AUSCERT

Allies in Cyber Security

The University Of Queensland
AUSTRALIA

CREATE CHANGE

UQSchoolsNet

AUSCERT
Allies in Cyber Security

THE UNIVERSITY OF QUEENSLAND
AUSTRALIA
CREATE CHANGE

UQSchoolsNet

Cyber security maturity assessment Q&A

School Cyber Risk Management

auscert.org.au
uqschoolsnet.com.au

Acknowledgement of Country

AUSCERT and UQSchoolsNet through the University of Queensland (UQ) acknowledges the Traditional Owners and their custodianship of the lands on which we meet.

We pay our respects to their Ancestors and their descendants, who continue cultural and spiritual connections to Country.

We recognise their valuable contributions to Australian and global society.

Image: Digital reproduction of A guidance through time by Casey Coolwell and Kyra Mancktelow

Presenters

James Chadwick

Principal GRC Specialist

AUSCERT: The University of Queensland

James has been working in the IT industry since 2005. His primary focus lies in cyber security GRC (Governance, Risk & Compliance) which is complemented by a wealth of experience across various IT domains.

His expertise spans Computer Networks, IT Governance, Business Analysis, IT Consultancy, Service Delivery Management, and Systems Administration.

FUN FACT:

Used to spin decks (in London & Ibiza) … and now is presenting decks

Salome Bowman

General Manager

UQSchoolsNet: The University of Queensland

Salome Bowman discovered her calling at UQSchoolsNet in Brisbane. Her transformative leadership emphasises innovation and inclusivity, positioning the organisation as a beacon of female leadership in delivering cutting-edge technology solutions through collaborative partnerships.

Her focus is advocating for enhanced partnership to significantly improve accessibility to top-tier technology solutions for schools.

FUN FACT:

I go by my husband's surname; my legal name is so long, scanners in airports don't recognise it

UQSchoolsNet | AUSCERT | The University Of Queensland AUSTRALIA CREATE CHANGE

Agenda

1. Why choose UQSchoolsNet Cybersecurity Assessment?
2. Australian school threat landscape
3. What’s included in our Cybersecurity assessment?
4. What is the NIST Cybersecurity Framework?
5. Which NIST controls are covered in our assessment?
6. What do the assessment reports look like?
7. FAQ
8. Q&A session

MATURITY ASSESSMENT PACKAGE

The key facts everyone wants to know

UQSchoolsNet | AUSCERT | The University Of Queensland AUSTRALIA CREATE CHANGE

Why choose UQSchoolsNet Maturity Assessment package?

- **Leverage AUSCERT Expertise and Guidance**
- **Take proactive steps: Evaluate your position before implementing measures to enhance your cybersecurity posture**
- **Mitigate Information Security risks**
- **Receive this service for a fraction of a corporate price**
- **Guidance and advice along the way**
- **Follow ups, further reports and strategy available post-assessment**

Australian school threat landscape

VULNERABILITY

Australia's national cybersecurity coordinator has warned that schools are becoming targets due to lean teams and resources

