



Engage



Respect



Inspire



Deliver

Briefing for audit committee chairs

3 December 2024

Acknowledgement of country

I begin today by respectfully acknowledging the Yugara and Turrbal People who are the Traditional Owners of the land on which this event is taking place, and Elders past and present.

I also recognise those whose ongoing effort to protect and promote Aboriginal and Torres Strait Islander cultures will leave a lasting legacy for future Elders and leaders.

Welcome



Agenda

10:30 am

Welcome

10:35 am–11:00 am

Auditor-General's address

Our forward work plan, upcoming audits, and areas of focus

Rachel Vagg, Auditor-General

11:00 am–11:30 am

Spotlight on cyber security awareness (followed by Q&A)

What to be across in this space, and the tools available to help

Joel Godwin with David Toma and Sumi Kusumo, Senior Directors

11:30 am–11:50 am

An update on climate reporting

Charles Strickland, Senior Director

11:50 am–12:00 pm

Discussion and questions

Darren Brown, Assistant Auditor-General – Performance Audit



Introduction

My role

- 24th Auditor-General started on 12 August
- Queensland public sector experience
- Previous roles in QAO and partnership in a chartered accounting firm



QAO today

- Our role
- Deputy Auditor-General – Patrick Flemming
- Relationship and reporting strategy
- Focus of Senior Directors
- Forward work planning and performance audit program

QAO's forward work plan

Our planning process



Environmental scanning

- Intelligence gathering
- Strategic risk assessment.



Topic development and prioritisation

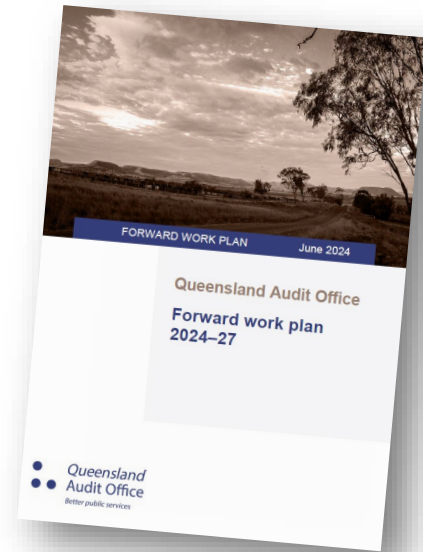
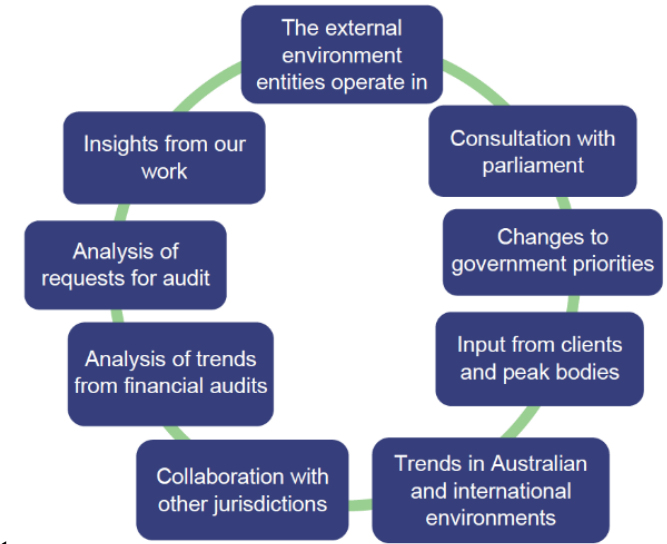
- Topic development and viability assessment
- Topic prioritisation (impact/importance/influence)
- Plan moderation
- Selection of audits for follow-up.



Finalisation and publication

- 42-day draft consultation period required under the *Auditor-General Act 2009*
- Annual publication on QAO's website
- Includes planned topics and focus areas for the forward 3-year period, changes and acquittal of plan.

