Australia Energy Sector Cyber Security Framework Education Workshop

AEMO
AUSTRALIAN ENERGY MARKET OPERATOR

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

General Education Session

Background
Evolving Energy Grid
Threats to the Energy Sector
Energy Incidents Around The Globe
Challenges in the Australian Energy Sector

Introduction to the AESCSF
High-Level Overview / Benefits
The AESCSF Journey So Far

2025 AESCSF Program
User Journey / Timeline
Portal Demonstration
Worked Example

Assessment Outcomes & Next Steps
FAQs

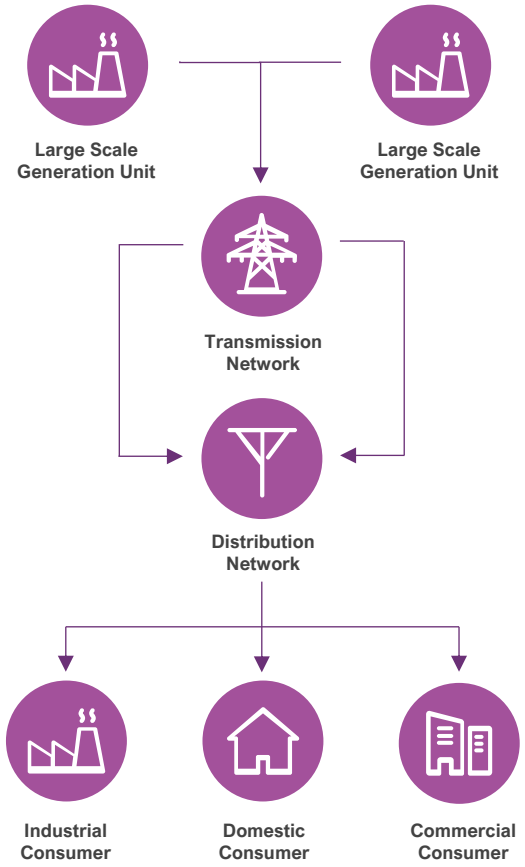
Optional: Framework Structure Deep Dive
How to use the Framework
AESCSF Explained

Background

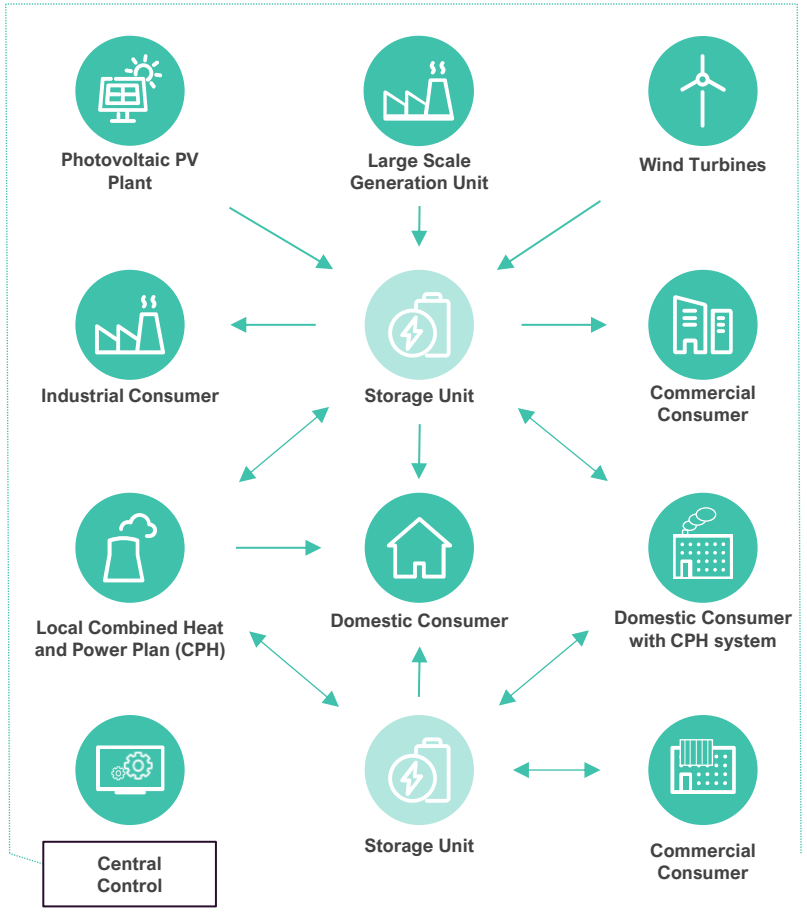
Evolving Energy Grid: From Centralised to Distributed Generation

This shift introduces increased complexity, expanded attack surfaces, and new cybersecurity challenges that organisations must address to ensure resilience, compliance, and operational security.

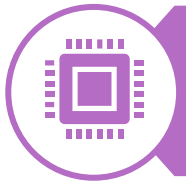
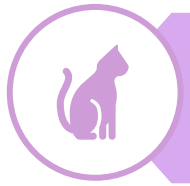
Centralised Power Generation



Distributed Power Generation



Who is Targeting Australia's Energy Sector

Attacker Name	Targets	Impact
 Volt Typhoon	• Critical infrastructure sectors including communications, utilities and transportation.	• Potential to disrupt energy operations undetected. • Threatens national resilience and supply chain continuity.
 Salt Typhoon	• Global telecom and infrastructure networks, with implications for Australian energy communications.	• Compromise of internal communications and SCADA-linked systems in energy operations.
 LockBit	• Australian energy companies, utilities, and contractors.	• May cause operational disruption, reputational damage and financial loss.
 APT40	• Targeting Australian government and private infrastructure.	• Rapid disclosed vulnerability exploitation and adaptive persistence which leads to data exfiltration and potential disruption.
 Sandworm/ Seashell Blizzard	• High value critical infrastructure and government targets.	• Targeted operational disruption with malware direct into ICS networks.

Energy Incidents Around The Globe

The increasing number of cyber incidents within the energy sector highlights the urgent need to enhance security measures to protect critical infrastructure. Several global documented incidents within the energy sector are covered below.

FrostyGoop/ Sandworm – Lvivteploenergo
Incident Type: OT Attack

- Jan 2024 600+ apartment blocks lost heat and hot water for around 48hrs.
- This group manipulated the set points of the hot water systems.
- Infiltration of the network had occurred nearly a year earlier by exploiting a router.
- FrostyGoop interacted directly with ICS via Modbu.

Littleton Electric Light and Water Departments (LELWD) (2023)
Incident Type: Advanced Persistent Threat (APT)

- Within 2023, the Chinese state-sponsored group Volt Typhoon gained access to a public utility company systems in Massachusetts, remained undetected for 300 days.
- The attackers initially compromised LELWD's IT network by exploiting vulnerabilities in internet-facing systems. They then used techniques to move laterally into the operational technology (OT) network.

Halliburton (2024)
Incident Type: Ransomware Attack

- In August 2024, Halliburton, a major oilfield services company, experienced a significant cyberattack that led to data breaches and operational disruptions.
- An unauthorized third party gained access to Halliburton's systems, resulting in the exfiltration of sensitive company data.
- The company incurred approximately $35 million in costs related to the breach, affecting earnings and operational income.

Hitachi Energy (2023)
Incident Type: Supply Chain Attack

- Hitachi’s third-party software supplier was targeted by a ransomware attack in 2023.
- A threat actor entered a third-party system through an injection vulnerability.
- They gained access to Hitachi employee information.

Challenges in the Australian Energy Sector

What are your current security challenges?

Introduction to the AESCSF

Introduction to the AESCSF

What is the AESCSF?

- Built on **global standards**, including NIST CSF* and C2M2, ensuring alignment with international best practices.
- Goes beyond compliance, supporting **proactive risk management** rather than just meeting minimum regulatory requirements.
- Covers **IT, OT environments** and **supply chain**, recognising the increasing convergence of cyber and operational risks in energy systems.
- Focuses on **resilience**, ensuring organisations can detect, respond to, and recover from cyber incidents with minimal disruption.
- Supports regulatory alignment, particularly with the **SOCI Act**, by helping organisations meet Risk Management Program (RMP) obligations.
- Enables **sector-wide benchmarking**, allowing energy providers to compare their cybersecurity maturity against industry peers
- **Continuously evolving**, with Version 2 enhancing guidance on supply chain security, emerging threats, and risk-based decision-making.

Benefits of Using the AESCSF

Completing AESCSF Assessment

- Standardised Cybersecurity Practices
- Consistent Board-Level Reporting
- Securing Compliance Funding
- Comprehensive Security Framework
- Strengthening Cybersecurity Business Cases

Achieving Practices within AESCSF

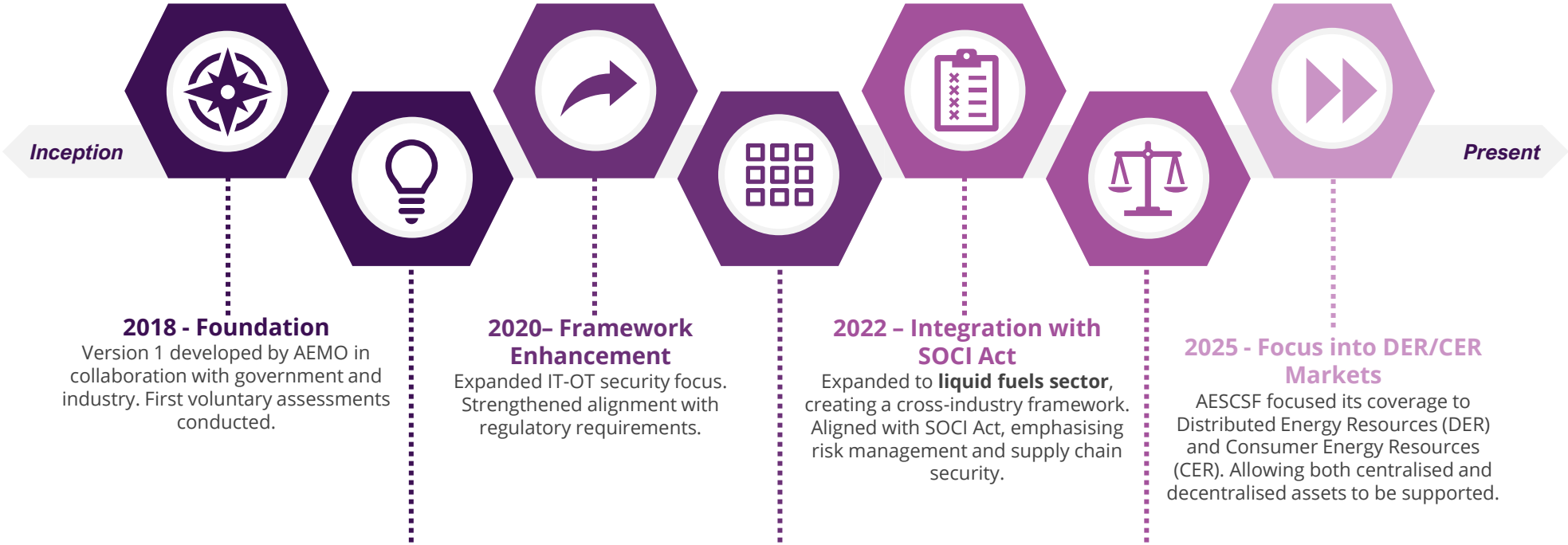
- Enhanced Risk Posture
- Holistic Cybersecurity Management
- Regulatory Compliance

Participating in the AESCSF Program

- Benchmarking and Community Engagement
- Industry Peer Insights
- Knowledge Leverage and Best Practice Sharing
- Influence on Policy and Investment
- Contribution to Energy Sector Resilience

The AESCSF Journey So Far

The timeline reflects the AESCSF's ongoing evolution to enhance cybersecurity resilience within Australia's energy sector.



Security of Critical Infrastructure Act

What is the SOCI Act?

The Security of Critical Infrastructure (SOCI) Act 2018 establishes legal requirements for protecting Australia's critical infrastructure sectors, including energy, water, gas, and communications.