EDUCATION

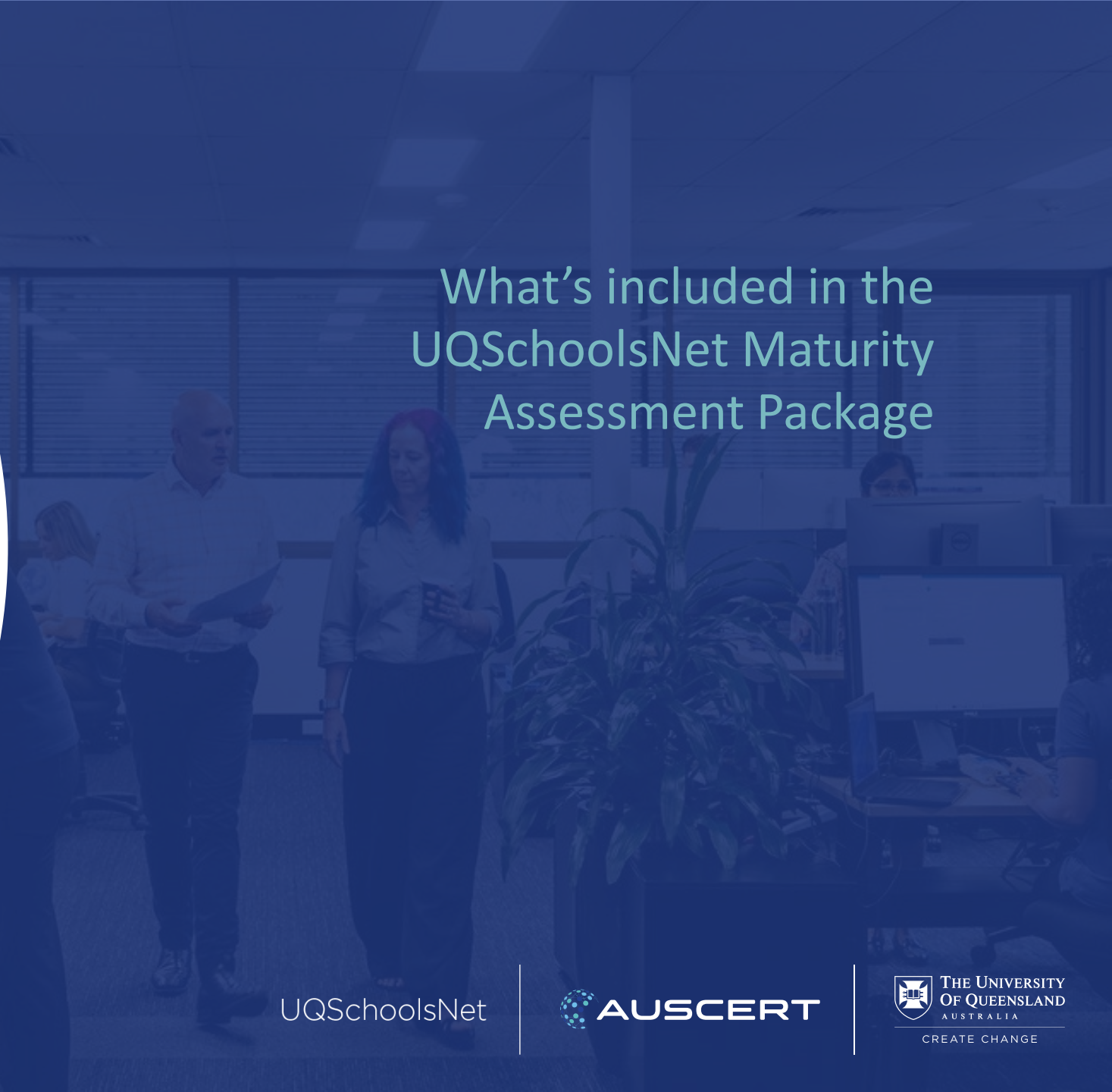
Education in the top 5 most attacked sectors (ACSC Annual Cyber Threat Report 2022)

INCIDENTS

Newcastle Grammar School in NSW, Marist College in Brisbane, and Loreto College in Melbourne are examples of cyber-attacks in schools over recent years

What's included in the UQSchoolsNet Maturity Assessment Package

1. Comprehensive Assessment (20 Critical NIST CSF controls)
2. Maturity Gap Report
3. Risk Assessment Scenario Report (Top 15 ISACA Risks)
4. Executive Summary and Strategy Document (Effective for board level)
5. Optional follow-up and consultations



UQSchoolsNet | AUSCERT | The University Of Queensland AUSTRALIA CREATE CHANGE

NIST Cyber Security Framework (CSF)

WHAT IS IT?

