

Risk-Based AESCFS

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

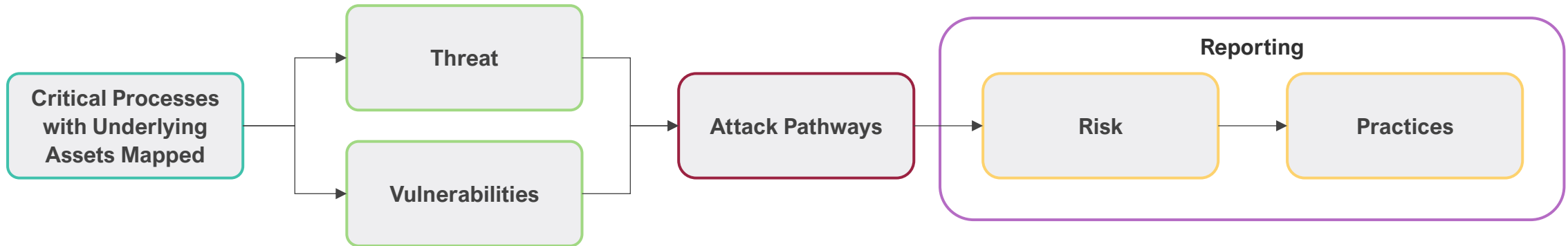
Good and bad behaviours defined across MILs

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

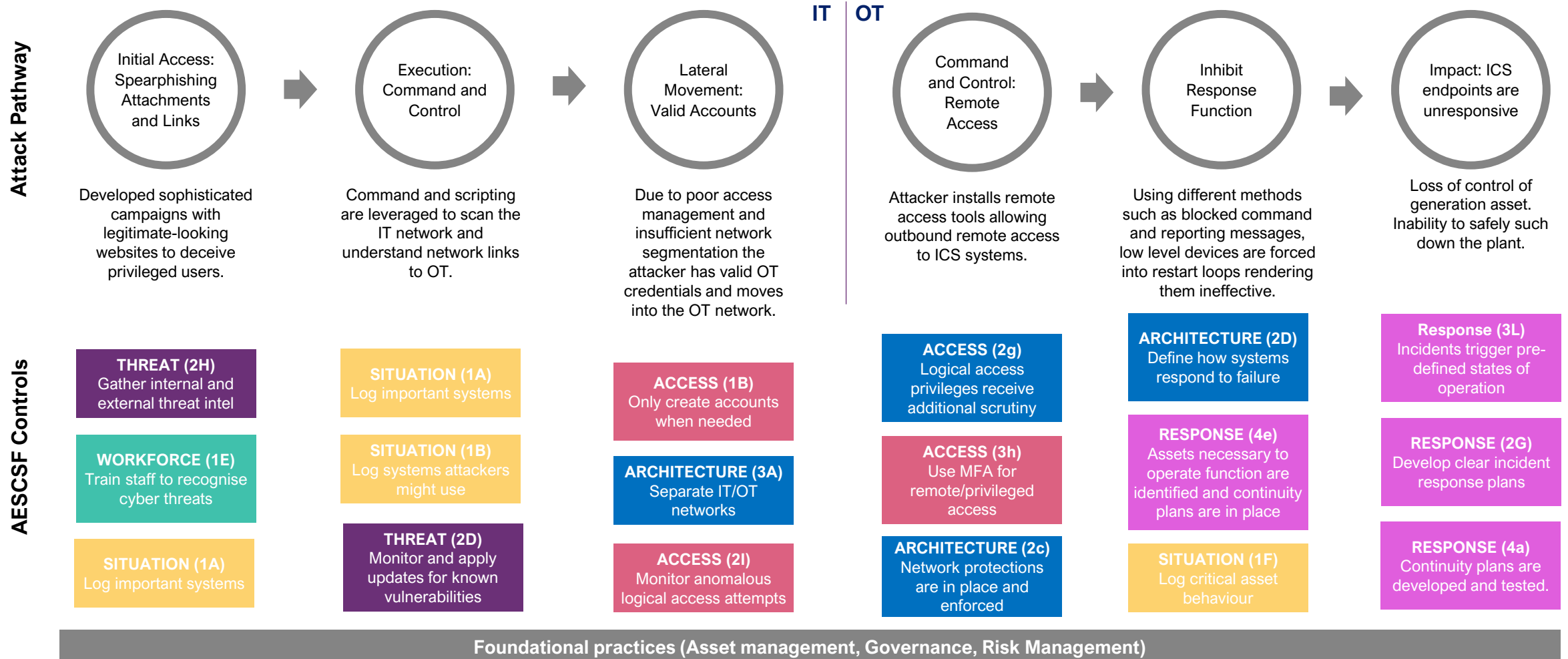
The MITRE ATT&CK framework is a widely used resource that outlines how threat actors behave based on real-world tactics, techniques, and procedures (TTPs). By mapping these behaviours to critical assets and known vulnerabilities, organisations can identify likely attack pathways and better prioritise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

