



Engage



Respect



Inspire



Deliver

# Briefing for audit committee chairs

5 May 2022

---

● *Queensland*  
● ● **Audit Office**  
*Better public services*

# Agenda

---

## **Welcome**

Damon Olive, Assistant Auditor-General

10.30am–10.50am

## **Considerations and advice as we approach year end**

Michelle Reardon, Senior Director

10.50am–11.05am

## **Forward work plan 2022–25**

Pat Flemming, Assistant Auditor-General

11.05am–11.30am

## **Advice on handling and recovering from a cyber attack**

David Toma, Senior Director

11.30am–11.45am

## **Closing remarks**

Brendan Worrall, Auditor-General

11.45am–12.00pm

## **Discussion and questions**





Engage



Respect



Inspire



Deliver

# Considerations and advice as we approach year end

**Michelle Reardon, Senior Director**

---

# Our reporting outcomes 2020–21

---



Local government



Education



Major projects

to table:





## Insights from across this year's audits

### Current and future challenges

- Sustainability – increasing demand and fiscal constraint
- Continued impact of COVID-19
- Environmental impacts – water and energy
- Major projects on time and within budget
- Machinery of government changes

### Focus areas

- Adapt internal controls for changes in services and workforce
- Reassess assumptions as conditions change – major projects and climate reporting

**Focus areas  
for this year**





# Key internal control findings

Internal controls are generally effective but the same, common weaknesses in internal controls have arisen.

These include entities not:

- securing their information systems
- making independent checks to confirm changes to supplier details
- reviewing payroll reports.

Local governments have the lowest number of unresolved internal control significant deficiencies in 5 years.

Governance continues to require strengthening in some councils: 15 without audit committees, 6 without internal audit functions, and another 6 without internal audit activity.



**Majority relate to information systems controls**

**Significant deficiencies mainly from access controls and fraud prevention and detection**

**Key issues identified**

# Internal control assessment

## Annual internal control assessment

This annual internal control assessment tool aims to help entities understand and evaluate their internal controls. It will identify where they sit on a maturity scale for effective internal controls, and highlight areas for targeted improvement or where a deep dive assessment should be performed.

|                      | Developing | Established | Integrated | Optimised |
|----------------------|------------|-------------|------------|-----------|
| Governance           |            |             | ← ● →      | ★         |
| Culture              |            |             | ← ● →      | ★         |
| Risk management      |            |             | ← ● →      | ★         |
| Financial statements |            |             | ← ● →      | ★         |
| Records management   |            |             |            | ● ★       |
| Information systems  | ← ● →      |             |            | ★         |
| Asset management     |            | ★           |            |           |
| Grants management    |            |             | ← ● →      | ★         |
| Procure-to-pay       |            |             | ← ● →      | ★         |
| Change management    |            | ● ★         |            |           |
| Monitoring           |            |             | ← ● →      | ★         |



Better practice | [www.qao.qld.gov.au/reports-resources/better-practice](http://www.qao.qld.gov.au/reports-resources/better-practice)