- **Purpose**: Strengthens cyber and operational resilience of critical infrastructure.
- **Key obligations**: Risk management, cyber incident reporting, and enhanced security measures for Systems of National Significance (SoNS).
- **Enforced by**: The Australian Government through the Cyber and Infrastructure Security Centre (CISC).

Who is covered?

1. Energy
2. Water & Sewerage
3. Communications
4. Transport
5. Data Storage & Processing
6. Financial Services & Markets
7. Healthcare & Medical
8. Higher Education & Research
9. Food & Grocery
10. Space Technology
11. Defence Industry

What do organisations need to do under SOCI?

Determine if Covered:

- Identify whether your organisation is classified as critical infrastructure under the SOCI Act.
- Check if your assets fall under Regulated Critical Infrastructure (RCI) or Systems of National Significance (SoNS).

Comply with Key Obligations:

- Risk Management Program (RMP): Identify and mitigate cyber, physical, supply chain, and personnel risks.
- Incident Reporting: Mandatory reporting of cyber security incidents within 12–72 hours, depending on severity.
- Enhanced Cyber Security Obligations (for SoNS): Includes regular cyber security exercises and system visibility requirements.

How does it relate to the AESCSF?

- AESCSF V1 SP-1 (Security Profile 1) is referenced as a cyber security framework within the Act and V2 is an equivalent framework.
- Provides a structured, industry-aligned approach to meeting SOCI's Risk Management Program (RMP) requirements.
- Helps organisations assess cyber maturity, identify gaps, and implement compliance-driven improvements.

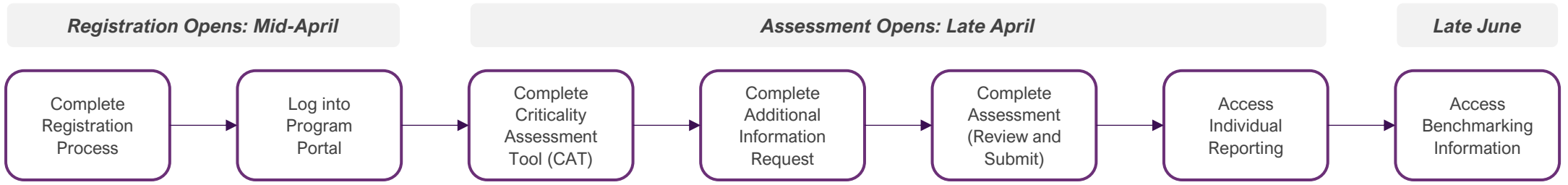
AESCSF v1 to v2 Comparison

In 2022, AEMO in partnership with the ACSC, leading Australian energy organisations and the Federal Department of Climate Change, Energy, the Environment and Water updated the AESCSF in 2022 to align with current international standards and address emerging technologies and the evolving cyber threat landscape.

New Updates	Why?
Aligned to C2M2 v2.1.	Strengthens protection against emerging threats by continuing to align AESCSF with global best practices and cybersecurity maturity models.
Enhanced Risk Management Domain to align with the intention of SOCI.	Integrates SOCI Act principles to shift risk management from reactive compliance checklists to a proactive, system-wide approach that strengthens operational resilience against cascading threats.
Addition of Architecture Domain.	Ensures security is embedded in system design from the outset, addressing the complexity of legacy and complex environments.
Changed Dependencies Domain to Third-Party Risk Management.	Strengthens supply chain security, acknowledging that modern cyber risks often originate from vendors and external service providers.
Updated guidance, context and practices to be pragmatic.	Moves beyond a compliance-driven mindset by incorporating real-world lessons and industry feedback, making the framework more actionable and adaptable.

Annual AESCSF Program

User Journey / Timeline



Step	Description
Complete Registration Process	• Participants to receive MFA registration link and create user account through ServiceNow
Log into Program Portal	• Log into ServiceNow platform using credentials
Complete Criticality Assessment Tool (CAT)	• Depending on whether an organisation is a market participant or not will result in them either receiving the CAT or not
Complete Company Setup Form	• All organisations will need to complete the company set up form which will provide additional information on the company which will be used for benchmarking purposes. This section will also allow for organisations to select the number and type of assessments they wish to complete
Complete Assessments	• Organisations will complete the number of full and lite assessments that was requested
Access Individual Reporting	• Immediately following the submission of the assessment, organisations will receive access to individual reporting of their results.
Access Benchmarking Information	• Once the survey has closed, benchmarking data will be provided for organisations.

Portal Demonstration

Portal Demonstration

2025 Australian Energy Sector Cyber Security Framework

Join us to improve the security of Australia's energy system

Dear Team,

The security of Australia's energy system is a national priority – one shared by all those who participate in the energy industry. The increasing diversity of Australia's energy systems, participants and geopolitical challenges makes protecting our Nation against cyber threats an ongoing and dynamic challenge.

Responding to the challenge requires individual and collective efforts. By protecting individual assets and organisations, we can safeguard the entire system. That is why we invite your organisation to join AEMO and your peers to assess your cyber security maturity using the Australian Energy Sector Cyber Security Framework (AESCSF).

What is the AESCSF?
The AESCSF is a risk-based cyber assessment framework that can be used to assess your organisation's cyber security posture. Developed collaboratively with industry and government in 2018 with a significant update in 2022, it draws upon global best practices to reflect emerging risks and contemporary threats to ensure it offers leading-edge cyber security maturity guidance, wherever you may be on the maturity curve.

Data from each assessment is anonymised and aggregated to enable an annual industry-wide health assessment which AEMO, industry and Australian and state governments can use to inform policy, investment, and sector-wide initiatives.

Participating in the AESCSF Program is voluntary but strongly encouraged for all participants in the energy industry, big and small.

Why participate?
Participating in the Program offers your organisation many benefits, in particularly enabling you to identify areas for improvement and the ability to benchmark your organisation's cyber security maturity against that of industry peers (benchmark data is anonymous).

You will also be fulfilling an important responsibility as part of Australia's energy industry by contributing to enhanced cyber resilience across the energy ecosystem.

Register for the AESCSF Program [AESCSF Registration Form]

2025 Australian Energy Sector Cyber Security Framework

Dear Patrick,

Thank you for your registration, and v
(AESCSF) Program. The AESCSF Pr
Your participation will contribute to st
appreciate your support with this imp

This email will cover:

- What is the AESCSF Program?
- Benefits of Participation
- 2025 Timeline
- Getting Started Guide
- Event Schedule
- Useful Links
- Help and Support

ACTION REQUIRED

Step 1: Set up your account access

*Refer to **Section 4: Getting Started***

Step 2: Register for the upcoming s

*Refer to **Section 5: Schedule of Su** scheduling.*

1 | WHAT

The AESCSF Program allows electricity, gas, liquid fuels, distributed & consumer energy resources organisations to assess their cyber security maturity and obtain insights into how they compare with their industry peers in their respective journeys.

2 | WHY

Participating in the AESCSF Program provides your organisation with several benefits including:

- **Maturity Insights:** Identify areas to strengthen your organisation's cyber resilience.
- **Risk Reduction:** Use assessment results to prioritise initiatives that reduce cyber risk.
- **Investment Justification:** Strengthen business cases for cybersecurity investment using sector-wide results.
- **Benchmarking:** Compare your organisation's cybersecurity maturity with industry peers.
- **Share Ideas:** Learn from a community of practitioners on the same journey.
- **Collective Resilience:** Enhance the overall cyber resilience of Australia's energy sector by contributing actionable data.
- **Regulatory Compliance:** Meet obligations under the Security of Critical Infrastructure (SOCI) Act. (Where applicable)

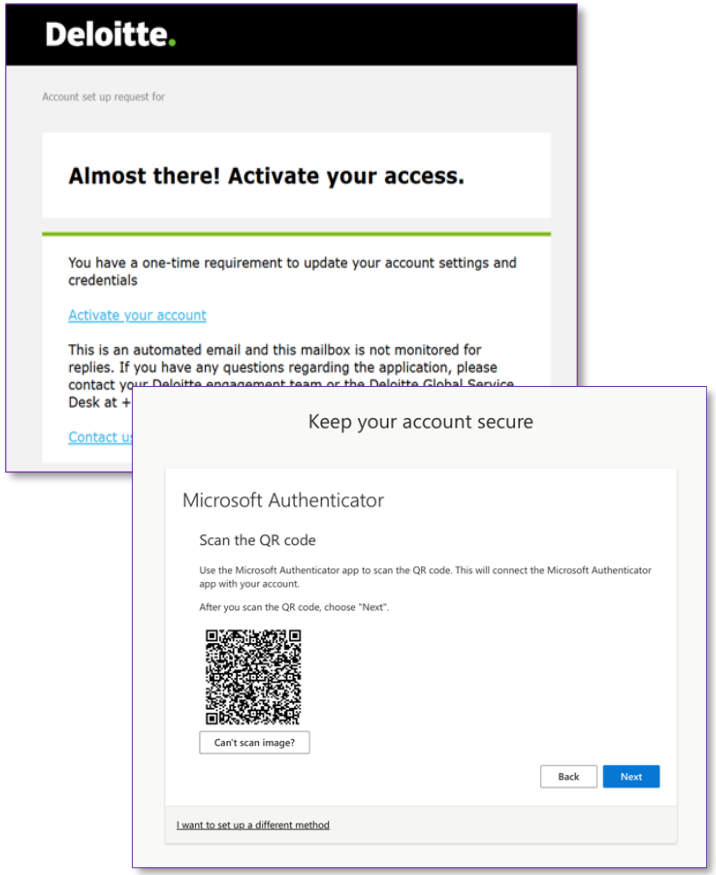
3 | 2025 TIMELINE

Mid-April – Portal Opens
Late April – Assessment Opens
April-May – Education Sessions
Early June – Assessment Closes
Late June – Benchmarking Results Ready

4 | GETTING STARTED

Follow these steps to complete your organisation's AESCSF submission:

1. **Registration:** Your organisation's point of contact (POC), and delegates have been registered using this link. Your ServiceNow accounts will be activated as per the below steps.
2. **MFA Setup:** Check your email for a message from noreply-logon@deloitte.com to set up Deloitte Multi-Factor Authentication (MFA). You can expect to receive this email within one business day. If you experience any issues, refer to the '***User Guide – Getting Started***' attached. Once this process is completed, you will be redirected to the ServiceNow portal to log in using your new credentials. If you aren't automatically redirected, use the link in Step 3 if necessary.



Deloitte.

Account set up request for

Almost there! Activate your access.

You have a one-time requirement to update your account settings and credentials

Activate your account

This is an automated email and this mailbox is not monitored for replies. If you have any questions regarding the application, please contact your Deloitte engagement team or the Deloitte Global Service Desk at +

Contact us

Keep your account secure

Microsoft Authenticator

Scan the QR code

Use the Microsoft Authenticator app to scan the QR code. This will connect the Microsoft Authenticator app with your account.

After you scan the QR code, choose "Next".

Can't scan image?

