the assessment of entities' strategies and plans against better practice frameworks. The team also conducted cyber security simulations, which assessed:

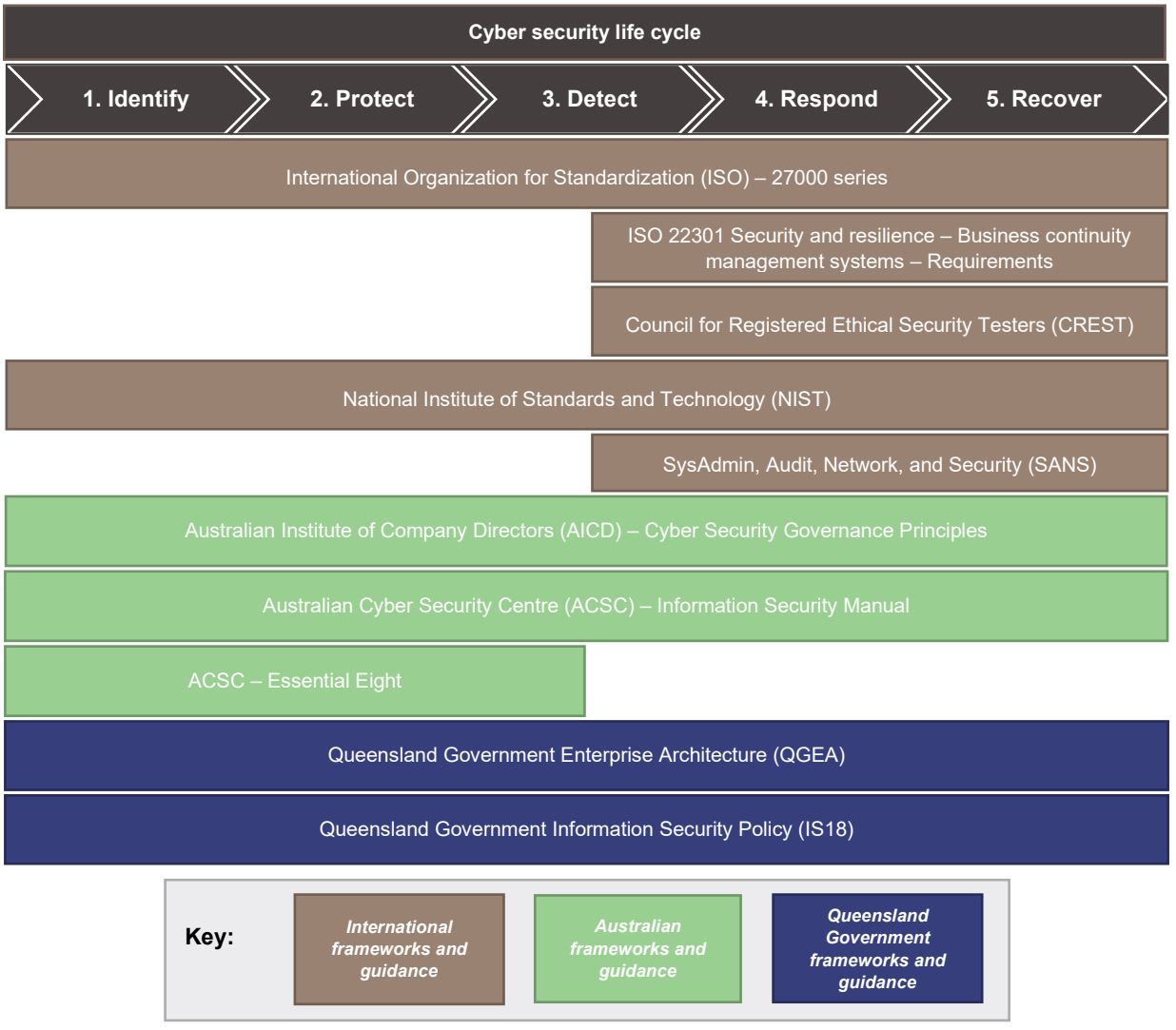
- technical skillsets, capabilities, and capacities for detecting, containing, and eradicating cyber incidents
- responses to a complex cyber incident, including communication and escalation of decision-making
- recovery from, reporting, and learning from an adverse event.