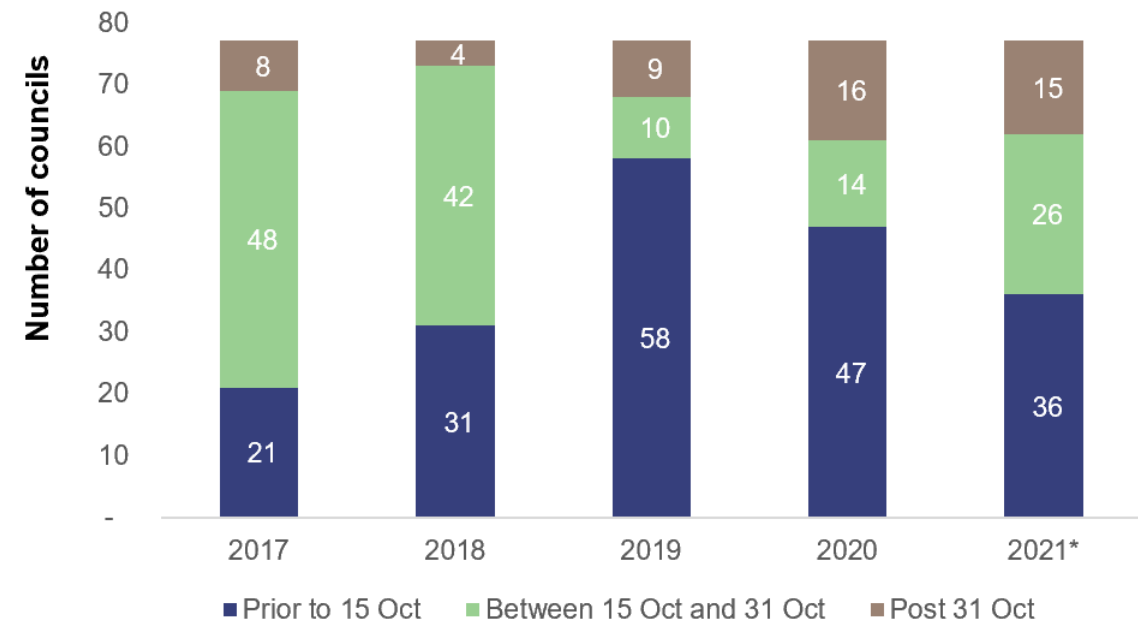
## Overall

- All departments, government owned corporations, most statutory bodies, are all reliable and compliant
- Some local governments have been delayed
- Ongoing delays in tabling state entity annual reports











## Reduced timeliness of council reporting

- Asset valuations
- Retention of staff
- Month-end processes





# Early identification and assessment of financial reporting issues:

-  Impairment of assets – indicators and discounted cash flows
-  Changes to cash generating units
-  Current replacement cost valuation outcomes – assessing, challenging and accounting for valuations
-  Financial instrument and hedge accounting changes
-  Assessment and adoption of key estimates
-  Adoption of new standards (AASB 1059 application issues)
-  Contingent liabilities
-  Changes to software accounting

## Financial reporting issues

**Guidance for technical accounting assessments**  
**Fact sheets | [www.qao.qld.gov.au/reports-resources/fact-sheets](http://www.qao.qld.gov.au/reports-resources/fact-sheets)**





## Financial reporting

# Financial reporting maturity model

Replaced traffic light assessments for state entities from 2020 and councils from 2021.

## Government departments in 2020

| Component   | Developing | Established | Integrated | Optimised |
|---|------------|-------------|------------|-----------|
| Quality month-end processes                                   |            |             | ← ● →      |           |
| Early financial statement close process                       |            |             | ← ● →      |           |
| Skilled financial statement preparation and use of technology |            | ← ● →       |            |           |
| Resolution of financial reporting matters                     |            |             | ← ● →      |           |



# Financial reporting

## Rating by council segments

| Segment        | Developing  | Established | Integrated | Optimised |
|----------------|-------------|-------------|------------|-----------|
| Coastal        | ←————●————→ |             |            |           |
| Indigenous     | ←————●————→ |             |            |           |
| Resources      | ←————●————→ |             |            |           |
| Rural/Regional | ←————●————→ |             |            |           |
| Rural/Remote   | ←————●————→ |             |            |           |
| SEQ            | ←————●————→ |             |            |           |