- NIST CSF is a widely recognised cybersecurity framework developed by the National Institute of Standards and Technology (NIST)
- Its broad acceptance worldwide underscores its value and effectiveness in addressing cybersecurity challenges on a global scale

Maturity Assessment NIST controls covered

20 controls are assessed in our assessment which span across the following domains:

- Asset Management
- Business Continuity & Disaster Recovery
- Change Management
- Configuration Management
- Continuous Monitoring
- Data Classification & Handling
- Endpoint Security
- Human Resources Security
- Identification & Authentication
- Incident Response
- Risk Management
- Security & Privacy Governance
- Security Awareness & Training
- Third-Party Management
- Vulnerability & Patch Management

What do the reports look like? – Asset management control – Maturity Gap Report 1

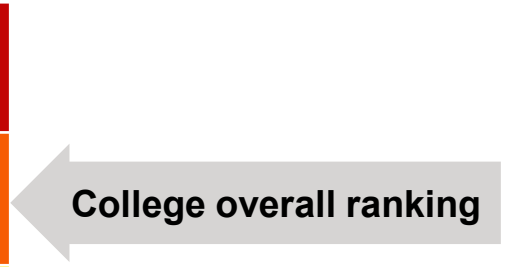
0	1	2	3	4	5
No evidence that this capability exists	The inventory system exists for physical assets, but it is largely manual and is not distributed or retrieved.	The inventory system exists for both physical and informational assets, but it is largely manual and occurs annually.	The inventory system is mostly automated covering physical and information assets, with scan/audits occurring regularly.	The system is mostly automated, capturing most assets, with metrics generated and reported to senior management.	The automated system captures most assets, with management using the metrics to enhance their decision making.

Domain: Asset Management: Manage all technology assets from purchase through disposition, both physical and virtual, to ensure secured use, regardless of the asset's location.

Asset Inventories	Current Maturity 2	TARGET Maturity 3
Control Question: Do you have asset tracking and reporting systems that drive asset accountability, and is available for review / audit? **Recommendations:** Asset register covers all system components and associated control requirements.	The inventory system exists for both physical and informational assets but is largely manual and occurs annually.	The inventory system is mostly automated covering physical and informational assets, with scans/audits occurring regularly.

What do the reports look like? – Maturity Gap Report 2

Maturity	Score Range
Very weak	0-17%
Weak	18-33%
Average	34-50%
Good	51-67%
Excellent	68-83%
World Class	84-100%