C. Better practice frameworks

Figure C1 shows a range of international, Australian Government, and Queensland Government frameworks, policies, and guidance that entities could consider in developing strategies and plans for cyber incident response and recovery. These are mapped to the various phases of the cyber security life cycle.

The Cyber Security Unit primarily references requirements and guidance within the ISO 27000 series, but public sector entities can select other frameworks for managing incident response and recovery.

Figure C1
Better practice cyber security frameworks



Source: Queensland Audit Office.

D. Other legislative requirements

Cyber incident reporting and response obligations

Public sector entities, including local governments, deliver a broad range of services. In Chapter 3, we refer to the specific 'core' Queensland legislative and policy requirements for these entities. In addition to these, due to the nature of the services some Queensland public sector entities provide, they must also comply with 'other' state and commonwealth requirements. Figure D1 shows the other key legislative obligations specific to cyber incident response for Queensland public sector entities, as reported by the Cyber and Infrastructure Security Centre, within the Department of Home Affairs (Commonwealth).

Figure D1
Other legislative requirements for cyber incidence response

Requirement and Act	Description	Applicable to
Personal information data breach obligations *Privacy Act 1988* (CWTH) and *Information Privacy Act 2009* (QLD)	Requirement to notify affected individuals, the Office of the Australian Information Commissioner (OAIC), and Office of the Information Commissioner Queensland (OIC) when a data breach is likely to result in serious harm to an individual whose personal information is involved. Requirement to conduct a reasonable and expeditious assessment of a suspected eligible data breach, taking all reasonable steps to ensure that this assessment is completed within 30 days.	May apply to any public sector entity that meets thresholds under the legislation.
Obligation to report cyber security incidents *Security of Critical Infrastructure Act 2018* (CWTH)	Obligation for an entity holding or operating critical infrastructure (services that are essential for everyday life, such as energy, communications, water, transport, and health, as defined by the *Security of Critical Infrastructure Act 2018*) to report a cyber security incident to the Australian Signals Directorate.	Applicable to those entities holding critical infrastructure as defined under the legislation. May include departments, statutory bodies, government owned corporations, or local governments.
Obligation to undertake a vulnerability assessment *Security of Critical Infrastructure Act 2018* (CWTH)	The Secretary of the Department of Home Affairs may give a notice requiring an entity holding a System of National Significance* (SoNS) to undertake a vulnerability assessment within a specified period.	Any entity holding critical infrastructure declared a System of National Significance (SoNS) as directed by the Minster for Home Affairs. May include departments statutory bodies, government owned corporations, or local governments.
Obligation to provide systems information *Security of Critical Infrastructure Act 2018* (CWTH)	The Secretary of the Department of Home Affairs may give a notice requiring an entity holding a SoNS to provide systems information. This notice can be in relation to periodic reporting of system information or in response to a specific event.	
Obligation to have incident response plans *Security of Critical Infrastructure Act 2018* (CWTH)	Obligation for entities holding a SoNS to have a written cyber security incident response plan detailing how the entity will respond to cyber security incidents that affect its systems.	

Requirement and Act	Description	Applicable to
Obligation to test an incident response plan *Security of Critical Infrastructure Act 2018* (CWTH)	Obligation for entities holding a SoNS to test preparedness, mitigation, and response capabilities to reveal whether existing resources, processes, and capabilities of an entity sufficiently safeguard being impacted by a cyber security incident.	Any entity holding critical infrastructure declared a System of National Significance (SoNS) as directed by the Minster for Home Affairs. May include statutory bodies, government owned corporations, or local governments.
Obligation to report to Australian Securities and Investments Commission (ASIC) *Corporations Act 2001* (CWTH)	Obligation to submit notifications about 'reportable situations' (which may include among other matters significant data breaches) to ASIC within 30 calendar days via the ASIC Regulatory Portal.	Government owned corporations who operate an Australian financial services licence.
Obligation to report to the Australian Digital Health Agency *My Health Records Act 2012* (CWTH)	Obligation to notify the Australian Digital Health Agency of any potential or actual data breaches that relate to the *My Health Record* system.	Any entity holding healthcare-related data which relates to the *My Health Record* system. May include departments or statutory bodies.