Back Next

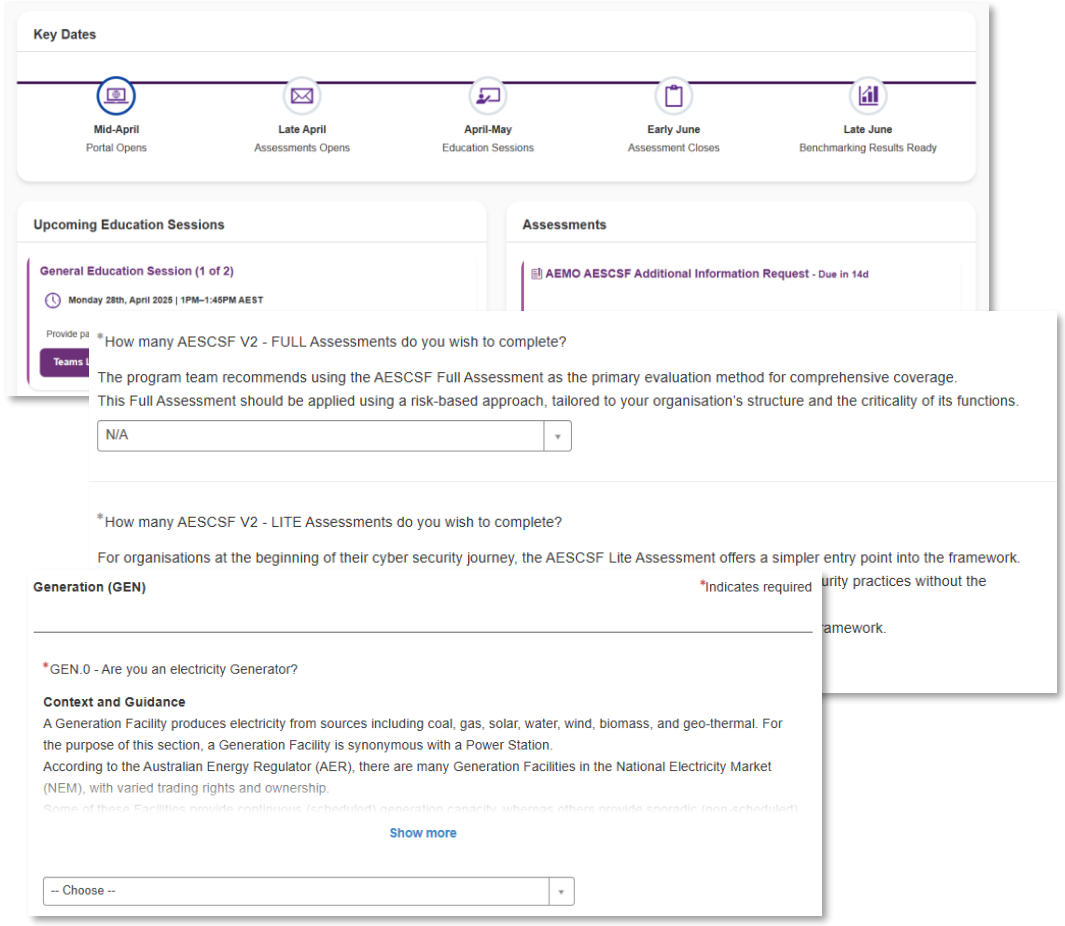
I want to set up a different method

Invitation to Participate

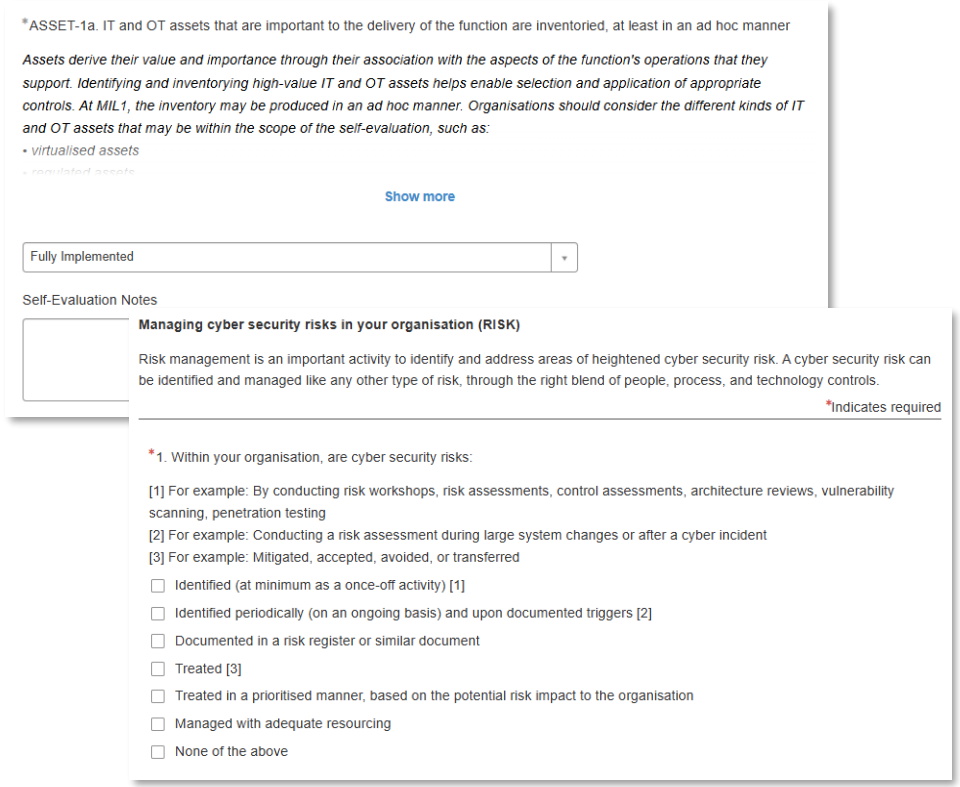
Account set-up

Verification code

Portal Demonstration



CAT and Additional Information Request Form



AESCSF Full and Lite

Worked Example

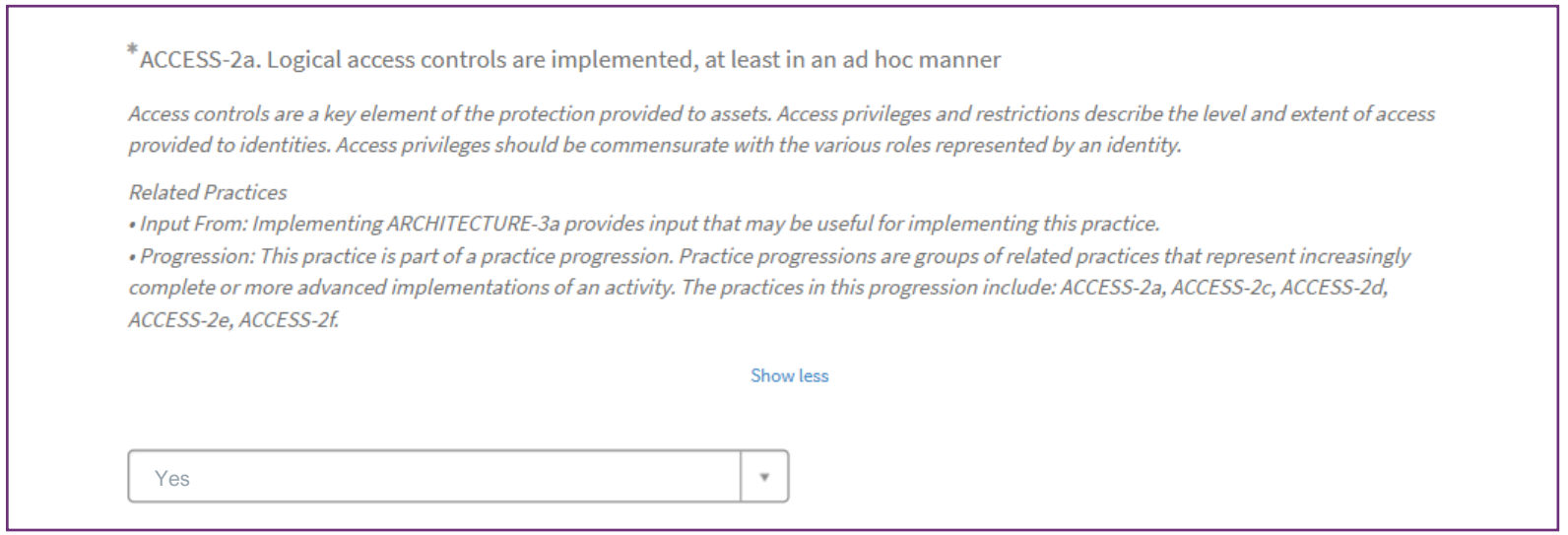
Worked Example 1

ACCESS-2A (MIL-1): Logical access controls are implemented, at least in an ad hoc manner

AESCSF Practice: *Access controls are a key element of the protection provided to assets. Access privileges and restrictions describe the level and extent of access provided to identities. Access privileges should be commensurate with the various roles represented by an identity.*

Assessment Scenario: At VoltEdge Energy, John, the OT lead, is aware of the need to control who can access the control systems. As a result, each technician has their own login to the SCADA interface, helping limit access based on roles. However, there's no formal process for managing or revoking these logins, and updates only happen when John remembers to check manually.

John from VoltEdge Energy understands ACCESS-2a and confirms that SCADA technicians use individual logins. There's no formal process, but access is limited by role and manually reviewed when staff leave.



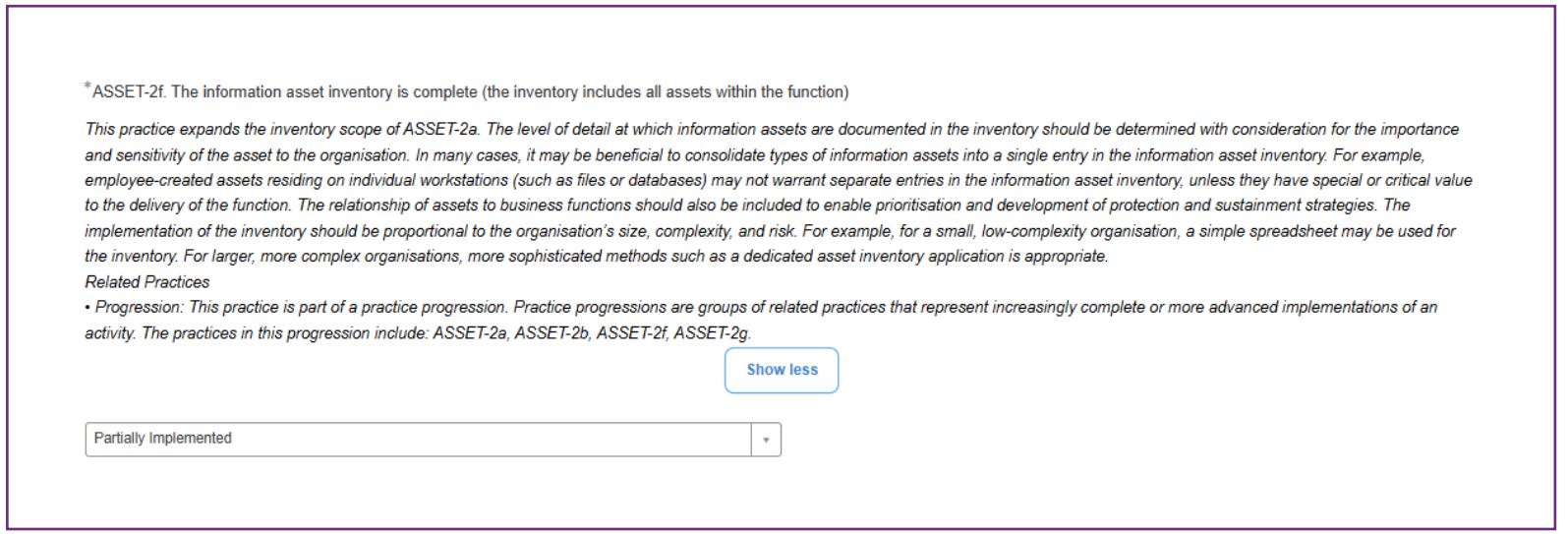
Worked Example 2

ACCESS-2F (MIL-2): Logical access requests are reviewed and approved by the asset owner

AESCSF Practice: *Privileges for logical access to an asset are assigned and approved by asset owners, custodians, or authorised delegates based on the role of the person, object, or entity that is requesting access. The asset owner or custodian is responsible for granting logical access privileges based on the identity's role and the asset's cybersecurity requirements. Asset owners and custodians must be aware of which particular identities require access to their assets and must validate the requirement with respect to business and cybersecurity requirements before granting approval.*

Assessment Scenario: John acknowledges that while some access requests to SCADA systems are checked with the asset owner, it's not always consistent. In many cases, John approves access directly based on assumed roles, without formal confirmation or documentation from the asset owner.

This practice is partially implemented because asset owners are sometimes consulted for access approvals, but the process is informal. There's no documented procedure, and approvals are often assumed As a result, access decisions don't always align with defined roles or cybersecurity requirements.