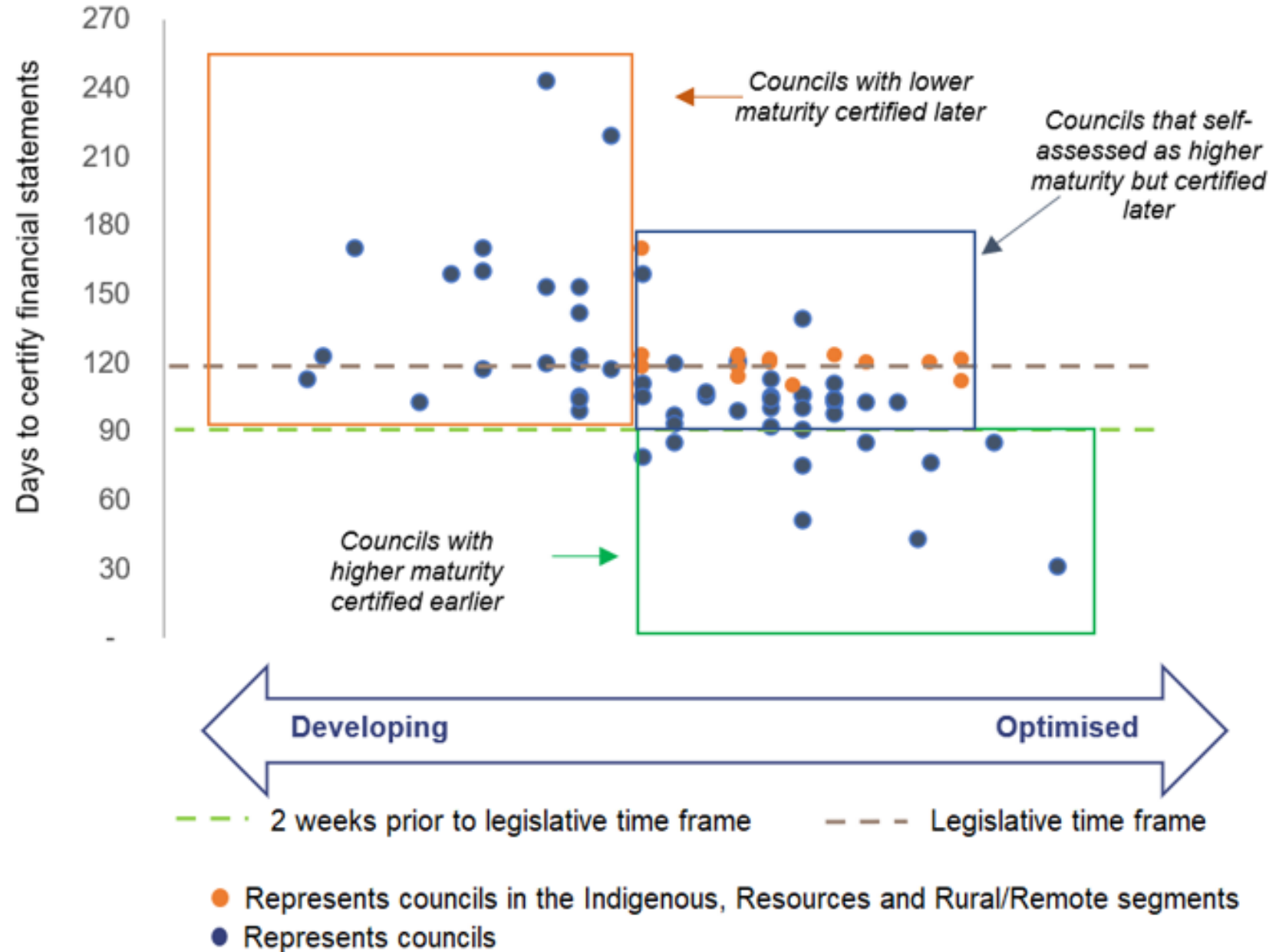


### Areas of focus

- Audit committee review function
- Month-end processes, particularly relating to classification
- Early engagement with valuers with clear instructions

# LG Maturity of financial reporting

## Maturity level and timeliness in having financial statements certified



An aerial photograph of a city skyline with several tall skyscrapers on the left, transitioning into a sandy beach and ocean waves on the right. The image is overlaid with a semi-transparent white box containing text.

## Advancing financial reporting

# Improving transparency of environment, social and governance issues

Erkki Liikanen, Chair of the IFRS Foundation Trustees, said:

“ Sustainability, and particularly climate change, is the defining issue of our time. To properly assess related opportunities and risks, investors require high-quality, transparent and globally comparable sustainability disclosures that are compatible with the financial statements. Establishing the ISSB and building on the innovation and expertise of the CDSB, the Value Reporting Foundation and others will provide the foundations to achieve this goal.

## **Queensland Treasury draft Financial Reporting Requirements**

*Queensland Government Agencies are NOT required, nor directed, to voluntarily adopt Task Force on Climate Related Disclosures (TCFD). Agencies should instead refer financial statement users to the whole-of-Government Queensland Climate Action Plan 2030 and Queensland Sustainability Report.*

1. Consider Queensland Government climate strategy documents
2. Would users reasonably expect that emerging climate-related risks could affect the amounts and disclosures in your entity's financial statements?
3. Identify accounting judgements and key estimates that would be affected
4. Seek approval from KMP and/or audit committee for proposed financial statement disclosures

# Discussion and questions

---





Engage



Respect



Inspire



Deliver

# Forward work plan 2022–25

Patrick Flemming, Assistant Auditor-General

---





## Our audit program

### Forward work plan 2022–25

Each year, we develop a 3-year plan that outlines our planned audits.

We prioritise our audit activity where we believe our insights can most effectively support entities and have a positive impact.

➔ Includes strategic risks to public service delivery we have identified

#### Eight focus areas guide our work:

 Technology risk and opportunities

 Sustainable environment & climate change

 COVID-19 recovery

 Governance of government

 Healthy and safe Queenslanders

 Infrastructure investment

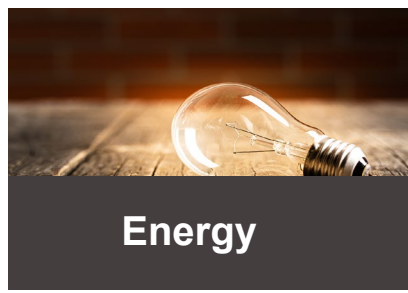
 State savings and debt

 Sustainable communities

Publishing the new plan *in* May 2022: [www.qao.qld.gov.au/audit-program](http://www.qao.qld.gov.au/audit-program)