Note: * Systems of National Significance are a subset of critical infrastructure assets. They are considered to be of the highest criticality by virtue of their interdependencies across sectors and potential impact to other critical infrastructure assets and sectors if disrupted.

Source: Queensland Audit Office based on Cyber Security Obligations for Corporate Leaders by the Cyber and Infrastructure Security Centre.

E. Cyber response and recovery governance checklist

Those charged with governance (such as executive management, boards, and councillors) of public sector entities, including local governments, have an important role to play in cyber response and recovery effectiveness. This includes, but is not limited to:

- confirming entities are well prepared prior to incidents occurring
- seeking updates and supporting management during an event
- contributing to key decisions such as when to seek external assistance, when to shut down and contain systems, when to then restore, and how to handle ransom demands if they are made
- endorsing escalation points and internal and external communications
- endorsing reporting to relevant authorities (for example, to CSU and/or the Australian Cyber Security Centre), depending on the incident and the requirements.

We have created a checklist of key questions for those charged with governance of public sector entities to consider with respect to cyber security incident response and recovery.

Figure E1
Cyber response and recovery governance checklist

Area	Detailed question	Have we considered?
Clarify compliance requirements	Are we required to comply with the Queensland Government's IS18:2018 information security policy? If not, should we voluntarily adopt it?	
	Should we be ISO 27001-certified for all our key systems that have significant cyber risk? What do we need to improve to be certified?	
Determine adequacy of strategies and plans	When did we last test our entity's incident response policies, plans, and procedures against best practice frameworks? Who was involved, what did we learn, and did we implement all the lessons learnt?	
	Have we identified all of the critical systems and information assets our entity holds that are susceptible to the risk of being exploited? Are they captured within our plans?	
	What scenarios has management tested incident response policies, plans, and procedures against? Are there other scenarios that we need to consider?	
	Have we integrated our cyber risk management, disaster recovery, business continuity, and information asset management processes, at both the organisational and whole-of-government levels (if applicable)?	
Clarify communication plans and reporting obligations	Does management have communication plans with prepared, consistent, and endorsed templates for a range of cyber scenarios that cater for internal and external stakeholders?	
	Are we clear on our escalation points within our incident response plans and on our reporting obligations during an event?	

Area	Detailed question	Have we considered?
	Do we have an alternative communications channel in the event email and telephone services are not available during the incident?	
Build or access capabilities needed to respond and recover	Have we done an assessment of the capabilities and toolsets our entity needs to respond to and recover from cyber incidents?	
	Based on that assessment, how well placed is our information technology team to respond to and recover from cyber incidents? Does management have a workforce plan to acquire or have access to the required skillsets and capabilities for cyber incident response and recovery?	
	What percentage of the required capabilities is internal versus external? Have we tested the external capabilities?	
Obtain assurance over third-party arrangements	How have we gained assurance that cyber security controls within outsourced management information systems and assets are operating effectively?	
	Have we tested our third-party arrangements for external capabilities to ensure that they will be available, familiar with our information system environments, and have the capabilities we require in a time of need?	
Develop a cyber-resilient culture	What mandatory training, penetration testing (simulated cyber attacks), phishing email testing, and other cyber resilience activities is management performing to raise awareness?	
	Are we contributing to and taking advantage of shared cyber threat intelligence and cyber incident learnings within the sector?	
Use existing public sector cyber expertise	How are we taking advantage of existing public sector cyber expertise (such as the Australian Cyber Security Centre and the Queensland Government Cyber Security Unit) and other entities within the sector to contribute to, promote, and share cyber threat intelligence?	
	Can our entity benefit from partnering with other public sector entities for collective research, investments, and buying power for cyber incident response technology, capabilities, and cyber insurance?	
Clarify cyber insurance details	Do we have cyber insurance and what is included? Are ransoms or extortion threats included or excluded from the policy?	
	At what stage in an incident response do we have to notify the insurer? Do we have to use the insurer's panel of nominated cyber consultants?	
	If the insurance policy specifies that we must use its panel of cyber consultants, have we tested working with them? Are they familiar with our information technology environment?	

