AES | CSF
Australian Energy Sector | Cyber Security Framework

Australia Energy Sector Cyber Security Framework Education Workshop

2022

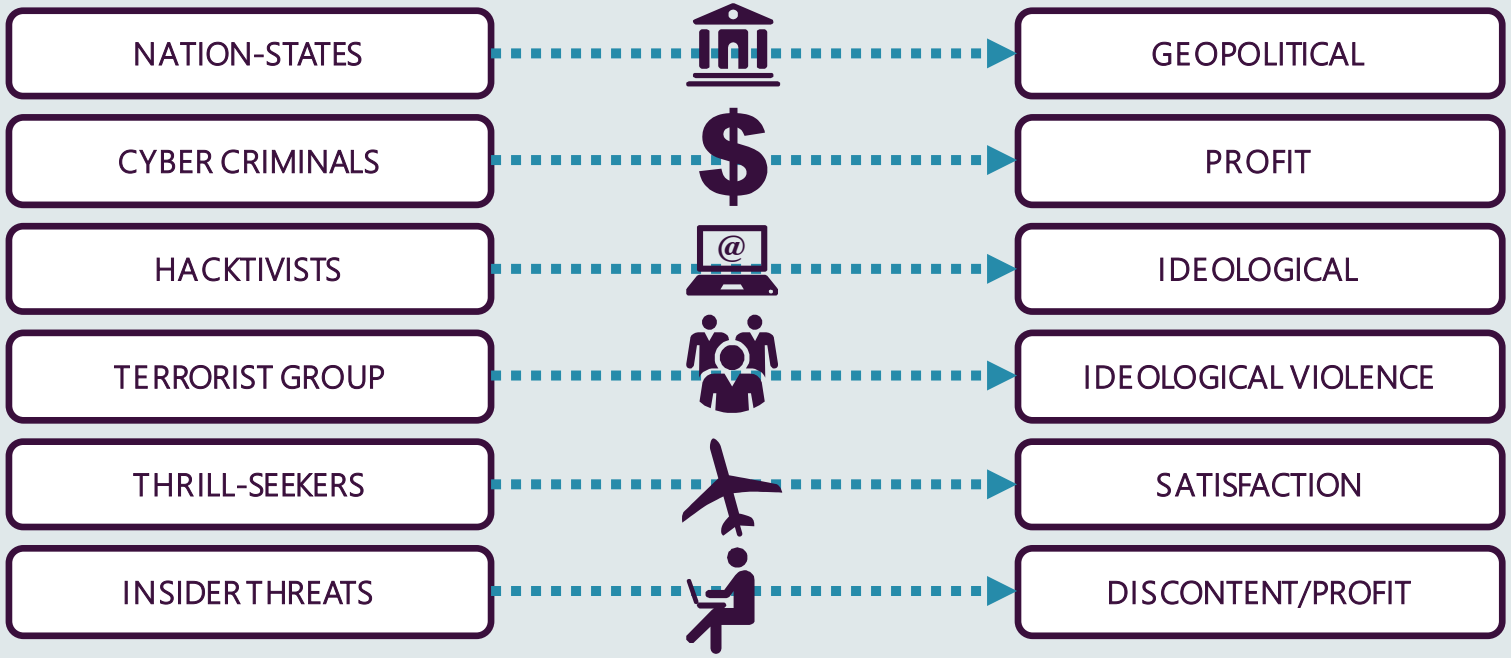
Education Workshop Agenda

Time	Topic
2.00pm	Background
	Introduction to the AESCSF
	Criticality Assessment
	Framework Structure
3:00pm	Break
3:10pm	Assessment Scoring Model
	AESCSF Lite
	Target State
	AESCSF Priority Practices
	Assessment Outcome and Next Steps
4:30pm	**AESCSF Toolkit Walkthrough Session (Optional)**
5:00pm	Close

AES CSF
Australian Energy Sector Cyber Security Framework

Background

Background - Cyber Threat Actors and Motivations*



Okta – Early 2022.

- Okta, a major Identity Access Management (IAM) firm supporting entities in both Government and Industry was attacked resulting in multiple customer environments being breached.
- This led to threat actors gaining access to privileged information.
- Initial breach was undisclosed for over a month.

US Gasoline Pipeline Attack – 7 May 2021.

- Ransomware attack on Colonial Pipeline Co. temporarily shutting down fuel transport operations from Texas to New York over a five-day period. Ransomware typically indicates a profit motivation.
- The attack caused petrol and diesel supplies to tighten as well as the price per gallon increase to the highest level since 2014.
- Colonial paid the USD $4.4 million ransom.

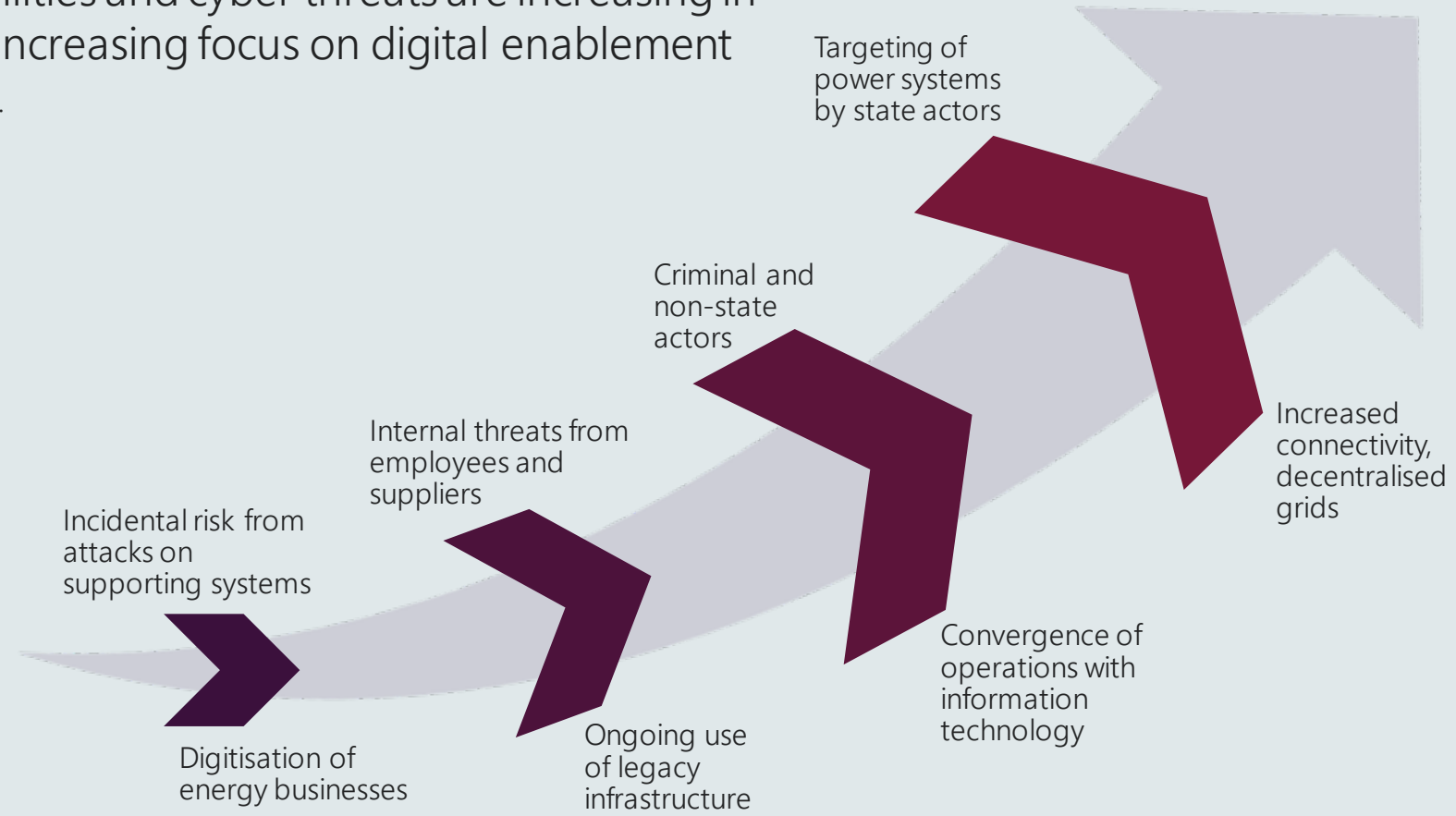
Nine News Network – 28 March 2021.

- Attack affected the entire network forcing nine news and associated channels offline.
- Allegedly caused by a "state actor" attempting to silence the broadcast of an investigative broadcast indicating a geopolitical motivation.

*informed by the Canadian Centre for Cyber Security (https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors)

Background - The Cyber Security Problem

Cyber vulnerabilities and cyber threats are increasing in part due to an increasing focus on digital enablement and innovation.



Background - Cyber activity in Australia

"...there is a heightened cyber threat environment globally, and the risk of cyber attacks on Australian networks, either directly or inadvertently, has increased." – ACSC 28/03/2022

Log4j targeting of Australian organisations

- In late 2021 a remote code execution vulnerability was identified in the Log4j library, one of the most widely used Java-based logging utilities globally.
- The ACSC has seen large volumes of reconnaissance scans by malicious actors attempting to find Australian entities vulnerable to the Log4j vulnerability.

Australian Critical Infrastructure under threat with vulnerabilities exposed in MobileIron.

- Mobile Device Management service, MobileIron have vulnerabilities across multiple product versions exposed by state-based cyber actors.
- Attacks target critical infrastructure, government, health and energy organisations.

The threat of a cyber attack on Australia's critical infrastructure is "immediate", "realistic" and "credible", and could take down the nation's electricity network.

Secretary of the Department of Home Affairs of Australia, Michael Pezzullo AO (24/05/2021)

https://www.cyber.gov.au/acsc/view-all-content/advisories/2022-02-australian-organisations-should-urgently-adopt-enhanced-cyber-security-posture
https://www.cyber.gov.au/acsc/view-all-content/news/cybercriminals-scanning-australian-entities-serious-cyber-vulnerability
https://www.cyber.gov.au/acsc/view-all-content/alerts/active-exploitation-vulnerable-mobileiron-products
https://www.abc.net.au/news/2021-05-24/cyber-attack-threat-critical-infrastructure-mike-pezzullo/100160894

Background - Drivers

Key considerations that drove AEMO to establish the AESCSF and uplift Cyber Security across the energy sector:

- AEMO's responsibility for maintaining the security of the grid means cyber considerations are a material concern.
- Finkel Recommendation 2.10 requires an annual report into the cyber security preparedness of the National Electricity Market.
- Increasing level of concern and urgency from Australian Government agencies in relation to cyber threats.
- International events and incidents related to Energy Critical Infrastructure that have been attributed to cyber threat actors.
- The trend of increasing digitisation and automation of critical energy system has increased the risk of disruption through cyber-attacks.

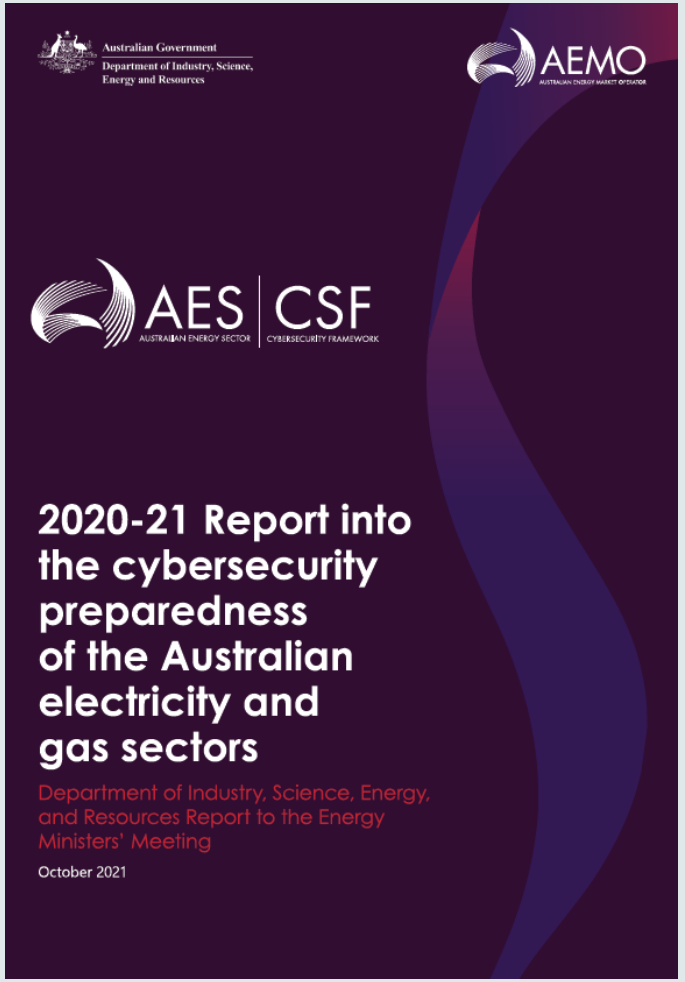
With the 2022 AESCSF being led by the Department of Industry, Science, Energy and Resources (DISER) and AEMO, the drivers for continued uplift are:

- Helping governments understand how industry is developing its cyber maturity which may guide the design of future support for the sector.
- Determining the current state of an organisation's cyber security capability and maturity while the energy sector transitions to an enhanced regulatory framework.
- Demonstrates the Australian Government's investment and involvement in supporting critical infrastructure to combat cyber threats nationwide.
- The large cascading impacts that have occurred as a result of cyber-attacks on Energy Critical Infrastructure globally.
- The rapid pace of change and innovation within the energy sector, including focus on digitising and transitioning the energy sector to renewables, could leave it increasingly vulnerable to cyber-attacks.

