Cyber Security

Update and Strategy Overview

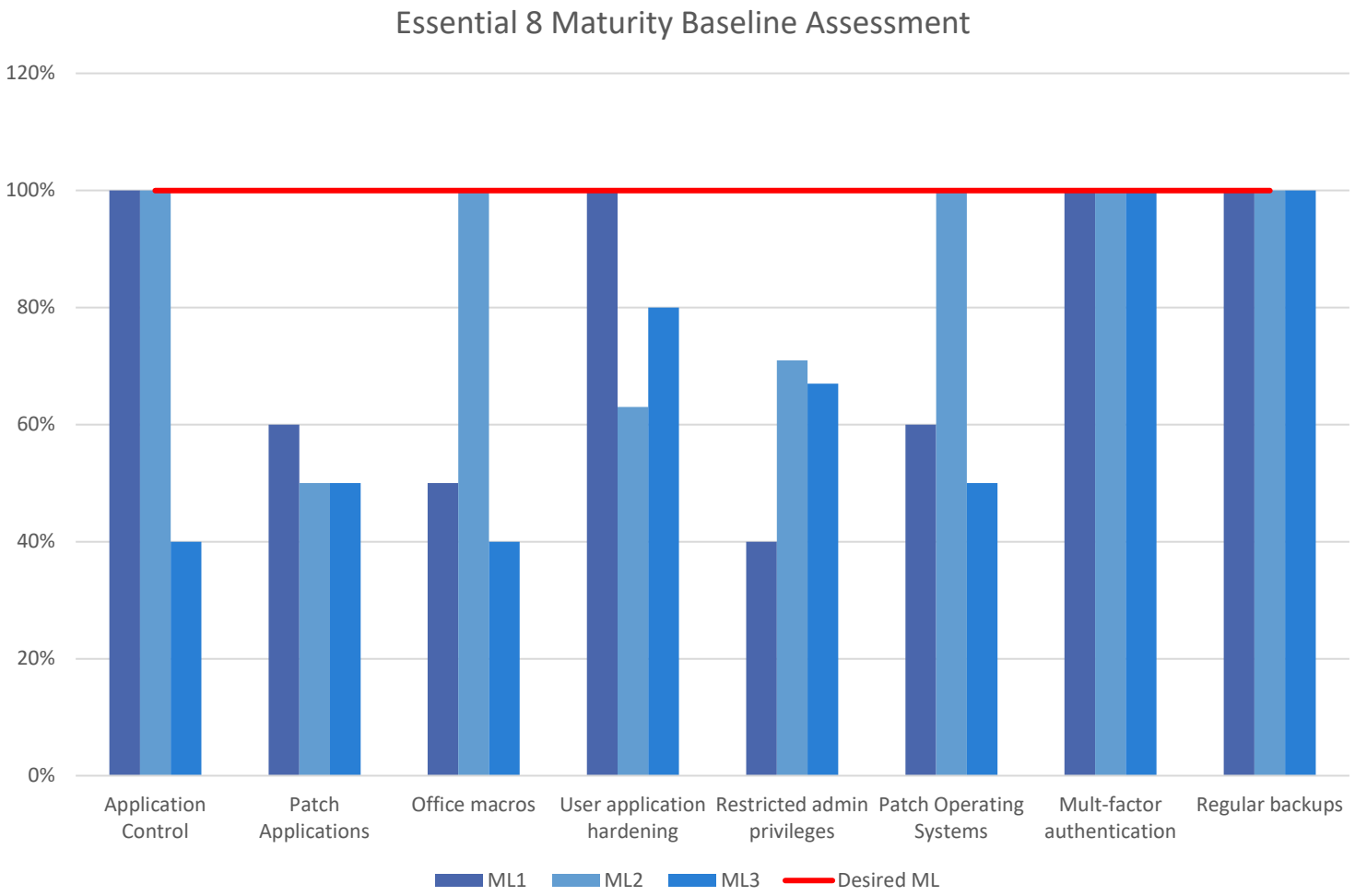
CITY OF ADELAIDE

Cyber security background

- Our formal cyber security activities started as part of our PCI compliance activities (started in 2018-19)
  - Introduction of mandatory cyber awareness training
  - Security hardening, multi-factor authentication, etc…
- As part of our ongoing program, recently we have completed the following activities:
  - Essential 8 baseline
  - Simulated cyber attack
  - Executive cybersecurity emergency management awareness activity

