AEMO
AUSTRALIAN ENERGY MARKET OPERATOR

Risk-Based AESCSF

2025

We acknowledge the Traditional Custodians of the land, seas and waters across Australia. We honour the wisdom of Aboriginal and Torres Strait Islander Elders past and present and embrace future generations.

We acknowledge that, wherever we work, we do so on Aboriginal and Torres Strait Islander lands. We pay respect to the world's oldest continuing culture and First Nations peoples' deep and continuing connection to Country, and hope that our work can benefit both people and Country.

'Journey of unity: AEMO's Reconciliation Path' by Lani Balzan

AEMO Group is proud to have launched its first Reconciliation Action Plan in May 2024. 'Journey of unity: AEMO's Reconciliation Path' was created by Wiradjuri artist Lani Balzan to visually narrate our ongoing journey towards reconciliation – a collaborative endeavour that honours First Nations cultures, fosters mutual understanding, and paves the way for a brighter, more inclusive future.

Read our RAP

Agenda

Introduction

Understanding Risk Through the Lens of AESCSF

Scenario-Based Case Study: Cyber Attack Simulation

Lessons Learned and Key Takeaways

Annual AESCSF Program

Assessment Outcomes & Next Steps

How the AESCSF Supports Risk Reduction

The AESCSF reduces cyber risk by helping organisations identify weaknesses, prioritise controls, and align security practices with operational impact.

Domains

Structured areas

Provides a structured approach to identify and address risk across IT, OT, and governance areas.

Ensures no critical area is overlooked by mapping practices to all functional layers of an organisation.

The domains can be separated into three scopes: Enterprise-wide, Operating Environments, External Parties.

Maturity Indicator Levels (MILs)

Levels from ad hoc to governed

Highlights weakest areas and guides progressive from ad hoc to governed practices.

Enables prioritisation of investment and effort by showing where capabilities are least mature.

Security Profiles (SP)

Risk based target state

Aligns security expectations with organisational criticality, ensuring higher-risk entities adopt stronger controls

Helps regulators and asset owners tailor expectations based on the organisation's role in the energy ecosystem.

Co-designed by industry with the ASD.

Practices and Anti-Patterns

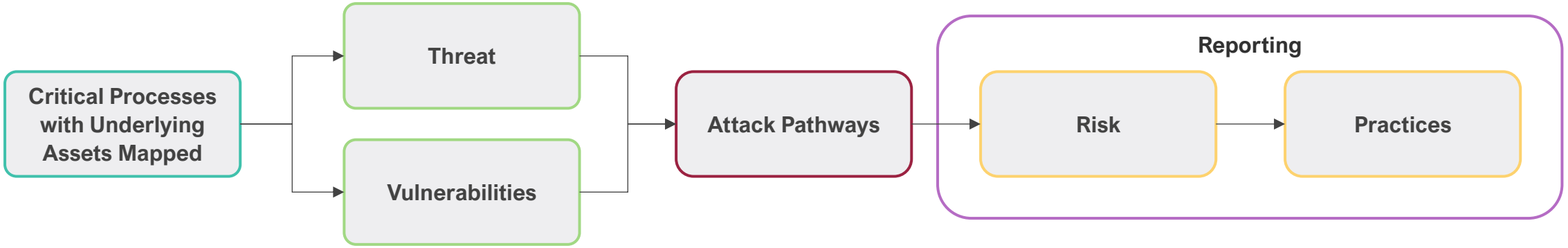
Good and bad behaviours defined across MILs

Aligns Promotes secure behaviours while flagging risky or non-negotiable bad practices that increase exposure

Encourages continuous improvement by showing both what to do and what to avoid.

Cyber Risk Identification and Mitigation Process

Cyber risk is inherently complex. With expansive attack surfaces and numerous interdependencies, traditional linear methods of risk identification fall short. This complexity often makes it challenging for executives to fully grasp the nature and implications of cyber threats. The process outlined below presents a simplified approach to identifying risks by focusing on the most likely attack pathways. This enables a clearer, more strategic view of cyber risk for informed decision-making.



Scenario: PowerGen Retail

PowerGen Retail is a fictional, energy provider specialising in electricity generation and retail distribution. The company serves residential, commercial, and industrial customers with reliable, sustainable, and cost-effective energy solutions.

Information Technology (IT)

- Systems support critical business operations, including customer billing, CRM, and employee productivity tools.
- These systems are cloud-based, enabling flexibility, and scalability.