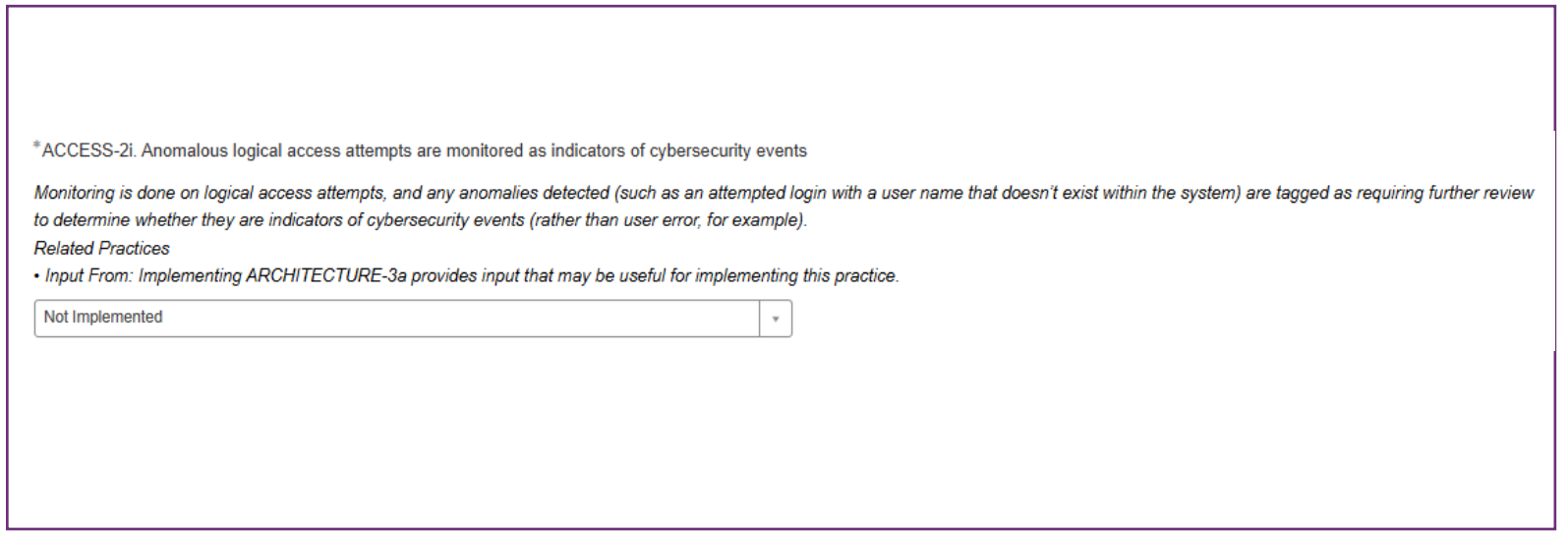
Worked Example 3

ACCESS-2I (MIL-3): Anomalous logical access attempts are monitored as indicators of cybersecurity events

AESCSF Practice: *Monitoring is done on logical access attempts, and any anomalies detected (such as an attempted login with a user name that doesn't exist within the system) are tagged as requiring further review to determine whether they are indicators of cybersecurity events (rather than user error, for example).*

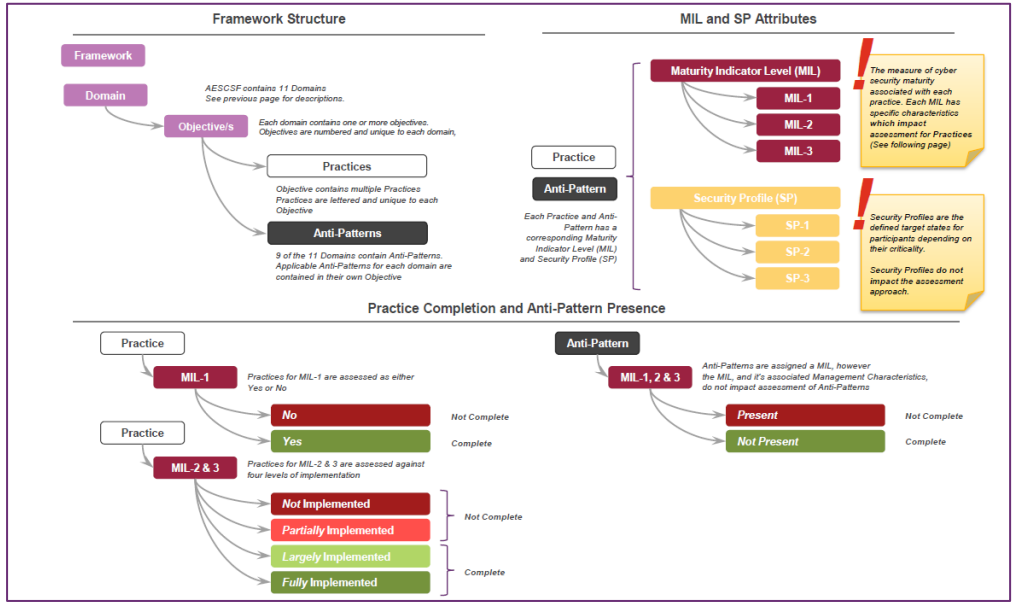
Assessment Scenario: John confirms there is no monitoring in place for unusual login attempts on OT systems. Failed or suspicious logins are not flagged or reviewed, and no alerts are generated for potential anomalies.

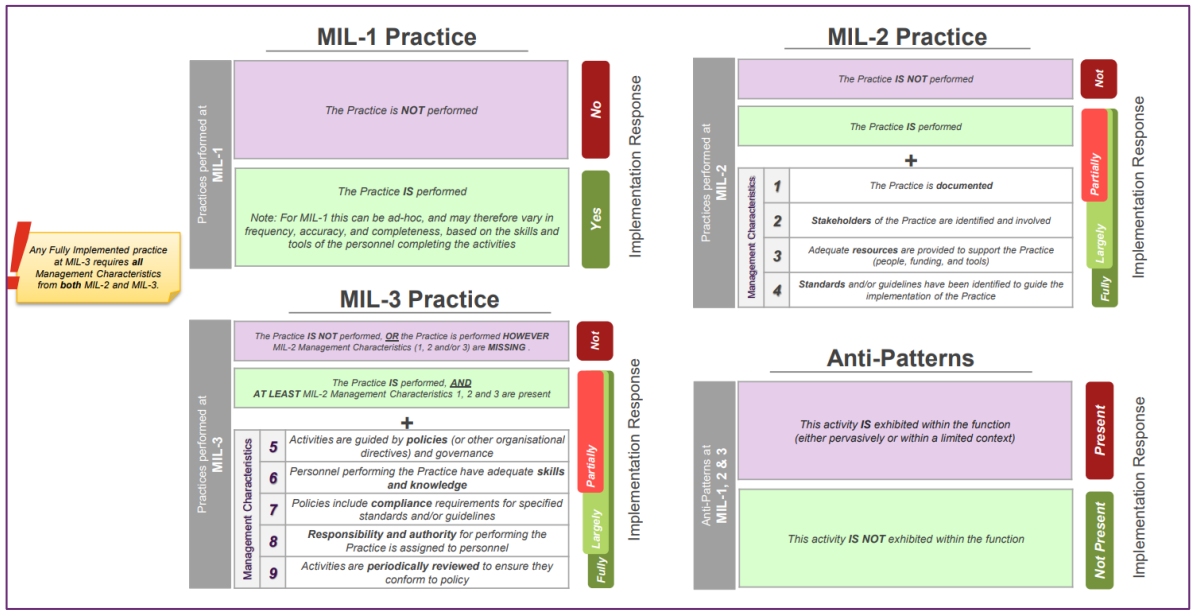
Anomalous access attempts are not monitored, and there are no alerts or reviews for failed logins or unusual activity. Logs exist but are not actively checked, leaving the organisation unable to detect or respond to early signs of a cybersecurity event.



Where to go for further information

Further information on the framework, including the structure and how to use MILs and SPs, is provided on the AEMO website (here). The supporting materials provide comprehensive context and guidance (for example, AESCSF Quick Reference Guide shown below) as to how elements of the framework fit together and enable organisations to gauge their cyber security maturity.





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.

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**

FAQs

Framework Structure Deep Dive

How To Use the Framework

How To Use the Framework

There are four key steps to using the Framework:

01 | Criticality Tool

Criticality Assessment Tools (CATs) deliver Key Criticality Indicators to classify entities within market sub-sectors by criticality bands, highlighting their potential impact on the Australian energy sector during a cyber incident.

Gas (G-CAT)

Electricity (E-CAT)

Liquid Fuels (L-CAT)

Note: CATs are applicable to only AEMO's NEM, WEM and Gas registered participants along with Liquid Fuels entities.

02 | Assessment Model

AESCSF Full Assessment
Version 1 | Version 2*

The AESCSF in 2022 was updated to align with current international standards and address emerging technologies and the evolving cyber threat landscape.

AESCSF Lite Assessment

The AESCSF Lite has been developed for DER/CER entities, and those with limited time and resources.

03 | Determine Scope

Cyber security capability may vary across an organisation's energy assets and adversaries will usually take advantage of the weakest security link – recommendation that organisations include all assets in their assessment collectively (rather than asset by asset), to get an aggregate view across the assets and organisation.

This provides a more accurate view of an organisation's overall security posture.

04 | Complete Assessment

Involve the right people
The people required to help the coordinator conduct an assessment will vary based on the size and structure of each organisation.

Keep records
Although, you don't need to upload evidence for your assessment, but keeping notes and referencing key documents (e.g. policies, processes, reports) can help clarify your rating and make future assessments easier.

Note: The AESCSF Program is only offering **V2 on the Portal. However, both V1 and V2 can be used to satisfy SOCI obligations.*
Supporting materials (including offline toolkits for V1 and V2) can be accessed on the AEMO Website.

Criticality Tool

Criticality Assessment Tool

Indicators are posed as questions, some of which are answered as "Yes" or "No", and some of which are single-select within pre-defined ranges.

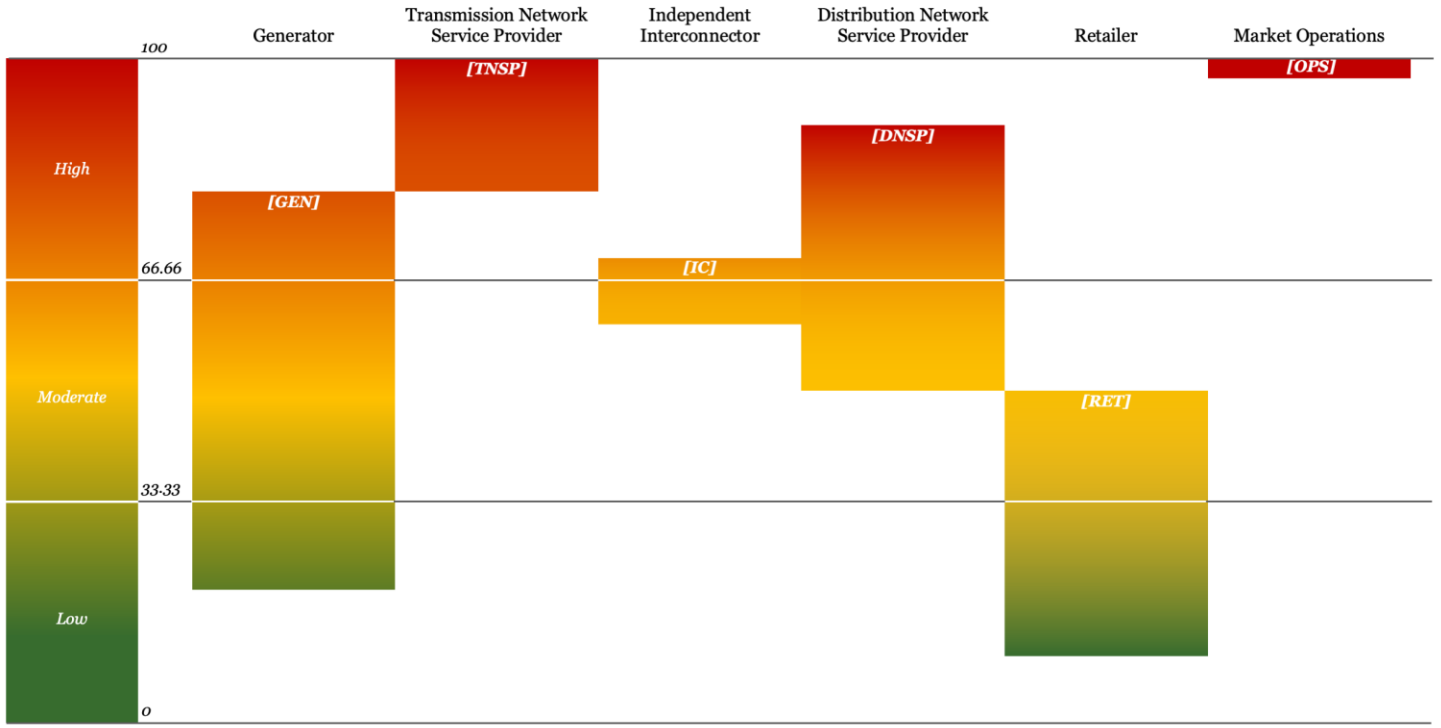
The assessment is **not intended as a comprehensive risk assessment** for each participant – it will not consider likelihood and mitigating controls, but rather **inherent risk of an entity to end user supply** and maximum potential impact (relative to other entities).