Background - Outcomes

- The AESCSF is a voluntary cyber security assessment framework for Australia's energy sector.
- The majority of Australia's energy market participants use the AESCSF program to assess, benchmark and use results to inform cyber security uplift investment.
- De-identified and aggregate scores are provided to Energy Ministers and government in an annual report (not public).
- The annual report provides government with a snapshot of how industry performance compares with previous annual assessments. Government may use results to inform support for the sector.
- Noting assessments are voluntary, energy market participant CEO engagement has increased substantially since program inception.
- Participation may help entities responsible for critical infrastructure to test whether their current cyber security arrangements meet their obligations under the Critical Infrastructure and Systems of National Significance (CI SONS) regulatory reforms.

2020-21 AESCSF Market Coverage			
Electricity (NEM & WEM)	Electricity (Other markets)	Gas	Liquid fuels
✓	✓	✓	Coming in 2022



AES CSF
Australian Energy Sector Cyber Security Framework

Introduction to the AESCSF

AESCSF – Guiding Principles

The guiding principles of the AESCSF are:

Uplift Cyber Security Capability

Enable organisations to assess, evaluate, prioritise, and improve their cyber security capability, and ultimately strengthen Australia's cyber resilience.

Adaptable & Fit-for-Purpose

Develop a robust, adaptable, and fit-for-purpose framework to ensure necessary coverage for energy organisations of all shapes and sizes, across IT and OT.

It is designed to evolve with the threat landscape and provide insights into new mitigation strategies.

Tailored to the Australian Energy Sector

Is tailored for the Australian energy sector and aligns with existing local policies and guidelines, for example, the Australian Privacy Principles and ACSC Essential 8.

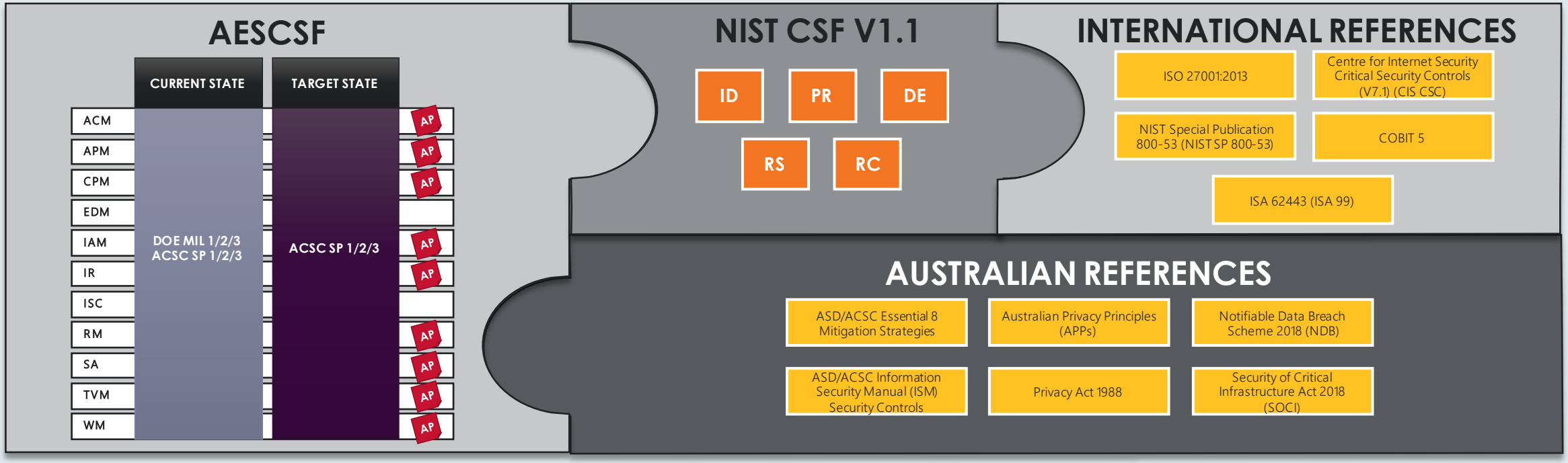
Leverage International Industry Standards

Leverages existing industry standards that have been adopted globally. C2M2* was used as the foundation of the AESCSF, with alignment to the NIST CSF^.

*C2M2 – United States Department of Energy Cyber Security Capability Maturity Model
^NIST CSF – National Institute of Standards and Technology Cyber Security Framework

Overview of the AESCSF

The AESCSF was developed by the AESCSF Working Group (led by AEMO), AEMO and government in 2018. The AESCSF is based on well-established and globally adopted frameworks – namely C2M2* and the NIST CSF^. The AESCSF augments areas where C2M2 has limited coverage (such as privacy), and supplements it with additional information including, but not limited to, Australian-specific requirements, contextual guidance, and anti-patterns developed in conjunction with the AESCSF Working Group. This provides the depth and breadth of coverage necessary for Australian market participants.



*C2M2 – United States Department of Energy Cyber Security Capability Maturity Model
^NIST CSF – National Institute of Standards and Technology Cyber Security Framework

AESCSF Elements

Below is a summary of the framework elements that have been developed and/or tailored to augment the AESCSF:

Anti-patterns		• The AESCSF Working Group identified a set of anti-patterns which describe issues and problem statements that may increase cyber risk. • They are intended to be the 'opposite' of good practice. If an anti-pattern exists, it will impact an organisation's ability to achieve the associated maturity level.
Contextual Guidance		• Practices are accompanied with additional context guidance to drive consistency, clarity, and a shared understanding across the energy sector. • Additional context to enable efficient and effective self-assessment activities, and to drive more accurate outcomes.
Informative References	Australian References	• The AESCSF integrates Australian specific requirements and guidelines to provide greater relevance and local context to Australian energy sector participants. • The Australian references are not prescriptive and are not part of the AESCSF assessment – they are sources of guidance, not mandatory requirements.
	International References	• The international references provide guidance on how to remediate and uplift capability. • The international references are not prescriptive and are not part of the AESCSF assessment – they are sources of guidance, not mandatory requirements.

AESCSF Key Artefacts

The following suite of artefacts is designed to complement and enable organisations to optimally use the AESCSF. The Framework and Guidance artefacts are available for download to use offline. Assessments will be completed via a web-enabled toolkit.

Artefact & Description:

Framework

- **Framework Core** – The core framework artefact which includes mapping of C2M2 Practices to NIST CSF, Contextual Guidance, Anti-Patterns, International and Australian informative references.
- **Framework Overview** - Companion document providing information about the AESCSF and 2022 self-assessment program. Included is a list of frequently asked questions (FAQ) about the AESCSF and assessments.

Guidance

- **AESCSF Quick Reference Guide -** A quick reference guide on how to use the assessment scoring model.
- **Education Workshop Pack –** This pack you are currently reading which is designed to assist organisations to understand the AESCSF, and to use as a template when training staff on the AESCSF.
- **AESCSF Animation** – A 15 min introductory video to the AESCSF
- **Glossary –** A document containing key terms used in the AESCSF to provide consistent understanding and clarity.
- **AESCSF Toolkit User Guide -** Documented guidance on how to use the AESCSF Toolkit.
- **AESCSF Guidance for Low Criticality Organisations** – A guide for smaller organisations getting started on their cyber security uplift journey.

Toolkit

- **Online Criticality Assessment Tool -** Questionnaire used to assess each market participant against a set of predefined criteria to determine their relative criticality to the sector.
- **Online AESCSF Self-Assessment toolkit** - Portal with two modules: (1) 'Collect' module used to collect and store self-assessment data. (2) 'Explore' module to view results against a de-identified AESCSF data set for benchmarking and Year-on-Year analysis.
- **Offline AESCSF Toolkit (Available after assessment period) –** An offline toolkit based in Microsoft Excel that can be used for scenario modelling. Includes both Criticality Assessment Tool and Full self-assessment.

The Framework and Guidance artefacts are available for download from AEMO's website. The offline toolkit will be available after the assessment period has closed. Login details for the online toolkit have been shared with nominated contacts in the lead up to the 2020-21 assessment window. If you are yet to receive details please contact aescsf@aemo.com.au

Key Updates to 2022 AESCSF

The framework has been updated to remain current with the latest version of the Australian Government Information Security Manual and with the NIST CSF. There were no material changes to the framework core but some informative reference mapping has been adjusted to align with revisions.

Expansion into the liquid fuels sub-sector
• In consultation with industry and peak bodies, the AESCSF has been expanded to cover the liquid fuels sub-sector. • This expansion will provide valuable national energy cyber security capacity and maturity insights. • The framework was designed to be applicable across the energy sector when it was initially developed. This was confirmed during the review of the framework in preparation for the expansion to liquid fuels markets.

AES CSF
Australian Energy Sector Cyber Security Framework

Criticality Assessment

Criticality Assessment Overview

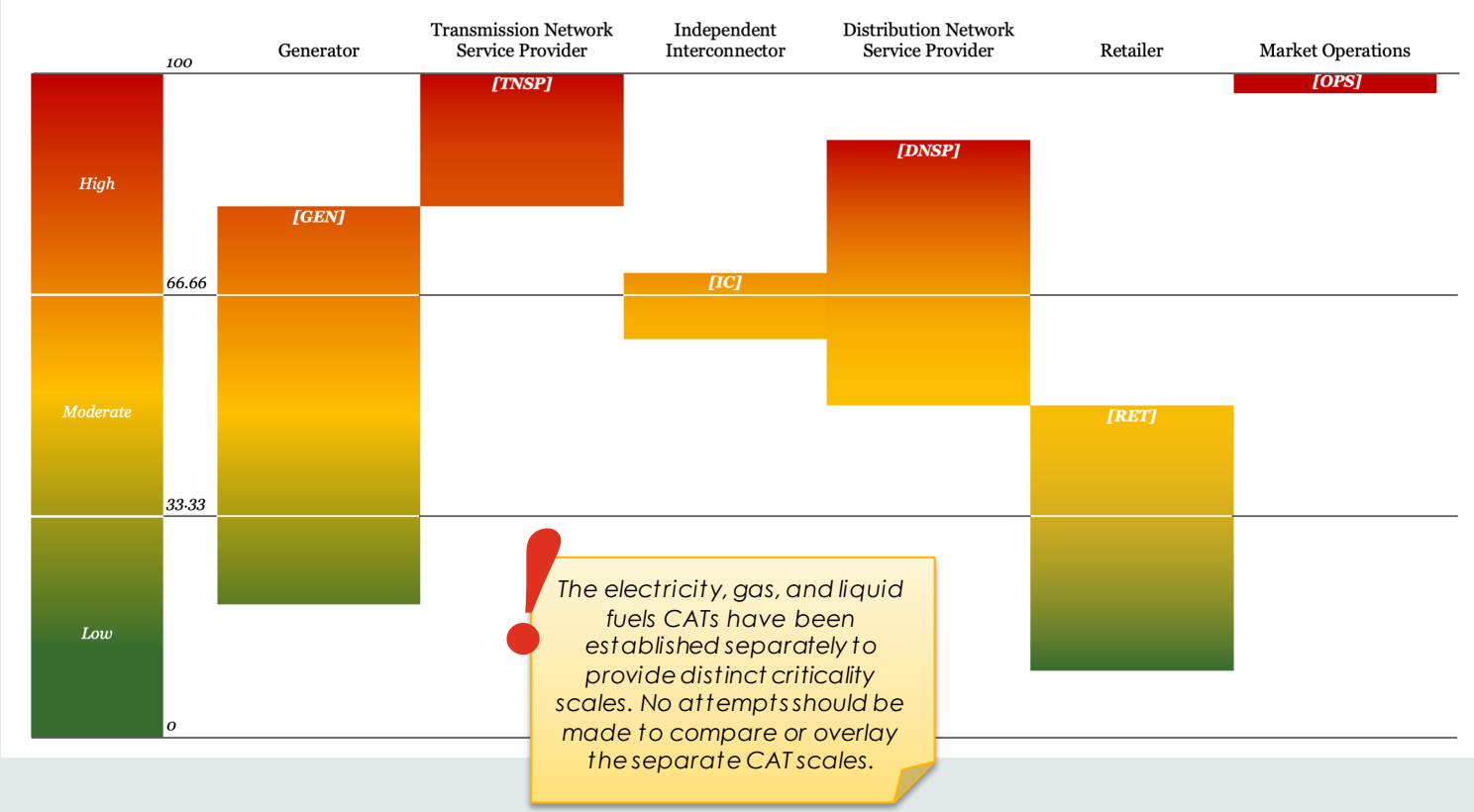
The AESCSF Criticality Assessment Tools (CATs) assess the relative criticality of entities participating in the electricity, gas or liquid fuels sub-sectors.

Key criticality indicators for each market sub-sector have been established to stratify participating entities within the sub-sector criticality bands.

These 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.

This criticality 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).

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



Note: This diagram represents the criticality banding for the electricity sub-sector only. There is a separate and different criticality scale and sub-sector criticality banding for gas markets and Liquid Fuels (refer to page 20 & 22).

