Waterstons

# Cyber Blueprint: Offer & Advisory

Details of the engagement offer & advisory on how our approach can help you and your business

# Cyber Maturity Journey

A journey that all organisations will increasingly need to embark on.

Where are you in the process?

## Vulnerable

- Ad-Hoc controls
- Little to no visibility
- Little to no planning

## Security Fundamentals

- Catalogue assets
- Map attack surfaces
- Discover and catalogue vulnerabilities
- Plan remediation

Australian Government
Australian Signals Directorate

ACSC
Australian Cyber Security Centre

Essential 8

## Australian Signals Directorate Essential Eight (ASD E8)

- Focused on mitigating most likely threats to organizations
- IT Led
- Heavy technology bias

Information Security Management System
ISO
27001
Certified

## Managed Risk

- Mature Repeatable Processes
- Exec Buy in
- Proactive Focus on monitoring and detection
- Managed 3rd party/supply chain risk
- Process, policy and people focus.

## Security First

- Security by design culture
- Regular board briefing
- Simulated Incident Response
- Monitoring of evolving threat landscape
- Technology, people and policy optimized

# Cyber Blueprint : Establish a Cyber Vision

## Governance

Establishing a data driven culture which defines clear policies, risk management and data ownership

## People

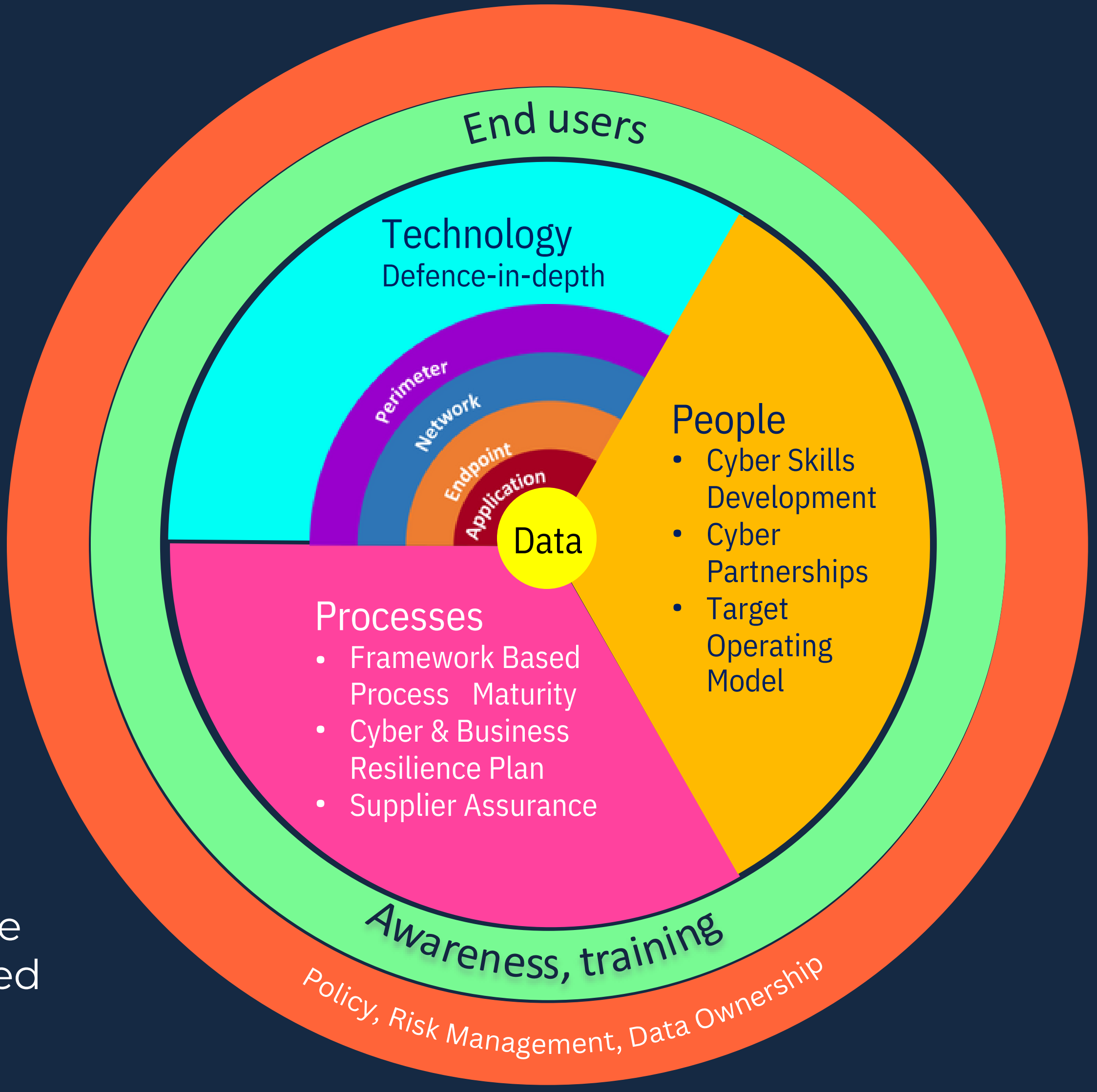
Equipping our people with the cyber skills needed to defend our systems alongside our strategic partners