Criticality Scale

- The responses to the questionnaire will provide an overall number score on the criticality scale - High, Medium and Low.
- Before undertaking the assessment, market participants must complete a criticality assessment, which provides a reference point to help determine whether a Full or Lite assessment is appropriate. For example, high criticality entities typically undertake the Full assessment, whilst lower criticality entities may complete the Lite. However, this is a guide only and not a mandatory requirement.

Results obtained from the CAT do not indicate that an entity has obligations under or is compliant with applicable Commonwealth (Cth) legislation.

Criticality Assessment Tools (CATs) provide *Key Criticality Indicators* for each market sub-sector have been established to stratify participating entities within the sub-sector criticality bands. This is an indication of the potential impact to the relevant Australian energy sector in the event of a cyber incident at the organisation.

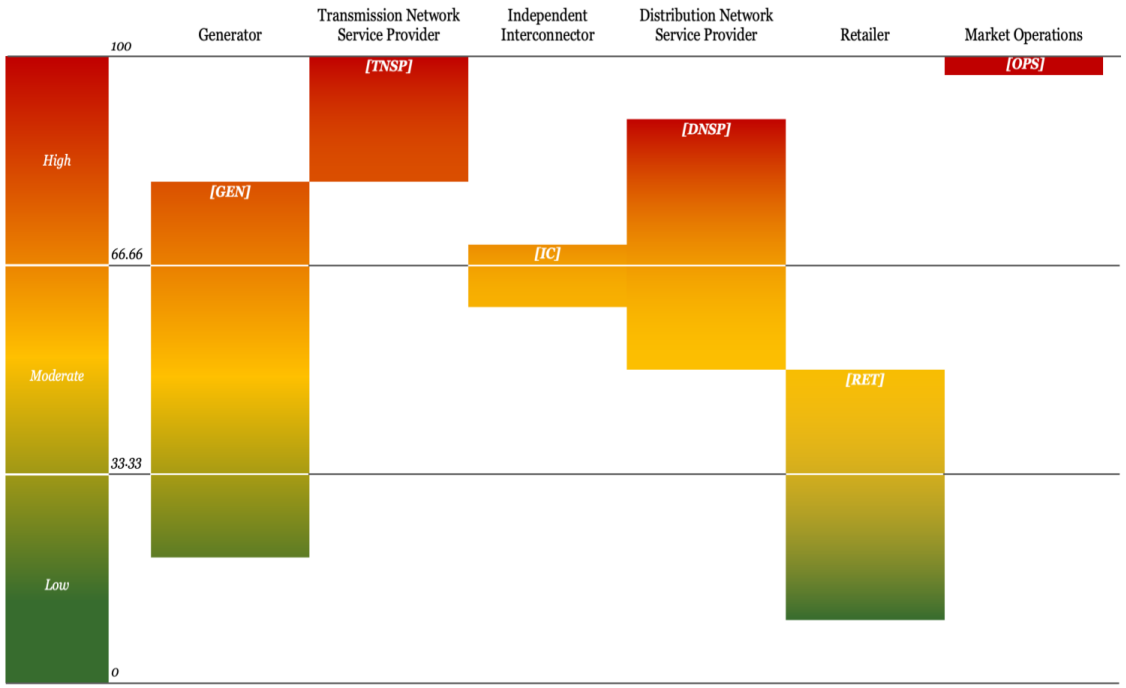


*Note: This diagram is an example showing the criticality banding for the **electricity** sub-sector only.*

***Refer to Appendix for additional information into the different criticality assessment tools**

Criticality bands by market sub-sector - Electricity

The E-CAT stratifies all participants across a single criticality scale based on a questionnaire designed to focus on an entity's operating profile across the sub-sectors.



*AESCSF CATs are designed to assess an entities relative criticality vs. other entities in the same sector. Whilst the CISC provided input, the CATs do not determine your criticality under SoCI**

Criticality Bands by Market Sub-sector

- The E-CAT scopes which market roles an entity operates in. Entities can operate in more than one market role – Transmission Network Service Provider, Distribution Network Service Provider, Generator, Retailer, Interconnector, and System/ Market operator (AEMO).
- The scope determines the set of criticality questions an entity is required to answer.
- The questionnaire contains the relevant focus areas of criticality for each sub-sector, and a weighting is assigned to each. The weighting assigned to each question was determined in consultation with AEMO, industry and government stakeholders.
- Organisations may find their response to some questions in the E-CAT will differ by region within the National Energy Market (NEM) and Wholesale Electricity Market (WEM). In these situations, please respond based on an overall NEM and WEM perspective.
- Additional guidance for completing the Electricity Criticality Assessment can be found within the E-CAT.

**Security of Critical Infrastructure Act 2018*

Criticality bands by market sub-sector - Electricity (cont.)

Each sub-sector questionnaire has ‘focus areas’ which determine the most crucial components of an entity’s operating environment. The weighting of ‘focus areas’ was determined in consultation with AEMO, industry and government stakeholders..

Focus Areas for each market role:

Generator

- Generation Capacity
- Asset classification – Synchronous Generators
- Ancillary Services
- Network Support Agreement
- Battery storage

Transmission

- Nominal Capacity
- Gigawatt hours

Interconnector (Transmission)

- Nominal Capacity

Independent Interconnector

- Nominal Capacity
- Regionally critical Interconnector

Distribution

- Gigawatt hours
- Number of customers (National Metering Identifiers)
- Critical and commercial numbers

Retailer

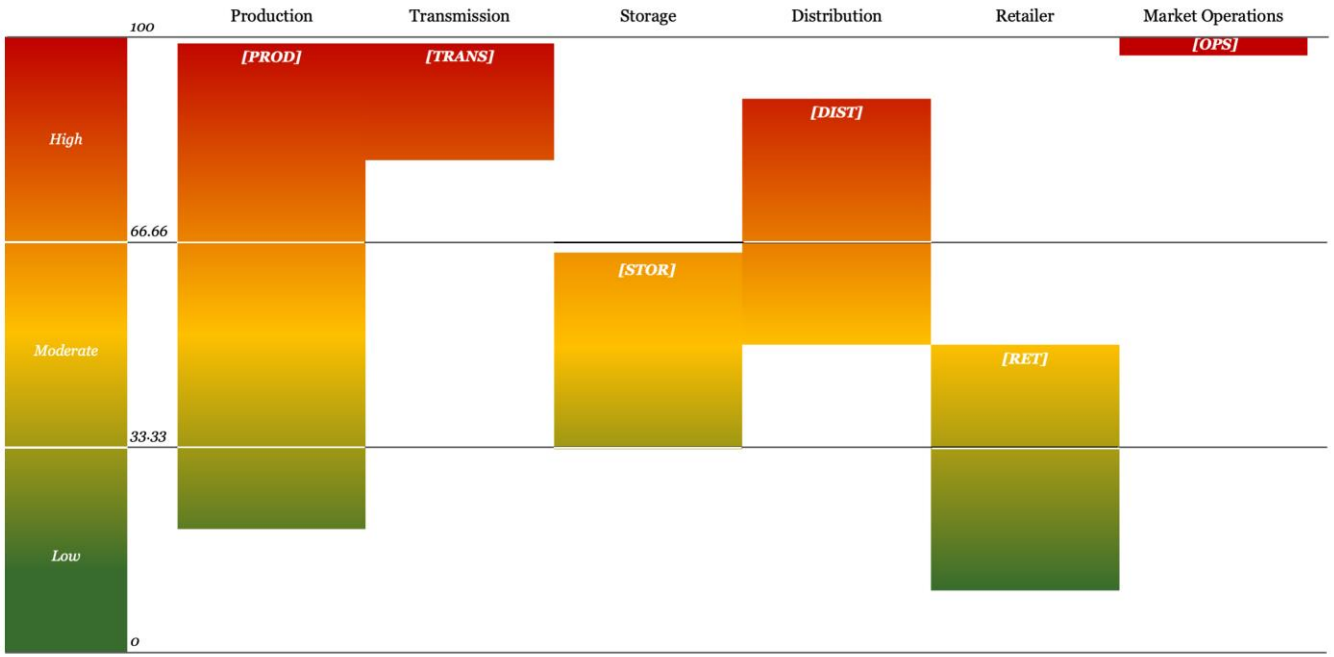
- Number of customers (National Metering Identifiers)
- Connection to Advanced Metering Infrastructure
- Critical and commercial numbers
- Virtual Power Plants
- Retailer of Last Resort
- Sole Retailer for a region

Market Operations

- If the entity is a system/market operator, it automatically has the highest criticality

Criticality bands by market sub-sector - Gas

The G-CAT stratifies all participants across a single criticality scale based on a questionnaire designed to focus on an entity's operating profile across the sub-sectors.



Criticality Bands by Market Sub-sector

- The G-CAT scopes which market roles an entity operates in. Entities can operate in more than one market role – Production, Transmission, Storage, Distribution, Retailer, and Market Operator.
- The scope determines the set of criticality questions an entity is required to answer.
- The questionnaire contains the relevant focus areas of criticality for each sub-sector, and a weighting is assigned to each. The weighting assigned to each question was determined in consultation with AEMO, industry and government stakeholders.
- Additional guidance for completing the Gas Criticality Assessment can be found within the G-CAT.

*AESCSF CATs are designed to assess an entities relative criticality vs. other entities in the same sector. Whilst the CISC provided input, the CATs do not determine your criticality under SoCI**

Criticality bands by market sub-sector - Gas (cont.)

Each sub-sector questionnaire has *'focus areas'* which determine the most crucial components of an entity's operating environment. Weighting of *'focus areas'* were determined in consultation with AEMO, industry and government stakeholders.

Focus Areas for each market role:

Production

- Production Quantity
  - Petajoules (PJ/y)
- Natural gas and Liquefied Natural Gas (LNG)

Transmission

- Nominal Capacity
  - Terajoules (TJ/d)
- Number of Critical and Commercial entities
- Number of Gas Powered Generation (GPG) entities.