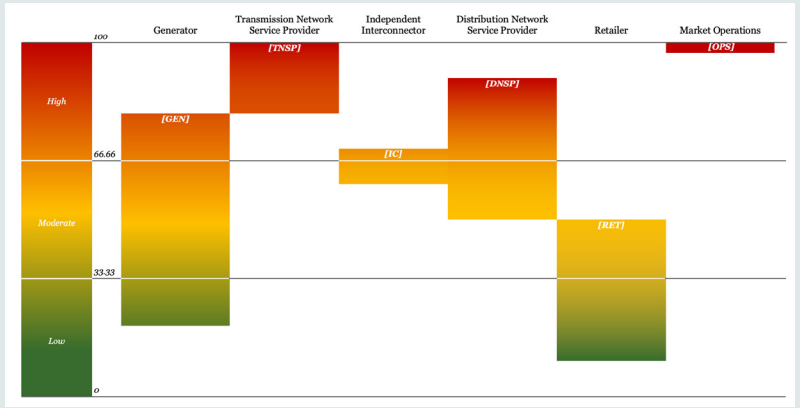
2020-21 Key Outcomes & 2022 Update

2020-21 Outcomes

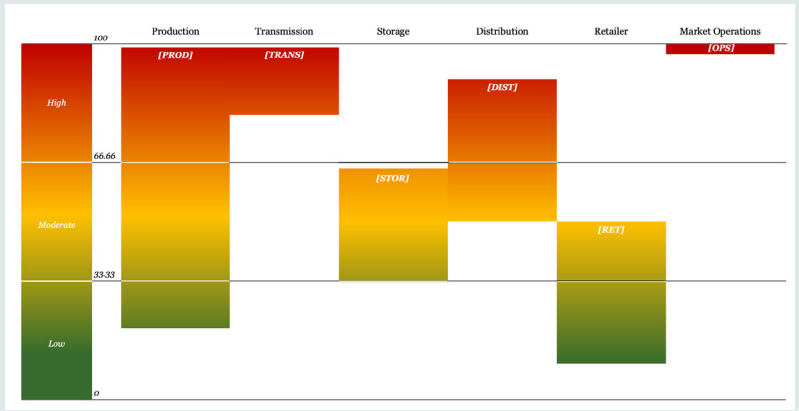
- In the 2020-21 program, the use of the E-CAT and G-CAT by market participants produced a good spread of electricity and gas organisations across the three criticalities (liquid fuels markets were not in scope).
- Based on the analysis of 2020-21 CAT data, no major changes to the E-CAT or G-CAT were made, with the only updates being minor wording adjustments.

2022 Update

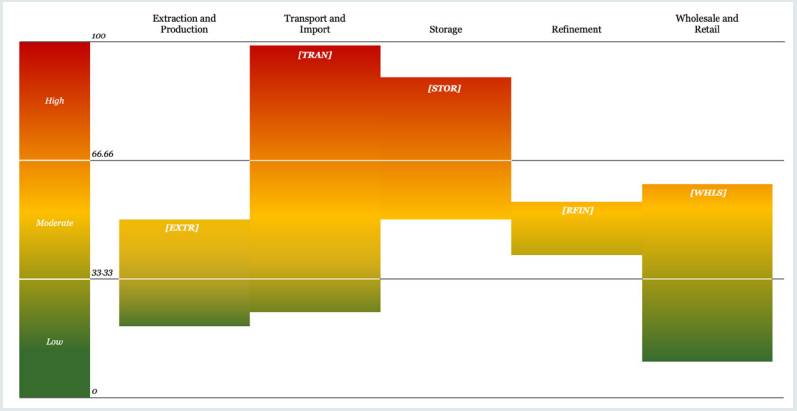
- The 2022 AESCSF program expands to include the liquid fuels sub-sector and the development of the L-CAT.
- A similar methodology was used in the development of the L-CAT to that used in development of the E-CAT and G-CAT, and focuses on an organisation's criticality and potential impact on end user supply.
- Battery storage added for E-CAT.



Electricity CAT (E-CAT) Overview



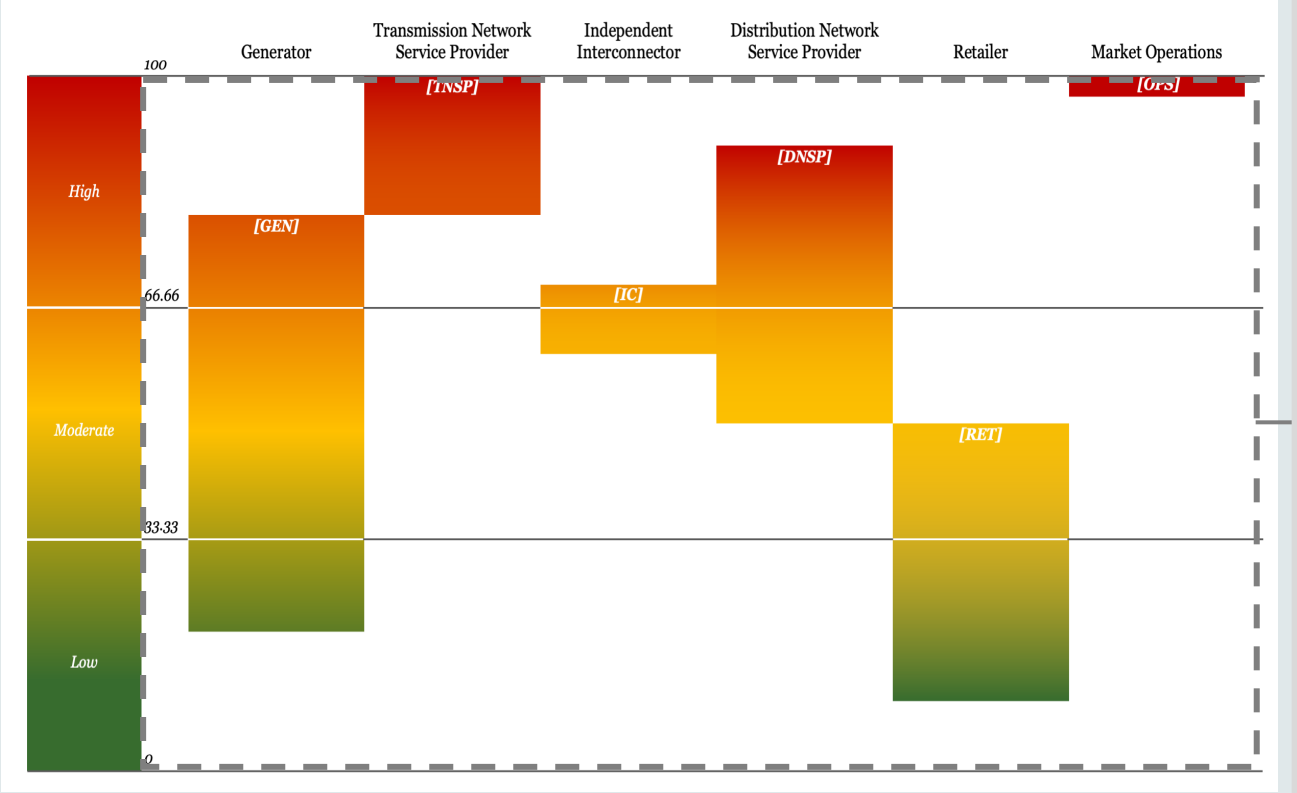
Gas CAT (G-CAT) Overview



Liquid Fuels CAT (L-CAT) Overview

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 CI-SONS**

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.

*Protecting Critical Infrastructure and Systems of National Significance (CISONS) - Security Legislation Amendment (Critical Infrastructure) Bill 2020.

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

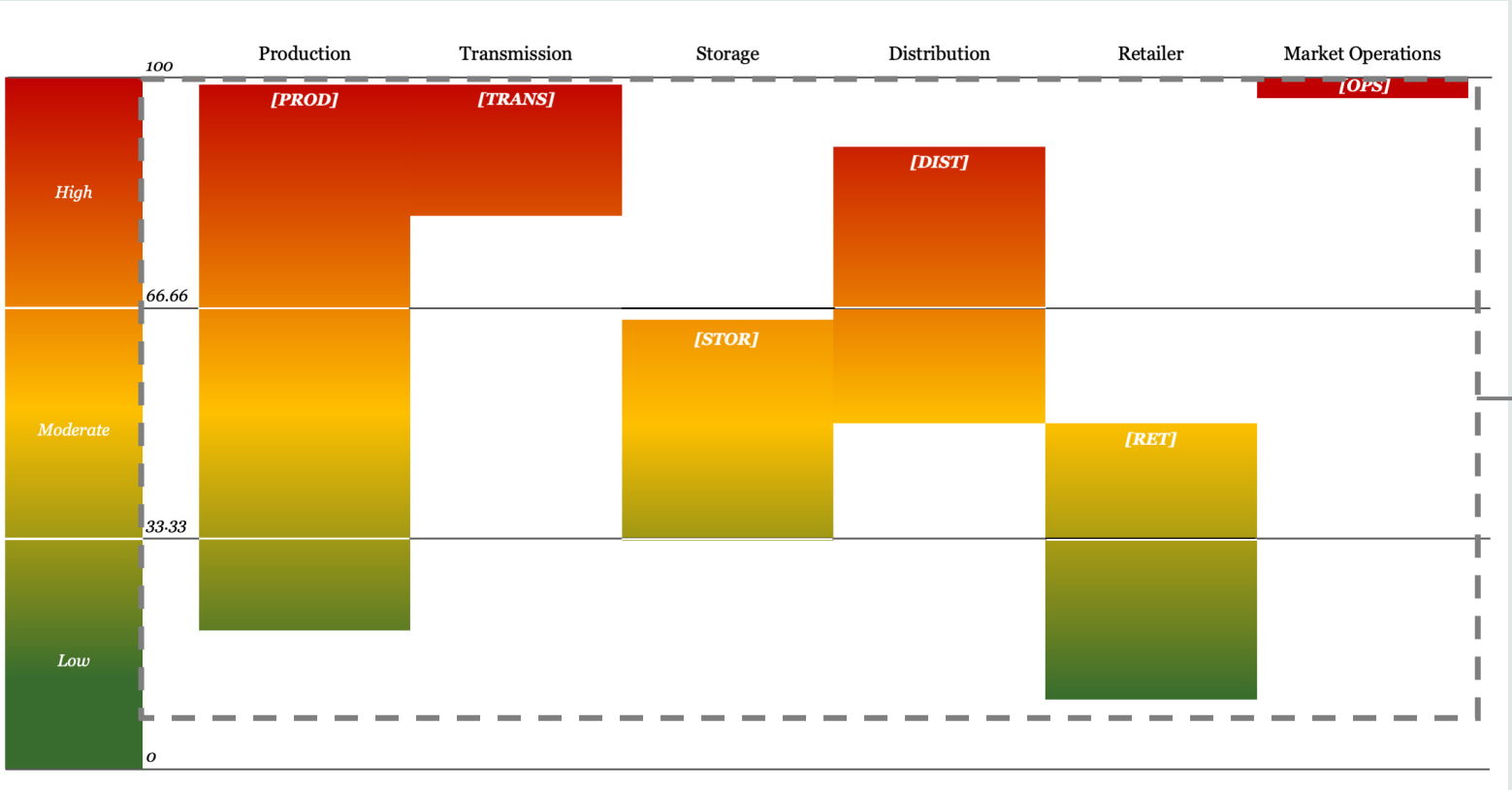
Market Operations

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

Additional criticality indicators to further explore battery storage are in discussion and will be trialled as a part of the 2022 AESCSF Program.

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.



*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 CI-SONS**

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.

*Protecting Critical Infrastructure and Systems of National Significance (CISONS) - Security Legislation Amendment (Critical Infrastructure) Bill 2020.

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

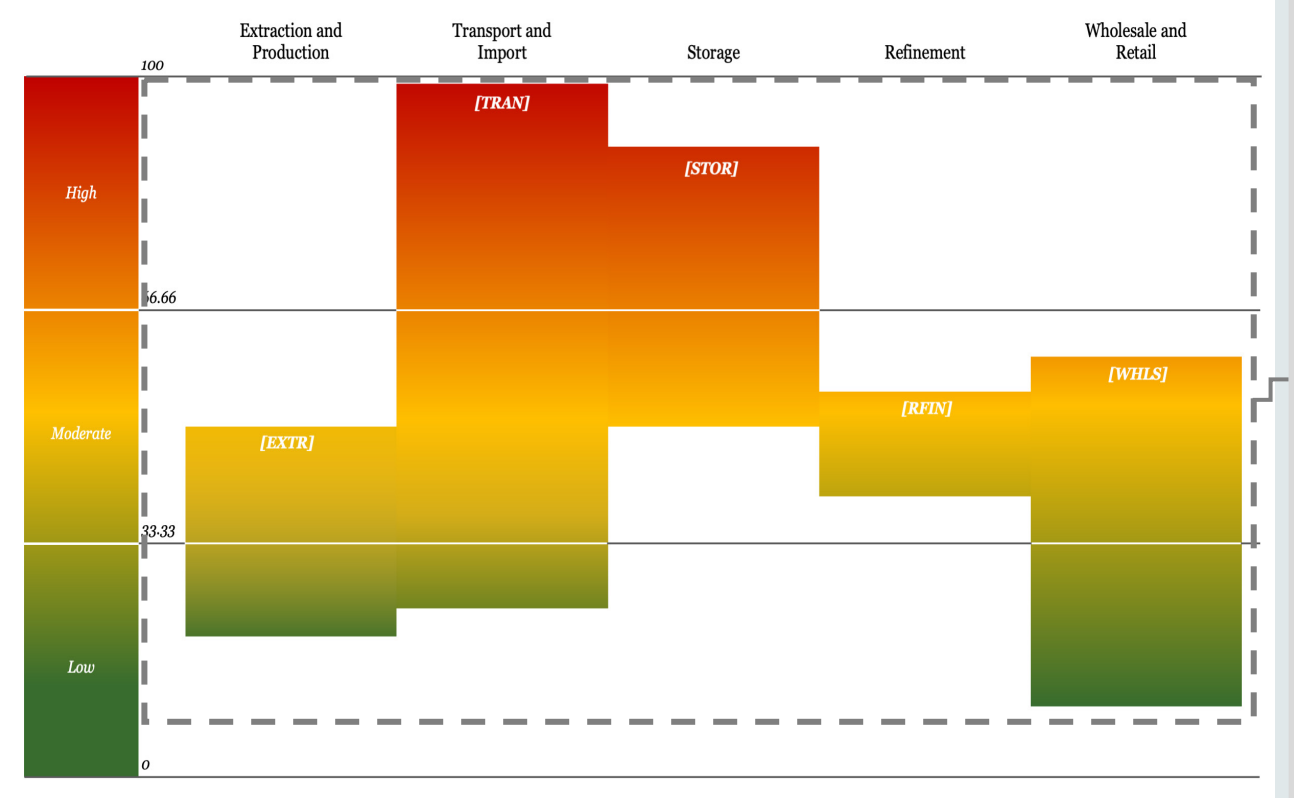
- Number of customers (National Metering Identifiers)
- Number of Critical and Commercial entities

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 2022, 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.