## Process

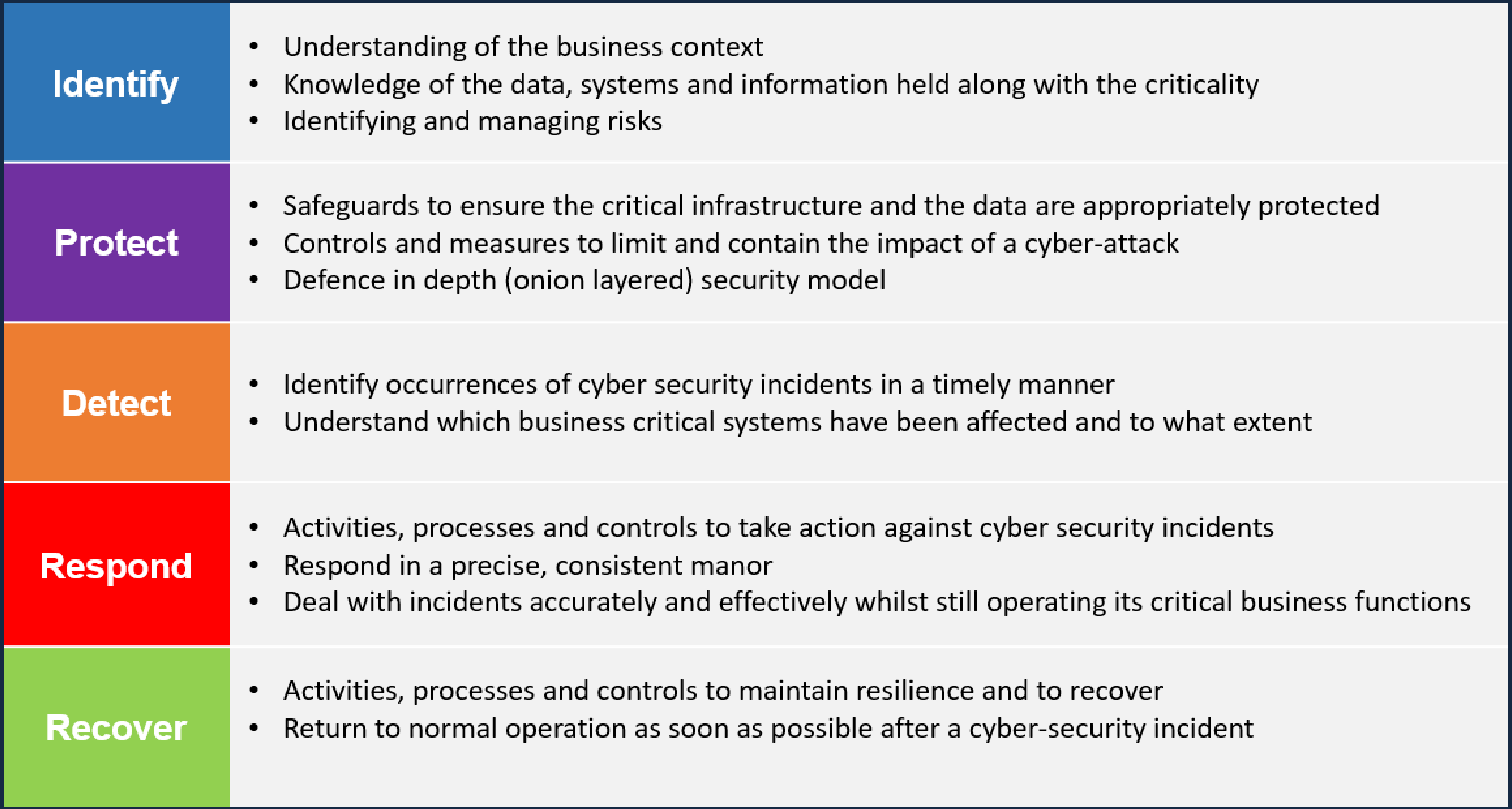
Adopting a major framework based maturity approach which extends across our digital supply chain