CITY OF ADELAIDE

Essential 8 baseline results



- Baseline assessment against ACSC Essential 8 Maturity model
- Desired maturity level is ‘3’ (highest)
- Assessed by independent 3rd party assessor

CITY OF ADELAIDE

Cyber Risk Landscape

Disruption to Service: **External threat actors** (criminals, nation states, activists) seek to deny access to (DoS), disrupt, deface and inappropriately access and use our systems and resources	**If we don't** protect our systems from external malicious disruption or influence, critical business process will be negatively impacted effecting the student experience, our ability to produce research and engage with our communities.
Reputational Risk: **Cyber incidents** can be highly visible in the media and broadly reported and discussed.	**If we fail** to broadly address cyber threats and account for reputational considerations, suffer impact due to perceived negativity about our brand, and degradation of our partnerships.
Loss of Data: **Data is valuable** and desirable for cyber criminals, nation states and malicious individuals to attain (theft) or deny access to (ransomware). Threats can be external actors, external actors who have managed to gain internal access, or internal. As a custodian of data (including sensitive research), its loss can not only affect USQ, but also those we hold data on behalf of.	**If we don't** protect our data, we run the risk of reduced user confidence, negative media coverage, negative external compliance scrutiny and impacted business processes.

Cyber Risk Landscape (continued)

<u>Financial Impact:</u> Key business process are increasingly **digitised and critical** to 'normal' business operation.	**If we don't** pay attention to cyber fraud, financially motivated threats, or business interruption motivated attacks, CoA faces a potential financial impact, impacting our ability to deliver for our community, ensure long term sustainability and growth imperative.
<u>Third Party Risk:</u> We **partner with and consume** services from external organisations. They have risks which we must be aware of and manage to mitigate impact upon CoA.	**If we don't** effectively manage our external partners, we risk failing to meet our aspirations and expectations due to failings in our supply chain and our partners.
<u>Regulatory and Compliance:</u> Government, regulators, funding bodies and partners **have expectations** and requirements. Expectations for protection against foreign and domestic interference is increasing and is forecast to continue to increase.	**If we fail** to maintain compliance, we will be subject to negative public and regulator perception, and increased cost of compliance going forward.

Cybersecurity Mission

To support CoA's strategic objective by securely enabling its initiatives and operations while protecting it from threats to the availability, integrity and confidentiality of systems and data protecting it from threats.

We will do this by establishing 4 key pillars:

Govern	Protect	Detect	Respond & Recover
• Maintain and Review our Strategies • Consult with stakeholders • Oversight on major initiatives • Monitor key risks & metrics • Ensure we resource appropriately	• Secure our network perimeter • Harden our devices and end points • Mitigate phishing attacks • Control identity and Access • Build Awareness & Education	• Seek external threat intelligence • Monitor for anomalies • Monitor systems, end points and access • Data loss prevention	• Automate response and recovery where possible • Analyse incidents • Communicate, • Practice recovery

We will be doing this by

Govern	Protect	Detect	Respond & Recover
• Maintain and Review our Strategies • Consult with stakeholders • Oversight on major initiatives • Monitor key risks & metrics • Ensure we resource appropriately	• Secure our network perimeter • Harden our devices and end points • Mitigate phishing attacks • Control identity and Access • Organisational Awareness & Education	• Seek external threat intelligence • Monitor for anomalies • Monitor systems, end points and access • Data loss prevention	• Automate response and recovery where possible • Analyse incidents • Communicate, • Practice recovery

- ✓ Develop Cyber Strategy
- ✓ Benchmark against Essential 8
- LGITSA Cybersecurity Framework
  - Data Identification and classification of Personal Identifiable Information (PII) @ CoA
- Implement regular internal and independent cyber security testing and auditing
  - i.e. phishing attacks
- Review and reduce PCI CDE scope
- Establish Cyber security KPIs