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.
- As this is the first year of L-CAT we welcome views on this to inform improvements for future years.

*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 CI-SONS**

*Protecting Critical Infrastructure and Systems of National Significance (CISONS) - Security Legislation Amendment (Critical Infrastructure) Bill 2020.

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

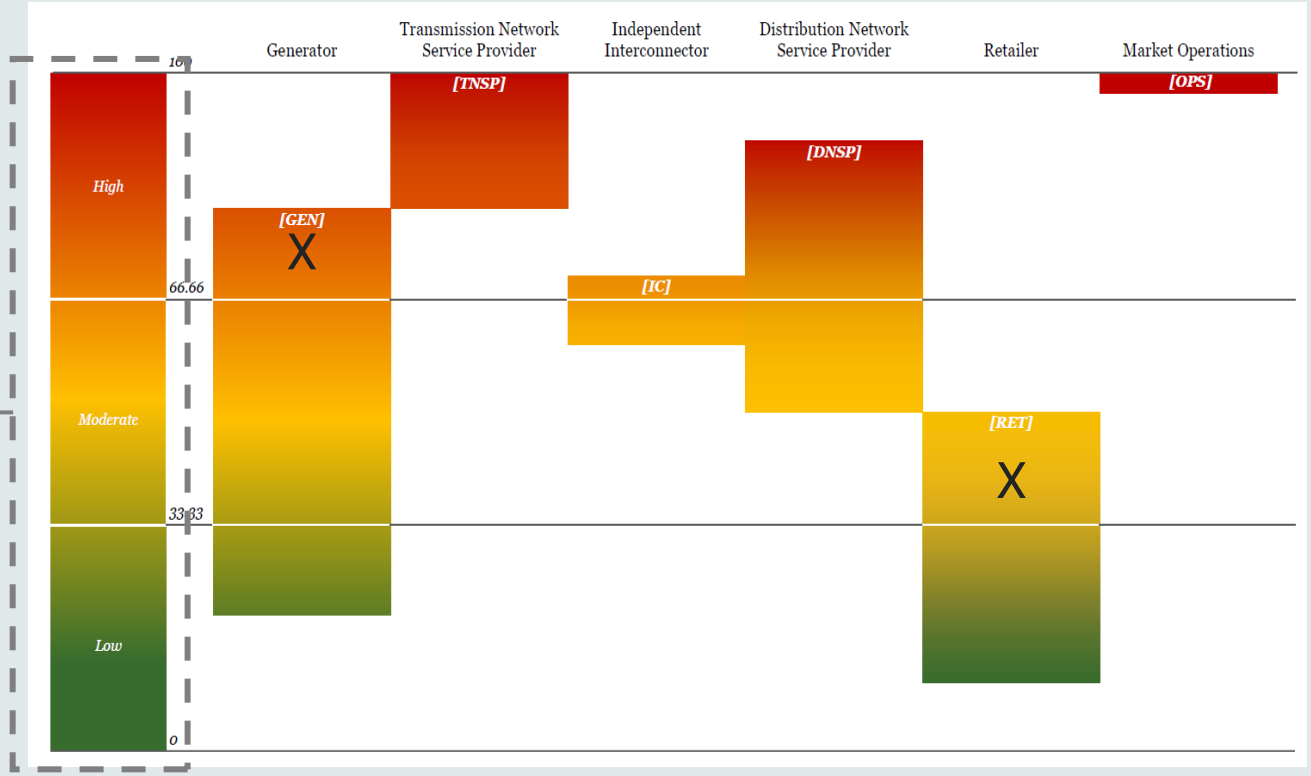
The Criticality Scale score of each entity will determine their cyber-security capability maturity target state.

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.



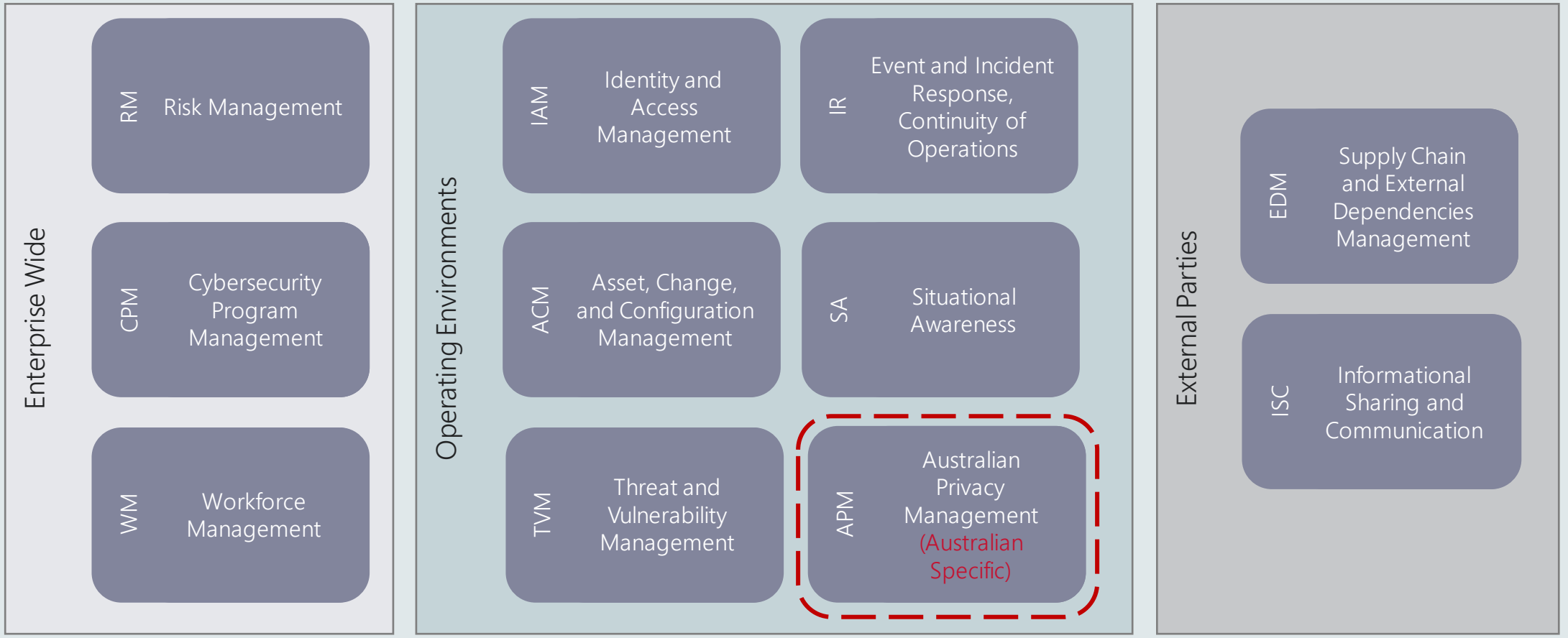
For example, a hypothetical organisation participates in both the Generation and Retail sub-sectors, with their criticality results shown with 'X's above. Their overall criticality result is the highest of all applicable sub-sector results – that means that in this example they would be assessed as a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

AES CSF
Australian Energy Sector Cyber Security Framework

Framework Structure

AESCSF Domains

The AESCSF is divided into 11 domains - 10 C2M2 domains, and the Australian Privacy Management domain. The domains are logical groupings of cyber-security Practices. Each domain has an acronym that cross references across the AESCSF Toolkit and Guidance Artefacts.



AESCSF Domains: Australian Privacy Management Domain

The purpose of the APM domain is to establish and maintain plans, procedures, and technologies to manage personal identifiable information through its lifecycle. This includes the collection, storage, use and disclosure, and disposal (including de-identification) of personal information.

APM

Australian Privacy Management

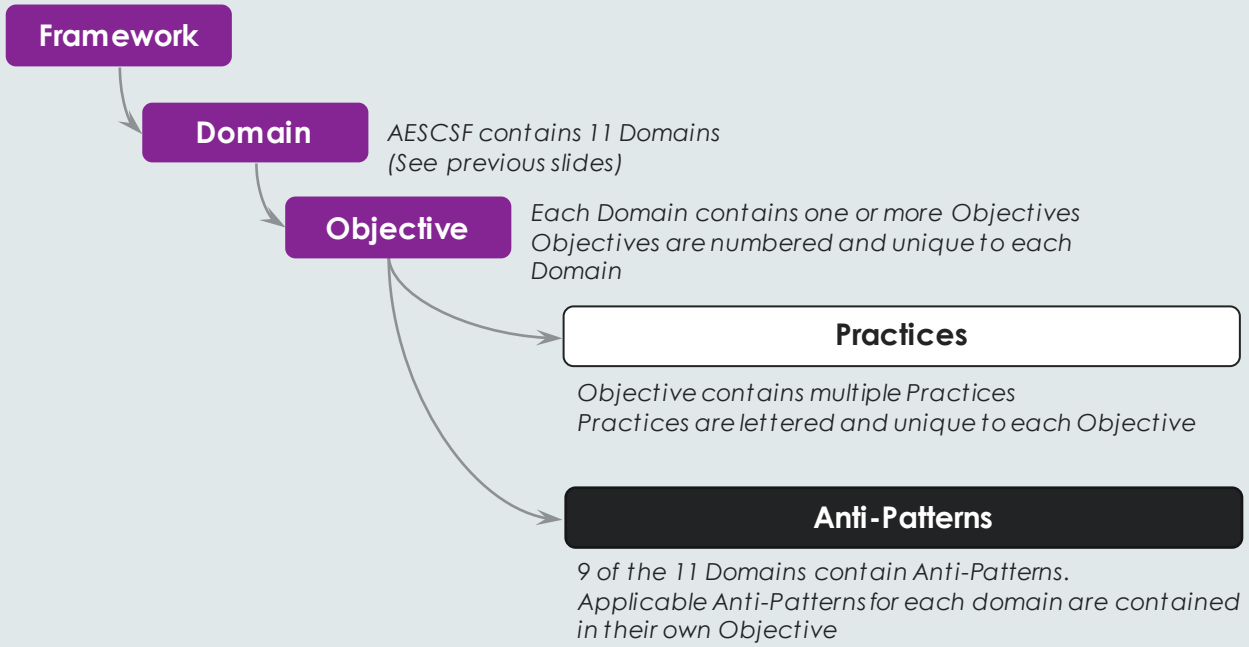
- The development of the APM Domain leveraged the Australian Privacy Principles and the Office of the Australian Information Commissioner Privacy Management Framework. International privacy standards such as ISO/IEC 27001 and NIST SP 800-53 were mapped to the privacy practices to assist organisations to achieve implementation of practices with a risk-based approach.
- *DISER, AEMO and the project team do not act as an authority on privacy law compliance to participants at any stage of the AESCSF.*

Please note: The AESCSF has included the Australian Privacy Management (APM) domain based on consultation with AEMO, Government and Industry in 2018, in recognition of the intersections between privacy management and robust cyber-security. If your organisation has any concerns or queries relating to the APM domain, please inform aescsf@aemo.com.au.

It is each organisation's responsibility to ensure it is compliant with state and federal privacy requirements, and other confidentiality and or related laws that may apply to you. Achieving MIL 3 in APM does not represent your compliance with privacy law, any of the Australian Privacy Principles or any other state or federal legal or regulatory obligations. Please consult with independent legal counsel or contact the Office of the Australian Information Commissioner if you have any questions about your compliance with privacy law.

Framework Structure

Within each Domain there are one or more Objectives. Objectives contain multiple Practices, which together describes an outcome, e.g. 'Establish and Maintain Identities'. Where applicable, some Domains have an 'Anti-Pattern' Objective which contains one or more Anti-Patterns.



Each Practice and Anti-Pattern is coupled with Contextual Guidance to provide clarity and drive consistency.

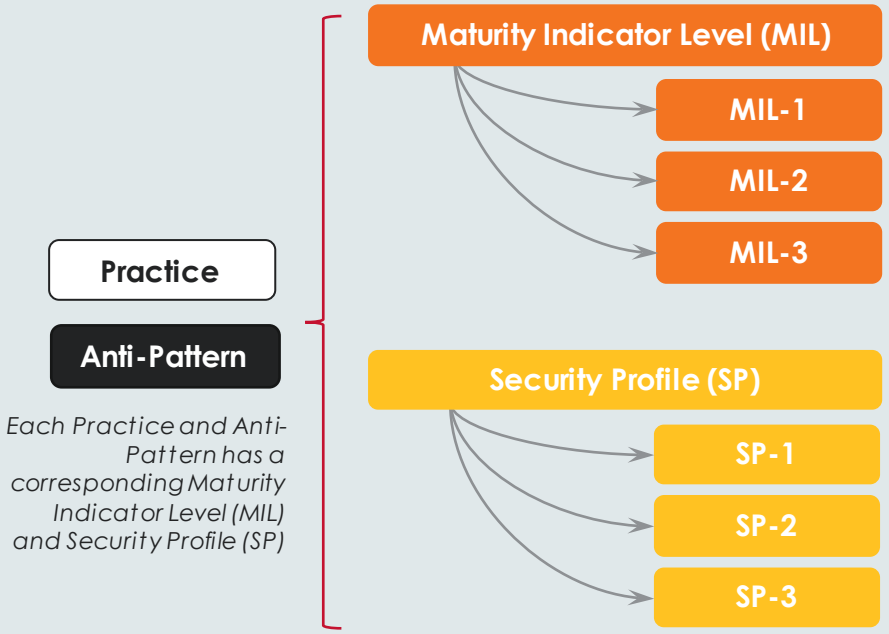
See later slides for worked examples of Framework components

What are Anti-Patterns?

