Engage

Challenge

Deliver

Care

Briefing for audit committee chairs

3 December 2019

Queensland
Audit Office
Better public services

Agenda

10.30 – 10.50: QAO update

Brendan Worrall, Auditor-General

10.50 – 11.20: Insights from Managing cyber security risks

David Toma, Director

11.20 – 11.50: Insights and trends for internal audit

Bron Davies, Director IAA-Australia

11.50 –12.00: Questions

Engage

Challenge

Deliver

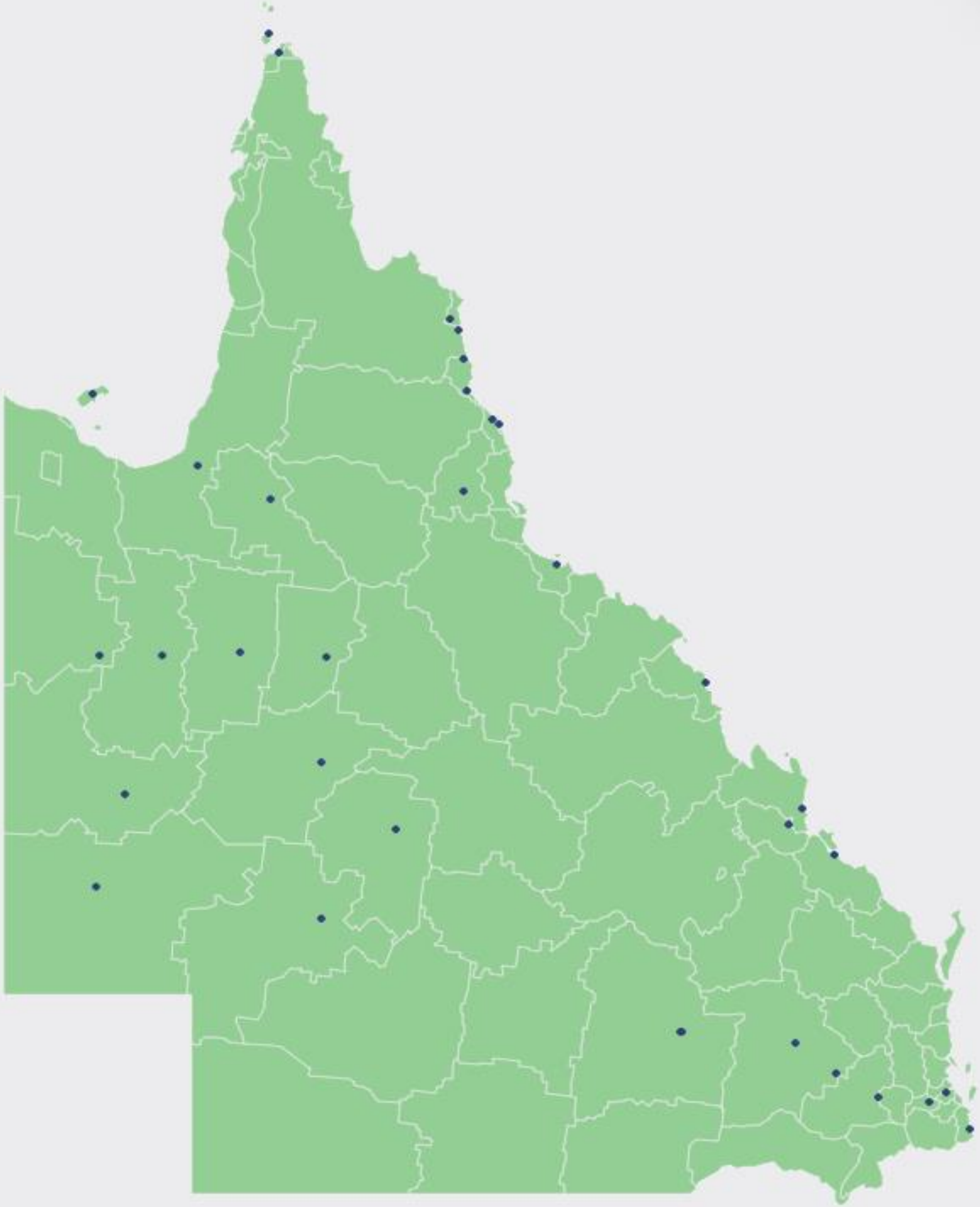
Care

QAO update

Brendan Worrall, Auditor-General

Queensland
Audit Office
Better public services

Client engagement AG visits



Strategic Audit Plan 2020–2023

New program 2020–23 early Dec 2019 on our website

—new timing gives entities more notice

Some timing shifts for existing topics. Nine new (were circulated as a potential year 4 with the current plan), some refocused