Education



Energy



Health



Local government

Procurement deep dive

For 2021–22

**Changes to**

Transport

Water

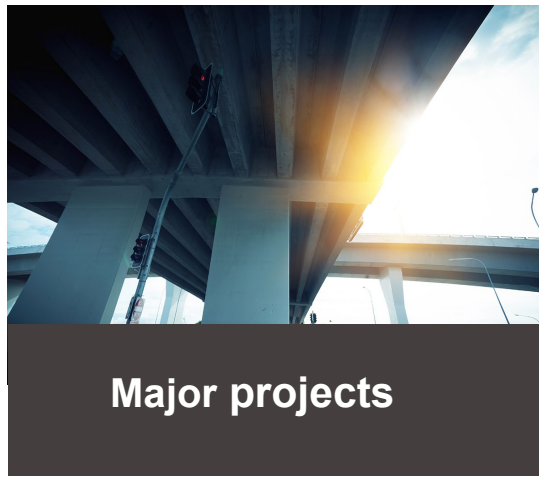
State finances

Deep dive report

Managing grants



Queensland's regions



Major projects



State entities



Managing Queensland's debt and investing for the future



## 2022 Status of recommendations

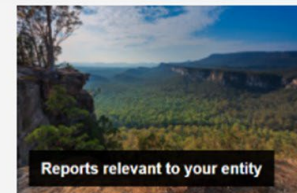
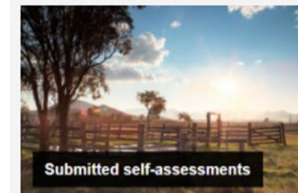
### 2018–19 reports

-  • Monitoring and managing ICT projects
-  • Access to the National Disability Insurance Scheme for people with impaired decision-making capacity
-  • Delivering shared corporate services in Queensland
-  • Managing transfers in pharmacy ownership
-  • Follow-up of Bushfire prevention and preparedness
-  • Delivering coronial services
-  • Digitising public hospitals
-  • Market-led proposals
-  • Follow-up of Maintenance of public schools
-  • Managing consumer food safety in Queensland
-  • Follow-up of Managing child safety information
-  • Delivering forensic services

We have asked entities to complete their self-assessments

### 2019–20 reports

- Investing in vocational education and training
  - Managing the sustainability of local government services
  - Managing cyber security risks
  - Effectiveness of the State Penalties Enforcement Registry ICT reform
  - Managing coal seam gas activities
  - Evaluating major infrastructure projects
  - Licensing builders and building trades
- \*Plus recommendations from the 2021 assessment (2015–16 to 2017–18) partially or not implemented.



# Discussion and questions

---





Engage



Respect



Inspire



Deliver

# Advice on handling and recovering from a cyber attack

David Toma, Senior Director

---

## Cyber attackers are targeting government entities



Aiming to compromise Australia's economic interests and national security

### Protecting government information assets with secure systems is critical

- increasing pressure on those charged with governance to understand their risks and know their businesses are doing enough
- cyber attackers are targeting entities and the attacks are intensifying in frequency and sophistication



*ACSC Annual Cyber Threat Report 2020–21 | [Cyber.gov.au](https://www.cyber.gov.au),  
Australian Cyber Security Centre*



## Cyber security



The *World Economic Forum's Global Risks Report 2022* found 'cybersecurity failure' is one of the risks that worsened the most through COVID-19.



The *Allianz Risk Barometer* listed cyber incidents as the most important global business risk for 2022 (44% of respondents, up from 3<sup>rd</sup> in 2021).

### Examples of recent attacks:

- 2021 – ASIC, vulnerability in a file transfer appliance
- 2021 – Tasmanian Ambulance Service, patient data leak from vulnerability in pager service
- 2017 – 47 UK public health trusts, affected by ransomware, leading to operations being cancelled and patients being turned away.