Storage

- Nominal Capacity
  - Withdrawal Capacity – Terajoules (TJ/d)
  - Storage Capacity - Petajoules

Distribution

- Distribution Quantity
  - Terajoules (TJ/y)
- Number of customers (National Metering Identifiers)
- Number of Critical and Commercial entities
- Operation of Gate Facilities

Retailer

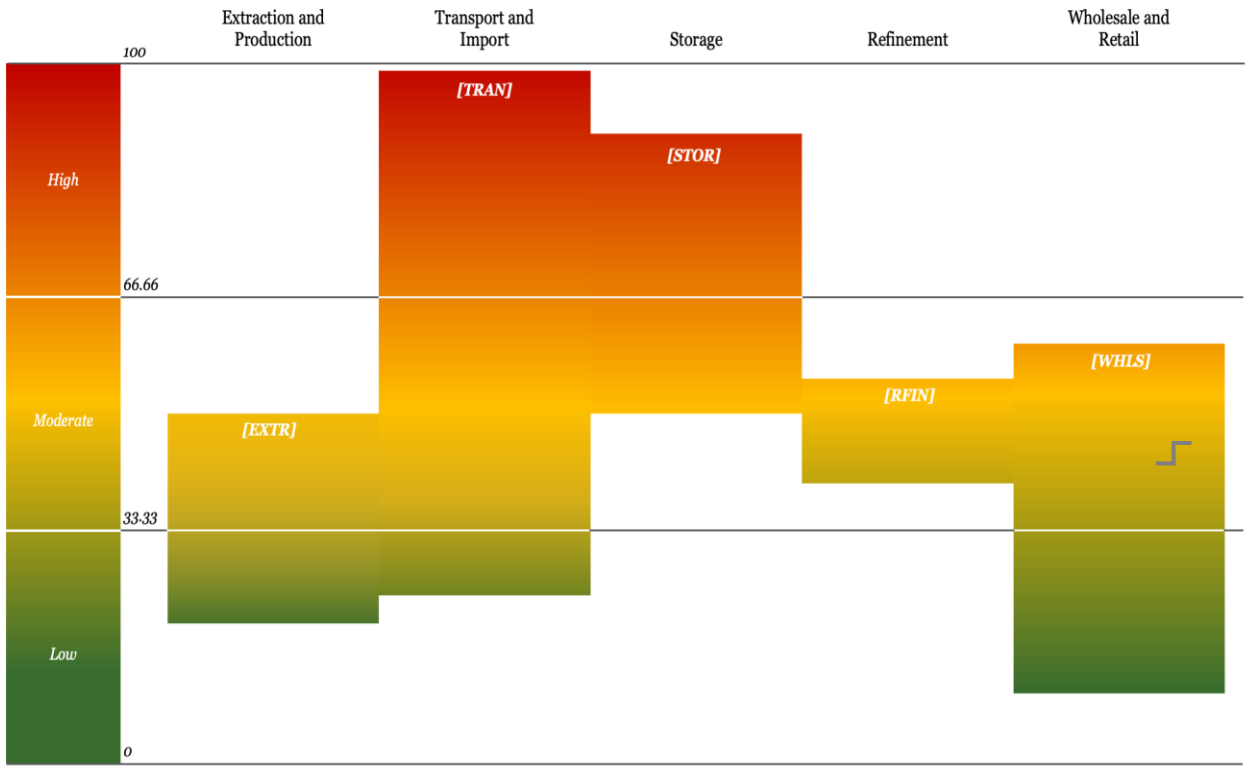
- Number of customers (National Metering Identifiers)
- Number of Critical and Commercial entities

Market Operations

- If the entity is a market operator, it automatically has the highest criticality

Criticality bands by market sub-sector - Liquid Fuels

Introduced in the 2023, the L-CAT stratifies all participants across a single criticality scale based on a questionnaire designed to focus on an entity's operating profile across the sub-sectors.



*AESCSF CATs are designed to assess an entities relative criticality vs. other entities in the same sector. Whilst the CISC provided input, the CATs do not determine your criticality under SoCI**

Criticality Bands by Market Sub-sector

- The L-CAT scopes which market roles an entity operates in. Entities can operate in more than one market role – Extraction and Production, Transport and Import, Storage, Refinement, and Wholesale and Retail.
- The scope determines the set of criticality questions an entity is required to answer.
- The questionnaire contains the relevant focus areas of criticality for each sub-sector, and a weighting is assigned to each. The weighting assigned to each question was determined in consultation with AEMO, industry and government stakeholders.
- Additional guidance for completing the Liquid Fuels Criticality Assessment can be found within the L-CAT.

*Security of Critical Infrastructure Act 2018

Criticality bands by market sub-sector - Liquid Fuels (cont.)

Each sub-sector questionnaire has ‘focus areas’ which determine the most crucial components of an entity’s operating environment. The weighting of ‘focus areas’ was determined in consultation with AEMO, industry and government stakeholders.

Focus Areas for each market role:

Extraction and Production

- Total quantity of Crude Oil produced

Transport and Import

- Total quantity of liquid fuel transported
- Combined maximum capacity of the entities transport network
- Percentage transported to Essential users

Storage

- Combined maximum storage capacity
- Quantity of liquid fuels held in reserve
- Maximum withdrawal capacity from on-land storage
- Dedicated storage facilities for Essential users

Refinement

- Total quantity of refined liquid fuels
- Peak maximum production quantity over a 30-day period

Wholesale and Retail

- Total quantity of liquid fuels sold
- Volume of liquid fuels sold to Essential Users
- The types of liquid fuel product sold

Criticality scale

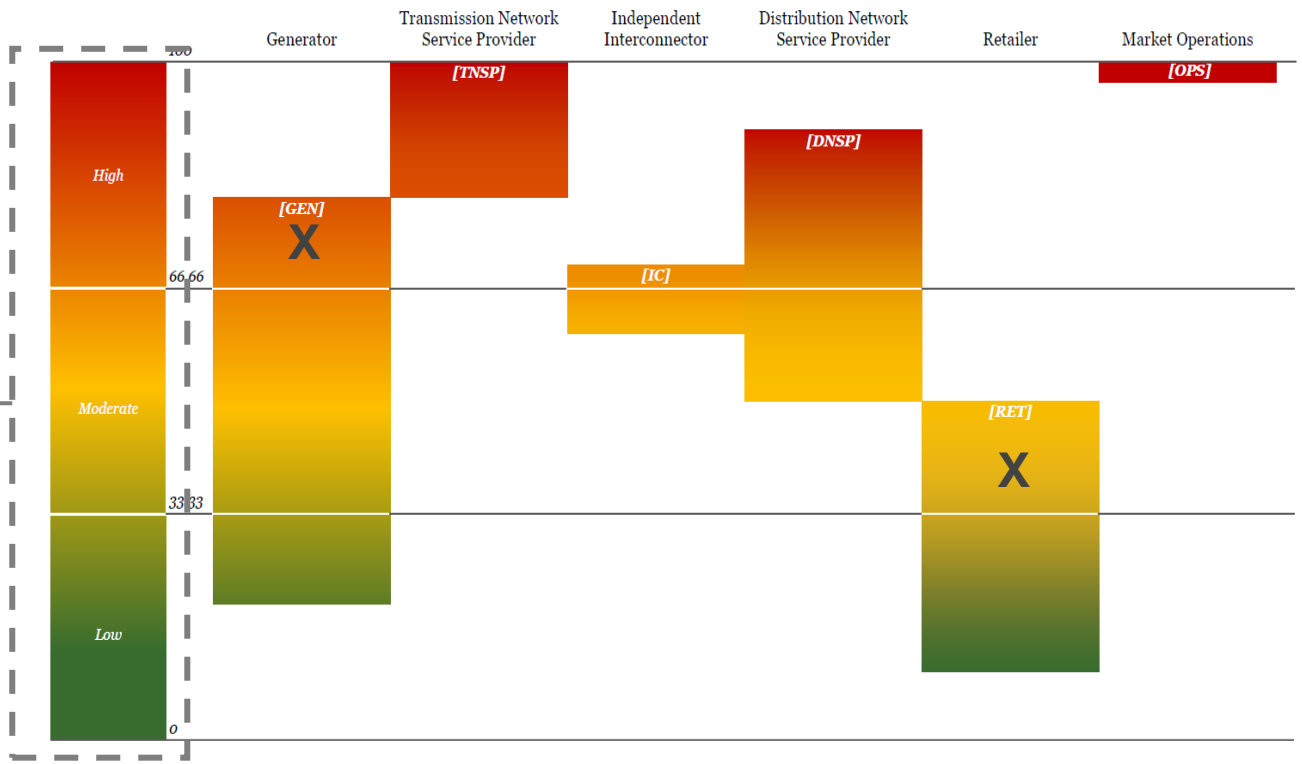
The Criticality Scale score of each entity will determine their cyber-security capability maturity target state.

Criticality Scale

- The responses to the questionnaire will provide an overall number score on the criticality scale - High, Medium and Low.
- This is an indication of the potential impact to the relevant Australian energy sector in the event of a cyber incident at the particular organisation.

The electricity, gas, and liquid fuels scales operate in the same way. The accompanying image displays only the electricity criticality scale.

Reminder: The CATs have been established separately to provide thee distinct criticality scales. No attempts should be made to compare or overlay the E-CAT, G-CAT, and L-CAT scales. Criticality is assessed relative to other entities in the relevant sector only.



For example, a hypothetical organisation participates in both the Generation and Retail sub-sectors, with their criticality results shown with 'X's above. Their overall criticality result is the highest of all applicable sub-sector results – that means that in this example they would be assessed as a High criticality market participant due to their High result for Generation.

Assessment Model

Framework Structure

AESCSF V2 Explained - Domains

AESCSF V2 has 11 domains. The domains are logical groupings of cyber security capability. Each domain has an acronym that cross references across the AESCSF Toolkit and Guidance Artefacts.

Enterprise-wide

- Risk Management (RISK)
- Cybersecurity Program Management (PROGRAM)
- Workforce Management (WORKFORCE)

Operating environments

- Identity and Access Management (ACCESS)
- Event and Incident Response, Continuity of Operations (RESPONSE)
- Asset, Change, and Configuration Management (ASSET)
- Situational Awareness (SITUATION)
- Threat and Vulnerability Management (THREAT)
- Australian Privacy Management (APM) *(Australian Specific)*
- Cybersecurity Architecture (ARCHITECTURE)

External parties

- Supply Chain and External Dependencies Management (THIRD-PARTIES)

AESCSF Explained – Domains, Objectives, Practice and Anti-Patterns

Domains are split into Objectives which are target achievements that support the domain. The objectives consist of numbers activities which are either positive security Practices or negative security Anti-Patterns.

Framework Breakdown

Domain

- Logical grouping of cyber capability
- The AESCSF contains 11 Domains.

Objective
Target achievements to support domain

- Target achievements to support domains
- Objectives are numbered and unique to each Domain.

Practices

- Positive security pattern, task or activity
- Each Objective contains multiple Practices.
- Practices are lettered and unique to each Objective
- 354 Practices and Anti-Patterns across 11 Domains

Anti-Patterns

- Outlines negative security patterns that shouldn't be present.
- 9 of the 11 Domains contain Anti-Patterns.
- Applicable Anti-Patterns for each domain are contained in their own Objective.

Example

RISK: Establish and maintain a cyber risk management program to identify, assess, and mitigate cybersecurity risks to the organisation's operations and critical infrastructure.

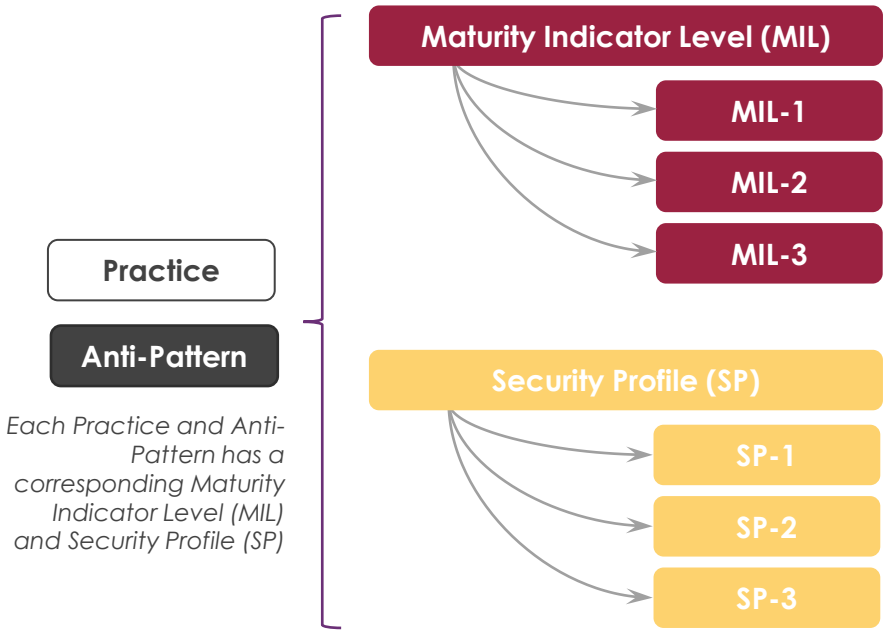
RISK-1: *Develop a comprehensive strategy to manage cybersecurity risks, aligning with the organisation's objectives and risk appetite.*

RISK-1a (MIL-1, SP-1): *The organisation has a documented cybersecurity risk management strategy that outlines its approach to identifying and mitigating cyber risks*

RISK-AP1 (MIL-2, SP-2): *Identified risks are not periodically reviewed.*

Framework Structure

Each Practice and Anti-Pattern has a corresponding Maturity Indicator Level (MIL) and Security Profile (SP)



Maturity Indicator Levels:

- Each Practice and Anti-Pattern has been assigned a MIL (MIL-1, MIL-2 or MIL-3) that indicates its maturity relative to other Practices.
- Each MIL has specific characteristics which impact assessment for Practices (See later slides on scoring model).