Topics to note

- Effectiveness of audit committees in state government entities, planning underway, aiming to table by end of 2019–20
- Effectiveness of local government audit committees, tabling 2022–23

We are wanting to shine a light on some of the common challenges that audit committees face

—looking to canvass a broad section of the sector. Learnings will be shared with all entities

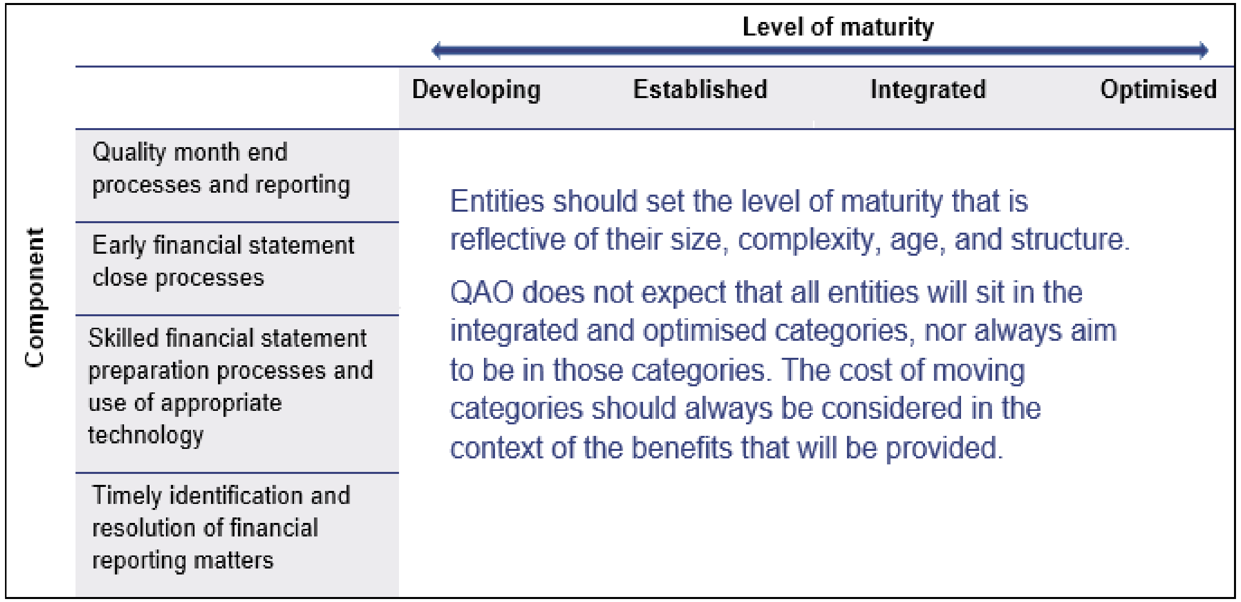
New financial reporting maturity model

We have been working on ways to improve our assessment model

One size doesn’t fit all—scalability, responding to client specific factors

Currently for state entities, planning for local government

- Key components for quality and timeliness
- Helps identify improvement areas
- Sharing better practice