Source: Queensland Audit Office.

F. Role capability checklist

In Chapter 4, we discussed the need for entities to undertake assessment of cyber capability. We have provided an example framework modelled after the people, processes, technology (PPT) framework and the key technical and non-technical capabilities required for cyber incident response and recovery. The framework is based on the work of Bruce Schneier, who is an academic and a world expert on cyber security.

The PPT framework helps build systems that effectively balance and coordinate how people, processes, and technology support each other. All 3 elements need to work for effective cyber incident response and recovery. If one aspect is weak or not aligned with the others, it can affect the overall efficiency and effectiveness of the cyber response.

The table below can be used by entities to map where they do or do not hold relevant capabilities across their people, processes or through technology. Entities should also understand whether these capabilities are internal or external, and when they were last tested. Definitions for each of the below capability areas are included in Figure F2.

Figure F1
Role capability checklist using the people, processes, technology framework

Team	Capability area	Internal/ external	People	Process	Technology
Non-technical related teams	Communications				
	Crisis management				
	Executive leadership team and/or those charged with governance				
	Human resources				
	Incident response officer				
	Legal				
	Privacy and data governance				
Information and communications technology teams	Applications				
	Cloud				
	Endpoints and infrastructure				
	Identity access management				
	Network				
	Operating system				
	Service desk				
Specialised technical teams	Cyber threat intelligence				
	Digital forensics				
	Operational technology				
	Penetration testing				
	Physical security				
	Security operations centre				

Source: Queensland Audit Office based on Bruce Schneier's people-process-technology framework.

Figure F2
Capability area definitions

Term	Definition
Communications team	The communication team's role in incident response is to communicate information related to the cyber incident to the organisation's employees, customers, suppliers, media, and the public. It is responsible for having adequate, consistent communication means available and for being transparent with external and internal stakeholders. The communications team usually works closely with the human resources team and legal team to save and restore trust in the entity.
Crisis management team	The crisis management team (CMT) or cyber incident response team (CIRT) is a team of professionals that are adept in disaster management, situational analysis, coordination, and response planning for extreme cyber events. In an extreme event, the CMT/CIRT becomes responsible for coordinating and managing an entity's responses. The composition of a CMT/CIRT varies based on an entity's size and available skills and resources (including third-party vendors that either manage ICT systems/applications or external incident response providers).
Executive leadership team and/or those charged with governance	Significant cyber incidents may require the formation of the executive leadership team (ELT) and/or those charged with governance (TCWG) to provide strategic oversight, direction, and support to the CMT, with a focus on: • identifying and managing strategic issues • engaging and communicating with stakeholders (including the board, councillors, and ministerial liaison, if applicable) • managing resource and capability demand (including urgent logistics or finance requirements and human resources considerations during the response effort). The composition and roles of the ELT or TCWG may vary depending on the incident impacts and size and structure of the organisation and the required experience for decision-making.
Human resources team	Human resources, in the context of incident response, assist in matters concerning insider threats (see 'insider privilege abuse' in Appendix G) or other human aspects of a cyber incident. This could include data exposure of employees, handling interviews with employees, and managing staff surge capacity and wellbeing in the prolonged event.
Incident response officer	A cyber security expert with the skills to rapidly address cyber security incidents within an organisation. In the role of a first responder, they use a host of tools to find the root cause of a cyber security incident, limit the damage, and significantly reduce the likelihood of it occurring again.
Legal team	Legal counsel or legal teams may be required in incident response scenarios to understand potential legal ramifications or compliance obligations, such as breaches in privacy legislation. Legal officers are also often involved with the administration of insurance for entities.
Privacy and data governance team	The team responsible for maintaining a digital asset (or data asset) inventory detailing where data is situated, what category of data is related to a specific location, and what the encryption level is. If an incident involves data, the privacy and data governance team is responsible for understanding any business risks and privacy risks related to this data, and for handling such risks.
Applications	An application is a software program or group of software programs designed for end users. Examples of an application include a word processor, a spreadsheet, an accounting application, a web browser, or an email client. This contrasts with system software, which is mainly involved with running the computer.