## Technology

Aligning with a Defence in Depth methodology to ensure that organisational systems and data are always protected from the evolving threat landscape



# NIST Cyber Security Framework



| | |
|---|---|
| **Identify** | - Understanding of the business context<br>- Knowledge of the data, systems and information held along with the criticality<br>- Identifying and managing risks |
| **Protect** | - Safeguards to ensure the critical infrastructure and the data are appropriately protected<br>- Controls and measures to limit and contain the impact of a cyber-attack<br>- Defence in depth (onion layered) security model |
| **Detect** | - Identify occurrences of cyber security incidents in a timely manner<br>- Understand which business critical systems have been affected and to what extent |
| **Respond** | - Activities, processes and controls to take action against cyber security incidents<br>- Respond in a precise, consistent manor<br>- Deal with incidents accurately and effectively whilst still operating its critical business functions |
| **Recover** | - Activities, processes and controls to maintain resilience and to recover<br>- Return to normal operation as soon as possible after a cyber-security incident |

# Mitre Att&ck Framework: Focus For Your Sector

This Framework focuses on specific risks for your sector….not just compliance for compliance's sake.

### Initial Access

- 🟨 Drive-by Compromise
- 🟨 Exploit Public-Facing Application
- 🟨 Phishing
- 🟩 Replication Through Removable Media

### Resource Development

- 🟥 Acquire Infrastructure
- 🟥 Compromise Infrastructure
- 🟥 Obtain Capabilities
- 🟨 Stage Capabilities
- 🟩 Develop Capabilities

### Execution

- 🟥 Command and Scripting Interpreter
- 🟥 User Execution
- 🟨 Scheduled Task/Job
- 🟨 Windows Management Instrumentation
- 🟩 Exploitation for Client Execution

### Persistence

- 🟨 Account Manipulation
- 🟨 Boot or Logon Autostart Execution
- 🟨 Create or Modify System Process
- 🟨 Hijack Execution Flow
- 🟨 Scheduled Task/Job

### Privilege Escalation

- 🟨 Abuse Elevation Control Mechanism
- 🟨 Boot or Logon Autostart Execution
- 🟨 Create or Modify System Process
- 🟨 Hijack Execution Flow
- 🟨 Scheduled Task/Job

### Defense Evasion

- 🟥 Obfuscated Files or Information
- 🟧 Masquerading
- 🟨 Abuse Elevation Control Mechanism
- 🟨 Deobfuscate/Decode Files or Information
- 🟨 Hijack Execution Flow
- 🟨 Modify Registry
- 🟨 System Binary Proxy Execution

