SOPAC®
CONFERENCE
RESILIENCE · RELEVANCE · RELIANCE

Session #4B

Assessing cybersecurity readiness

Presented by:
Ellie Knight
Head of Internal Audit – Technology, Projects & Data Analytics
TAL

The Institute of
Internal Auditors
Australia

cybersecurity (n): the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this

Cybersecurity Threats & Risks

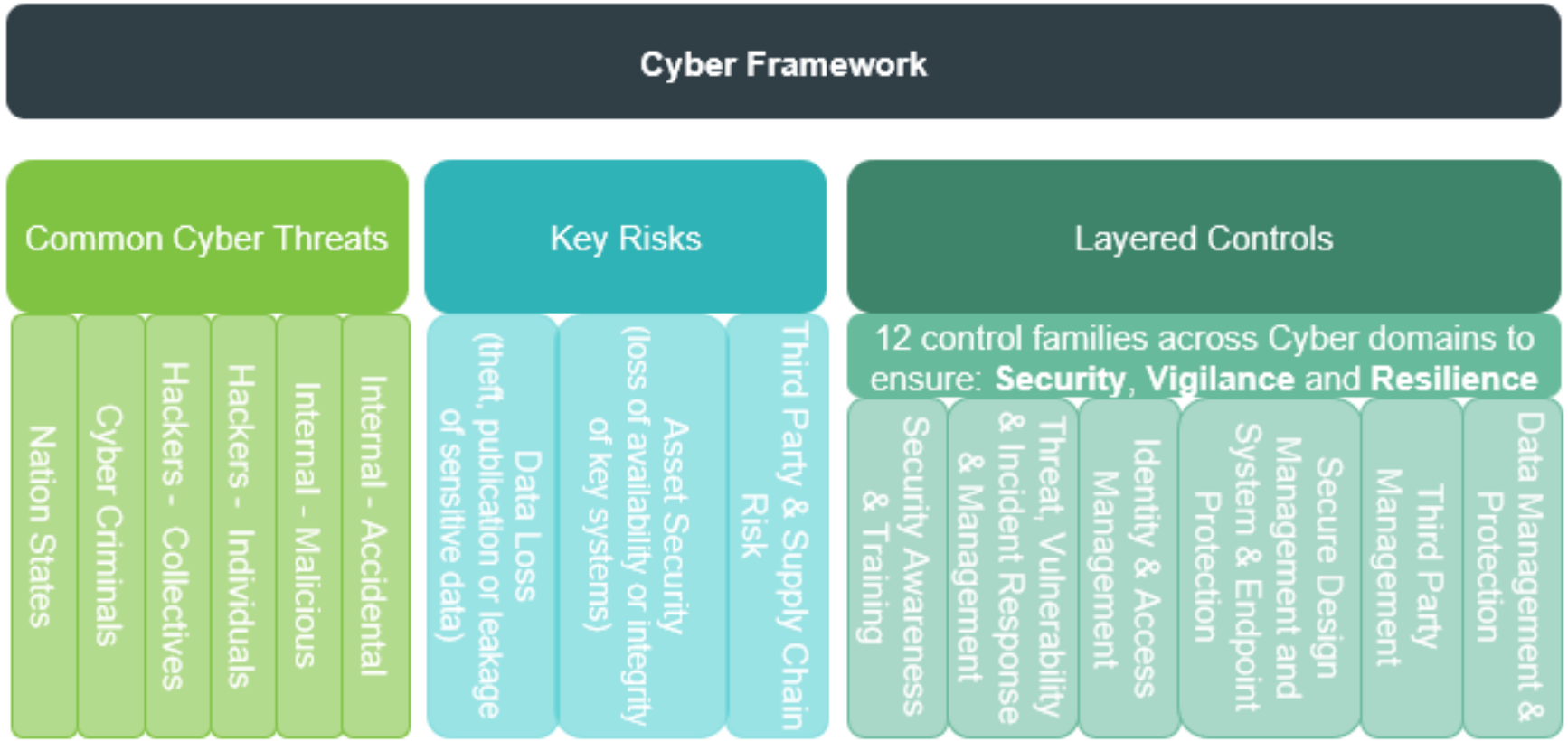
Common Threats

- Nation States
- Cybercriminals
- Hackers or Hacktivists
- Internal
- Service Providers