Term	Definition
Cloud	Cloud computing is a model for enabling, convenient, on-demand network access to a shared pool of computing resources (for example networks, servers, storage, applications, and services) that can be rapidly configured and released with minimal management.
Endpoints and infrastructure	A personal computer, personal digital assistant, smart phone, or removable storage media (for example a USB flash drive or external hard drive) that can store information. All these endpoints communicate through the network server – a computer that provides services to users or other systems, for example a file server, email server, or database server.
Identity and access management	The process used in businesses and organisations to grant or deny employees and others authorisation to secure systems.
Network	The infrastructure used to carry information between workstations and servers or other network devices.
Operating system	System software that manages hardware and software resources and provides common services for executing various applications on a computer.
Service desk	Service desk teams respond to minor or moderate incidents and maintain communication with users and stakeholders. They use their service management platform to assist in following adequate processes, triaging and documenting the incident, and maintaining contact with end users who are reporting incidents.
Cyber threat intelligence	Information that helps organisations better protect against cyber incidents by providing an understanding of current and emerging threats and vulnerabilities. It can incorporate recent threat actor behaviours, and successful remedial procedures, tools, and techniques.
Digital forensics	Capabilities that enable incident responders to investigate the source, entry point, and extent of a cyber incident or data breach.
Operational technology (OT) team	A team of specialists that understand data from operational technology (programmable systems or devices that interact with the physical environment) monitoring solutions, assist with reconfiguring or rerouting OT equipment, and understand software related to the OT environment. The OT team maintains an updated and precise inventory of asset specifications (for example IP addresses and data flow) and physical location. It is also tasked with backing up systems and maintaining disaster recovery versions.
Penetration testing	Simulated cyber attacks to evaluate the security of a system and identify its exploitation risks to gain access to systems and data.
Physical security	Physical security, in the context of incident response, physically secures information assets and systems by making them inaccessible. The information assets could include swipe card access for lockable doors, security cameras monitored by a security team, or lockable cabinets for paper records.
Security operations centre (SOC)	The focal point for security operations and computer network defence for an organisation. The SOC defends and monitors an organisation's systems and networks (that is, cyber infrastructure) on an ongoing basis. The SOC is also responsible for detecting, analysing, and responding to cyber security incidents in a timely manner. This may not be located within an organisation.

Sources: Queensland Audit Office from Australian Signals Directorate and the National Institute of Standards and Technology.