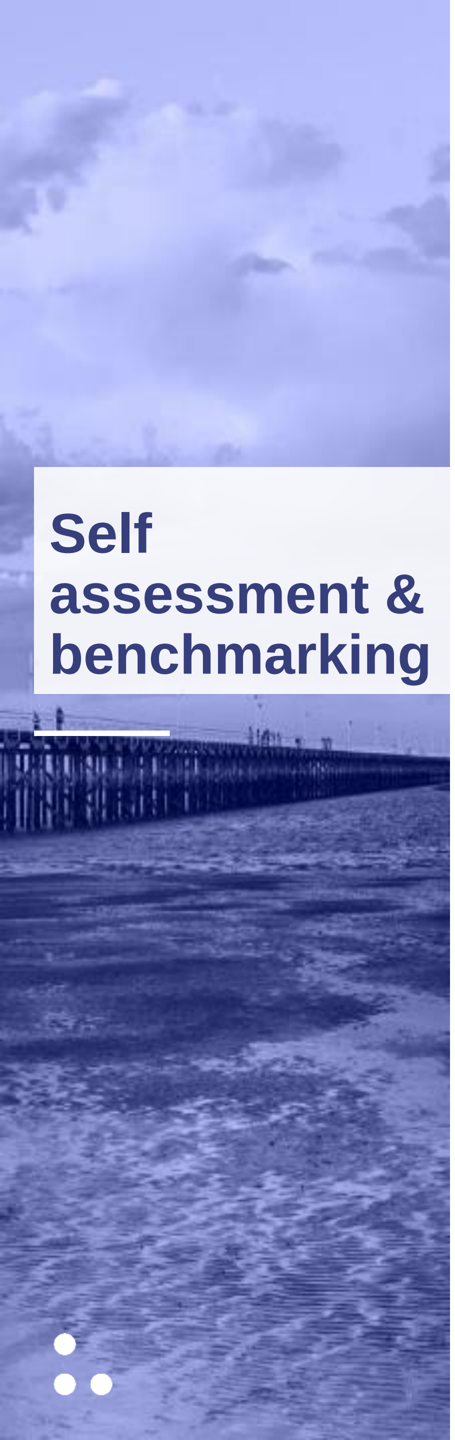
	Level of maturity			
Component	Developing	Established	Integrated	Optimised
Quality month end processes and reporting				
Early financial statement close processes				
Skilled financial statement preparation processes and use of appropriate technology				
Timely identification and resolution of financial reporting matters				

Entities should set the level of maturity that is reflective of their size, complexity, age, and structure.

QAO does not expect that all entities will sit in the integrated and optimised categories, nor always aim to be in those categories. The cost of moving categories should always be considered in the context of the benefits that will be provided.

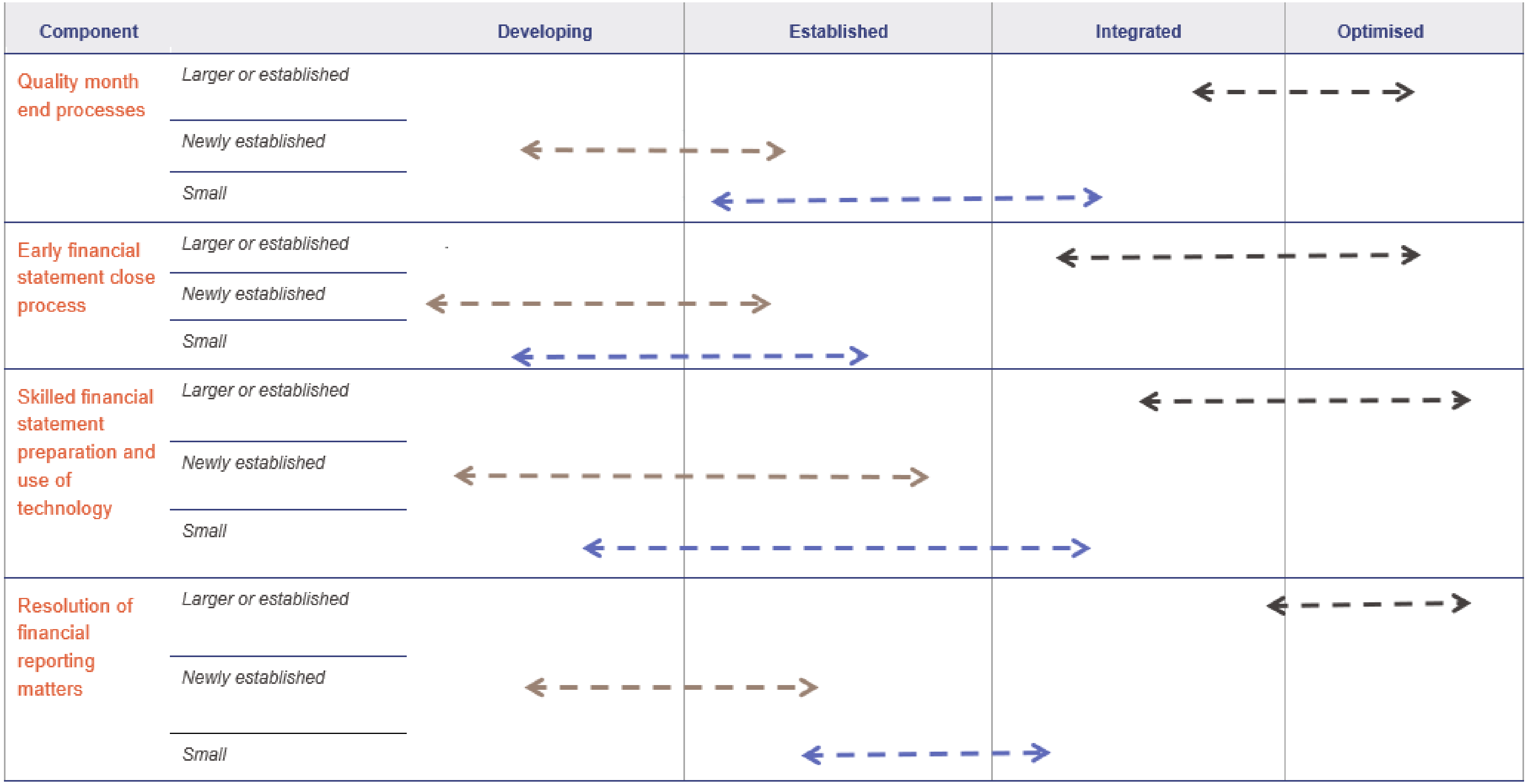
We will discuss our judgements with clients, and use their self-assessments —outcomes reported to TCWG in management letters and closing reports