- Anti-Patterns are included in the AESCSF to enable identification of behaviours/practices that hinder an organisation from achieving a higher maturity and they have remained in subsequent AESCSF versions.
- Anti-Patterns were developed in consultation with AEMO, industry and government stakeholders.
- In essence, they are 'bad' activities that undermine the effectiveness of a cyber-security capability. Therefore, additional focus is given to them to encourage organisations to fix these behaviors.

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). The SPs have been defined by the Australian Cyber Security Centre, in consultation with AEMO and industry representatives, as a measure of target state maturity. The target state maturity SP a Participant should pursue is determined based on their overall criticality result (per the CAT).

Consultation to ratify if existing Target State guidance is applicable to the Gas and Liquid Fuels sub-sectors is ongoing.

Key aspects of MILs and SPs

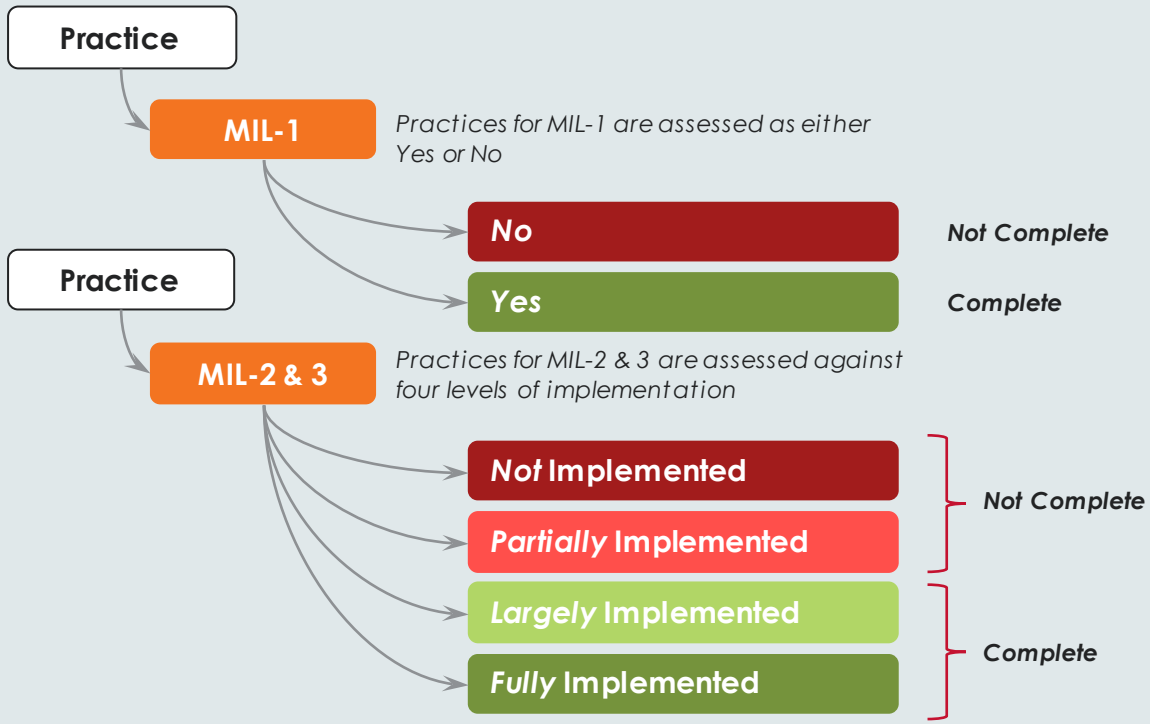
1. MILs apply independently to each domain. As a result, entities may be operating at different MIL ratings for different Domains.
2. SPs apply collectively across all Domains. As a result, entities only achieve a SP if they have completed all Practices in the SP across all Domains.
3. The MILs and SPs 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).

AES | CSF
Australian Energy Sector | Cyber Security Framework

AESCSF Full Self-Assessment Scoring Model

Assessment Scoring Model Key Features

The AESCSF uses a revised United States Department of Energy Cyber Security Capability Maturity Model (C2M2) scoring model to drive consistency and clarity.



Description of MILs:

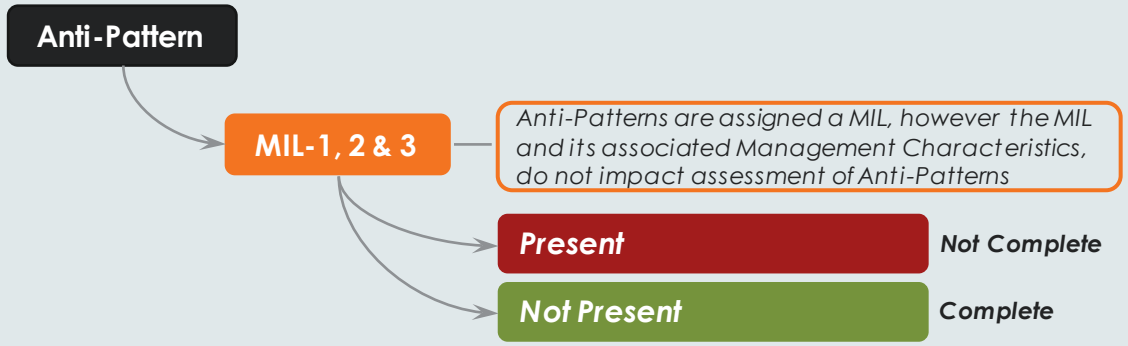
- **MIL 1 (Initiated):** Initial Practices are performed but may be ad-hoc.
- **MIL 2 (Performed):** Practices are more complete or advanced than at MIL 1 with the introduction of management characteristics that drive consistency and repeatability.
- **MIL 3 (Managed):** Practices are more complete or advanced than at MIL 2 with the addition of further management characteristics that drive governance and continuous improvement.

Key features of the scoring model include:

- 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".
- Scored based on a combination of "**Practice implementation**" and "**Management Characteristics**".

Assessment Scoring Model Key Features

Anti-Patterns are scored using a similar approach to MIL-1 Practices, however, do not require consideration of Management Characteristics.



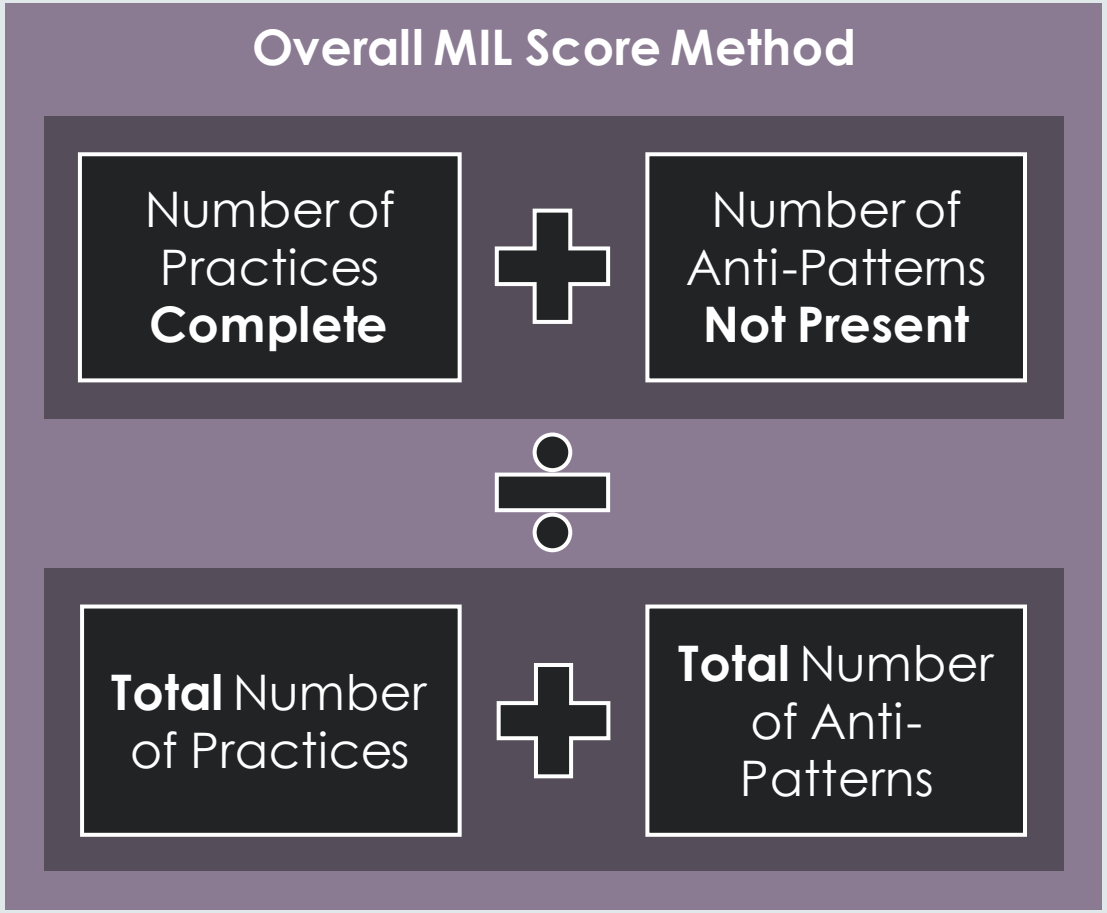
Assessment scoring of Anti-Patterns:

- 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 Scoring Methods

Per the Framework Structure Section, AESCSF results can be expressed either in terms of Maturity Indicator Level (MIL) or Security Profiles (SP).

- There are three MILs (MIL-1, MIL-2 and MIL-3) that are assigned to all practices in all the Domains in the Framework and define the maturity progression.
- The MILs apply independently to each domain and are cumulative.
- For a participant to gain a MIL in each domain, they must Complete all practices, and not exhibit any Anti-Patterns, at that MIL in that Domain.
- For example, to achieve a MIL-3 the participant would have to perform all Practices and not exhibit any of the Anti-Patterns, in MIL-1, MIL-2, and MIL-3.



Assessment Scoring Methods

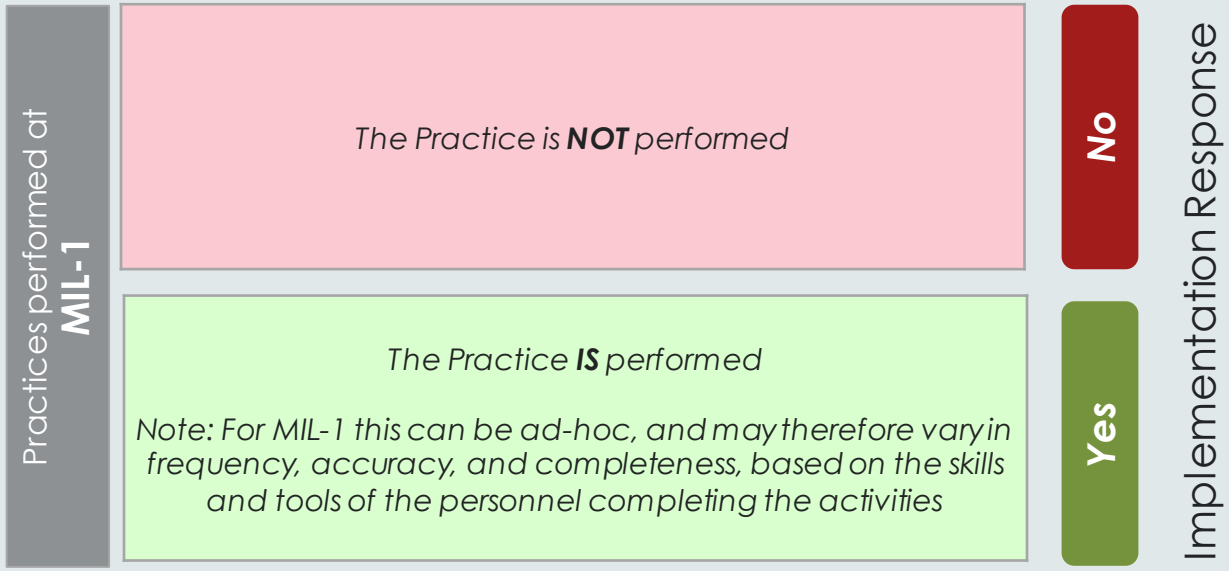
In addition to the MIL, AESCSF has three alternate groupings of Practices referred to as Security Profiles (SP) outlined in further detail on a preceding slide:

- SPs cannot be applied to each Domain unlike MIL.
- For a participant to be recognised for a Security Profile, 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.