Sources for intelligence gathering





Reports

Recently tabled and upcoming reports

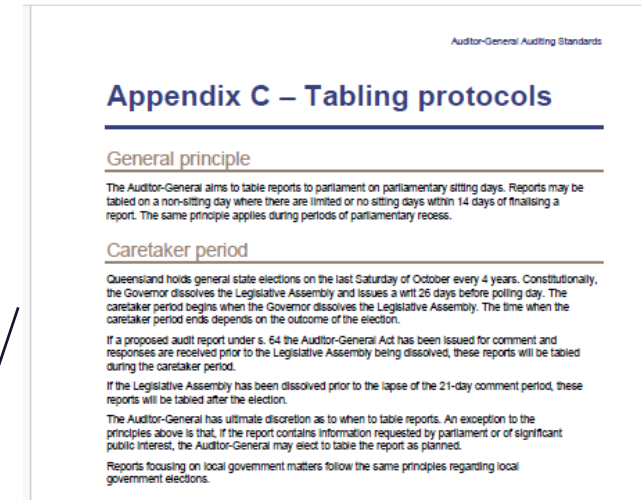
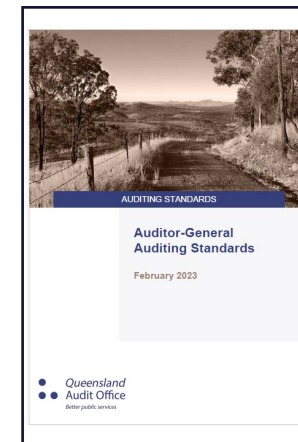
Reports tabled this financial year

- ✓ 2024 Status of Auditor-General's recommendations
- ✓ Delivering forensic medical examinations (follow-up audit)
- ✓ Central agencies' coordination of the state budget



Reports tabling before the end of 2024/early 2025:

- Managing Queensland's regional water quality
- Preparing for the Brisbane Games
- Protecting students from bullying
- Energy 2024
- Health 2024
- Major projects 2024



Caretaker protocols

QAO's forward work plan

Performance audits ahead



Technology risk and opportunities

Tabling 2024–25

- Overseeing the use of artificial intelligence

Tabling 2025–26

- Managing third-party cyber security risks
- Protecting information held by government

Tabling 2026–27

- Defending critical infrastructure from cyber risk



Sustainable communities and environment

- Reducing landfill waste
- Managing regional water quality
- Attracting and retaining teachers in regional and remote Queensland

- Mitigating risk from future floods

- Managing volunteer services
- Planning for liveable communities



Governance of government

- Preparing for the Brisbane Games
- Effectiveness of local government audit committees

- Managing consultants and contractors

- Improving public sector culture
- Lobbying in the QLD Government
- Strengthening government reporting



QAO's forward work plan



Healthy and safe Queenslanders

Tabling 2024–25

- Protecting students from bullying

Tabling 2025–26

- Accessing mental health services
- Reducing road fatalities
- Preventing prisoners from reoffending

Tabling 2026–27

- Ensuring the quality and safety of health services
- Delivering equitable legal aid services



Infrastructure investment

- Transferring risk in infrastructure projects

- Follow-on audit: Licensing builders and building trades

- Ensuring disability access to transport
- Olympics progress review



Economic risk and response

- Attracting industries to Queensland

- Enhancing the sustainability of local governments

- Grants audit (program to be selected)
- Reducing labour and skill shortages

2024 Status of Auditor-General's recommendations report

Status of AG's recommendations



Most common types of recommendations

- Workforce capability and planning
- Information systems and data management
- Governance

Machinery of government changes and internal controls

Machinery of government changes usually result in the transfer of specific functions and legislative responsibilities from one department to another.

Machinery of government changes

Impacts on financial statement preparation

- Movement of key finance staff between departments
- Changes required to financial systems
- Lack of timely access to financial information

Impacts can be wide-ranging

- Changes to organisational structures
- Transfers of employees
- Transfers of assets and liabilities
- Changes to information systems
- Changes to corporate policies and procedures

Helpful resources

Visit our website for a range of resources that can help with managing machinery of government changes.



Blog

[Implementing machinery of government changes](#)



Report to parliament

[Implementing machinery of government changes \(Report 17: 2022–23\)](#)



Better practice guides

[Checklist for managing machinery of government changes](#)
[Implementing machinery of government changes maturity model](#)

Areas of focus

Areas of focus

Some of the topical issues in focus for us include:

- ✓ probity, propriety, and compliance
- ✓ machinery of government changes
- ✓ cyber security and awareness
- ✓ climate reporting.