Communicated extensively with clients and incorporated feedback



Self assessment & benchmarking

Finance teams can ensure they sit at their expected level of maturity, and benchmark actual level to expectation



Component		Developing	Established	Integrated	Optimised
Quality month end processes	*Larger or established*			←	→
	Newly established	←	→		
	Small		←	→	
Early financial statement close process	*Larger or established*			←	→
	Newly established	←	→		
	Small	←	→		
Skilled financial statement preparation and use of technology	*Larger or established*			←	→
	Newly established	←	→		
	Small	←		→	
Resolution of financial reporting matters	*Larger or established*			←	→
	Newly established	←	→		
	Small		←	→	

Further details: www.qao.qld.gov.au/fact-sheets & www.qao.qld.gov.au/blog

Think and Act One QAO

We’re ensuring QAO is best placed to deliver on better public services

Further embedding our approach of providing **more consistent client services**—engagement or project approach to work instead of division

Meaning we’ll serve our clients more efficiently and give them the best skills and resources to do the job

- implementing a new operating model that focuses on client groups
- giving our staff contemporary, relevant skills
- implementing the right systems and methodologies
- exploring and improving our leadership styles

Relevant & engaged
Better public services
Transformational change
THINK AND ACT
Being valued
Relationships
Building capability

New operating model

Auditor-General		
Parliamentary services	**Client services**	**Audit practice**
Executive	**Executive x 3**	**Executive**
• Reports to parliament • Parliamentary engagement • Strategic audit planning • Strategic communications • Referrals • Internal audit • Reporting on government-wide strategic IT and project management	• Professional leads for client groups • Delivery of audits and reports • EQCR roles for audit and report engagement • Data analytics • Information systems	• Audit methodologies • Audit toolkits • Quality framework and program • Accounting and reporting • Audit technical support • Information technology • Finance • Human resources

Sector directors/directors	Dual reporting lines regarding audit engagement and reports to parliament
Managers and below	Centrally resourced through Retain/shared resourcing and capability building
Audit service providers	Audit engagement support

Q&A

Engage

Challenge

Deliver

Care

Insights from our cyber security audit

David Toma, Director

Queensland
Audit Office
Better public services

Cyber security

Cyber attackers are targeting government entities

—trying to compromise Australia’s economic interests and national security

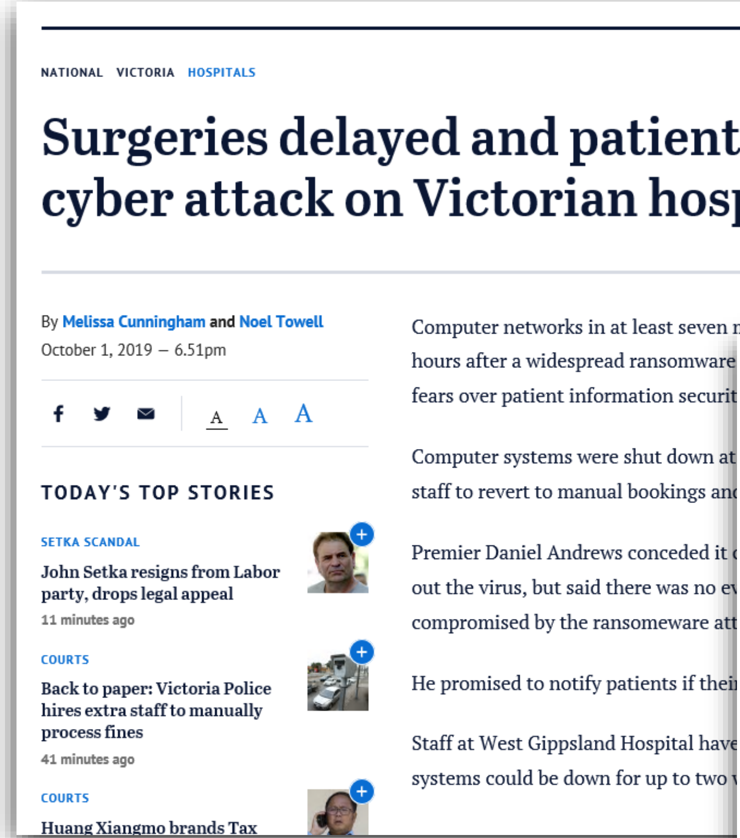
Protecting government information assets with secure systems is critical