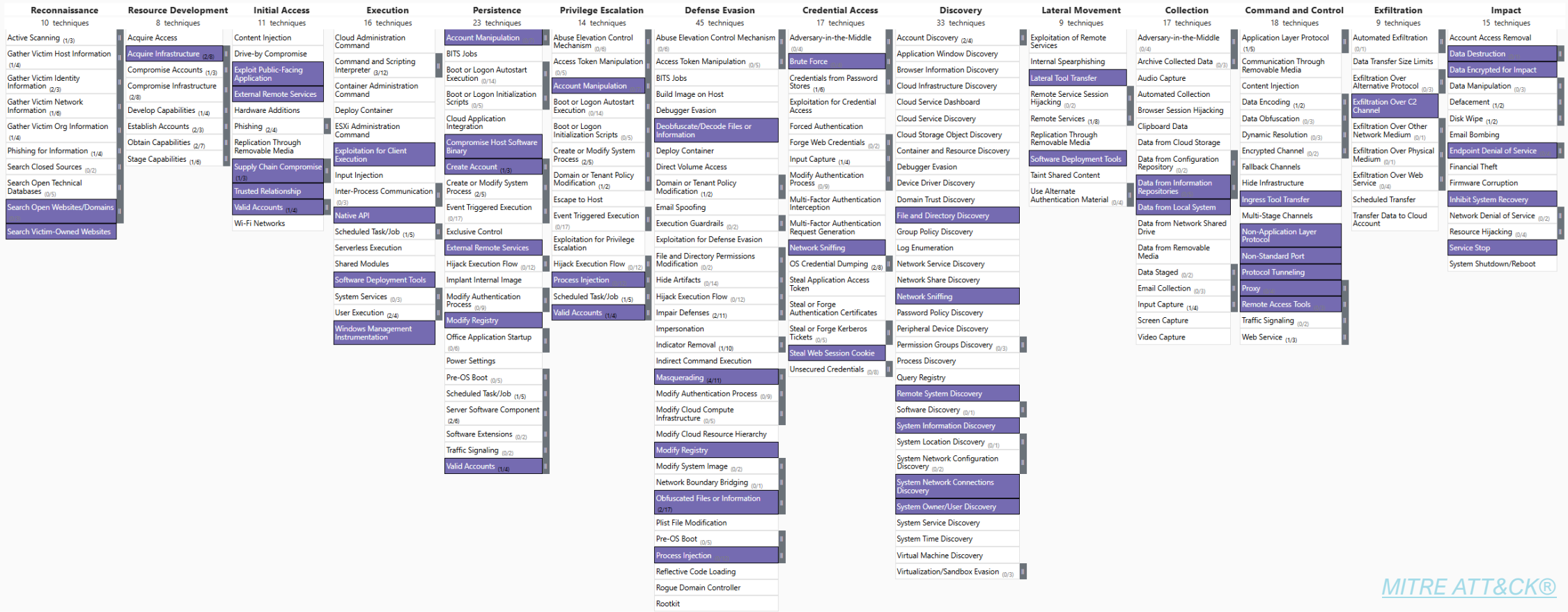
Operational Technology (OT)

- Oversees the real-time control and monitoring of electricity generation and distribution.
- This includes SCADA systems, industrial control systems, and a smart metering network that enables efficient grid management.

MITRE ATT&CK Threat Mapping

The MITRE ATT&CK framework is a widely used resource that outlines how threat actors behave based on real-world tactics, techniques, and procedures (TTPs). By mapping these behaviours to critical assets and known vulnerabilities, organisations can identify likely attack pathways and better prioritise risk mitigation efforts.