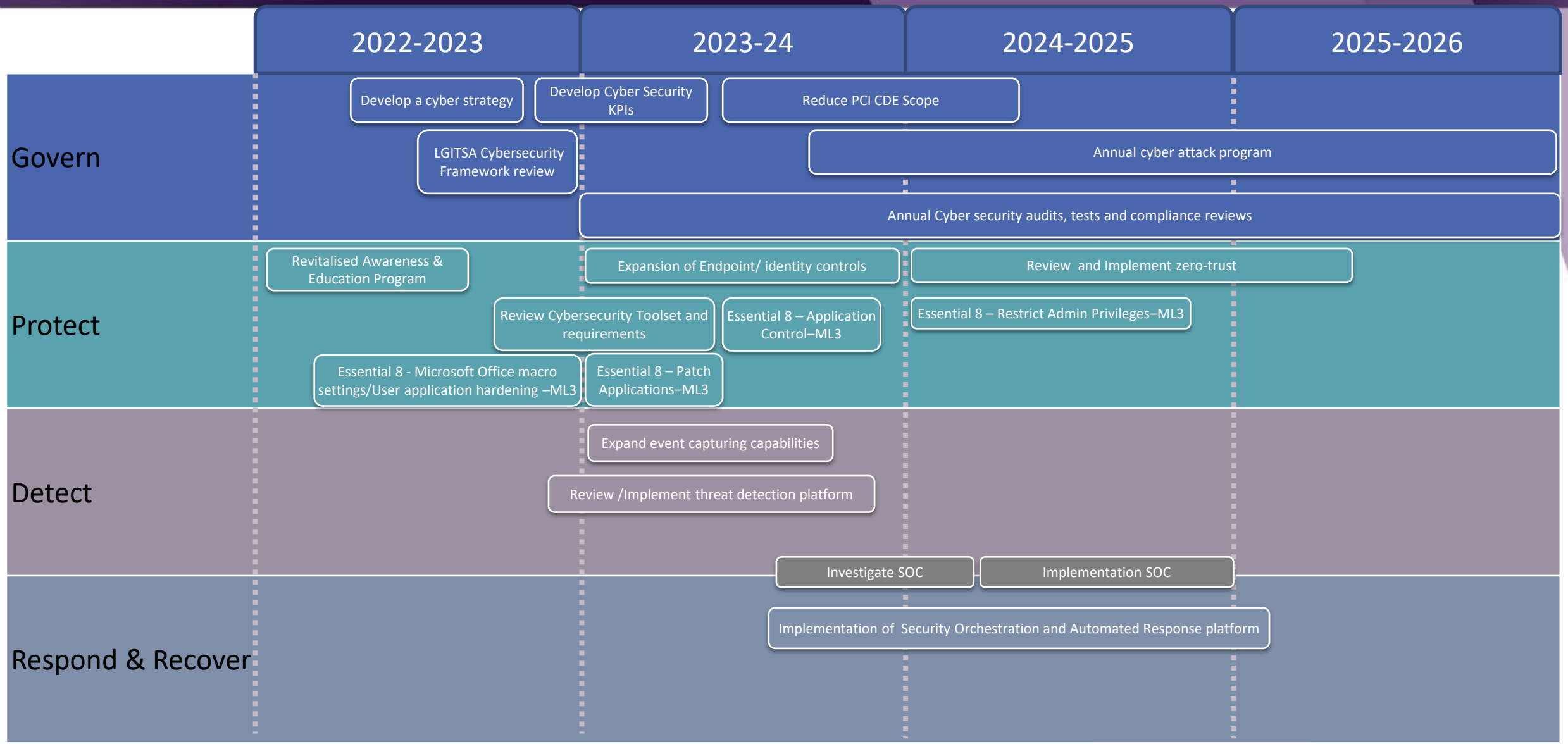
- ✓ Update and revitalise Awareness & Education Program
- ✓ Phishing Simulation
- Review and implement Cybersecurity toolsets that enable:
  - Endpoint/identity controls
- Complete Essential 8 maturity level 3 controls

- Expand event capture and analysis capabilities
- Review and implement Cybersecurity toolsets that enable:
  - Network Threat Analytics
  - Threat Intelligence

- Review and implement Cybersecurity toolsets that enable:
  - Security Orchestration, Automation & Response (SOAR)
- Annual cyber attack program

Investigate cyber security operations centre (SOC)

When will we be doing this by



Key next steps

- Continue to work through remediation activities in the program of work
- Review current capacity and capability and realign internal resources where appropriate
- Develop business case submissions for the provision of new capabilities:
  - Security Orchestration and Automated Response platform
  - Event capture
  - Zero-trust network
  - Annual cyber attack program

CITY OF ADELAIDE

Thank you!

CITY OF ADELAIDE