Security Profile (SP)	Participant criticality	Practices and anti-patterns			Total required to achieve SP
		MIL-1	MIL-2	Mil-3	
Security Profile 1 (SP-1)	Low	57	27	4	88
Security Profile 2 (SP-2)	Medium	0	94	18	200 (112+88 from SP-1)
Security Profile 3 (SP-3)	High	0	0	82	282 (82+200 from SP-2)

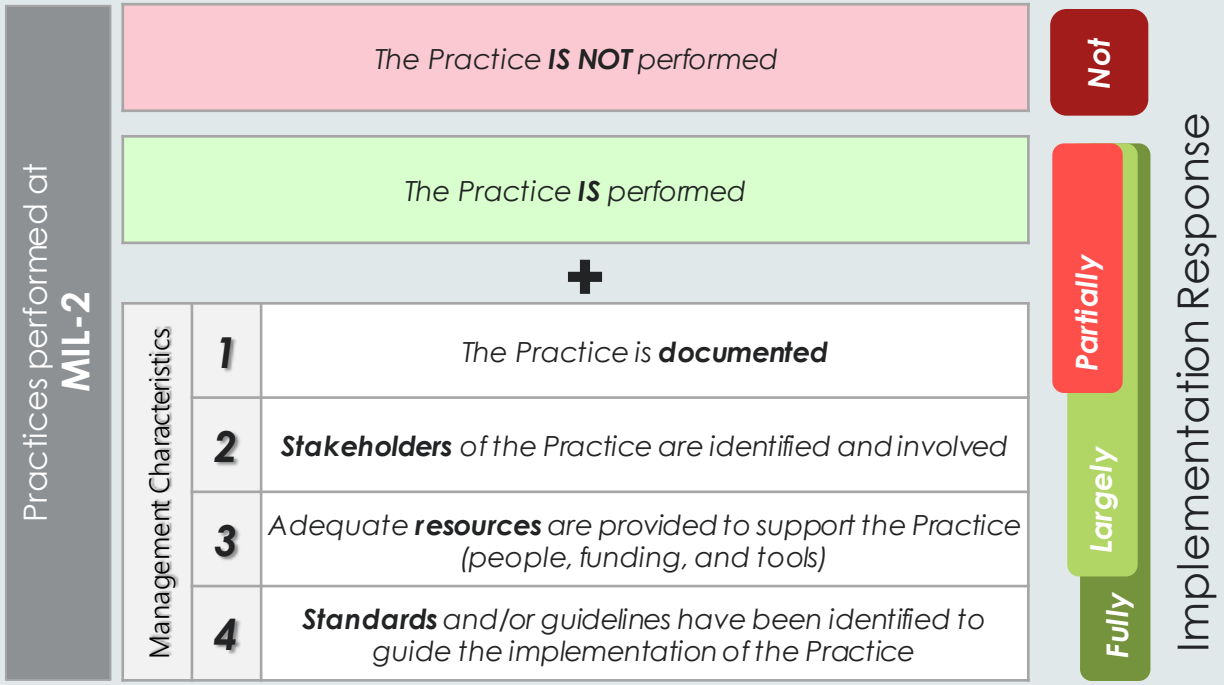
Assessing Implementation

MIL-1 Practice



The Framework leverages the MILs established within the C2M2. Maturity indicator levels (MIL's) relate to Security Profiles (SP) but, unlike MILs, SPs cannot be applied independently to each Domain. To achieve an SP, Participants must be performing all the Practices, and not exhibiting any of the Anti-Patterns within that SP, and any preceding SPs, across all Domains. The cumulative nature of MILs continues to apply to SPs (i.e., SP-2 can only be achieved if SP-1 is also achieved).

MIL-2 Practice



Assessing Implementation

MIL-3 Practice

Practices performed at **MIL-3**

*The Practice **IS NOT** performed, **OR** the Practice is performed **HOWEVER** MIL-2 Management Characteristics (1, 2 and/or 3) are **MISSING** .*

*The Practice **IS** performed, **AND** **AT LEAST** MIL-2 Management Characteristics 1, 2 and 3 are present*

+

Management Characteristics		
	5	*Activities are guided by **policies** (or other organisational directives) and governance*
	6	*Personnel performing the Practice have adequate **skills and knowledge***
	7	*Policies include **compliance** requirements for specified standards and/or guidelines*
	8	***Responsibility and authority** for performing the Practice is assigned to personnel*
	9	*Activities are **periodically reviewed** to ensure they conform to policy*

Implementation Response: **Not** | **Partially** | **Largely** | **Fully**

*Any Fully Implemented Practice at MIL-3 requires **all** Management Characteristics from **both** MIL-2 and MIL-3.*

Anti-Patterns

Anti-Patterns at **MIL-1, 2 & 3**

*This activity **IS** exhibited within the function (either pervasively or within a limited context)*

*This activity **IS NOT** exhibited within the function*

Implementation Response: **Present** | **Not Present**

Management Characteristics DO NOT impact the assessment of Anti-Patterns.

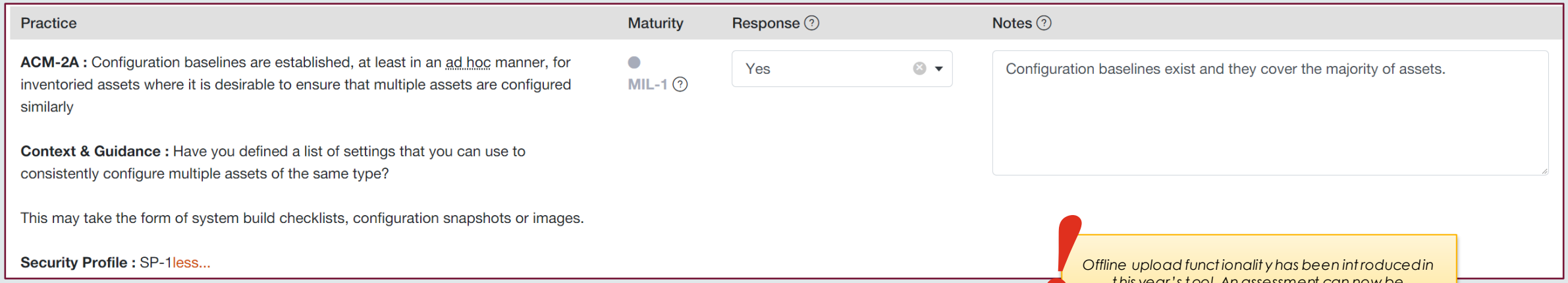
Assessment Scoring Model – Worked Example 1

AESCSF Practice:	ACM-2A (MIL-1): "Configuration baselines are established for inventoried assets where it is desirable to ensure that multiple assets are configured similarly".
Assessment Scenario:	John from *Samplepower Co* reads this Practice and considers whether the organisation creates templates for settings, standard configurations for equipment in the field, and a standard operating environment across information technology assets. He knows that the security team creates these things for key systems, and has done so for quite a while.

Assessment Scoring Model – Worked Example 1

AESCSF Practice: ACM-2A (MIL-1): "Configuration baselines are established for inventoried assets where it is desirable to ensure that multiple assets are configured similarly".

Assessment Scenario: John from *Samplepower Co* reads this Practice and considers whether the organisation creates templates for settings, standard configurations for equipment in the field, and a standard operating environment across information technology assets. **He knows that the security team creates these things for key systems, and has done so for quite a while.**



Practice	Maturity	Response	Notes
ACM-2A : Configuration baselines are established, at least in an ad hoc manner, for inventoried assets where it is desirable to ensure that multiple assets are configured similarly **Context & Guidance :** Have you defined a list of settings that you can use to consistently configure multiple assets of the same type? This may take the form of system build checklists, configuration snapshots or images. **Security Profile :** SP-1less...	MIL-1	Yes	Configuration baselines exist and they cover the majority of assets.

Offline upload functionality has been introduced in this year's tool. An assessment can now be completed in offline and uploaded, with the results being automatically populated into the online tool.

Assessment Scoring Model – Worked Example 1 (Cont.)

AESCSF Practice:	ACM-2C (MIL-2): "The design of configuration baselines includes Cyber-Security objectives".
Assessment Scenario:	Building on the response at MIL 1, John reads this Practice and considers the configuration baselines that the security team creates. He knows that the baselines have been used in the organisation for more than a few years, and that they cover the most important assets in IT and OT. When new assets are procured, configuration baselines are created for these assets as a part of their rollout. The security team has three full-time personnel who have many responsibilities, one of which is to establish and maintain cyber-security objectives for *Samplepower Co*, and another of which is to create configuration baselines. He is quite confident that the team has created the baselines in alignment with the cybersecurity objectives. John has seen the baselines documented within many systems, one of which is ServiceNow, and feels that there is a good level of awareness across IT and OT personnel regarding where to find the configuration baselines.

Assessment Scoring Model – Worked Example 1 (Cont.)

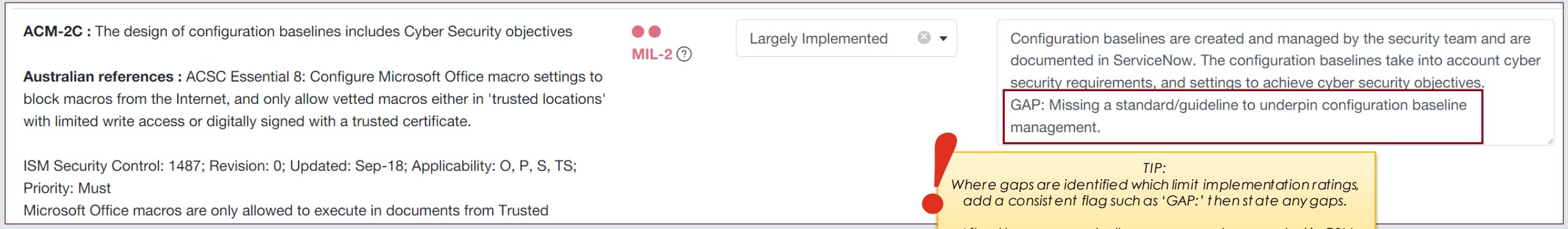
AESCSF Practice: ACM-2C (MIL-2): "The design of configuration baselines includes Cyber-Security objectives".

Assessment Scenario:

Building on the response at MIL 1, John reads this Practice and considers the configuration baselines that the security team creates. **He knows that the baselines have been used in the organisation for more than a few years, and that they cover the most important assets in IT and OT**.

When new assets are procured, configuration baselines are created for these assets as a part of their rollout. The security team has **three full-time personnel (Characteristic 3)** who have many responsibilities, one of which is to establish and maintain cyber-security objectives for *Samplepower Co*, and another of which is **to create configuration baselines (Characteristic 2)**. He is quite confident that the team has created the baselines in alignment with the cybersecurity objectives.

John has seen the baselines **documented in ServiceNow (Characteristic 1 & 3),** and feels that there is a good level of awareness across IT and OT personnel regarding where to find the configuration baselines . With all of this in mind, John feels that the Practice is complete and has the first three management characteristics present, **but not the fourth (Standard & Guidelines).**



TIP:
Where gaps are identified which limit implementation ratings, add a consistent flag such as 'GAP:' then state any gaps.

After the assessment, all responses can be exported in CSV format, and filtering can be performed to extract a list of all known gaps against the AESCSF.

Assessment Scoring Model – Worked Example 1 (Cont.)

AESCSF Practice:	ACM-2E (MIL-3): "Configuration baselines are reviewed and updated at an organizationally-defined frequency".
Assessment Scenario:	Building on the responses at MIL 1 and MIL 2, John reads the Practice and considers whether the security team has ever reviewed and updated the configuration baselines. Given that they have been in place for the past few years, he recalls that they are reviewed annually by the team as a part of the organisation's cyber-security calendar, which is mandated by their CISO. With this in mind, John is confident that review and update does occur at a defined and regular interval. Given that this Practice is at MIL 3, John considers the Management Characteristics that must be present. He knows that the security calendar is documented, and the previous updates of many baselines are retained in ServiceNow. Additionally, John knows that the team has the skills and enough bandwidth for the annual review, and it has been included in their 3-year rolling budget. The budget is allocated to John and the security team by executive management (who are invested in keeping the baselines up to date), and responsibility has been assigned. Despite this, he knows that there is no formal policy in place yet, and that the baselines have never been reviewed by a third party or anyone outside the security team.

Assessment Scoring Model – Worked Example 1 (Cont.)

AESCSF Practice:	ACM-2E (MIL-3): "Configuration baselines are reviewed and updated at an organizationally-defined frequency".
Assessment Scenario:	Building on the responses at MIL 1 and MIL 2, John reads the Practice and considers whether the security team has ever reviewed and updated the configuration baselines. Given that they have been in place for the past few years, he recalls that they are **reviewed annually by the team (Characteristic 2)** as a part of the organisation's **cyber-security calendar, which is mandated by their CISO (Characteristic 5).** With this in mind, John is confident that review and update does occur at a defined and regular interval. Given that this Practice is at MIL 3, John considers the Management Characteristics that must be present. He knows that the **security calendar is documented**, and the previous updates of many baselines are **retained in ServiceNow (Characteristic 1)**. Additionally, John **knows that the team has the skills and enough bandwidth for the annual review**, and it has **been included in their 3-year rolling budget (Characteristic 3, 6).** The budget is allocated to John and the security team by executive management (who are invested in keeping the baselines up to date), and **responsibility has been assigned (Characteristic 8).** Despite this, he knows that there is **no formal policy in place yet**, and that the baselines have **never been reviewed by a third party or anyone outside the security team (Characteristics 7, 9).**

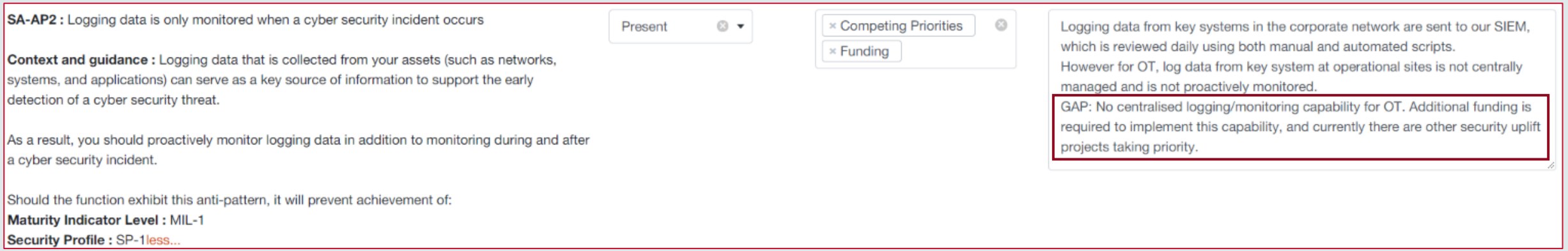
If any of the MIL 2 Management Characteristics required to achieve a status of "Largely Implemented" (i.e. Characteristics 1 -3), are not being exhibited, this MIL-3 Practice would need to be assessed as Not Implemented.