Security Profiles:

- The Framework has three alternate groupings of Practices and Anti-Patterns referred to as Security Profiles (SPs).
- These profiles were developed by the Australian Cyber Security Centre (ACSC) in collaboration with AEMO and industry experts, using a risk-based approach.
- The target state maturity SP a Participant should pursue is determined based on their overall criticality result (per the CAT).

Key aspects of MILs and SPs

1. MILs apply independently to each domain. As a result, entities may be operating at different MIL ratings for different Domains.
2. SPs apply collectively across all Domains. As a result, entities only achieve a SP if they have completed all Practices in the SP across all Domains.
3. The MILs and SPs are cumulative; to earn a MIL or SP, an organisation must perform all of the Practices, and not exhibit any of the anti-patterns, in that level and its predecessor level(s).

Priority Practices

The ACSC 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 first priority is to complete Practices in any 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**

AESCSF Security Profile 1

In 2022 the Australian Cyber Security Centre, in consultation with the AEMO and the AESCSF Working Group, defined Security Profiles using Practices from AESCSF v2. Profiles contain Practices from multiple MILs.

- Security Profile 0 contains no Practices. Performance at Security Profile 0 simply means that Security Profile 1 has not been achieved.
- 109 Practices must be completed, along with 14 Anti-Patterns being 'Not Present' to achieve Security Profile 1 (123 total).
- All Practices and Anti-Patterns at MIL-1 are included within Security Profile 1 with the addition of select Practices and Anti-Patterns at MIL-2 and MIL-3.
- MIL-2 and MIL-3 Practices from all of the 11 AESCSF domains have been included within Security Profile 1.
- Security Profile 1 contains 29 Practices that have been identified by the ACSC as a priority for completion. These Practices should be considered when sequencing Practice remediation activities. (See later slides).

MIL-2 and MIL-3 Practices and Anti-Patterns in Security Profile 1		
Domain	**Practice ID**	**Anti-Pattern ID**
ASSET	1B, 2B, 3D, 4C, 4D, 4E, 4F	AP4, AP5
PRIVACY	1D	AP1
PROGRAM	1G	AP1, AP2
THIRD-PARTIES	2E	None
ACCESS	1D, 1F, 1G, 1H, 2C, 2G, 3D, 3E, 3H	AP4, AP5, AP9
RESPONSE	1B, 1C, 2F, 2G, 3E, 3F, 3G, 3H, 4E, 4F, 4J, 4K, 4I, 4P	AP1, AP2, AP3
ARCHITECTURE	12C, 2F, 2G, 2J	AP1, AP2
RISK	1B, 1E, 2B, 2E, 2G	None
SITUATION	1C, 2E, 3A	AP7, AP8
THREAT	1H, 2H	None
WORKFORCE	1E, 3D, 4D	None

Note: MIL-1 Practices are not shown in the above table

AESCSF Security Profile 2

In 2022 the Australian Cyber Security Centre, in consultation with the AEMO and the AESCSF Working Group, defined Security Profiles using Practices from AESCSF v2. Profiles contain Practices from multiple MILs.

- 239 Practices and 36 Anti-Patterns must be completed to achieve Security Profile 2 (123 total within Security Profile 1 and 152 total within Security Profile 2).
- All Practices and Anti-Patterns at MIL-2 are included in Security Profile 2 with the addition of select Practices and Anti-Patterns at MIL-3.
- MIL-3 Practices from 10 of the 11 AESCSF domains have been included within Security Profile 2.
- Security Profile 2 contains 28 Practices that have been identified by the ACSC as a priority for completion. These Practices should be considered when sequencing Practice remediation activities.

MIL-3 Practices and Anti-Patterns in Security Profile 2		
Domain	**Practice ID**	**Anti-Pattern ID**
ASSET	1G, 2G, 4H	None
PRIVACY	1L	None
PROGRAM	2I	None
THIRD-PARTIES	1F, 2H, 2L, 2M	None
ACCESS	1J, 2H, 2I, 3I, 3J	AP8, AP11
RESPONSE	1F, 3K, 3L, 4N	None
ARCHITECTURE	2H, 2I, 2K	None
RISK	2K, 2M	None
SITUATION	2G	AP11
THREAT	None	None
WORKFORCE	3E	AP1

Note: MIL-1 and MIL-2 Practices are not shown in the above table

AESCSF Security Profile 3

In 2022 the Australian Cyber Security Centre, in consultation with the AEMO and the AESCSF Working Group, defined Security Profiles using Practices from AESCSF v2. Profiles contain Practices from multiple MILs.

- **All 312 Practices and 42 Anti-Patterns must be completed to achieve Security Profile 3**
- (123 total within Security Profile 1, 152 total within Security Profile 2, and 79 total which are specific to Security Profile 3).
- All Practices and Anti-Patterns at MIL-3 are covered in Security Profile 3.
- Achieving Security Profile 3 is identical to achieving Maturity Indicator Level (MIL) 3.
- Security Profile 3 contains 13 Practice that have been identified by the ACSC as a priority for completion. This Practice should be considered when sequencing Practice remediation activities.

AESCSF Full Assessment Scoring

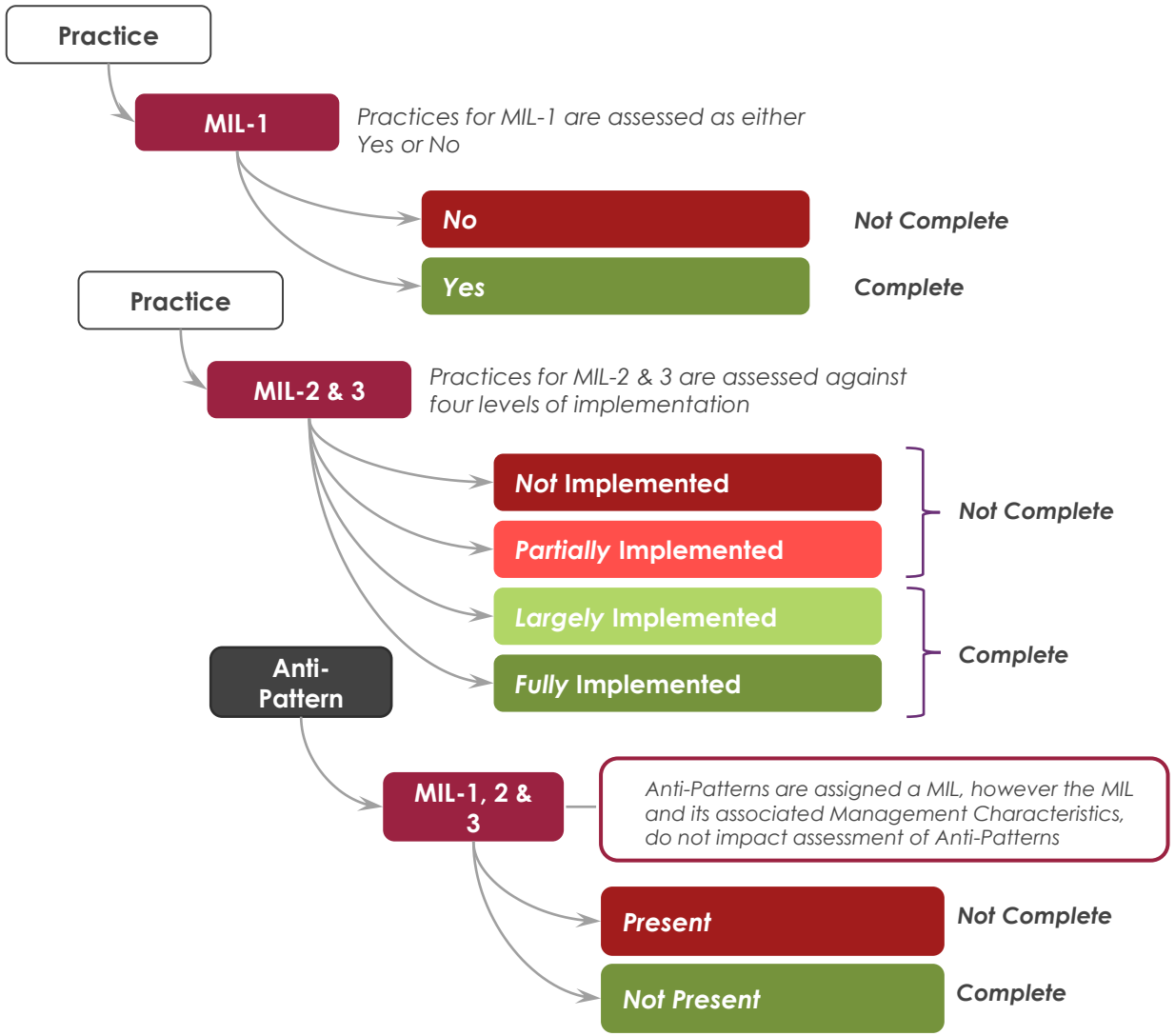
Assessment Scoring

Key considerations of the scoring model include:

- Scoring is based on a combination of "**Practice Implementation**" and "**Management Characteristics**".
- A Practice is "**Complete**" if it is assessed as "***Largely Implemented***" or "***Fully Implemented***".
- A MIL is "**Achieved**" if all Practices within it are "**Complete**".
- Different domains may have different MILs.
- All Practices and Anti-Practices indicated for an MIL must be present or absent within a domain, to achieve that level for the domain.
- An organisation's overall MIL reflects the lowest MIL obtained in any domain.

Assessment scoring of Anti-Patterns:

- Anti-Patterns are either *Present* or *Not Present.*
- There are no Management Characteristics that need to be considered when scoring Anti-Patterns. Instead, the rating depends on whether the Anti-Pattern activity is present with the entity.
- Anti-Patterns are assigned a MIL rating from 1 to 3. However, the MIL rating does not impact the assessment approach for Anti-Patterns. This means. a MIL-3 Anti-Pattern is assessed as either *Present* or *Not Present*, the same as a MIL-1 Anti-Pattern.