Potential Risks

- Data Loss
- IT Service Failure
- Threat Actors Risk
- System Integrity Risk
- Third Party Security Risk

Cybersecurity Control Framework



SOPAC CONFERENCE
RESILIENCE · RELEVANCE · RELIANCE

The Institute of Internal Auditors Australia

Understanding your Organisation

Security Legislation Amendment (Critical Infrastructure Protection) Act 2022

Privacy Act 1988

Essential Eight Maturity Model

Prudential Standard CPS 234 Information Security

The Institute of Internal Auditors Australia

Determining Audit Scope

Example Domains

- Data Management & Protection
- Third Party Management
- Secure Design Management and System & Endpoint Protection
- Identity & Access Management
- Threat, Vulnerability & Incident Response & Management
- Security Awareness & Training

Potential Audits

- Information Classification & Handling
- Asset Management / CMDB
- CPS 234 Third Party Management
- Secure Development Lifecycle
- System & Endpoint Protection
- Penetration Testing
- Privileged Access Management
- Incident Response & Management
- Threat & Vulnerability Management
- Standard Operating Environment Assessment
- Cybersecurity Governance
- User Access Management
- Security Configuration Management
- Data Protection
- Third Party Security Assessments
- Vendor Management

Cybersecurity Frameworks

The NIST Cybersecurity Framework

- **Identify** – understanding the business context, resources (systems, people, assets, data and capabilities) that support critical functions and related cybersecurity risks
- **Protect** – develop and implement appropriate safeguards to ensure delivery of critical services
- **Detect** – activities that support the discovery and identification of cybersecurity events
- **Respond** – actions to contain the impact of a potential cybersecurity incident
- **Recover** – plans for resilience to restore any impacted capabilities or services post a cybersecurity incident.

Cybersecurity Frameworks

Essential Eight Maturity Model

- Application control
- Patch applications
- Configure Microsoft Office macro settings
- User application hardening
- Restrict administrative privileges
- Patch operating systems
- Multi factor authentication
- Regular backups

ACSC
Australian
Cyber Security
Centre

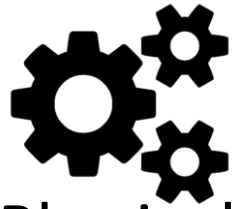
SOPAC®
CONFERENCE
RESILIENCE · RELEVANCE · RELIANCE

The Institute of
Internal Auditors
Australia

Penetration Testing

Application

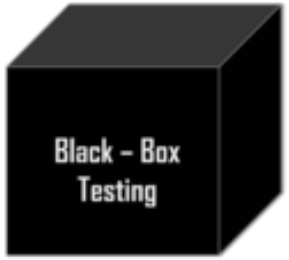
Network



Physical

Internal

External



Zero Knowledge

Some Knowledge

Full Knowledge

SOPAC® CONFERENCE
RESILIENCE · RELEVANCE · RELIANCE

The Institute of Internal Auditors Australia

Determining Audit Approach

Example 1

Co-source engagement with specialist auditors from a consultancy firm managed by Internal Audit team

Process / risk / control focused review

Example 2

Co-source engagement with specialist auditors from a cybersecurity specialist firm managed by Internal Audit team

Security configuration focused review

Supplemented by process / risk / control assessment by Internal Audit staff

Example 3

Co-source engagement with tool specific specialist auditors from a consultancy firm managed by Internal Audit team

Process / risk / control review of the CMDB

Supplemented by data analytics over CMDB data performed by Internal Audit staff

Example 4

Governance related process / risk / control review

Performed by technology audit members of the Internal Audit team

Communicating Results

Internal Audit Testing

- Highlight any observations when identified to allow for discussion and clarifications
- Work collaboratively to confirm impact based on risk and SME perspectives
- Give adequate attention to understanding and providing context