Assessment Scoring Model – Anti-Pattern Worked Example 2

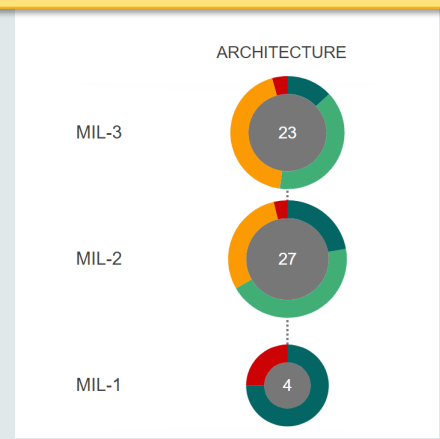
AESCSF Anti-Pattern:	SA-AP2: "Logging data is only monitored when a cyber-security incident occurs".
Assessment Scenario:	John knows that *Samplepower Co* have a well-established monitoring capability, with a centralised Security Incident Event Management capability, where logs from key systems within their corporate environment are automatically ingested. Automated scripts have been created to monitor these logs and trigger alarms when defined thresholds or situations arise. John Is confident for the IT environment that this Anti-Pattern is Not Present. However, John knows that their OT environment does not have the same capability as their Corporate environment. Logs from key OT systems are captured however there is no centralised collation capability, making it impractical for staff to perform proactive monitoring. This is an area that John would like to improve on, however funding for this is not yet available, and there are other more pressing priorities within the security uplift program.

Assessment Scoring Model – Anti-Pattern Worked Example 2

AESCSF Anti-Pattern:	SA-AP2: "Logging data is only monitored when a cyber-security incident occurs".
Assessment Scenario:	John knows that *Samplepower Co* have a well established monitoring capability, with a centralised SIEM, where logs from key systems within their corporate are automatically ingested. Automated scripts have been created to monitor these logs and trigger alarms when defined thresholds or situations arise. John is confident for the IT environment that this Anti-Pattern is Not Present. However, John knows that their OT environment does not have the same capability as their Corporate environment. Logs from key OT systems are captured however there is no centralised collation capability, **making it impractical for staff to perform proactive monitoring**. This is an area that John would like to improve on, however **funding** for this is not yet available, and there are other **more pressing priorities** within the security uplift program. John marks the Anti-Pattern as Present for OT, and lists the reasons why (selecting as many as are appropriate). He adds commentary under the Notes section to articulate his assessment selection.



Overview of Assessment Results & Reporting



*The 2022 online tool includes an **optional** section for architecture in anticipation for the proposed solution in a future update.*

- The results show the 11 Domains and the Anti-Pattern results, divided by different MIL. The number in the middle of the 'Donuts' are the number of Practices within each domain at each MIL.
- The Summary of Results by Domain chart can also be viewed in cumulative mode given that organisations must complete all the Practices in a given MIL as well as all the Practices from predecessor MIL(s) for that Domain to be complete.
- Organisation's will have the ability to export the chart above and a .csv file of responses including notes.
- Energy participant results will be de-identified and aggregated to report to the Energy Ministers' Meeting.
- The Donut layering has been reordered to now have MIL-3 on the top and MIL-1 on the bottom.

AES CSF
Australian Energy Sector Cyber Security Framework

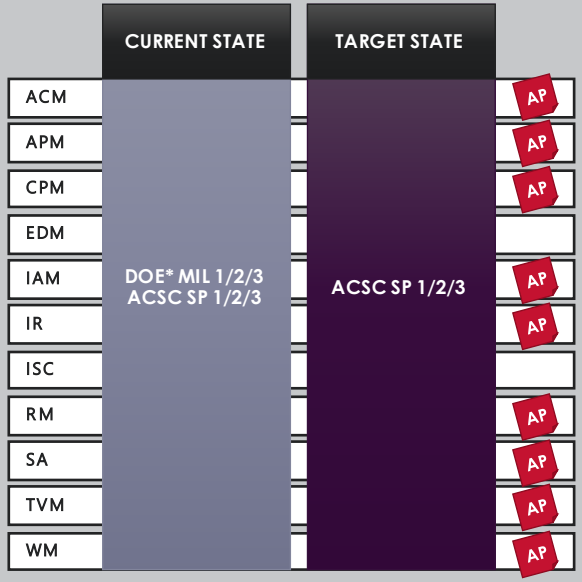
AESCSF Lite Self-Assessment

AESCSF Lite – Overview

- The AESCSF Lite framework has been developed to facilitate self-assessment against the AESCSF by lower-criticality market entities, and those with limited time and security resources.
- The assessment consists of 29 multi-select easy to follow questions written in plain English. Simply select as many responses that are applicable to your organisation. If none of responses apply, select 'None of the above'.

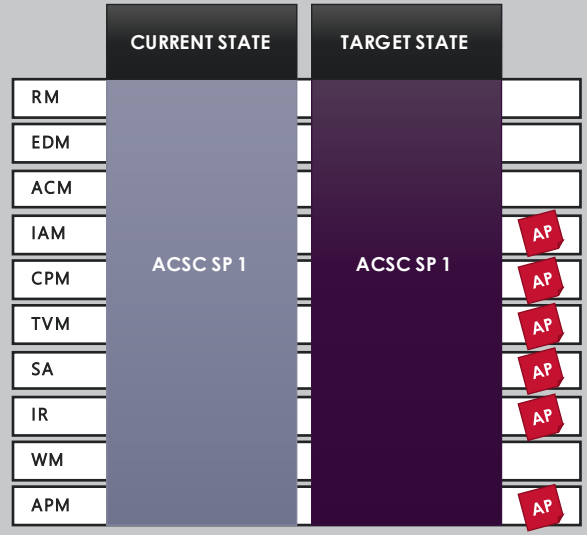
AESCSF

- 282 Practices & Anti-Patterns (2020-21).
- Detailed assessment of 11 Domains.
- Suitable for High, Medium and Low criticality participants across all electricity sub-sectors.
- Coverage of all 3 Australian Cyber Security Centre Security Profiles.



AESCSF Lite

- 29 multiple-select questions.
- High-level assessment across 10 'Topics'.
- Suitable for lower-criticality market participants.
- Coverage of Australian Cyber Security Centre Security Profile 1.

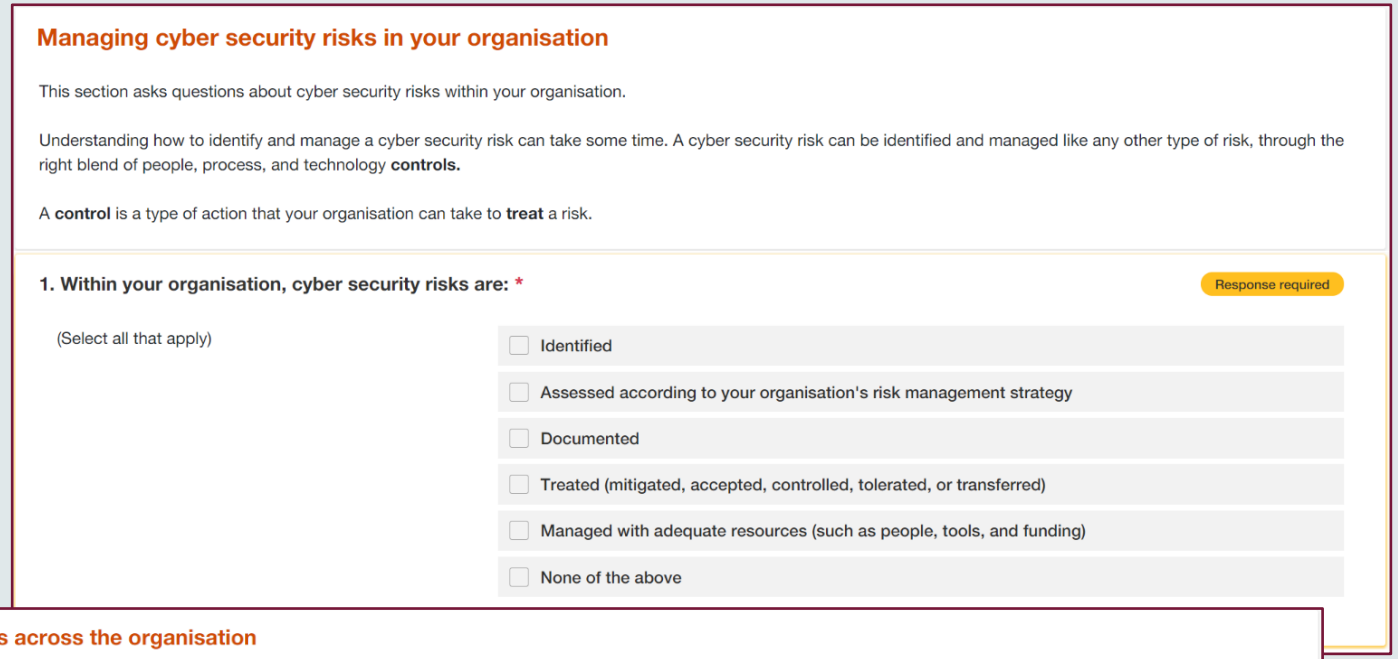


Whilst consultation to ratify if existing Target State guidance is applicable to the Gas and Liquid Fuels sub-sectors is ongoing, all low criticality participants are welcome to complete a Lite Assessment.

*United States Department of Energy (Publisher of the ES/ONG-C2M2)

AESCSF Lite – Completing Assessments

- The duration required to complete the assessment will vary - if responses to all questions are known, the survey can be completed in around 15-20 minutes. However, some clarification with specialists and outsourced providers may be required in order to answer the questions accurately, in which case the total time to complete the assessment will increase.
- Results from an AESCSF Lite framework self-assessment can be transposed into a full framework self-assessment based on a mapping of Lite questions to AESCSF Practices.



Managing cyber security risks in your organisation

This section asks questions about cyber security risks within your organisation.

Understanding how to identify and manage a cyber security risk can take some time. 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.**

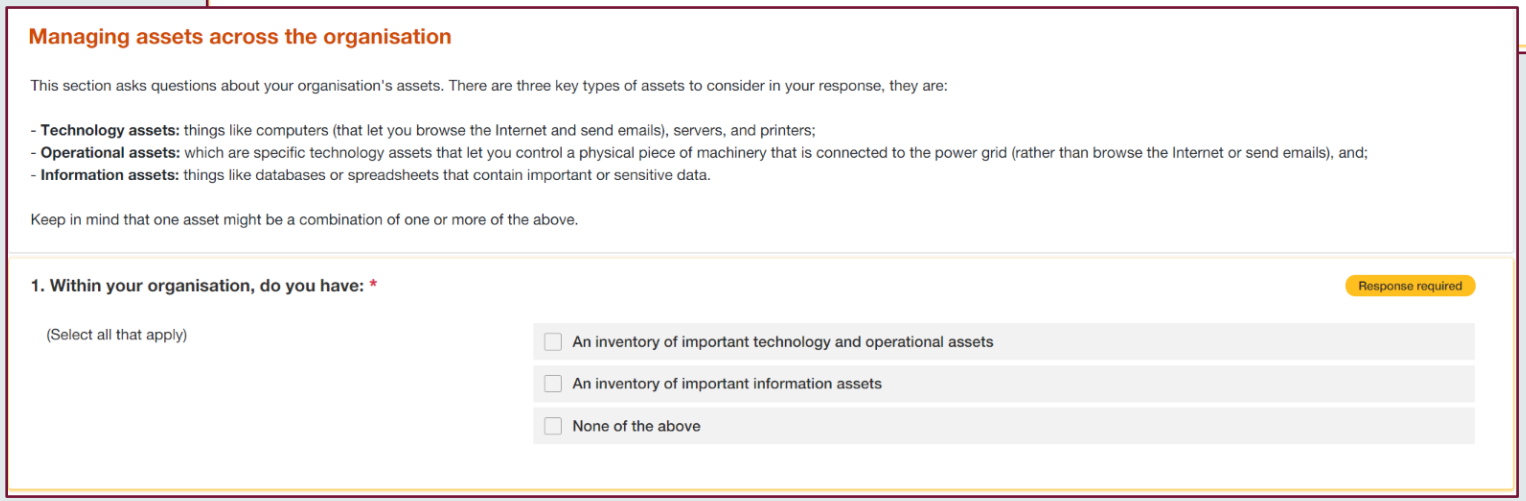
A **control** is a type of action that your organisation can take to **treat** a risk.

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

Response required

(Select all that apply)

- ☐ Identified
- ☐ Assessed according to your organisation's risk management strategy
- ☐ Documented
- ☐ Treated (mitigated, accepted, controlled, tolerated, or transferred)
- ☐ Managed with adequate resources (such as people, tools, and funding)
- ☐ None of the above



Managing assets across the organisation

This section asks questions about your organisation's assets. There are three key types of assets to consider in your response, they are:

- **Technology assets:** things like computers (that let you browse the Internet and send emails), servers, and printers;
- **Operational assets:** which are specific technology assets that let you control a physical piece of machinery that is connected to the power grid (rather than browse the Internet or send emails), and;
- **Information assets:** things like databases or spreadsheets that contain important or sensitive data.

Keep in mind that one asset might be a combination of one or more of the above.