Helping our clients work more effectively with us:

- Tools and practical resources
- Our blogs and dashboards
- A focus on fostering stakeholder engagement



Home » Reports and resources » Better practice » Fraud risk assessment and planning model

Reports to parliament

Published: November 2023 • Sector: State and local government entities

Status of recommendations

[Download \(XLSX, 188.22 KB\)](#)



Better practice

To effectively manage and identify fraud risks, entities need to examine their business environments to understand their potential exposure to fraud. Their overarching risk management plans need to effectively target and address fraud risks.

Events

Fact sheets

Our fraud risk assessment and planning model gives entities a step-by-step process for self-assessing how they identify fraud risk, control and treat risks, and monitor and report on the risks. It helps entities examine their business environment, develop overarching risk management plans, and conduct their fraud risk assessments in a comprehensive and consistent way.

Interactive dashboards

QAO Queensland dashboard

The model reflects our insights on fraud management from our audit work across entities.

Podcasts

We refreshed the model in 2023 to align with the updated Australian Standard AS/ISO 31000:2018 *Risk management – Guidelines*; Queensland Treasury's *A Guide to Risk Management* (2020); and Australian Standard 8001:2021 *Fraud and Corruption Control*. It supersedes the Queensland Audit Office's original model published in 2018 alongside our report [Fraud risk management \(Report 6: 2017-18\)](#).

We have also refreshed our [Fraud and corruption self-assessment tool](#), which entities can use to identify areas where they can improve their fraud controls and focus resources for detection on high-risk areas.

Discussion and questions





Engage



Respect



Inspire



Deliver

Spotlight on cyber awareness

Joel Godwin with David Toma and Sumi Kusumo, Senior Directors

Responding to and recovering from cyber attacks

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

- assessment of central strategies, guidance, and support available to entities
- preparedness of selected entities to effectively respond and recover.



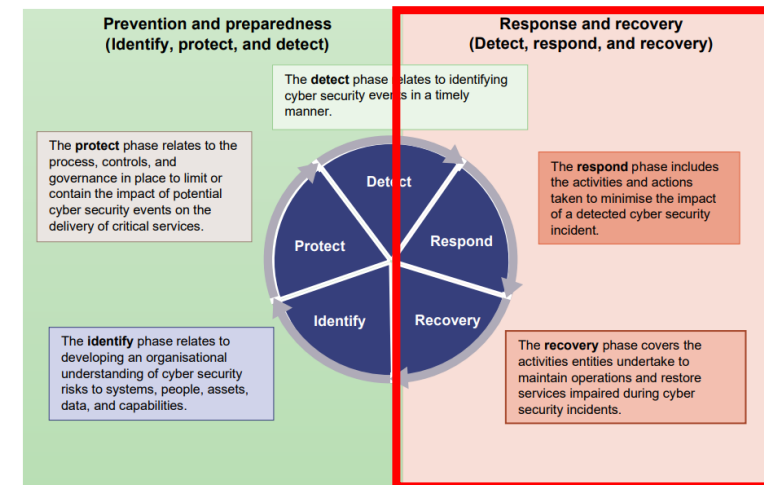
Spotlight on cyber awareness

Who did we audit?

- Queensland Government Cyber Security Unit (Department of Transport and Main Roads)
- Department of Housing, Local Government, Planning and Public Works
- 3 public sector entities with varying sizes and resources.

What did we include in the scope?

- This audit focused on response and recovery elements of the cyber security life cycle – **Detect, Respond, and Recover**
- Our 2018–19 audit, *Managing cyber security risks*, covered the other elements of the life cycle.



Cyber incidents in Queensland and Australia

- Cyber security should be a high priority for all organisations, big or small, public or private.
- Public sector entities are attractive targets given the information they hold.
- Cyber incidents are continuing to increase in frequency and severity, as reported by the Australian Cyber Security Centre (ACSC):

Why is this important?