Specialist Testing

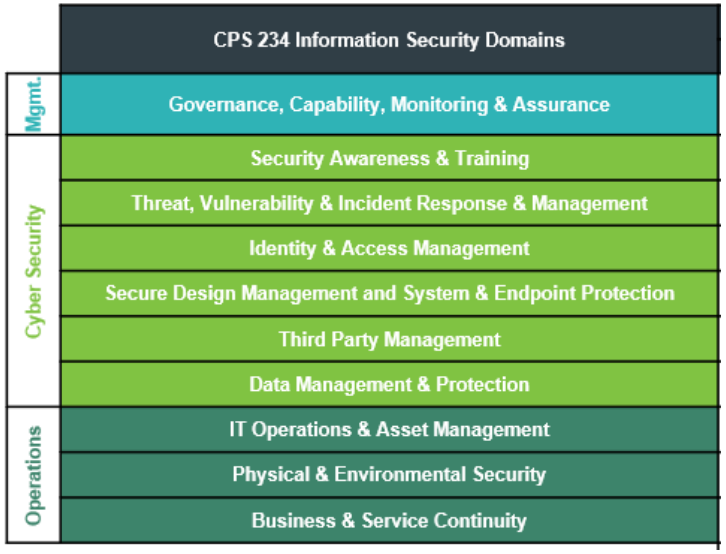
- Focus first on accuracy of technical results
- Understand any compensating controls in controls “stack”
- Rate based on external view combined with internal impact
- Assess level of detail the Audit Committee requires, but provide full detail to technical teams

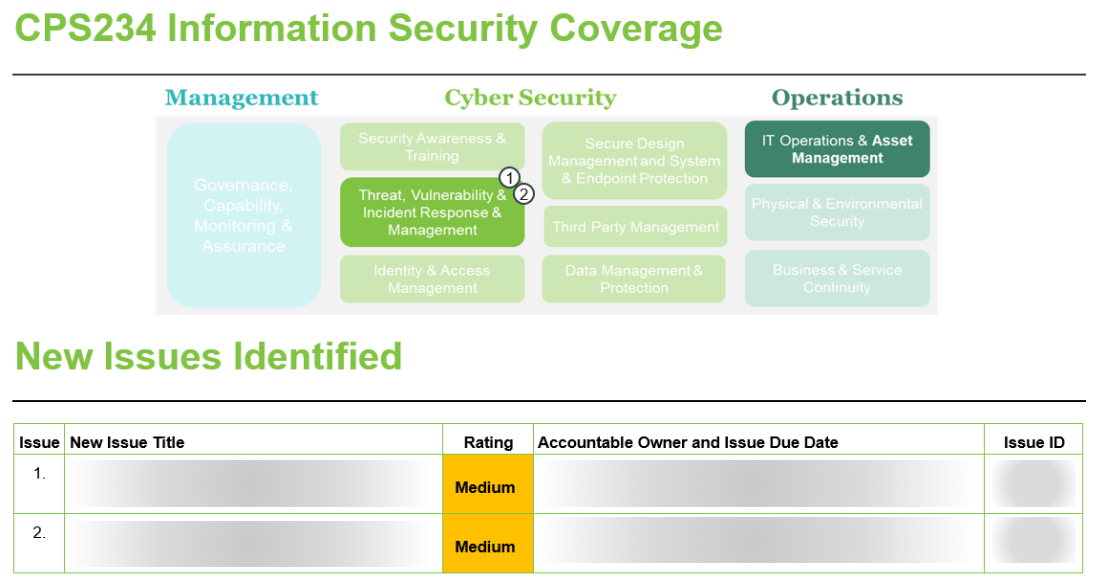
Penetration Testing

- Ensure common understanding of the type of penetration testing performed and approach
- Where gaps are identified, confirm any additional or compensating controls
- Involve relevant support teams as well as the cybersecurity team
- Summarise for Audit Committee