### Discovery

- 🟨 Domain Trust Discovery
- 🟨 Process Discovery
- 🟨 Remote System Discovery
- 🟨 System Network Configuration Discovery
- 🟨 System Network Connections Discovery
- 🟨 System Owner/User Discovery
- 🟨 System Service Discovery
- 🟩 File and Directory Discovery

### Reconnaissance

- 🟨 ActiveScanning

### Collection

- 🟨 Archive Collected Data

### Command and Control

- 🟨 Proxy

### Exfiltration

- 🟨 Exfiltration Over Web Service

### Credential Access

- 🟥 OS Credential Dumping

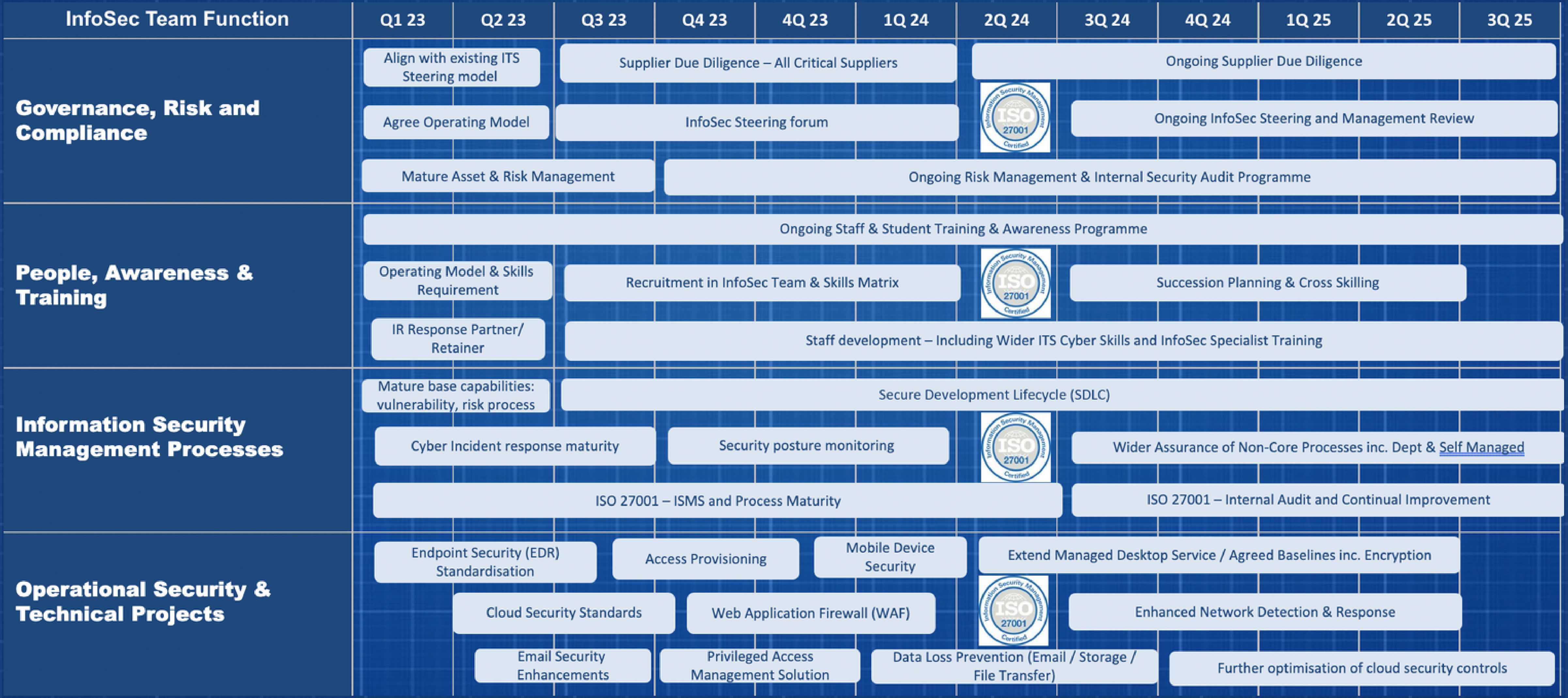
### Lateral Movement

- 🟨 Exploitation of Remote Services
- 🟩 Lateral Tool Transfer
- 🟩 Replication Through Removable Media