6 minutes – how often a cyber crime report was submitted in 2023–24, consistent with 2022–23 and up from every 7 minutes in 2021–22 and every 8 minutes in 2020–21.



29% of cyber crimes reported are from Queensland (30% in 2022–23), the highest in Australia.



12% of all cyber incidents affected state and local government entities in 2022–23 (consistent with 2022–23). 37% affected the Australian Government (up from 30% in 2022–23).

Cyber incidents in Queensland and Australia

YEAR IN REVIEW

Sustained disruption of essential systems and associated services	C6	C5	C4	C3	C1	C1
Extensive compromise	C6	6	20	15	1	C1
Isolated compromise	1	57	93	75	46	C2
Coordinated low-level malicious attack	C6	1	6	6	7	3
Low-level malicious attack	1	81	53	60	95	11
Unsuccessful low-level malicious attack	C6	13	20	70	360	28
	Member(s) of the public	Small organisation(s) Sole traders	Medium-sized organisation(s) Schools Local government	State government Academia/R&D Large organisation(s) Supply chain	Federal government Government shared services Regulated critical infrastructure	National security Systems of National Significance

Figure 1: Cyber security incidents by severity category for FY2023–24 (total 1,129)

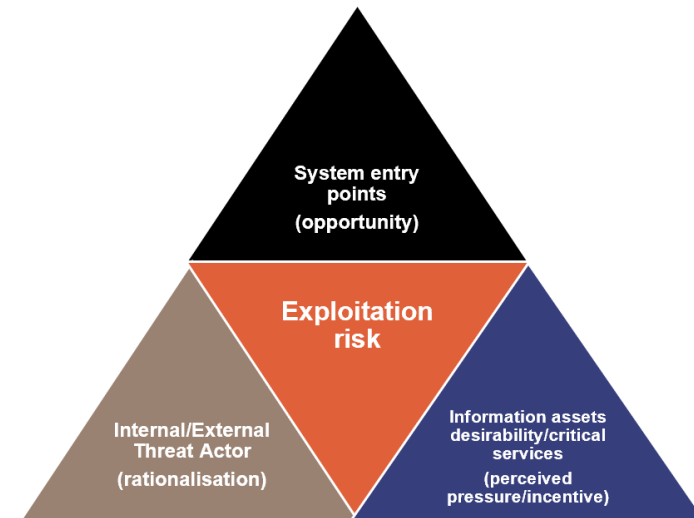
Why is this important?



What did we find?

Finding – Understanding cyber risks in system and information assets

- Entities must understand their systems and information held within them to enable risk identification and adequate planning.
- Two out of the 3 entities we audited did not have an up-to-date or complete listing of systems and information assets held.
- None of the entities had adequately considered management of risks from systems operated by third parties.



Recommendation to all entities (summarised)

- We recommend that all entities maintain an up-to-date register of those systems and information assets that are critical to their operations.
- For those systems, regular risk assessments should be undertaken to identify security concerns, and mitigating strategies put in place.

What questions should we consider as audit committee members?

Finding – Understanding cyber risks in system and information assets

Audit findings



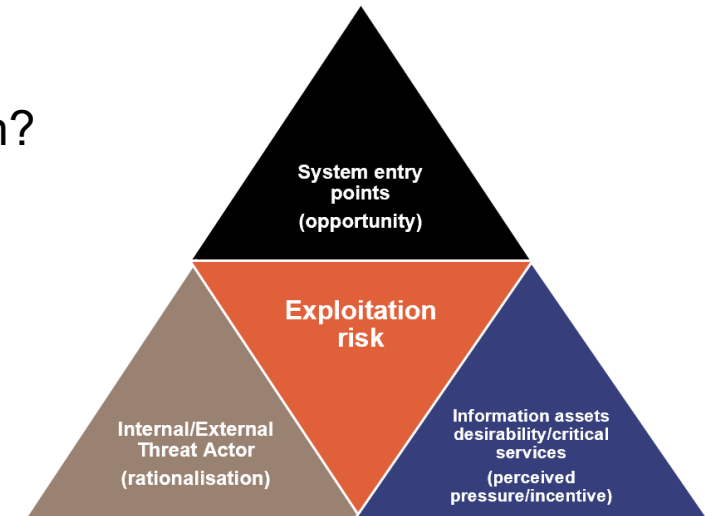
Have we identified all of the critical systems and information assets our entity holds that are susceptible to the risk of being exploited?