Sandworm TTPs

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 11 techniques	Execution 16 techniques	Persistence 23 techniques	Privilege Escalation 14 techniques	Defense Evasion 45 techniques	Credential Access 17 techniques	Discovery 33 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 18 techniques	Exfiltration 9 techniques	Impact 15 techniques
Active Scanning (1/3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation	Abuse Elevation Control Mechanism (0/6)	Abuse Elevation Control Mechanism (0/6)	Adversary-in-the-Middle (0/4)	Account Discovery (2/4)	Exploitation of Remote Services	Adversary-in-the-Middle (0/4)	Application Layer Protocol (1/5)	Automated Exfiltration (0/7)	Account Access Removal
Gather Victim Host Information (1/4)	Acquire Infrastructure (2/8)	Drive-by Compromise	Command and Scripting Interpreter (0/12)	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force	Application Window Discovery	Internal Spearphishing	Archive Collected Data (0/3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (2/3)	Compromise Accounts (1/3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (0/14)	Account Manipulation	BITS Jobs	Credentials from Password Stores (1/8)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
Gather Victim Network Information (1/6)	Compromise Infrastructure (2/8)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (0/5)	Build Image on Host	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Automated Collection	Data Encoding (1/2)	Exfiltration Over C2 Channel	Defacement (1/2)
Gather Victim Org Information (1/4)	Develop Capabilities (1/4)	Hardware Additions	ESXi Administration Command	Cloud Application Integration	Boot or Logon Autostart Execution (0/14)	Boot or Logon Autostart Execution (0/14)	Forced Authentication	Cloud Service Dashboard	Remote Services (1/8)	Browser Session Hijacking	Data Obfuscation (0/3)	Exfiltration Over Other Network Medium (0/1)	Disk Wipe (1/2)
Phishing for Information (1/4)	Establish Accounts (2/3)	Phishing (2/4)	Exploitation for Client Execution	Compromise Host Software Binary	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Forge Web Credentials (0/2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (0/3)	Exfiltration Over Physical Medium (0/1)	Email Bombing
Search Closed Sources (0/2)	Obtain Capabilities (2/7)	Replication Through Removable Media	Input Injection	Create or Modify System Process (2/5)	Create or Modify System Process (2/5)	Create or Modify System Process (2/5)	Input Capture (1/4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel (0/2)	Exfiltration Over Web Service (0/4)	Endpoint Denial of Service (1/1)
Search Open Technical Databases (0/5)	Stage Capabilities (1/6)	Supply Chain Compromise (1/3)	Inter-Process Communication	Create Account (1/3)	Domain or Tenant Policy Modification (1/2)	Domain or Tenant Policy Modification (1/2)	Modify Authentication Process (0/9)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (0/2)	Fallback Channels	Exfiltration Over Other Network Medium (0/1)	Financial Theft
Search Open Websites/Domains	Wi-Fi Networks	Trusted Relationship	Native API	Event Triggered Execution (0/17)	Event Triggered Execution (0/17)	Event Triggered Execution (0/17)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (0/4)	Data from Information Repositories	Hide Infrastructure	Exfiltration Over Web Service (0/4)	Firmware Corruption