Assessment Outcomes

	Implementation response	The practice is performed	The practice is documented	Stakeholders of the practice are identified and involved.	Adequate resources are provided to support the practice (people, funding, and tools).	Standards and/or guidelines have been identified to guide the implementation of the practice	Activities are guided by policies (or other organisational directives) and governance	Personnel performing the practice have adequate skills and knowledge	Policies include compliance requirements for specified standards and/or guidelines	Responsibility and authority for performing the practice is assigned to personnel	Activities are periodically reviewed to ensure they conform to policy
MIL 1	No										
	Yes	✓									
MIL 2	Partially Implemented	✓	✓								
	Largely Implemented	✓	✓	✓	✓						
	Fully Implemented	✓	✓	✓	✓	✓					
MIL 3	Partially Implemented	✓	✓	✓	✓	✓	✓	✓			
	Largely Implemented	✓	✓	✓	✓	✓	✓	✓	✓	✓	
	Fully Implemented	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

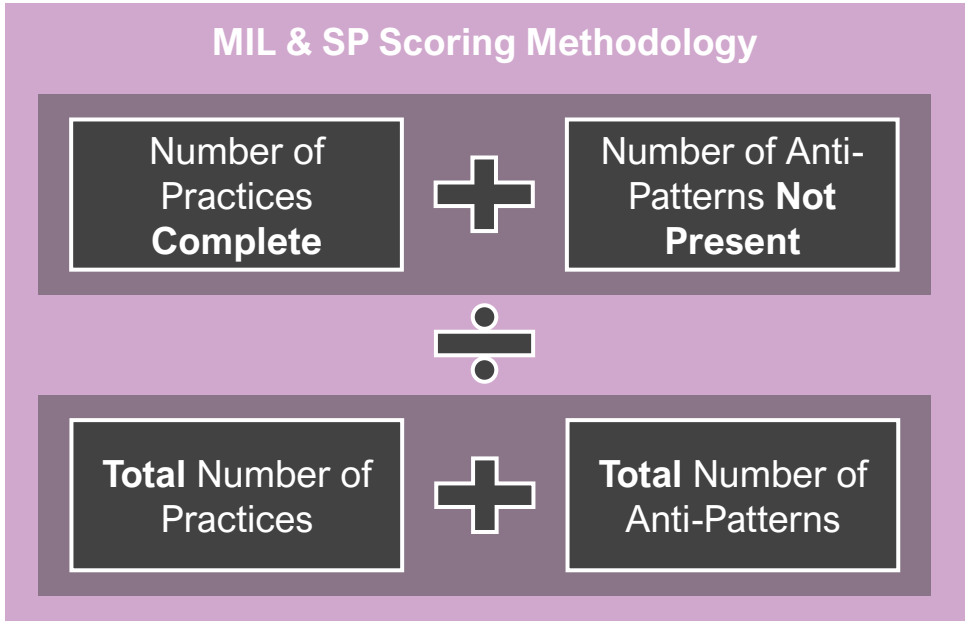
Assessment Scoring Methods

AESCSF results can be expressed either in terms of MILs or SPs.

- There are three MILs (MIL-1, MIL-2 and MIL-3) that are assigned to all practices in all the Domains in the Framework.
- MILs apply independently to each domain and are cumulative.
- To gain an MIL in a domain, all Practices must be completed, and no Anti-Patterns exhibited.
- E.g. to achieve an MIL-3, organisations have to perform all Practices and not exhibit any of the Anti-Patterns, in MILs 1, 2 and 3.
- Overall MIL reflects the lowest MIL obtained in any domain.

In addition to the MIL, AESCSF has three alternate groupings of Practices referred to as SPs.

- Unlike MILs, SPs cannot be applied to each Domain.
- For organisations to be recognised for an SP, they need to have achieved 100% of all the Practices.
- SPs follow the same cumulative nature of MILs. (i.e., SP-2 can only be achieved if SP-1 has been achieved.



E.g. for an organisation that has completed all SP 1 Practices & Anti-Patterns and is progressing towards SP 2 using *using version 1 of the AESCSF*

Number of SP 1 Practices Complete = 74
Number of SP 2 Practices Complete = 45
+
Number of SP 1 Anti-Patterns Not Present = 14
Number of SP 2 Anti-Patterns Not Present = 18

÷

Total Number of SP 1 Practices = 74
Total Number of SP 2 Practices = 90
+
Total Number of SP 1 Anti-Patterns = 14
Total Number of SP 2 Anti-Patterns = 22

SP Score 1.56

The organisation has completed all of the related SP1 Practices and Anti Patterns and has completed 56% of SP 2 (45 of 90 Practices + 18 of 22 Anti-Patterns and has a SP score of 1.56

As detailed above – for both MIL and SP, scoring is cumulative. (i.e., SP-2 can only be achieved if SP-1 has been achieved.

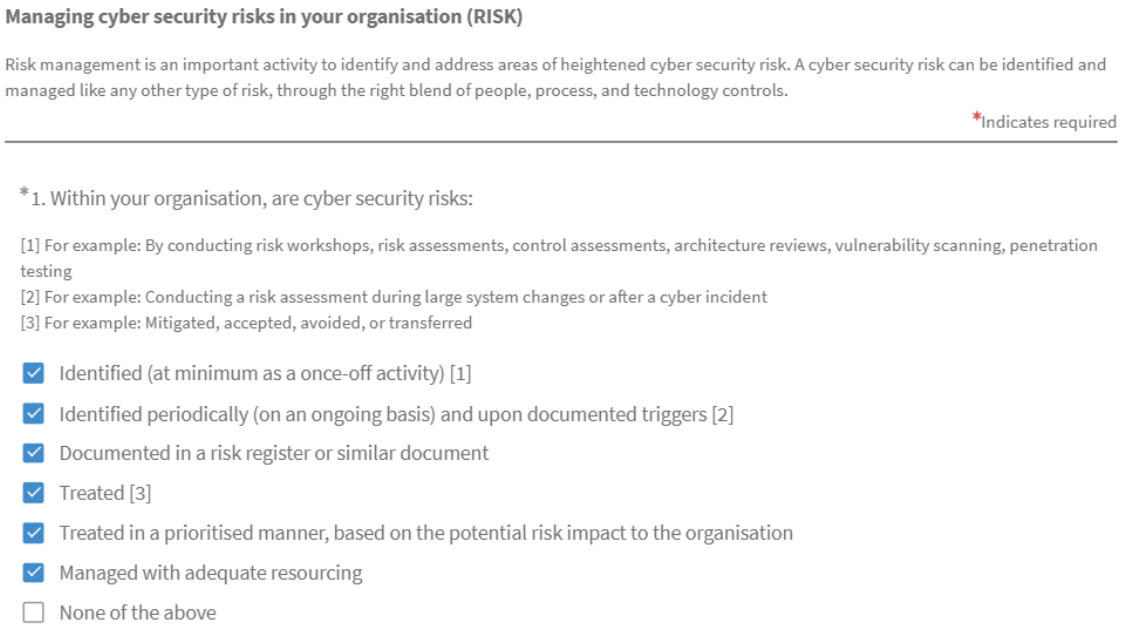
AESCSF Lite Assessment

AESCSF Lite

The AESCSF Lite framework has been developed to facilitate Assessment against the AESCSF by low criticality entities including DER/CER organisations, and those with limited time and security resources; the Lite Framework is only available in Version 2 and via the Annual Assessment Program.

- **Overview:** The Lite Framework consists of 28 questions, grouped into 11 sections.
- **Suitability:** Specifically designed to support assessment against the AESCSF by lower-criticality market entities, and those with limited time, resources and competing priorities.
- **Time Commitment:** If responses to all questions are known, the survey should take around 15-20 minutes.

EXAMPLE: LITE FRAMEWORK QUESTIONS AND RESPONSES



Managing cyber security risks in your organisation (RISK)

Risk management is an important activity to identify and address areas of heightened cyber security risk. A cyber security risk can be identified and managed like any other type of risk, through the right blend of people, process, and technology controls.

*Indicates required

*1. Within your organisation, are cyber security risks:

[1] For example: By conducting risk workshops, risk assessments, control assessments, architecture reviews, vulnerability scanning, penetration testing
[2] For example: Conducting a risk assessment during large system changes or after a cyber incident
[3] For example: Mitigated, accepted, avoided, or transferred

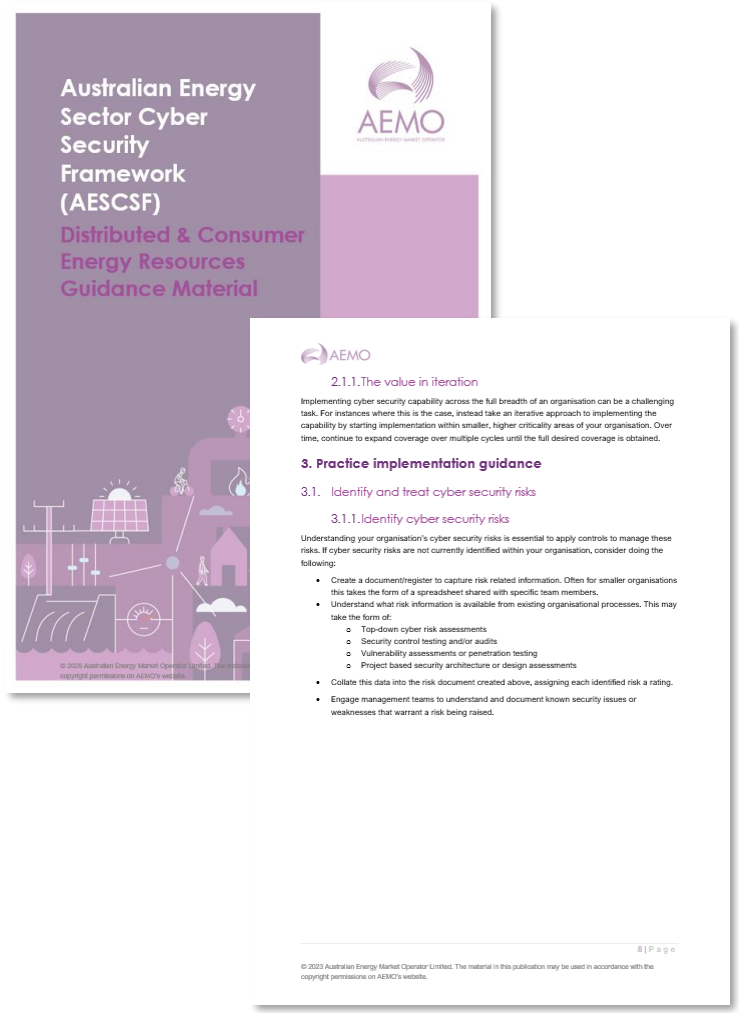
- [x] Identified (at minimum as a once-off activity) [1]
- [x] Identified periodically (on an ongoing basis) and upon documented triggers [2]
- [x] Documented in a risk register or similar document
- [x] Treated [3]
- [x] Treated in a prioritised manner, based on the potential risk impact to the organisation
- [x] Managed with adequate resourcing
- [ ] None of the above

The sections are derived from the Domains in the underlying "Full" version of the AESCSF:

1. Managing cyber security **risks** in your organisation.
2. Managing **third parties**.
3. Managing **assets** across the organisation.
4. Establish and maintain cyber security **architecture**.
5. Managing **identities** and access.
6. Setting up a cyber security **program of work**.
7. Managing cyber security **threats** and **vulnerabilities**.
8. Detecting potential **cyber security events**.
9. Responding to cyber security **incidents**.
10. Creating a cyber secure **workforce**.
11. Managing the **privacy** and confidentiality of personal information

AESCSF Guidance for DER/CER Organisations

- Based on feedback from prior AESCSF Assessment Programs, smaller/newer market entrants requested additional guidance to support their implementation of the AESCSF. In response, this document provides guidance material to assist organisations in getting started on their uplift journey.
- The capabilities included in this guidance are based off the ACSC's Priority Practices and have been selected based on being high-impact and foundational in nature to the organisations overall cyber security capability.



Determine Scope

Assessment Scope

Cyber security capability may vary across an organisation's energy assets and cyber criminals will usually take advantage of the weakest security link. That's why AEMO recommends that organisations include all assets in their assessment collectively (rather than asset by asset), to get an aggregate view across the assets and organisation

Assess all assets collectively

Organisations should assess all assets together rather than individually to prevent weak links in security and gain a comprehensive view of their cybersecurity posture.

Cross-sub-category assessment

If an organisation operates in multiple energy sub-sectors such as electricity, gas, or liquid fuels, the assessment should include all relevant assets and, in some cases, key elements of the supply chain.

Parent company responsibility

The ultimate Australian legal entity (parent company) is responsible for conducting a single assessment unless:

- There is no shared network infrastructure.
- There is no inter-network integration.
- There are no shared IT or OT management functions.

Licensing & ringfencing compliance

Organisations must consider licensing and ringfencing requirements set by the Australian Energy Regulator (AER) when determining asset inclusion in the assessment.