Are they captured within our incident response plans?



How frequently are these reviews being undertaken?





Audit findings

What did we find?

Finding – The need for entities to continually improve incident response plans

- Incident response plans are a key document to guide an entity through its response and recovery processes.
- All entities we audited could have had better plans. Key areas for improvement included
 - preparing for a greater range of incidents/scenarios
 - understanding and incorporating insurance arrangements
 - having clarity of roles and accountabilities – including with third parties.

 **Our report includes an overview of better practice approaches**

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.

Recommendation to all entities (summarised)

We recommend that all entities review their incident response plans against better practice frameworks and ensure:

- they integrate with other key plans such as BCPs
- include any relevant insurance requirements
- include playbooks for common risks and cyber incident scenarios
- recognise that accountability for cyber security rests with the chief executive (or equivalent).

Recommendation to the Cyber Security Unit

We recommend that the Cyber Security Unit update its *Incident Management Guideline* and develop a range of playbooks (cyber scenario plans) to better assist entities with their own plans.



What questions should we consider as audit committee members?

Finding – The need for entities to continually improve incident response plans



When did we last assess our entity's incident response policies, plans, and procedures against best practice frameworks?



Has the entity set an appetite for compliance with better practice frameworks?



Who was involved, what did we learn, and did we implement all the lessons learnt? Are they captured within our plans?



Have we integrated our plans with other key corporate documents such as disaster recovery plans and business continuity plans?



Are key elements such as insurance requirements and escalation points to third parties embedded in plans?

What did we find?

Finding – Entities need to regularly test their incident response plans

- Cyber simulations test entities' response to cyber scenarios – they give great intelligence on preparedness, can identify any vulnerabilities in approaches.
- **Only one of the 3 entities we audited had tested its plan** through a cyber simulation or equivalent exercise.
- Simulations were held with each of audited entities as part of the audit. Common themes and lessons from these included
 - importance of documenting key decisions and events as they occur
 - the need to clear decision-making thresholds
 - integrating BCP and other documents into response plans, how will you maintain operations while under attack?
- **Understanding and testing of third-party capabilities were lacking in all entities**, despite a high reliance on these services.

! Cyber incident response needs to be a **business-led process**, it is *not* just a technical exercise

- ✓ Legal
- ✓ Executive
- ✓ Communications
- ✓ IT/Technical
- ✓ Business areas

! Whole-of-government cyber simulations do **not** give entities assurances over their own plans and preparedness

An entity we audited believed that this gave it comfort over its own internal controls and processes, which it does not.

Recommendation to all entities (summarised)

We recommend that all entities test their incident response plans regularly against a variety of different scenarios.

This should incorporate any external parties who are relied upon in the process.

Recommendation to the Cyber Security Unit

We recommend that the Cyber Security Unit assist entities in conducting cyber simulations, including involvement of CSU experts (where relevant).

CSU should also amend policy requirements to mandate testing of incident response plans through cyber simulations.

Audit findings

What questions should we consider as audit committee members?

Finding – Entities need to regularly test their incident response plans



When did we last test our entity level incident response plans?



What scenarios has management tested incident response policies, plans, and procedures against? Are there other scenarios that we need to consider? Are they captured within our plans?



How have/will lessons from these sessions be captured and reflected in our plans?



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?



Audit findings

What did we find?

Finding – Entities need to be better prepared for communications in a cyber incident

- During a cyber incident, entities need to be prepared to release communications to a range of stakeholders – internally (e.g. staff), and externally (e.g. customers, ministers, regulators).
- We found a lack of consistent content ready to assist entities during a cyber attack
 - Most crisis communication plans were in draft.
 - Content was not adequately prepared and ready for use.
 - Thresholds for communications and escalation were not readily defined.

Recommendation to all entities (summarised)

We recommend that all entities improve their crisis communication plans by:

- developing templates and communications for a variety of cyber incident scenarios
- ensuring thresholds for escalation are included within the plan for all stakeholders.