In *Managing cyber security risks* we compromised entities’ ICT environments and accessed sensitive data, demonstrating gaps in mitigation strategies

Everyone is responsible for protecting their entity’s data

—staff and third party providers can be the weak link in line of defence

Cyber attacks



NATIONAL VICTORIA HOSPITALS

Surgeries delayed and patient security fears after cyber attack on Victorian hospitals

By Melissa Cunningham and Noel Towell
October 1, 2019 — 6.51pm

TODAY'S TOP STORIES

SETKA SCANDAL
John Setka resigns from Labor party, drops legal appeal
11 minutes ago

COURTS
Back to paper: Victoria Police hires extra staff to manually process fines
41 minutes ago

COURTS
Huang Xiangmo brands Tax

Computer networks in at least seven major regional hospitals remain locked down more than 24 hours after a widespread ransomware

fears over patient information securit

Computer systems were shut down at

staff to revert to manual bookings and

Premier Daniel Andrews conceded it

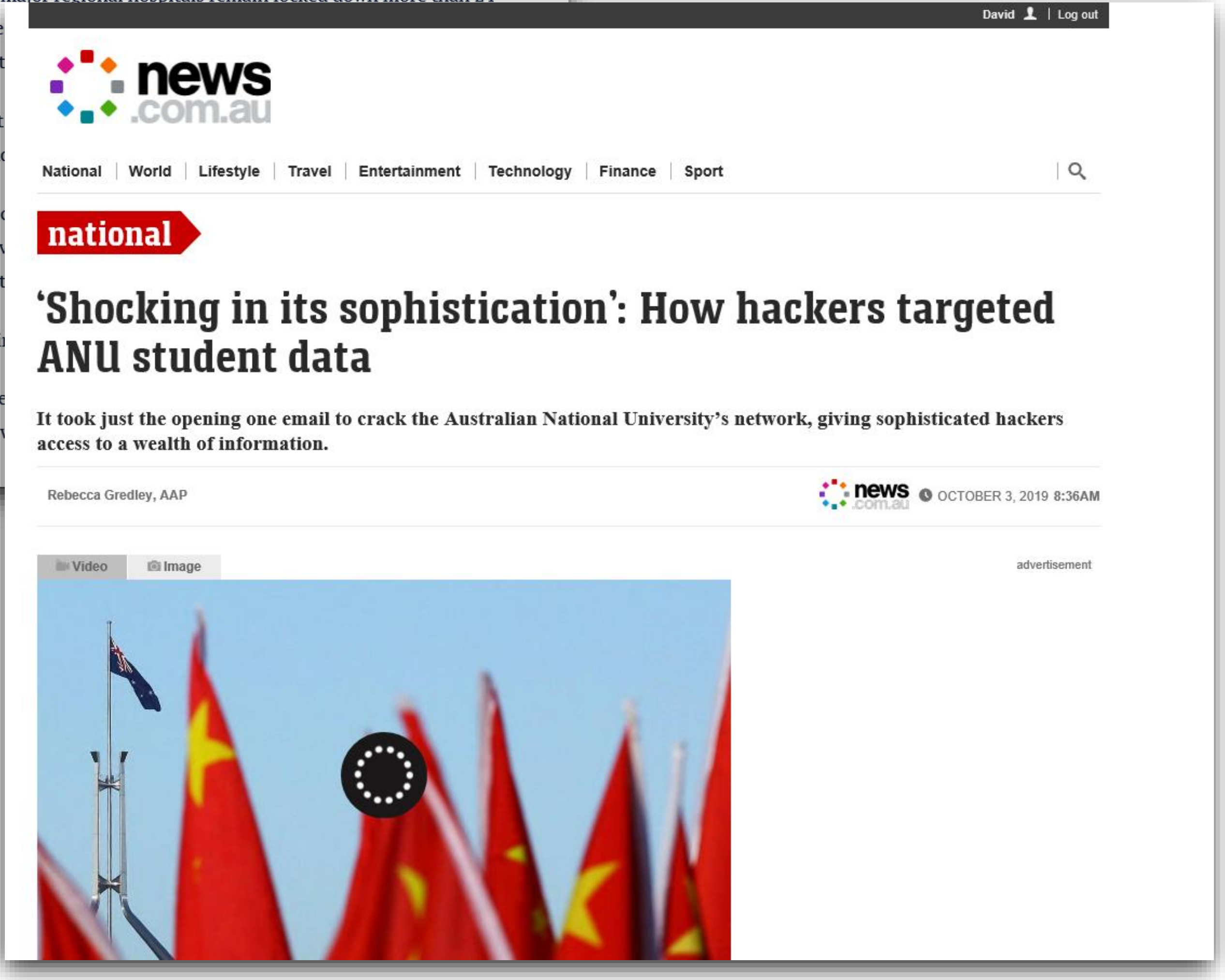
out the virus, but said there was no e

compromised by the ransomeware att

He promised to notify patients if thei