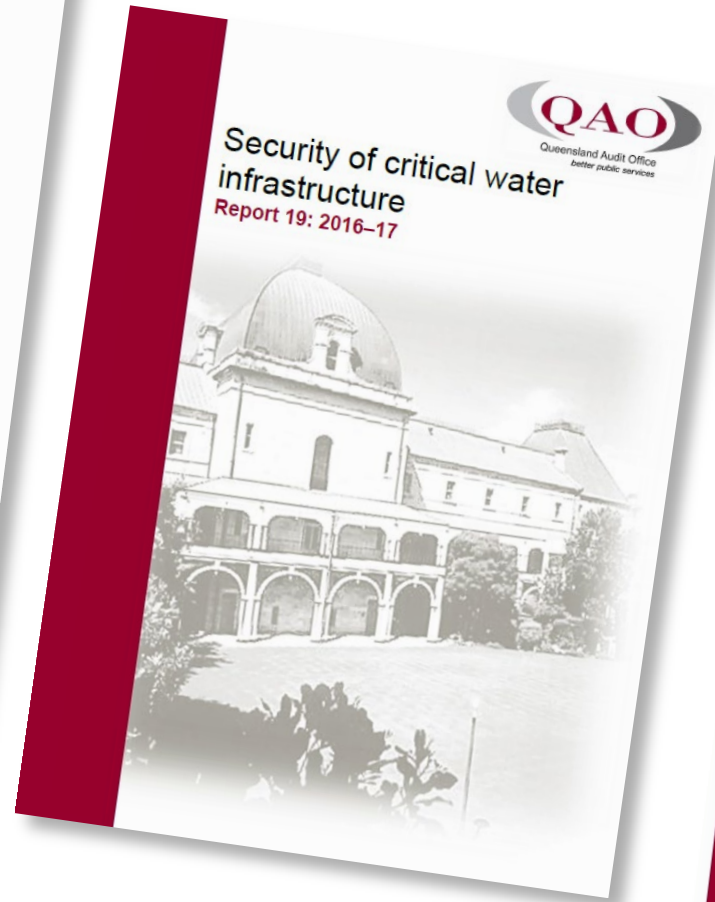




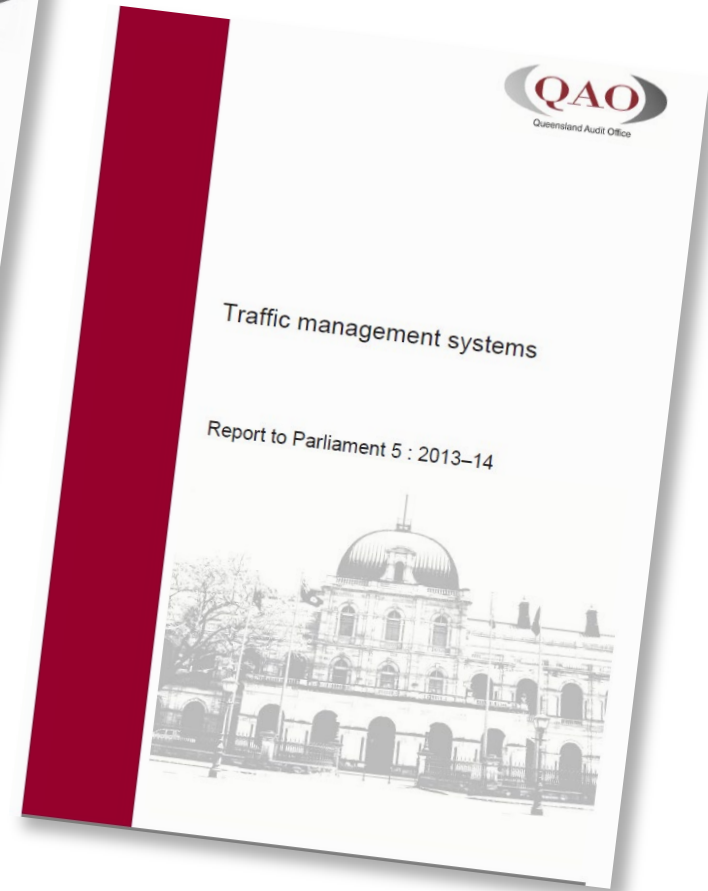
QAO reports



Oct 19



Jun 17



Nov 13

[www.qao.qld.gov.au/reports-resources/reports-parliament](http://www.qao.qld.gov.au/reports-resources/reports-parliament)





## Critical risk area that audit and risk committees need to monitor

What key questions can members ask?

- What are our 'crown jewels' and where are they located?
- Who has access to our critical assets, who is responsible for protecting them and how well are they protected?
- What are our compliance obligations and the implications if we are in breach of them?
- What is our people strategy around cyber security?
- Do we know what the consequences are for a major cyber incident at our entity?
- Do we know how to respond to a cyber security incident?

Further reading:

- QAO blog: [The role of governance committees in managing cyber security risks](#)
- [7 questions directors need to ask about cyber](#), Australian Institute of Company Directors
- [Key questions for an organisation's board of directors](#), ASIC

## Better practice frameworks

- Information security policy (IS18:2018)
- Australian Cyber Security Centre's 'Essential Eight'

### The Top 4 mitigation strategies include:

- ✓ **application whitelisting** – blocking all non-approved or malicious applications from being executed in an IT environment
- ✓ **patching applications** – addressing known vulnerabilities in the security of applications that can be exploited by threat actors executing malicious code
- ✓ **restricting administrative privileges** – minimising the risk of threat actors exploiting privileged system access
- ✓ **patching operating systems** – addressing known vulnerabilities in the security of operating systems that can be exploited by threat actors executing malicious code



## Ransomware

Ransomware attacks are among today's most significant organisational threats.