What questions should we consider as audit committee members?

Finding – Entities need to be better prepared for communications in a cyber incident



Audit findings



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 and decision-makers for communications within our incident response plans?



Do we know our reporting obligations during an event?

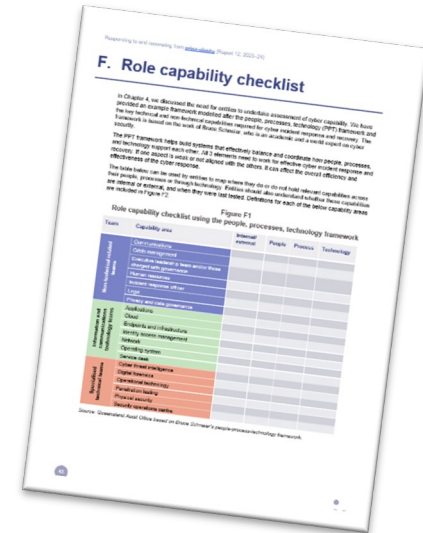


Audit findings

What did we find?

Finding – Identifying, developing, and contracting cyber capabilities

- During a cyber incident, entities may need a broad range of technical and non-technical capabilities.
- While all CIOs of audited entities knew of technical capability gaps, none had done a formal assessment to confirm known gaps and inform development/sourcing through external parties.
- We developed a checklist (see right) to assist agencies in this process.



Recommendation to all entities (summarised)

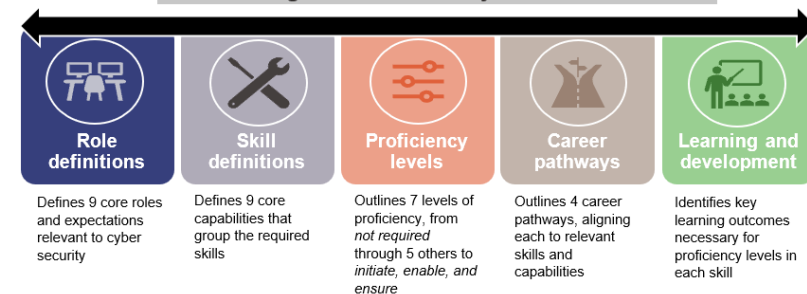
- We recommend that all entities assess and document their cyber capabilities.
- Develop plans to address any gaps (through either training or external sourcing).

Recommendation to the Cyber Security Unit

We recommend that the Cyber Security Unit increases its understanding of public sector capabilities and gaps through:

- developing or adopting a cyber skills framework for entities to apply
- coordinating delivery of a training program which addresses known capability gaps (once understood) across the public sector.

Australian Signals Directorate Cyber Skills Framework



What questions should we consider as audit committee members?

Finding – Identifying, developing, and contracting cyber capabilities



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?



Have we tested any external capabilities we are relying upon?



Do we have access to adequate training to support ongoing development of technical teams and to build broader cyber resilience across the organisation?



Audit findings

What did we find?

Finding – Capturing and sharing cyber intelligence

- Entities understood the importance of sharing intelligence, however weaknesses were found in how each entity captured and shared lessons. This spanned
 - where and how to capture an incident, and how incidents should be assessed
 - tracking and monitoring follow-up activities resulting from an incident
 - knowing what external stakeholders to share information with.
- The importance in taking part of central communities of practice to share and obtain insights

Recommendation to all entities (summarised):

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

Recommendation to the Cyber Security Unit

We recommend that the Cyber Security Unit strengthen its cyber threat sharing by:

- developing a more standardised process for entities to share intelligence
- raising awareness of its communities of practice and similar avenues for sharing
- continuing to promote and share better practice with entities.

What questions should we consider as audit committee members?

Finding – Capturing and sharing cyber intelligence



Are we contributing to and taking advantage of shared cyber threat intelligence and cyber incident learnings within the sector?



Are our teams taking part in government-wide communities of practice?



Do we have adequate internal processes to capture, analyse, learn from, and share intelligence on cyber incidents?

What did we find?