Staff at West Gippsland Hospital have

systems could be down for up to two



David | Log out
news.com.au
National | World | Lifestyle | Travel | Entertainment | Technology | Finance | Sport
national

‘Shocking in its sophistication’: How hackers targeted ANU student data

It took just the opening one email to crack the Australian National University’s network, giving sophisticated hackers access to a wealth of information.

Rebecca Gredley, AAP

OCTOBER 3, 2019 8:36AM

Video
Image
advertisement

Cyber security

Our report provides 17 recommendations relevant for all

Implement controls on cost-benefit basis. But assess against our first three recommendations to:

- ✓ have a framework for managing cyber security risks
- ✓ know what information assets you have
- ✓ know to what extent those assets are exposed

Eight insights statements provide examples of better practice

Areas that our report recommendations cover

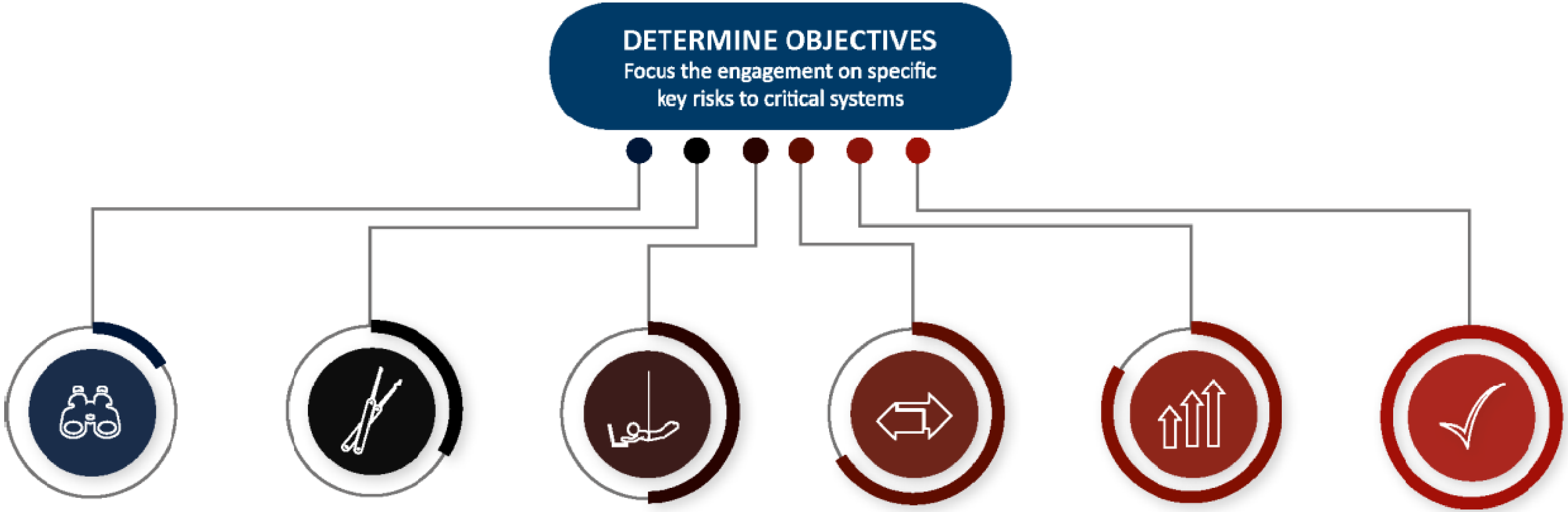
- Cyber security framework
- Information classification
- Identifying and assessing cyber security risks
- Information asset management
- Cyber security risk management strategies
- Monitoring and logging