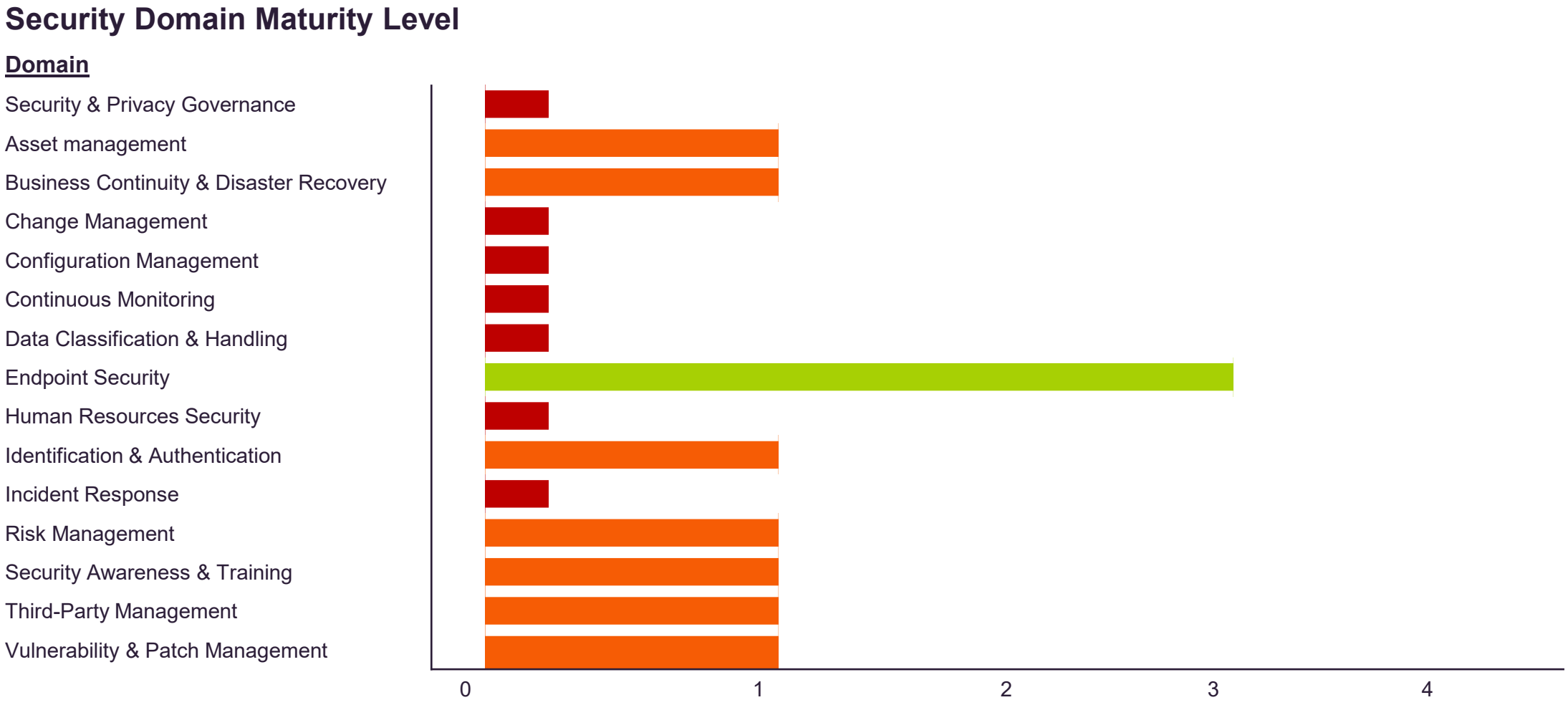


Maturity Average
1.5

Maturity Goal
3

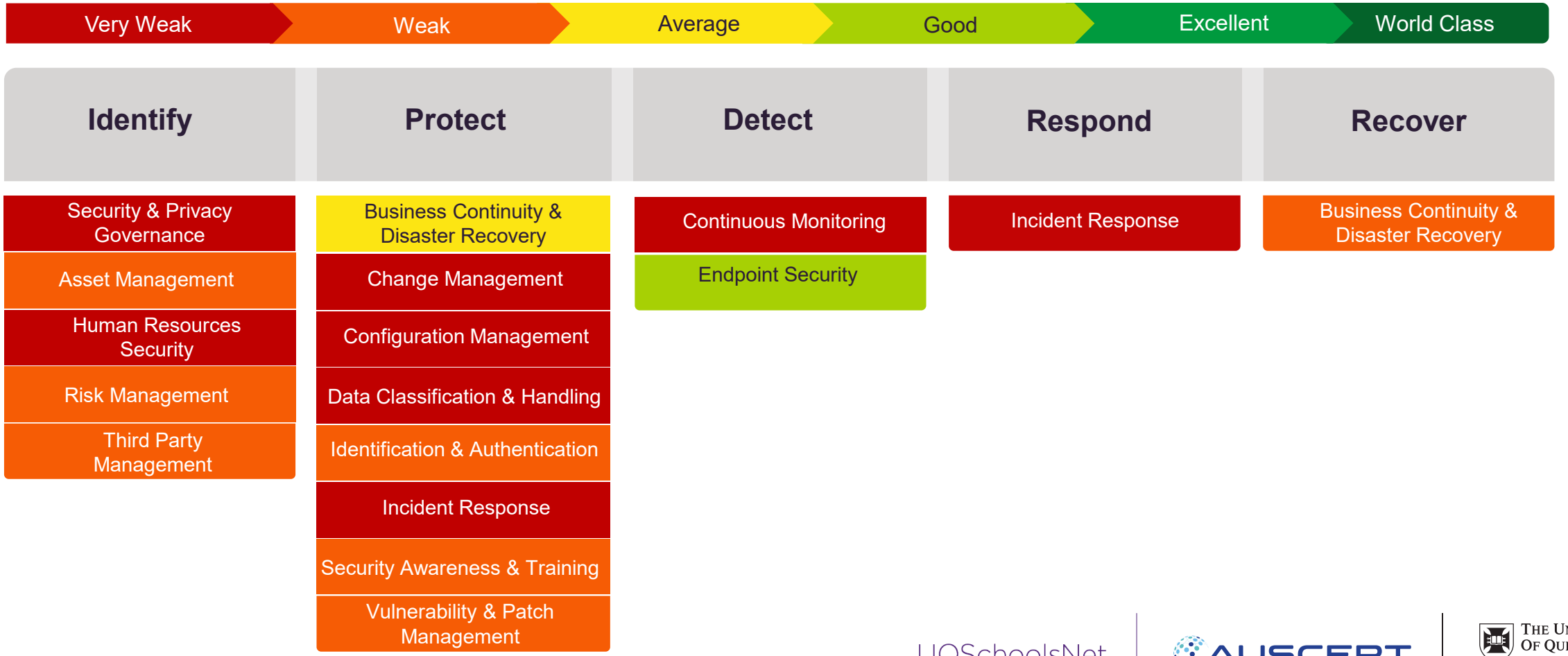
Maturity Percentage
31%