Finding – Creating greater awareness and understanding of central support

- The Cyber Security Unit (CSU) has enhanced its support and capabilities in relation to cyber incident management and other areas of cyber security. This includes
 - establishing a panel of expert providers to assist all entities as required
 - expanding assistance to local governments and GOCs.
- We found the CSU needs to improve awareness of its service offerings and make more information available to entities and the public on its role and services.

Many local governments would benefit from more assistance

- Local governments can be attractive targets given the information assets they hold and the critical services they operate.
- Many councils do not have access to the resources required to effectively respond and recover in a timely manner, and they must consider assistance available through CSU, or through partnering with other local governments to gain access.
- The department of local government needs to better connect councils to these services.

Recommendation to the Cyber Security Unit

We recommend that the Cyber Security Unit develop and publish a strategic plan and create greater awareness of the services it offers.

Recommendation to the department of local government

We recommend that the department of local government works with councils to improve their understanding of supports available to them through CSU, including communities of practice. It should also encourage local governments to collaborate where possible to increase access to specialist skills and capabilities.

What questions should we consider as audit committee members?

Finding – Creating greater awareness and understanding of central support



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)?



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?



How are we keeping across developments and opportunities within the sector?



Audit findings

What did we find?

Finding – Scope and application of IS18

- IS18 is a mandated policy for Queensland Government departments and some statutory bodies.
- The policy states that all statutory bodies must have regard to it – meaning they must consider and document whether the framework applies to their circumstances in setting their own internal controls and policies.
- CSU does not know whether statutory bodies or other entities are applying IS18.
- Government owned corporations and local governments do not have any requirements, but are encouraged to do so.

Recommendation to all statutory bodies

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 to all government owned corporations/local governments

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.

What questions should we consider as audit committee members?

Finding – Scope and application of IS18

-  Are we required to comply with the Queensland Government's IS18:2018 information security policy? If not, should we voluntarily adopt it?
-  What frameworks are we building our strategies and responses against (if not IS18)?
-  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?

Audit findings

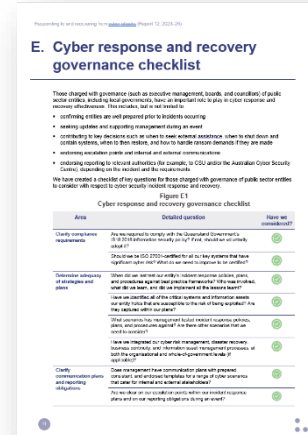


Key resources

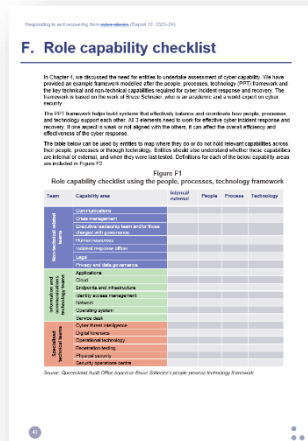
We developed some additional resources as part of this audit to assist entities and those charged with governance:

Cyber response and recovery governance checklist

- Those charged with governance (boards, councillors, executive management, audit committees, etc.) have an important role to play in cyber risk management.
- Checklist of key questions for those charged with governance of public sector entities to consider with respect to cyber security incident response and recovery.
- Two-page document covers a range of key areas TCWG should ask of entities.



Resources for entities



Role capability checklist

- Example framework to help entities identify the people, processes, and technology relevant to cyber response and recovery.
- Entities can map where they do or do not hold relevant capabilities across their people, process, and technology.
- Entities should also understand what is internal vs. external (and when external capabilities were last tested).

We have released our first podcast on this topic – be sure to listen!

Discussion and questions with David Toma, Joel Godwin, and Sumi Kusumo





Engage



Respect



Inspire



Deliver

An update on climate reporting

Charles Strickland, Senior Director

Sustainability/climate reporting

Commonwealth Act now passed

Treasury Laws Amendment (Financial Market Infrastructure and Other Measures) Act 2024

Challenges

- AASB S1 and S2 approved.
- S2 mandatory for certain entities reporting under the Corporations Act.
- Significant governance and reporting change.