Cyber security

Our audit included detailed technical testing by specialist security consultants:

- Open source threat intelligence
- Red Team assessment

Cyber kill chain



DETERMINE OBJECTIVES
Focus the engagement on specific key risks to critical systems

1. **Reconnaissance**
Initial reconnassiance identifies exploitable vulnerabilities

2. **Intrusion**
Gain initial access into target environment

3. **Exploitation**
Exploit additonal devices or systems to maintain persistance

4. **Lateral Movement**
Learn additional information about the network and gain access to target systems

5. **Escalation**
Gain additional credentials or authorisation to access the target

6. **Completion**
Proof of concept information is gathered

Conclusions

None of the three entities has effectively implemented the **Top 4 mitigation strategies** for cyber security risks

Our security consultants **successfully compromised** all three entities' ICT environments and gained access to their sensitive or non-public data, demonstrating gaps in the entities’ mitigation strategies

None of the three entities could demonstrate that they **understood the extent to which its information assets were exposed** to cyber security risks

Entities need to make sure their **staff are aware of their responsibilities** in managing cyber risks. In particular, we found poor password practices unnecessarily exposed the three entities to attack

Path of access

Physical security

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

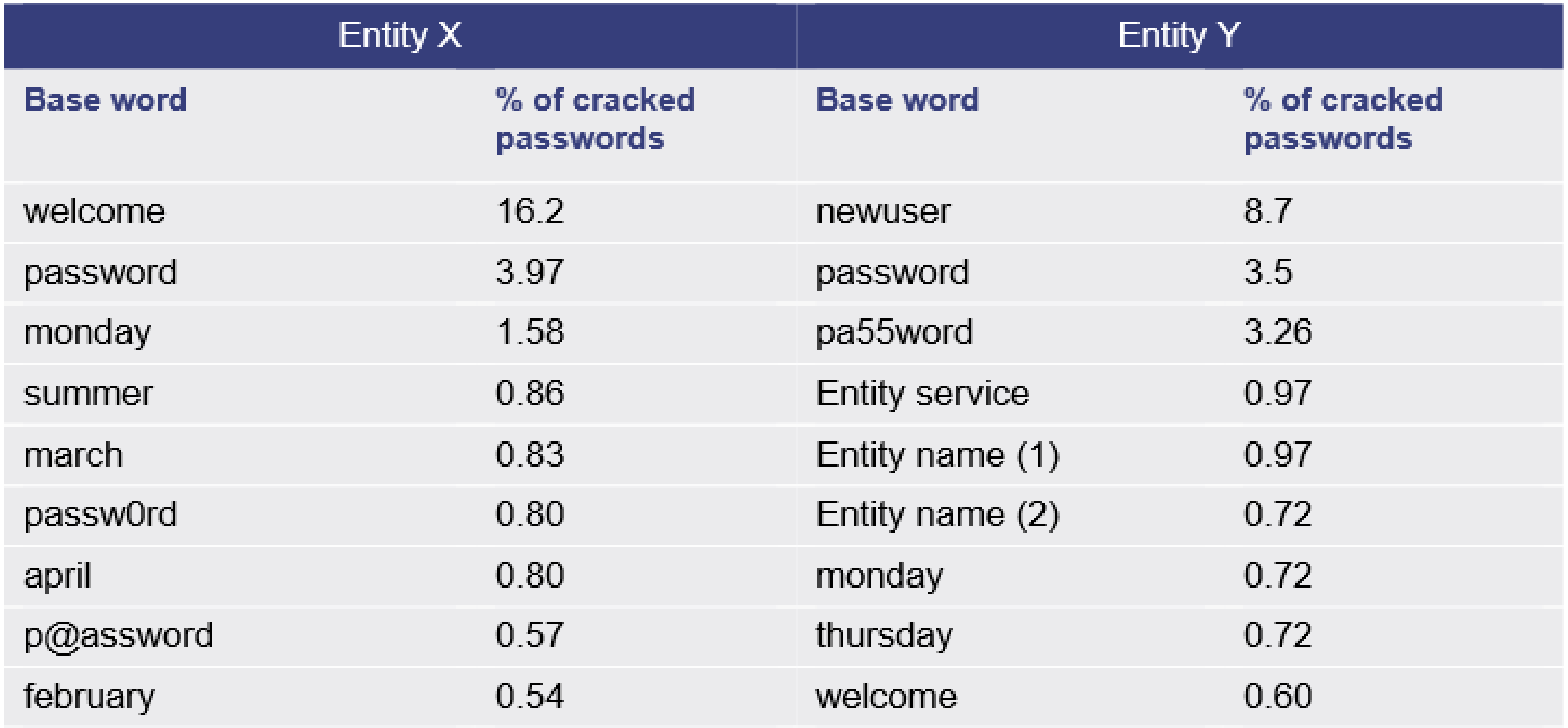
Path of access

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 three 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.

Cyber security

Known password breaches

Our consultants found over 500 user accounts, associated with the three 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

Cyber security

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

Mitigating risks

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

Cyber security

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

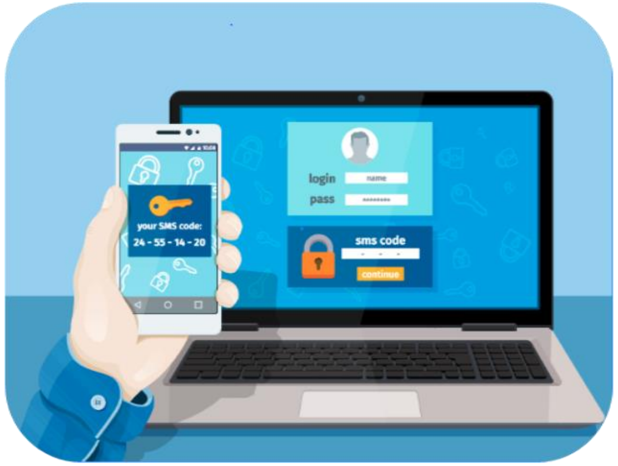
Path of access

Multi factor authentication

The combination of easily guessable passwords and the lack of two-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



Path of access

Network segmentation

A lack of network segmentation allows an attacker to move laterally within an entity’s networks once they access the internal networks

Path of access