- Typically delivered by email
- Preventable with correct **controls** and **user education**



**Alert:** recovery system could be rendered useless if the ransomware is able to spread to other systems, including the replicas and recovery sites

### What can entities do?

- Research and understand the value of traditional backup and recovery systems, particularly those with offline/immutable copies
- Implement additional encryption and security controls on backups
- Challenge all accepted disaster recovery norms and assumptions
- Plan for an attack and test ransomware recovery by simulating scenarios
- Make sure your software service providers, cloud service providers, and so on, have their own plans and testing
- Make sure backups are secured, immutable and kept away from corporate networks
- LEARN and DOCUMENT, ensuring recovery playbooks consider the above and are updated annually

**QAO blog:** [Advice on ransomware prevention and recovery](#)



## Cyber resilience

Key elements that help entities to be **resilient** against cyber attacks:

- ✓ Implementing the Essential Eight
- ✓ Incident detection
- ✓ Backup and recovery

In our audit *Managing cyber security risks (Report 3: 2019–20)*, we found:

*None of the three entities detected our security testing or prevented our consultants from accessing our set targets. In all three cases, we needed to advise the chief information officers that our security consultants had succeeded in accessing the targets.*



Definition: **Cyber resilience** is the ability to adapt to disruptions caused by security incidents while maintaining continuous business operations. This includes the ability to detect, manage and recover from cyber security incidents. ([Cyber resilience | Cyber.gov.au](#))



**Audit on  
response and  
recovery**

## Responding to and recovering from cyber attacks



Performance audit, planned for tabling in 2022–23

The Australian Cyber Security Centre reported that in 2020–21 there was an increase of 13 per cent in cybercrime reports, with organisations self-reporting a loss of \$33 billion.

Of the cyber security incidents, one-third of the affected entities are associated with Australia's critical infrastructure.

This audit will provide insights and lessons learned on entities' preparedness to respond and recover from cyber attacks.

## Establishing a framework for cyber security

Entities need to establish a framework and governance arrangements for cyber security to ensure they have the right control environment and culture regarding the risks.

- Outline high-level approach for managing cyber risks
- Information security policy to define objectives for managing cyber risks
- Mandatory information security training for staff
- Periodic reporting from the CIO – threat level, vulnerabilities, stats, progress on risk awareness activities

## Identifying cyber security risks

Ensures an entity is aware of its risk exposure and whether it has the right controls in place to mitigate those risks.

- Identify and classify information assets
- Define risk appetite
- Integrate cyber risk assessments processes with enterprise risk assessments
- Identify and assess the exposure of specific information assets to cyber security risks
- Use threat intelligence services and security testing to help identify risks
- Test physical security as well

## **Supply chain risks**

As entities use more cloud-based services that provide remote access into their systems, they need to be vigilant in assessing how vulnerabilities in their service providers could expose them to cyber risks

- Risk assessment process to determine the suitability of potential suppliers
- Defining information security responsibilities with which suppliers must comply
- Processes for starting and finishing engagements with external suppliers
- Regularly monitoring, reviewing, auditing, or evaluating service delivery to ensure suppliers are meeting their security obligations





**Path of  
access**

## Physical security

- Poor physical security controls allowed our consultants to gain initial access to an entity's network
- This facilitated direct access to the entity's internal assets and increased the available ways to target the entity



**Path of  
access**

## Password practices

- Easily guessable passwords made it easier for our consultants to compromise user accounts and use them to gain control of the entities' networks
- At one entity, our consultants were able to crack and recover clear text passwords for over 6,000 user accounts. They cracked the majority of these in less than 3 minutes



## Passwords

**Figure 4A**  
**Common base passwords**

| Entity X  |                        | Entity Y        |                        |
|-----------|------------------------|-----------------|------------------------|
| Base word | % of cracked passwords | Base word       | % of cracked passwords |
| welcome   | 16.2                   | newuser         | 8.7                    |
| password  | 3.97                   | password        | 3.5                    |
| monday    | 1.58                   | pa55word        | 3.26                   |
| summer    | 0.86                   | Entity service  | 0.97                   |
| march     | 0.83                   | Entity name (1) | 0.97                   |
| passw0rd  | 0.80                   | Entity name (2) | 0.72                   |
| april     | 0.80                   | monday          | 0.72                   |
| p@assword | 0.57                   | thursday        | 0.72                   |
| february  | 0.54                   | welcome         | 0.60                   |