### legend

| 🟩 | 🟩 | 🟨 | 🟧 | 🟧 | 🟥 |
|---|---|---|---|---|---|
| 1.0 | 2.8 | 4.6 | 6.4 | 8.2 | 10 |

# Cyber Maturity Blueprint - Example



InfoSec Team Function

Q1 23 | Q2 23 | Q3 23 | Q4 23 | 4Q 23 | 1Q 24 | 2Q 24 | 3Q 24 | 4Q 24 | 1Q 25 | 2Q 25 | 3Q 25

**Governance, Risk and Compliance**

Align with existing ITS Steering model

Supplier Due Diligence – All Critical Suppliers

Ongoing Supplier Due Diligence

Agree Operating Model

InfoSec Steering forum

Ongoing InfoSec Steering and Management Review

Mature Asset & Risk Management

Ongoing Risk Management & Internal Security Audit Programme

**People, Awareness & Training**

Ongoing Staff & Student Training & Awareness Programme

Operating Model & Skills Requirement

Recruitment in InfoSec Team & Skills Matrix

Succession Planning & Cross Skilling

IR Response Partner/ Retainer

Staff development – Including Wider ITS Cyber Skills and InfoSec Specialist Training

**Information Security Management Processes**

Mature base capabilities: vulnerability, risk process

Secure Development Lifecycle (SDLC)

Cyber Incident response maturity

Security posture monitoring

Wider Assurance of Non-Core Processes inc. Dept & Self Managed

ISO 27001 – ISMS and Process Maturity

ISO 27001 – Internal Audit and Continual Improvement

**Operational Security & Technical Projects**

Endpoint Security (EDR) Standardisation

Access Provisioning

Mobile Device Security

Extend Managed Desktop Service / Agreed Baselines inc. Encryption

Cloud Security Standards

Web Application Firewall (WAF)