Reporting components



Reporting components





Climate reporting



Queensland Treasury is developing a whole-of-government framework and piloting it over the coming months



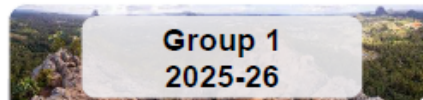
QAO will undertake pre-assurance work over the framework before it is finalised



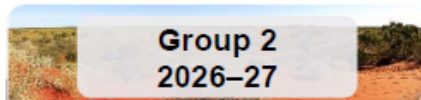
The reporting and assurance commencement dates have not been determined



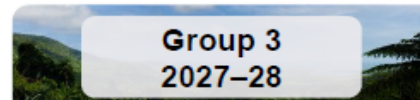
Mandatory reporting groups under *Corporations Act*:



- NGER reporting
- N/A
- 2 or more (consolidated)
Revenue >= \$500 mil.
Assets >= \$1,000 mil.
500 employees



- NGER registered
- \$5 billion assets
- 2 or more (consolidated)
Revenue >= \$200 mil.
Assets >= \$500 mil.
250 employees



- N/A
- N/A
- 2 or more (consolidated)
Revenue >= \$50 mil.
Assets >= \$25 mil.
100 employees

Some controlled entities may be in scope



No mandatory application to unis & LGs (yet)

Illustrative phasing-in of audit requirements

Diagrammatic representation of assurance phasing

Reporting year	1 st *	2 nd	3 rd	4 th	5 th	6 th **
Governance	Limited	Limited	Limited	Reasonable	Reasonable	Reasonable
Strategy – risks and opportunities***	Limited	Limited	Limited	Reasonable	Reasonable	Reasonable
Climate resilience assessments/scenario analysis	None	Limited	Limited	Reasonable	Reasonable	Reasonable
Transition plans	None	Limited	Limited	Reasonable	Reasonable	Reasonable
Risk management	None	Limited	Limited	Reasonable	Reasonable	Reasonable
Scope 1 and 2 emissions	Limited	Reasonable	Reasonable	Reasonable	Reasonable	Reasonable
Scope 3 emissions	N/A	Limited	Limited	Reasonable	Reasonable	Reasonable
Climate-related metrics and targets	None	Limited	Limited	Reasonable	Reasonable	Reasonable

* Group 1 – years commencing 1 January 2025. Group 2 – years commencing 1 July 2026. Group 3 – years commencing 1 July 2027.

** Group 3 is to be subject to reasonable assurance across all disclosures by years commencing 1 July 2030.

*** The phasing for assurance on statements where there are no material climate-related financial risks and opportunities is the same as for 'Strategy – risks and opportunities'.

ED ASSA 5010 Timeline for Audits and Reviews of Information in Sustainability Reports under the *Corporations Act 2001*

Auditing



Understanding impacts

Physical risks

- Rainfall variability
- Extreme weather events
- Sea level rising
- Extreme heat

Transition risk

- Emission controls
- Carbon pricing
- Debt/equity investor demands
- Customer/stakeholder preferences



Action

ARCs should assess their entity's preparedness for complying with AASB S2, but not develop public reports or engage external consultants.

Questions and discussion





Recent reports and resources



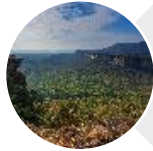
Reports to parliament

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



QAO blog

www.qao.qld.gov.au/blog



Fact sheets

www.qao.qld.gov.au/reports-resources/fact-sheets



Better practice guides

www.qao.qld.gov.au/reports-resources/better-practice



Interactive dashboards

www.qao.qld.gov.au/reports-resources/interactive-dashboards



Audit program

www.qao.qld.gov.au/audit-program



Subscribe for news and updates

www.qao.qld.gov.au/subscribe



Discussion

Presentation slides will be emailed to you and made available on our website

www.qao.qld.gov.au/reports-resources/events

We also welcome your feedback via a short survey: www.surveymonkey.com/r/ACCBDec24





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

To view a copy of this licence, visit <https://creativecommons.org/licenses/by/4.0/>

In essence, you are free to copy, communicate and adapt this presentation, as long as you attribute the work to the State of Queensland (Queensland Audit Office) Briefing for audit committee chairs – 3 December 2024.



© The State of Queensland (Queensland Audit Office) 2024.