Report Visualisation

Providing consistent messaging for management and the Audit Committee



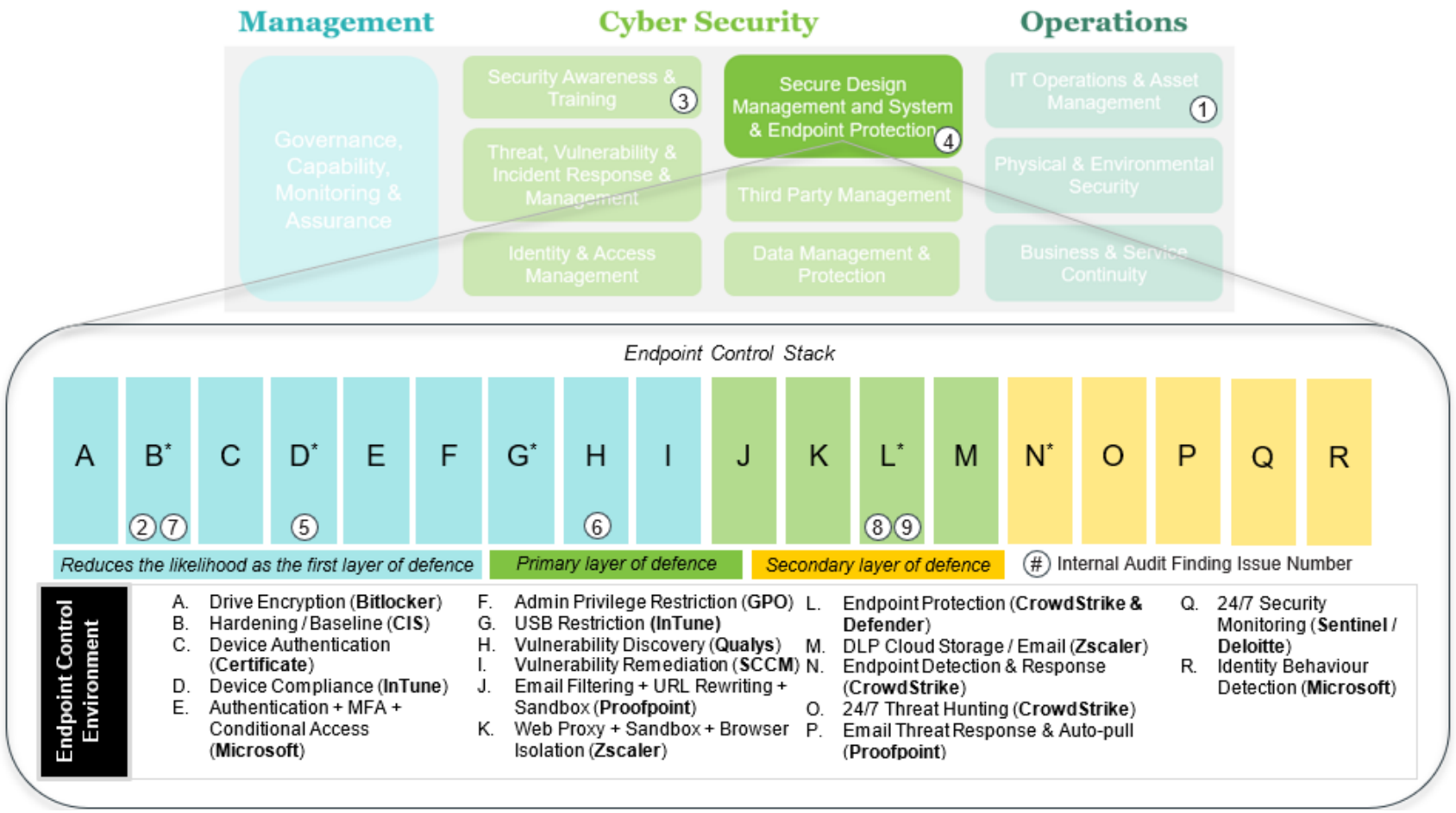


Issue	New Issue Title	Rating	Accountable Owner and Issue Due Date	Issue ID
1.		Medium		
2.		Medium		