What do the reports look like? – Maturity Gap Report 3



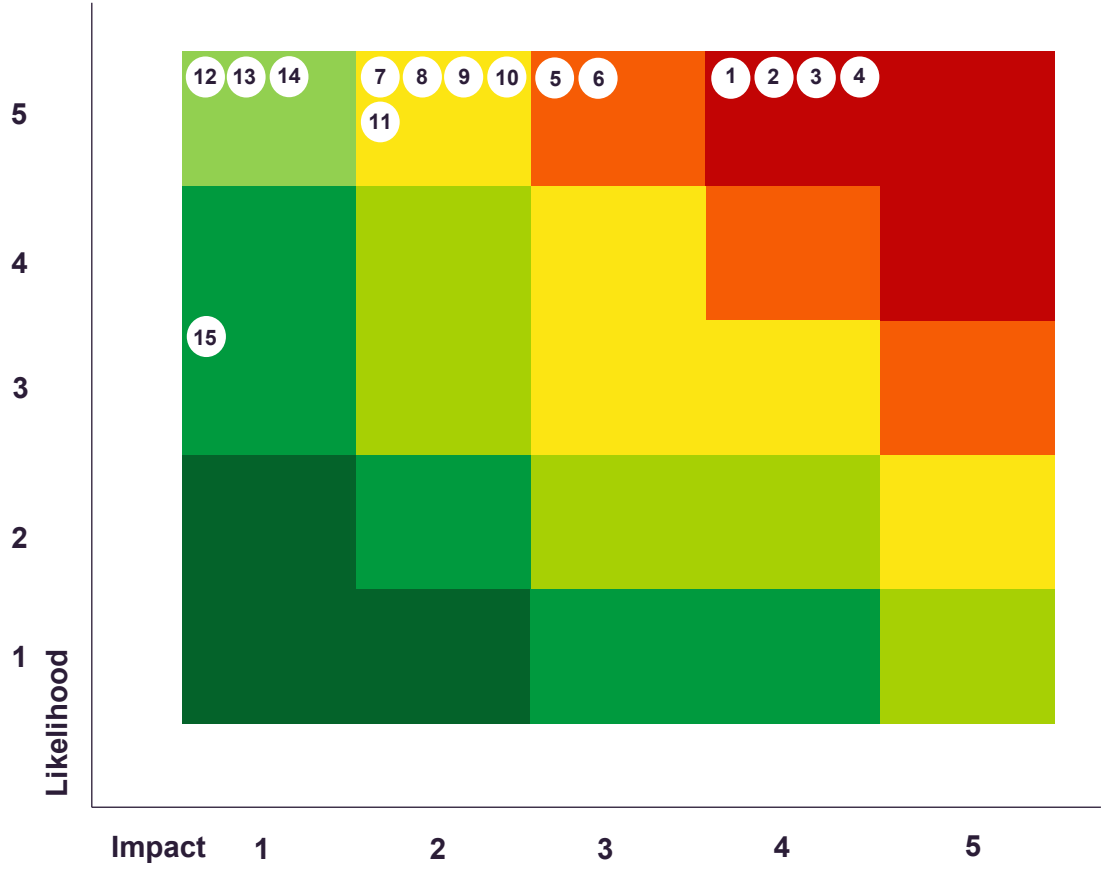
What do the reports look like? – Maturity Gap Report 4