Enhanced Network Detection & Response

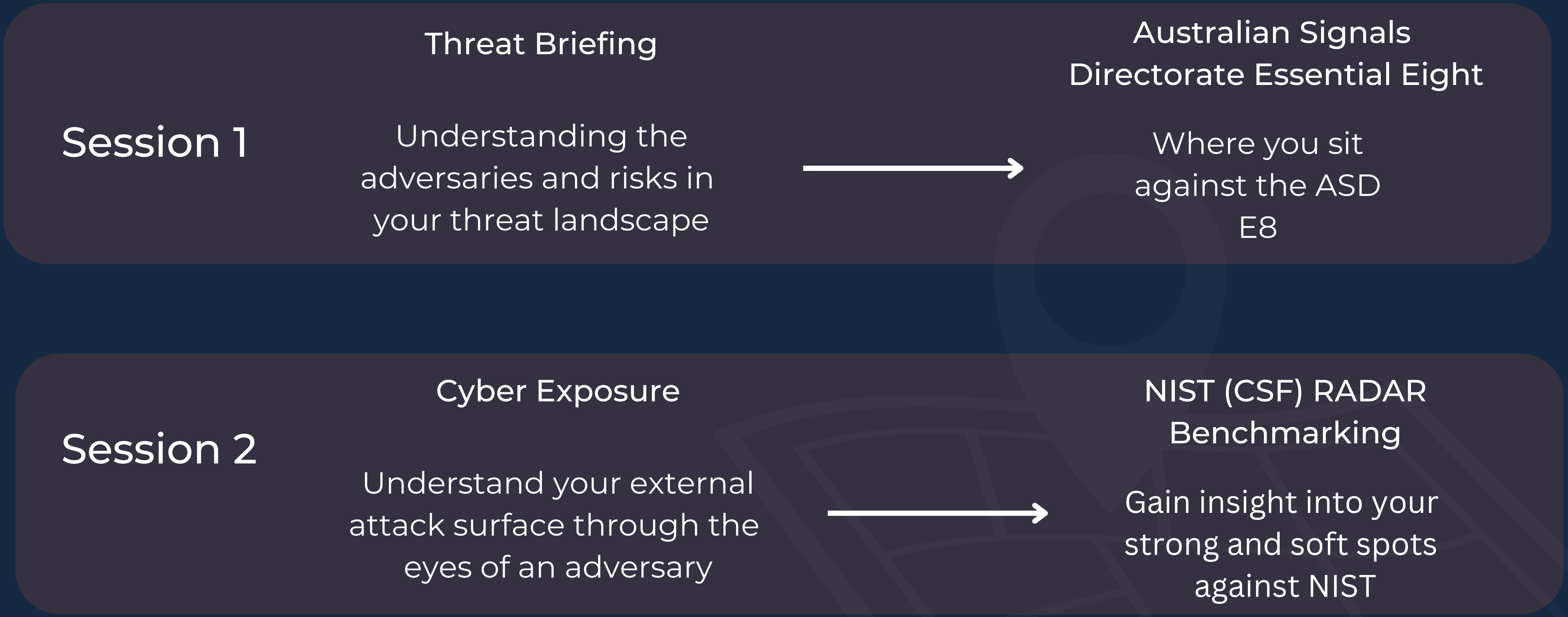
Email Security Enhancements

Privileged Access Management Solution

Data Loss Prevention (Email / Storage / File Transfer)

Further optimisation of cloud security controls

# Mapping your Blueprint



## Session 1

**Threat Briefing**

Understanding the adversaries and risks in your threat landscape

→

**Australian Signals Directorate Essential Eight**

Where you sit against the ASD E8

## Session 2

**Cyber Exposure**

Understand your external attack surface through the eyes of an adversary

→

**NIST (CSF) RADAR Benchmarking**

Gain insight into your strong and soft spots against NIST

# Mapping your Blueprint: Session One

Australian Government
Australian Signals Directorate

ACSC
Australian
Cyber Security Centre

Essential 8

## Threat Briefing

- Current Industry Trends
- Risks to Higher Education
- Highlight Environmental Blind Spots