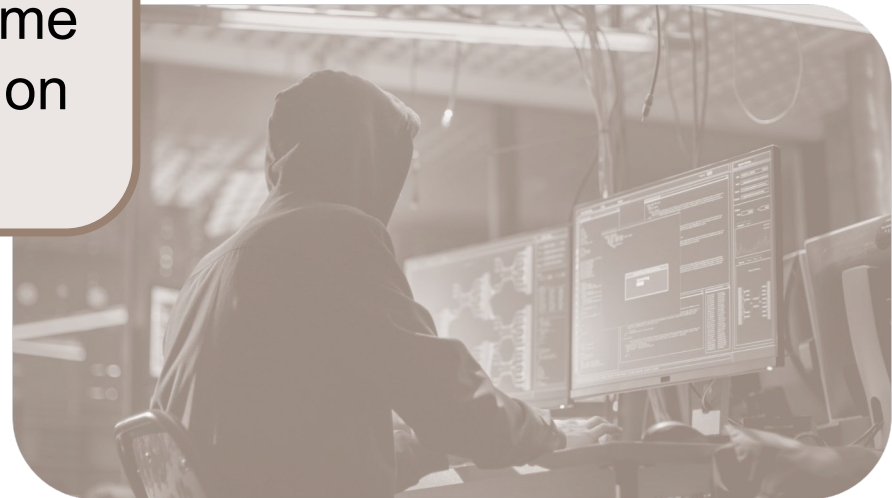
*Source: Queensland Audit Office.*



## 🔑 Known password breaches

Our consultants found over 500 user accounts, associated with the 3 entities' email addresses, to have passwords that have been compromised and disclosed in multiple data breaches that are publicly available.

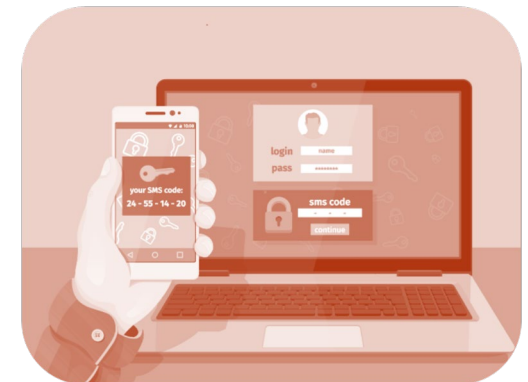
Entities should make staff aware of the risk they create for their entities when they use the same user account and passwords on multiple online services



## Multi factor authentication

The combination of easily guessable passwords and the lack of 2-factor authentication for:

- **external-facing services** could enable an attacker to gain access to the entity's network through password guessing
- **internal services** could enable an attacker who can gain access to a valid highly privileged username and password to use those login credentials to gain access to sensitive internal network servers.



## ↓ Managing ICT assets

Ensures that unauthorised users do not have access to the entity's ICT devices to connect to the entity's network.

- Maintain a record of all ICT assets
- Have a monitoring process to ensure information asset registers have been reviewed and kept up to date
- Have a process to ensure employees return any ICT assets they have been accountable for when they cease their employment



## **Administrative privileges**

Attackers use admin privileges to execute malicious code to exploit security vulnerabilities in workstations and servers.

- Secure communication for remote system administrative privileges
- Restrict internal and email access on privileged accounts
- Log and monitor privileged operations



## Application whitelisting

Ensures only authorised applications can be run and installed.

- Application whitelisting strategy and controls
- Exception logs
- Restriction of dynamic link libraries, scripts and installers
- Application whitelisting methods



# Patching operating systems and applications

To fix known vulnerabilities that attackers could exploit

FIGURE 3B PATCHING OPERATING SYSTEMS AND APPLICATIONS

| Processes and controls  | Entity #1 | Entity #2 | Entity #3 |
|---|-----------|-----------|-----------|
| Patch management strategy   | ●         | ●         | ●         |
| Patching approach and processes   | ●         | ●         | ●         |
| Patching and mitigating extreme risk security vulnerabilities             | ●         | ●         | ●         |
| Patching and mitigating below extreme risk security vulnerabilities       | ●         | ●         | ●         |
| Replacing/updating legacy (outdated) systems to vendor-supported versions | ●         | ●         | ●         |
| Mitigating vulnerability risks when patches are not available             | ●         | ●         | ●         |

Legend: ● Process/control implemented and operating effectively ● Control partly implemented or evidence of some compensating controls ● Control not implemented and compensating controls ineffective or lacking.