SOPAC® CONFERENCE
RESILIENCE · RELEVANCE · RELIANCE

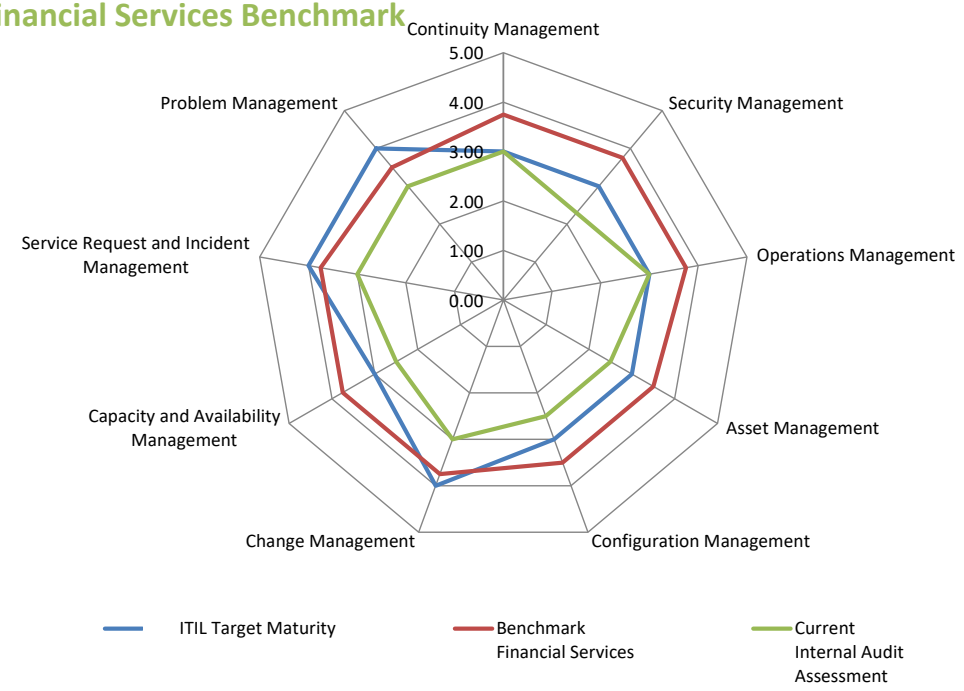
The Institute of Internal Auditors Australia

Report Visualisations

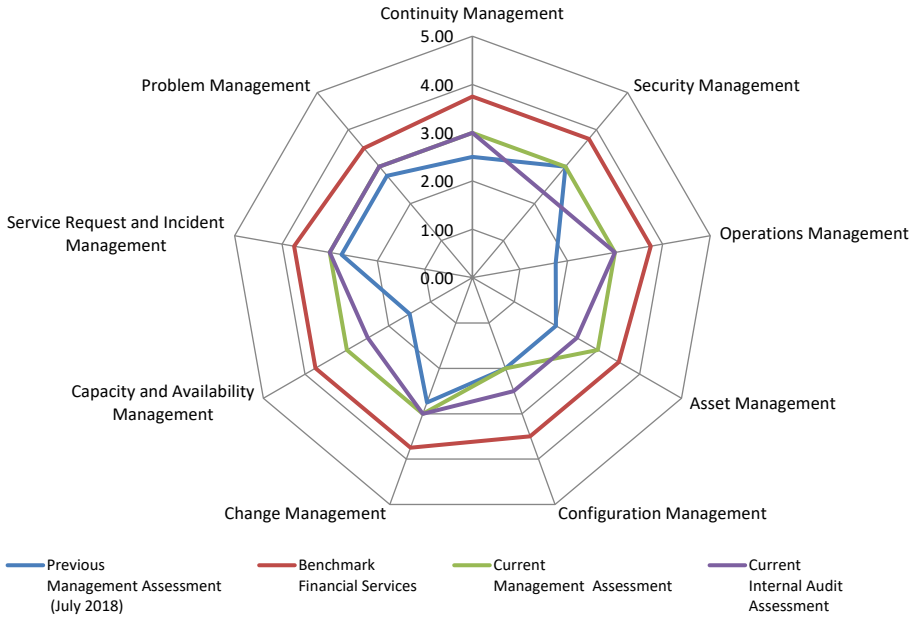


Report Visualisations

Financial Services Benchmark



Assesed Maturity



SOPAC® CONFERENCE
RESILIENCE · RELEVANCE · RELIANCE

The Institute of Internal Auditors Australia

SOPAC®
CONFERENCE
RESILIENCE • RELEVANCE • RELIANCE

The Institute of
Internal Auditors
Australia

Questions?

SOPAC® CONFERENCE
RESILIENCE • RELEVANCE • RELIANCE

The Institute of Internal Auditors Australia