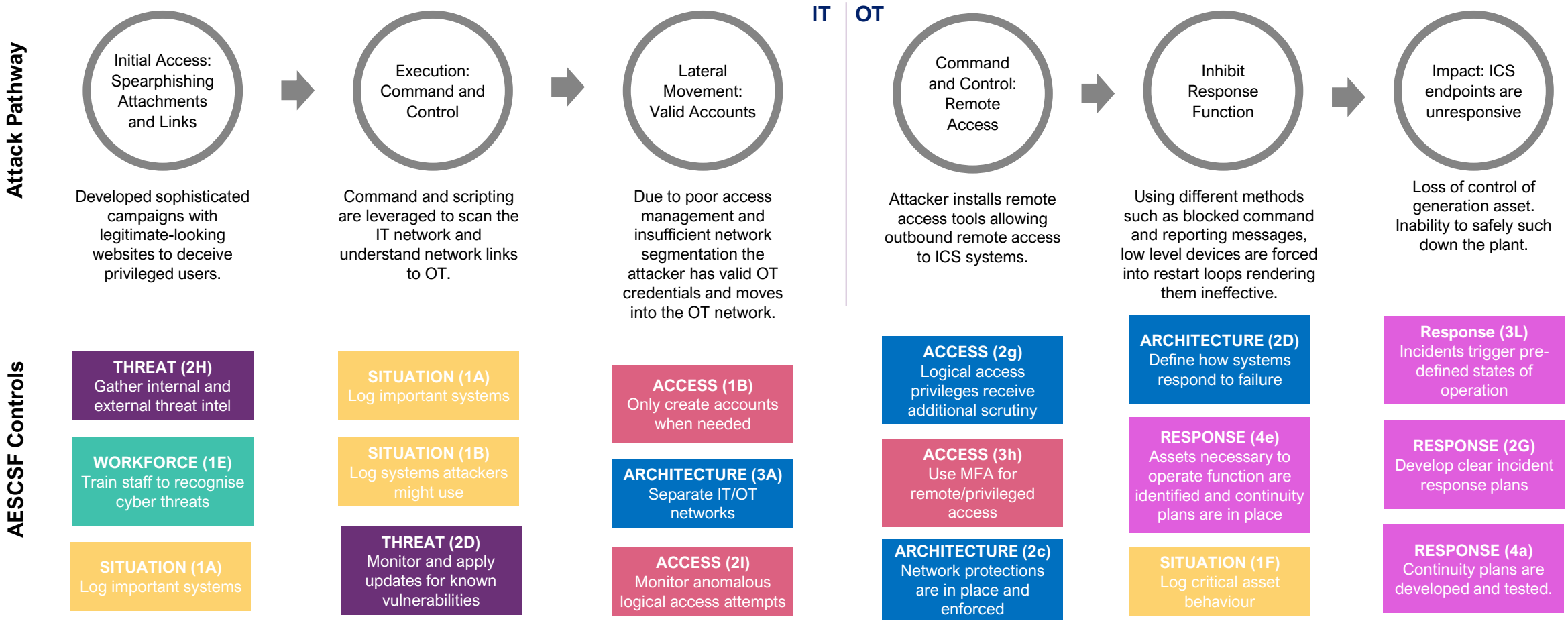
Sandworm TTPs



MITRE ATT&CK®

Case Study: Cyber Attack on a Generation + Retailer with IT & OT

Disruption of electricity transmission in PowerGen Retail's industrial control systems (ICS) caused by a nation state attacker's meticulously crafted advanced persistent threat (APT), leveraging a combination of techniques and tactics to infiltrate and traverse from the enterprise IT system into the OT environment, leading to potential operational outages and critical infrastructure compromise.



Priority Practices

The ASD has defined Practices within each Security Profile that should be completed as a priority as key practices for cyber security best practice.

- The table (right) details these Practices (26 total).
- Refer to the AESCSF Framework Core for more information on Practices and their MIL.
- When prioritising Practices, the advice from the ASD is to complete Practices in the related preceding Security Practices (i.e. Practices in Security Profile 1 should be prioritised over Priority Practices in Security Profile 2).

AESCSF Priority Practices by Security Profile			
Domain	**Profile 1**	**Profile 2**	**Profile 3**
ASSET	ASSET-1A ASSET-2A ASSET-3A ASSET-4D	ASSET-1G *ASSET-2G* ASSET-3D ASSET-4G	ASSET-1F ASSET-2F ASSET-3E
PRIVACY	PRIVACY-1B	PRIVACY-1I	PRIVACY-1M
PROGRAM	PROGRAM-2A	PROGRAM-2E	PROGRAM-1H
THIRD-PARTIES	THIRD-PARTIES-1A THIRD-PARTIES-1B THIRD-PARTIES-2A THIRD-PARTIES-2B	THIRD-PARTIES-1C THIRD-PARTIES-2F THIRD-PARTIES-2M	None
ACCESS	ACCESS-1B ACCESS-1F ACCESS-2G ACCESS-3H	ACCESS-2I ACCESS-3J	None
RESPONSE	RESPONSE-2G RESPONSE-3C RESPONSE-4E	RESPONSE-1F RESPONSE-3L RESPONSE-2D	RESPONSE-3J
ARCHITECTURE	ARCHITECTURE-2B ARCHITECTURE-2C ARCHITECTURE-3A	ARCHITECTURE-1C ARCHITECTURE-3F ARCHITECTURE-3G ARCHITECTURE-3I ARCHITECTURE-3H	ARCHITECTURE-1I ARCHITECTURE-4G
RISK	RISK-2A RISK-3A RISK-4A	RISK-1F RISK-2F RISK-2M RISK-3D	RISK-3G RISK-4E
SITUATION	SITUATION-1A	SITUATION-1B	SITUATION-1F
THREAT	THREAT-2D THREAT-2H	THREAT-1G THREAT-2G	THREAT-2I
WORKFORCE	WORKFORCE-1A WORKFORCE-1B WORKFORCE-1E	WORKFORCE-1F WORKFORCE-3C WORKFORCE-3E	WORKFORCE-2G
Total	**29**	**28**	**13**

Assessment Outcomes & Next Steps

The next steps for energy sector participants are:

1. Please complete your organisation's assessment – which was made available on **1 May 2025**. The portal will remain open until **6 June 2025** to complete the assessment.

2. The specific closure date of the assessment portal will be **6 June 2025**. Your submission can include your CEO's attestation response letter for full AESCSF assessments if desired (Not mandatory).

3. All entities who submit a 2025 Assessment will have access to the AESCSF 2025 Benchmarking Portal. Organisations will be able to compare against deidentified industry benchmarks based on the population of 2025 Assessments submitted.

Support:
For any AESCSF related queries, please email the Program Team via **aescsf@aemo.com.au**