G. Glossary

Term	Definition
Business continuity plan	A plan which outlines how an organisation's critical business functions will either – continue to operate despite serious incidents or disasters that might otherwise have interrupted them; or will be recovered to an operational state within a reasonably short period.
Communities of practice – Cyber Security Unit	CSU's communities of practice aim to raise awareness of information security and develop and share information, methods, and tools to create a knowledge base for public sector entities, including local governments.
Cyber communication plan	A plan which outlines an entity's approach to communicating with internal and external stakeholders in the event of a cyber incident.
Cyber incident	An unwanted or unexpected cyber security event or series of such events that have a significant probability of compromising business operations.
Cyber resilience	The ability to adapt to disruptions caused by cyber security incidents while maintaining continuous business operations. This includes the ability to detect, manage, and recover from cyber security incidents.
Cyber security	A process for protecting an entity's information by preventing, detecting, and responding to cyber incidents. Such attacks could be through breaches of physical and network security, or through using information obtained through social networks.
Cyber security simulations	Workshops to test how key incident response personnel (both technical and non-technical) respond to a cyber incident within their information systems or networks. Simulations can help identify vulnerabilities, assess risks, and improve security measures.
Cyber threat intelligence	Information that helps organisations better protect against cyber incidents by providing an understanding of current and emerging threats and vulnerabilities. It can incorporate recent threat actor behaviours, and successful remedial procedures, tools, and techniques.
Denial of service attacks	A malicious, targeted attack that floods a network with false requests to disrupt business operations.
Digital forensics	Capabilities that enable incident responders to investigate the source, entry point, and extent of a cyber incident or data breach.
Exploitation risk	The likelihood and the impact of a threat actor (refer to definition below) intentionally exploiting a weakness in a system, causing disruptions or losses.
Incident response plan	A plan which outlines the activities undertaken to support an effective response and prompt recovery in the event of a cyber security incident.
Information asset	A collection of data that is recognised as having business value and enables an entity to perform its business functions.
Information security management system (ISMS)	A system that preserves the confidentiality, integrity, and availability of information by applying a risk management process. It gives confidence to interested parties that risks are adequately managed.
Insider privilege abuse (insider threats)	Internal actors, such as current or former employees, who can pose a threat to an organisation because they have direct access to the company network, sensitive data, and intellectual property (IP), as well as knowledge of business processes, company policies, or other information that would help carry out such an attack.

Term	Definition
IS18:2018	The Queensland Government Information Security Policy (IS18:2018) aims to ensure all departments apply a consistent, risk-based approach to the implementation of information security to maintain confidentiality, integrity, and availability. While IS18:2018 only applies to departments defined under the *Public Sector Act 2022*, all statutory bodies should be aware of and consider implementing the policy. Local governments and government owned corporations can also consider it and whether it is suitable for their needs.
ISO 27000 series	A set of standards for establishing an information security management system (ISMS) and underlying controls. It not only includes a large library of technical controls but also requires entities to commit to maintaining a culture of cyber safety and resilience.
ISO 27001 certification	An international certification that demonstrates to stakeholders and customers that an entity is committed to and able to manage information securely and safely based on ISO 27001 *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*.
Machine learning	A type of artificial intelligence which is focused on teaching computers to learn from data.
Malware	Malware is any software used to gain unauthorised access to IT systems to steal data, disrupt system services, or damage IT networks in any way.
National Institute of Standards and Technology (NIST) Cyber Security Framework	A risk-based approach to managing cyber security risk that reinforces the connection between business drivers and cyber security activities.
Phishing	Phishing refers to online scams enticing users to share private information using deceitful or misleading tactics.
Playbooks	Incident response procedures for a particular incident type. Examples could include ransomware, insider privilege abuse, social engineering, denial of service attacks, malware, and phishing.
Public sector entities	In this report, this refers broadly to all Queensland public sector entities (departments, statutory bodies, and government owned corporations) and local government entities.
Ransomware	Ransomware is a type of malware (refer to definition above) identified by specified data or systems being held captive by attackers until a form of payment or ransom is provided.
Social engineering	Social engineering is a term that describes cyber attacks that use psychological tactics to manipulate people into taking a desired action, like giving up confidential information. Social engineering attacks work because humans can be compelled to act by powerful motivations, such as money, love, and fear. Adversaries play on these characteristics by offering false opportunities to fulfill those desires.
Threat actor	Any person or organisation that intentionally exploits weaknesses in computers, networks, and systems to disrupt individuals or organisations.

qao.qld.gov.au/reports-resources/reports-parliament

qao.qld.gov.au/contact-us

T: (07) 3149 6000
E: qao@qao.qld.gov.au
W: www.qao.qld.gov.au
53 Albert Street, Brisbane Qld 4000
PO Box 15396, City East Qld 4002

Queensland Audit Office
Better public services