Outdated systems

Our consultants identified numerous systems were running outdated applications and operating systems that had not been supported by the vendor for several years.

Cyber security

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.

Cyber security

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

Questions to ask

What questions should audit committees be asking about cyber security?

1. Do we have a sound strategy for managing cyber security risks?
2. Is management doing what they have committed to do in the cyber security strategy?
3. Have we identified our ‘crown jewels’ and tested whether we have effective controls to mitigate any risks?

Get the latest

Subscribe to QAO’s news and blog

for insights, wider learnings and tips

- www.qao.qld.gov.au/contact-us
- www.qao.qld.gov.au/blog

Follow ‘Queensland Audit Office’ on LinkedIn

Q&A

Connect › Support › Advance

The Institute of Internal Auditors Australia

Insights & Trends for Internal Audit including emerging risks

Presented by

Bron Davies
IIA Australia

Trends in Internal Auditing

“agile” (flexible) auditing

data analytics

aligned assurance

Trends in Internal Auditing

- rolling audit plan
- end of year reporting – value focus
- visual and succinct reporting

Can you rely on Internal Audit ?

skills of CAE and the team

professional standards

subject matter expertise support

contemporary audit practices

Can you rely on Internal Audit ?

quality of work

annual self assessment

5 yearly independent assessment

Emerging risks and hot topics

Multiple sources

Internal Audit Foundation – Internal Auditor’s response to disruptive innovation (2019)

CRO Forum – emerging risks initiative – major trends and emerging risks radar (May 2019 update)

Gartner – Q2 2019 emerging risks (30 June 2019)

Swiss Re Institute – Swiss Re SONAR – new emerging risk insights (May 2019)

Examples

Cloud computing
Agile processes
Regulatory changes
Digitalisation
Critical infrastructure blackouts
Cyber risk | cyber vulnerabilities
Organisation resilience
Supply chain | third party eco-systems
Retirement skills gap | strategic workforce planning
Digital tech meets legacy hardware
Data privacy
Project management
Risk culture & decision making
Chemicals in our bodies and environment

How does Internal audit support change ?

Organisations are doing new things in new ways

Is Internal Audit flexible or static ?

Q&A

Queensland
Audit Office

Better public services