Source: Queensland Audit Office.

Mitigating risks

# Discussion and questions

---





 Engage

 Respect

 Inspire

 Deliver

# Closing remarks

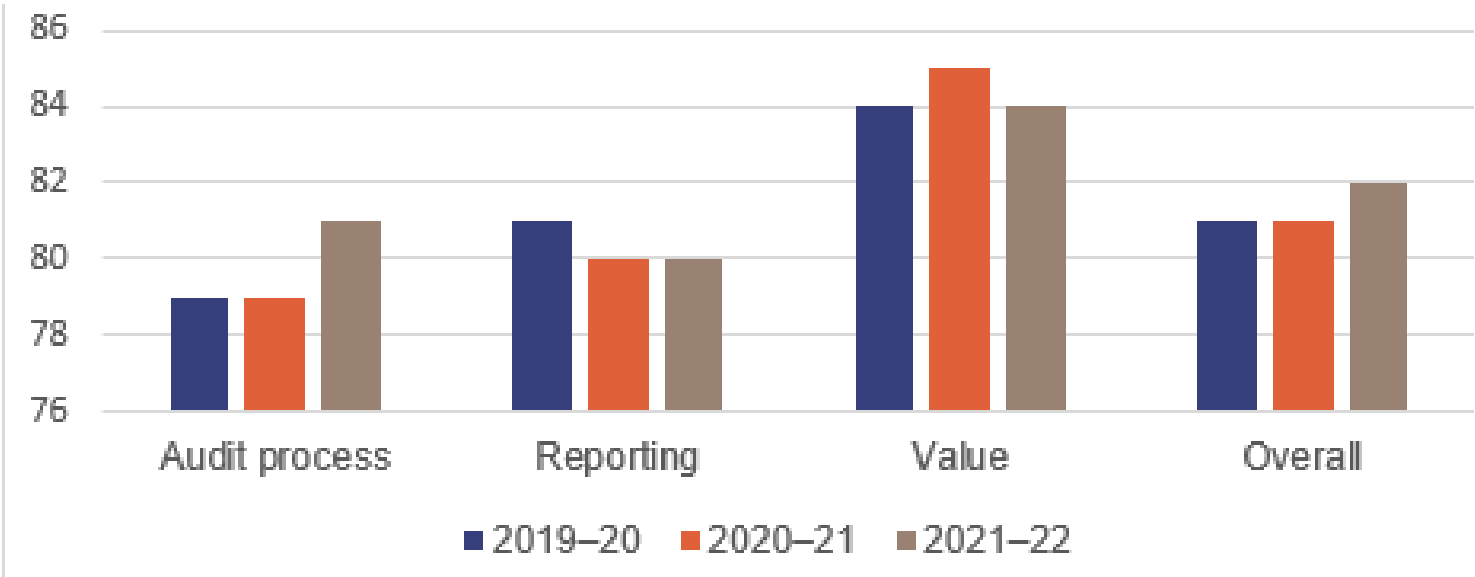
**Brendan Worrall, Auditor-General**

---

# Our independent client surveys give us important information on our services, inform our decision-making and influence innovation

Auditor-General remarks

Overall performance for 2021–22 this year to date



*\*Rounds 1, 2 & 3 financial audits and rounds 1 & 2 assurance audits*

 We welcome feedback any time

## Reminder on regulatory better practices

Recommendation 5 in our report on regulating animal welfare services pertains to all entities

QAO insights session  
Tuesday 10 May 2022



Plan – intelligence-led, risk-based approach



Learn – updating improvement processes, staff learning



Act – executing improvements and providing clear guidance



Report – performance monitoring on compliance levels

[www.qao.qld.gov.au/reports-resources/reports-parliament/regulating-animal-welfare-services](http://www.qao.qld.gov.au/reports-resources/reports-parliament/regulating-animal-welfare-services)

[www.qao.qld.gov.au/reports-resources/better-practice](http://www.qao.qld.gov.au/reports-resources/better-practice)



**Timing of our briefings for you – does  
May and December each year still suit?**

**Auditor-General  
remarks**

# Discussion and questions

---



● *Queensland*

● ● **Audit Office**

*Better public services*

## Disclaimer

---

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 [www.creativecommons.org/licenses/by/4.0/](http://www.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 – 5 May 2022.



© The State of Queensland (Queensland Audit Office) 2022.







## Any questions please contact us

T: (07) 3149 6000

E: [qao@qao.qld.gov.au](mailto:qao@qao.qld.gov.au)

W: [qao.qld.gov.au](http://qao.qld.gov.au)

 [Queensland Audit Office](#)

---