Security Domains & Sub-domains



What do the reports look like? – Risk Report

Risk Scenario Heat Map



Risk Scenario's

1. Advanced Persistent Threat (APT) against privileged end devices.
2. Internal unmanaged change error exposes sensitive data to unauthorised people
3. Shadow IT exposes sensitive data
4. Third-party service supplier is compromised
5. End user device malware
6. Ransomware attack
7. Data centre outage due to natural or manmade disaster
8. Externally exposed vulnerabilities are exploited for unauthorised access
9. Failure to prevent an external attacker intrusion of critical servers and databases
10. Human error to access authorisations exposes sensitive data to unauthorised persons.
11. Privileged user account takeover from remote access
12. Configuration change caused data loss or unavailability.
13. Loss of sensitive data due to human error
14. System unavailability due to failed patch
15. Distributed denial of service (DDOS) attack

What do the reports look like?
Executive summary and strategy

- The executive summary and strategy document is based on the gap and risk assessments
- Effective tool for board-level communication

Gap assessment overview

Risk scenario heatmap

Security improvement roadmap

Strategy on a page (SOAP)

UQSchoolsNet | AUSCERT | The University Of Queensland AUSTRALIA CREATE CHANGE

What do the reports look like? – Executive Summary (SOAP)

Business Context

The rising complexity and breadth of the threat landscape, combined with increased digitalisation of business has resulted in the need for enhanced security for organisations of all sizes and your college is no different.

Cybercrime is rife, where stealing money continues to be the driving force behind many attacks, whilst phishing, ransom ware and stolen credentials represent over 80% of all incidents according to recent OAIC breach notification data.

Therefore, a defence in-depth approach to security is required, centred around risk mitigation and developing a security-aware culture, protecting people and assets, while ensuring the continuity of operations to enable your college to achieve its business objects in 2023 and beyond.

Strategic Vision

The college shall build proactive security capabilities and reorganise the information security function to help the organisation more effectively manage risk in the current threat landscape. Key measurements:

- Achieve a maturity rating against the framework of 3.
- Implement and maintain comprehensive security risk management.
- Develop a security-aware culture with shared accountability.
- Resolve at least 80% of the 11 deficient controls identified.
- Identify Crown jewels and build robust defences around them.
- Provide management with metrics that demonstrate the security posture in near real time.

Current State

A control review was conducted using the framework where 20 NIST controls on a maturity scale of 0-5 were assessed.

The overall maturity was 1.5 with 11 deficient controls (controls ranked either 0 or 1) found.

A risk scenario assessment was conducted, analysing the ISACA top 15 risk scenarios, considering the likelihood and impact of the risk on a scale of 1-5 which were multiplied to create a risk rating. An average risk rating of 8 was achieved against a targeted risk rating of low to moderate (8 or under). From 15 risk scenarios, 1 were rated red (20-25), 8 were rated amber and 6 were rated green

Recommendations

Whilst there are many areas where security could be improved, improvements shall be prioritised using the NIST (National Institute for Standards and Technology) maturity model, following the Identify > Protect > Detect > Respond > Recover sequence.

This approach focuses on building capability from the ground up. The roadmap (detailed below) outlines the specific controls and estimated effort required. Where possible selected controls can be delivered within a 24-month timeframe, although further analysis and planning of security initiatives will enable more accurate estimates for duration and budget.

In summary, there are 18 controls requiring uplift which will move security maturity from 1.5 to 3.

Frequently asked questions

- **What does the assessment consist of and what do we receive?**
- **What is the difference with Essential 8 and why is it more suitable for schools and the K-12 sector?**

Frequently asked questions

- **How long does the process take?**
- **Do you prepare a cyber incident response plan as part of the assessment?**

Frequently asked questions

- **Does the assessment include penetration testing?**
- **Does the assessment include a phishing campaign?**

Frequently asked questions

- **How would I sell it to the Board, CEO or Business Manager?**

Do you have any questions for us?

Find us on...

James Chadwick

Cyber Security Governance, Risk and Compliance

Salomé Caso de los Cobos

Strategy Development, Leadership, Organisational Culture, International Project.

Allies in Cyber Security

AUSCERT | The University of Queensland CREATE CHANGE

The University of Queensland | St Lucia, Q 4072 Australia

ABN: 63 842 912 684

t +61 7 3365 4417

e membership@auscert.org.au

w auscert.org.au