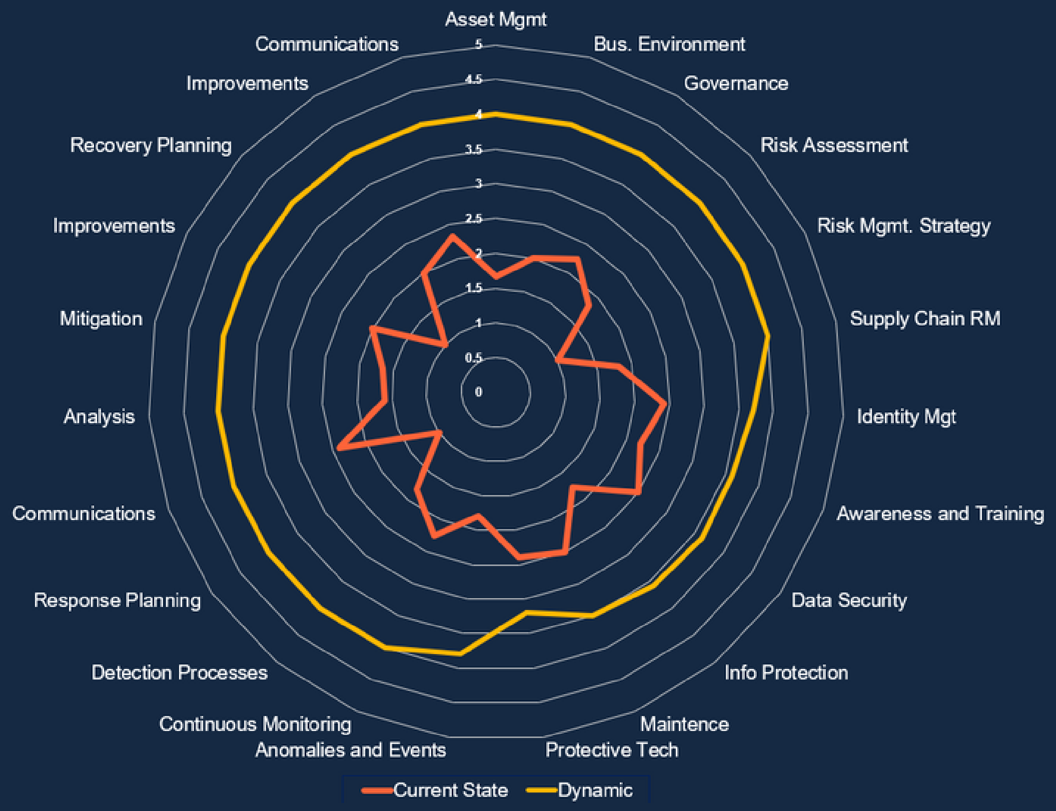
## ASD Essential 8 Whiteboard Session

- Understand maturity levels and mappings
- Review current controls and standings
- Identify potential for maturity growth

# Mapping your Blueprint: Session Two

## Cyber Exposure

- Understand how motivated attackers find organizational weaknesses.
- See how your organization looks from the outside looking in



## NIST (CSF) RADAR Benchmarking

- Map out your current controls and process against NIST
- View maturity scored in specific areas to better understand individual potential for growth

# Mapping your Blueprint: Next Steps

## Use insights gained to outline goals, objectives & vision

- High level strategy & tactical plans
- Design operating model

## Identify the activities required to meet goals

- Leverage current environment and resources
- System Selection & Prioritization
- Understanding area's of investment

## Assign priority to activities and map to blueprint

- Outline long term strategy
- Order the prioritization of activities
- Align budgetary requirements and resources with prioritization timelines

## *Testimonials from our clients..*

I just wanted to say once again that you were amazing when the cyber-attack hit, everybody pulling together worked together for the benefit of the students, staff, our institution, and the wider community.

Once again, thank you Waterstons for all you have done, are doing, and will continue to do to maintain vigilance and keep our University and our sector as safe as we can"

**David Conway**
Deputy Technical Director and Head of IT
University of Sunderland

We understand that the Cyber risk to the HE sector is one which no institution can afford to ignore. As an IT service we are committed to deploying the appropriate people, processes and technology controls to safeguard our data and reputation.

Waterstons has been our trusted partner to help us not only to build an in house security function but also act as our strategic advisor in the field of cyber security.
Their specialists have worked with us side by side as one virtual team to make our cyber security strategy a reality

**Rachel Bence**
CIO, Queen Mary University of London

The level of engagement and professionalism displayed by the Waterstons Team has been first class at every level. All the requirements were fully understood, and the review was mobilised with the full support and confidence of the LBU stakeholders both in the wider business and in IT."

“Waterstons have demonstrated a depth of knowledge in both the needs of the University and the wider HE Sector, as well as detailed technical knowledge which has ensured that we have been able to gain maximum value from the investment we are making in the review.”

“Of note has been the high level of engagement and direct ownership from senior colleagues in Waterstons in both the direction and management of the review, and in developing a genuine partnership”.

**Nigel Buckland**
Associate Director, IT Operations
Leeds Beckett University

Still have questions, comments or concerns?

Waterstons

Our helpful team are able to get you on track.

☎ 02 9160 8430

🌐 www.waterstons.com.au

✉ info@waterstons.com.au