Search Victim-Owned Websites		Valid Accounts (1/4)	Scheduled Task/Job (1/5)	Exclusive Control	Event Triggered Execution (0/17)	Event Triggered Execution (0/17)	Multi-Factor Authentication Request Generation	Device Driver Discovery		Data from Local System	Ingress Tool Transfer	Scheduled Transfer	Inhibit System Recovery
			Serverless Execution	External Remote Services	Execution Flow Hijack (0/12)	Execution Flow Hijack (0/12)	Network Sniffing	Domain Trust Discovery		Data from Network Shared Drive	Multi-Stage Channels	Transfer Data to Cloud Account	Network Denial of Service (0/2)
			Software Deployment Tools	Hijack Execution Flow (0/12)	Process Injection	Process Injection	OS Credential Dumping (2/8)	File and Directory Discovery		Data from Removable Media	Non-Application Layer Protocol		Resource Hijacking (0/4)
			System Services (0/3)	Implant Internal Image	Scheduled Task/Job (1/5)	Scheduled Task/Job (1/5)	Steal Application Access Token	Group Policy Discovery		Data Staged (0/2)	Non-Standard Port		Service Stop
			User Execution (2/4)	Modify Authentication Process (0/9)	Valid Accounts (1/4)	Valid Accounts (1/4)	Steal or Forge Authentication Certificates	Log Enumeration		Email Collection (0/3)	Protocol Tunneling		System Shutdown/Reboot
			Windows Management Instrumentation	Modify Registry	Office Application Startup (0/8)	Office Application Startup (0/8)	Steal or Forge Kerberos Tickets (0/5)	Network Service Discovery		Input Capture (1/4)	Proxy		
				Power Settings	Indirect Command Execution	Indirect Command Execution	Steal Web Session Cookie	Network Share Discovery		Screen Capture	Remote Access Tools		
				Pre-OS Boot (0/5)	Masquerading (4/11)	Masquerading (4/11)	Unsecured Credentials (0/8)	Network Sniffing		Video Capture	Traffic Signaling (0/2)		
				Scheduled Task/Job (1/5)	Modify Authentication Process (0/9)	Modify Authentication Process (0/9)		Peripheral Device Discovery			Web Service (1/3)		
				Server Software Component (2/8)	Modify Cloud Compute Infrastructure (0/5)	Modify Cloud Compute Infrastructure (0/5)		Permission Groups Discovery (0/3)					
				Software Extensions (0/2)	Modify Cloud Resource Hierarchy	Modify Cloud Resource Hierarchy		Process Discovery					
				Traffic Signaling (0/2)	Modify Registry	Modify Registry		Query Registry					
				Valid Accounts (1/4)	Modify System Image	Modify System Image		Remote System Discovery					
					Network Boundary Bridging (0/1)	Network Boundary Bridging (0/1)		Software Discovery (0/1)					
					Obfuscated Files or Information (2/17)	Obfuscated Files or Information (2/17)		System Information Discovery					
					Plist File Modification	Plist File Modification		System Location Discovery (0/1)					
					Pre-OS Boot (0/5)	Pre-OS Boot (0/5)		System Network Configuration Discovery (0/2)					
					Process Injection	Process Injection		System Network Connections Discovery					
					Reflective Code Loading	Reflective Code Loading		System Owner/User Discovery					
					Rogue Domain Controller	Rogue Domain Controller		System Service Discovery					
					Rootkit	Rootkit		System Time Discovery					
								Virtual Machine Discovery					
								Virtualization/Sandbox Evasion (0/3)					

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