1. Within your organisation, do you have: *

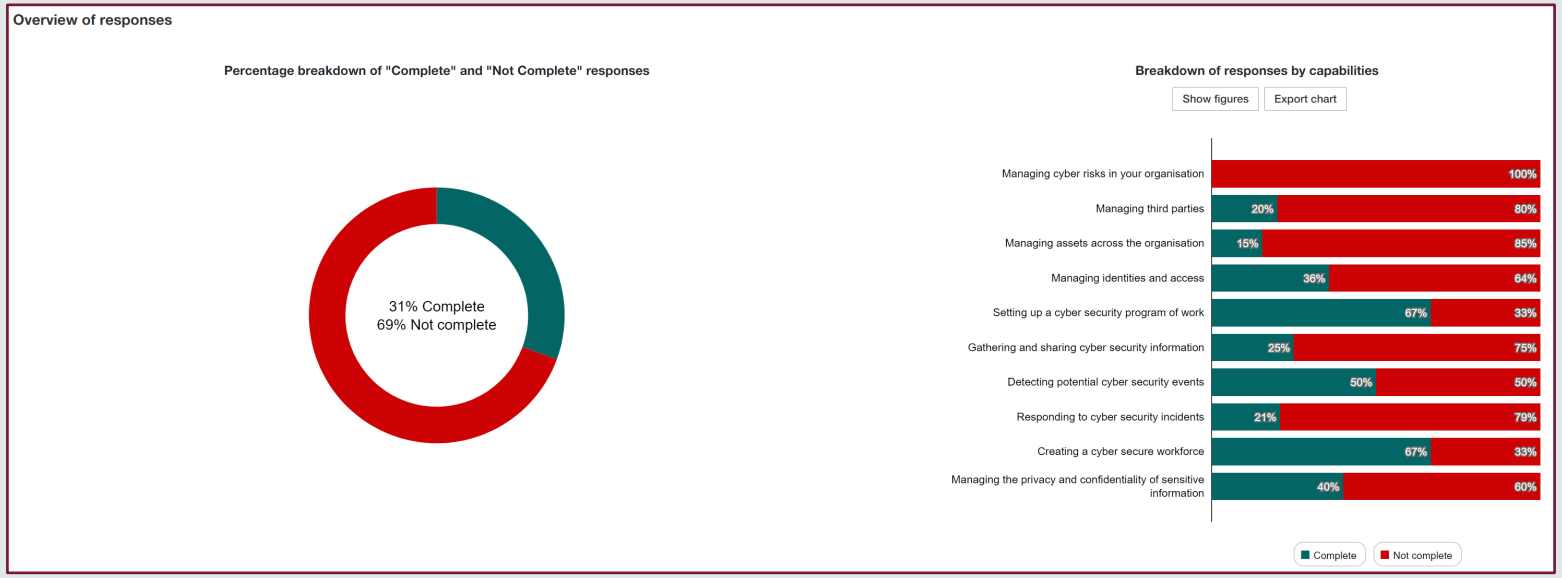
Response required

(Select all that apply)

- ☐ An inventory of important technology and operational assets
- ☐ An inventory of important information assets
- ☐ None of the above

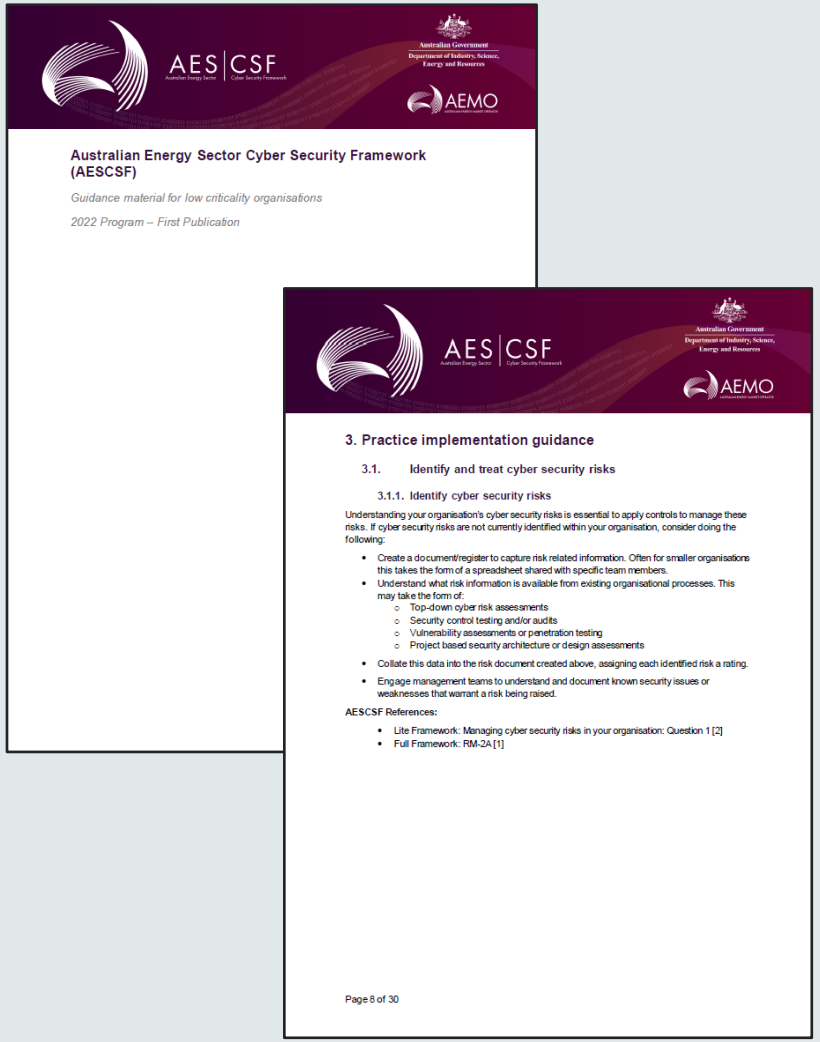
AESCSF Lite – Overview of results

- Instead of the 'Donuts' used in the full AESCSF assessment, a bar chart is used to visually depict the entity's maturity in comparison to AESCSF Security Profile 1.
- Topics covered by the Lite framework are listed on the left, with the associated ratio of 'Complete' responses on the right.
- 'Complete' response options correspond to the entity exhibiting desired cyber-security capabilities.



AESCSF Guidance for Low Criticality Organisations

- Based on feedback from prior AESCSF assessment programs, smaller organisations have 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 (see later in the Education Workshop Presentation) and have been selected based on being high-impact and foundational in nature to the organisations overall cyber security capability.



Australian Energy Sector Cyber Security Framework (AESCSF)

Guidance material for low criticality organisations

2022 Program – First Publication

3. Practice implementation guidance

3.1. Identify and treat cyber security risks

3.1.1. Identify cyber security risks

Understanding your organisation's cyber security risks is essential to apply controls to manage these risks. If cyber security risks are not currently identified within your organisation, consider doing the following:

- Create a document/register to capture risk related information. Often for smaller organisations this takes the form of a spreadsheet shared with specific team members.
- Understand what risk information is available from existing organisational processes. This may take the form of:
  - Top-down cyber risk assessments
  - Security control testing and/or audits
  - Vulnerability assessments or penetration testing
  - Project based security architecture or design assessments
- Collate this data into the risk document created above, assigning each identified risk a rating.
- Engage management teams to understand and document known security issues or weaknesses that warrant a risk being raised.

AESCSF References:

- Lite Framework: Managing cyber security risks in your organisation: Question 1 [2]
- Full Framework: RM-2A [1]

Page 8 of 30

AES CSF
Australian Energy Sector Cyber Security Framework

Security Profiles

AESCSF Security Profile 1

In 2019, the Australian Cyber Security Centre, in consultation with the AEMO and the AESCSF Working Group, defined three target state Security Profiles using Practices from the AESCSF. 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.
- **Security Profile 1 is the target state for organisations with an overall criticality rating of Low.** 74 Practices must be completed, along with 14 Anti-Patterns being 'Not Present' to achieve Security Profile 1 (88 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 10 of the 11 AESCSF domains have been included within Security Profile 1.
- Security Profile 1 contains 20 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).
- **Security Profile 1 is the Target State for some Generation and some Retail market participants depending on results of the E-CAT for each entity.**

Consultation to ratify if existing Target State guidance is applicable to the Gas and Liquid Fuels sub-sectors is ongoing.

MIL-2 and MIL-3 Practices and Anti-Patterns in Security Profile 1		
Domain	Practice ID	Anti-Pattern ID
ACM	3C	None
APM	1D	AP1
CPM	None	AP1, AP2
EDM	None	None
IAM	1F, 2F, 1G	AP4, AP5, AP9
IR	1D, 1E, 3E, 4J	AP1, AP2, AP3
ISC	1C	None
RM	1A, 2C, 2D	None
SA	1B, 2D, 3A	AP7, AP8
TVM	2G, 2H	None
WM	1D, 3D	None

Note: this SP relates to the electricity sector only, MIL-1 Practices are not shown in the above table
MIL-2 Practices shown in blue

AESCSF Security Profile 2

- **Security Profile 2 is the target state for organisations with an overall criticality rating of moderate.**
- 164 Practices and 36 Anti-Patterns must be completed to achieve Security Profile 2 (88 total within Security Profile 1 and 112 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 7 of the 11 AESCSF domains have been included within Security Profile 2.
- Security Profile 2 contains 5 Practices that have been identified by the ACSC as a priority for completion. These Practices should be considered when sequencing Practice remediation activities.
- **Security Profile 2 is the Target State for some DNSP, Generation, Independent Interconnectors and Retail market participants depending on results of the E-CAT for each entity.**

Consultation to ratify if existing Target State guidance is applicable to the Gas and Liquid Fuels sub-sectors is ongoing.

MIL-3 Practices and Anti-Patterns in Security Profile 2		
Domain	Practice ID	Anti-Pattern ID
ACM	1F, 3E	None
APM	1L	None
CPM	None	None
EDM	2L, 2M	None
IAM	2G, 2I	AP8, AP11
IR	3J, 3K, 3O	None
ISC	None	None
RM	None	None
SA	2G, 3D	AP11
TVM	None	None
WM	1E, 2H	AP1

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

AESCSF Security Profile 3

- **Security Profile 3 is the target state for organisations with an overall criticality rating of high.**
- All 240 Practices and 42 Anti-Patterns must be completed to achieve Security Profile 3 (88 total within Security Profile 1, 112 total within Security Profile 2, and 82 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 1 Practice that has been identified by the ACSC as a priority for completion. This Practice should be considered when sequencing Practice remediation activities.
- **Security Profile 3 is the Target state for Market Operators, some Independent Interconnections and TNSPs, and some DNSPs and Generators depending on results of the E-CAT for each entity.**

Consultation to ratify if existing Target State guidance is applicable to the Gas and Liquid Fuels sub-sectors is ongoing.

Breakdown of Security Profile 3		
Maturity Indicator Level (MIL)	Practices in Security Profile 3	% of MIL in Security Profile 3
MIL-1	0	0%
MIL-2	0	0%
MIL-3	76	82% (18% in SP-1 + SP-2)
Total	76	

Security Profile 3 is the target state for:			
Market Operator	*All*	Distribution	*Some*
Independent Interconnector	*Some*	Generation	*Some*
Transmission	*All*	Retail	*None*

Security Profile Summary

Summary of Practices and Anti-Patterns per Security Profile						
Security Profile	Market participant Criticality Target State	Practices introduced in this Security Profile	Anti-Patterns introduced in this Security Profile	Practices covered in prior Security Profiles	Anti-Patterns covered in prior Security Profiles	Total required to achieve Security Profile
SP-1	Low	74	14	0	0	88
SP-2	Moderate	90	22	74	14	200 (112+88 from SP1)
SP-3	High	76	6	164	36	282 (82+200 from SP2)

AES CSF
Australian Energy Sector Cyber Security Framework

AESCSF Priority Practices

AESCSF Priority Practices

The ACSC and AEMO have selected 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).

*MIL-2 Practices shown in blue.

AESCSF Priority Practices by Security Profile			
Domain	Profile 1	Profile 2	Profile 3
ACM	1A, 1B	1F	2D
APM	1B	None	None
CPM	2A, 2B	3B	None
EDM	1A, 2A	2L	None
IAM	1F, 2F	2I	None
IR	3C, 4A, 4B	None	None
ISC	1C	None	None
RM	2A, 2B	None	None
SA	1B	None	None
TVM	1C, 2G	2E	None
WM	2A, 2B	None	None
Total	20	5	1

AES | CSF
Australian Energy Sector | Cyber Security Framework

Assessment Outcomes & Next Steps

Benchmarking Assessment Results & Reporting

AES | CSF
Australian Energy Sector | Cyber Security Framework

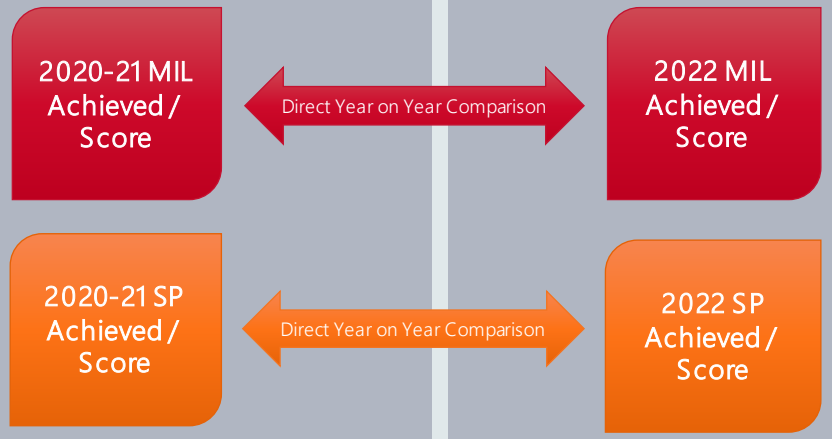
Australian Government
Department of Industry, Science, Energy and Resources

AEMO
AUSTRALIAN ENERGY MARKET OPERATOR

Year on Year Comparison

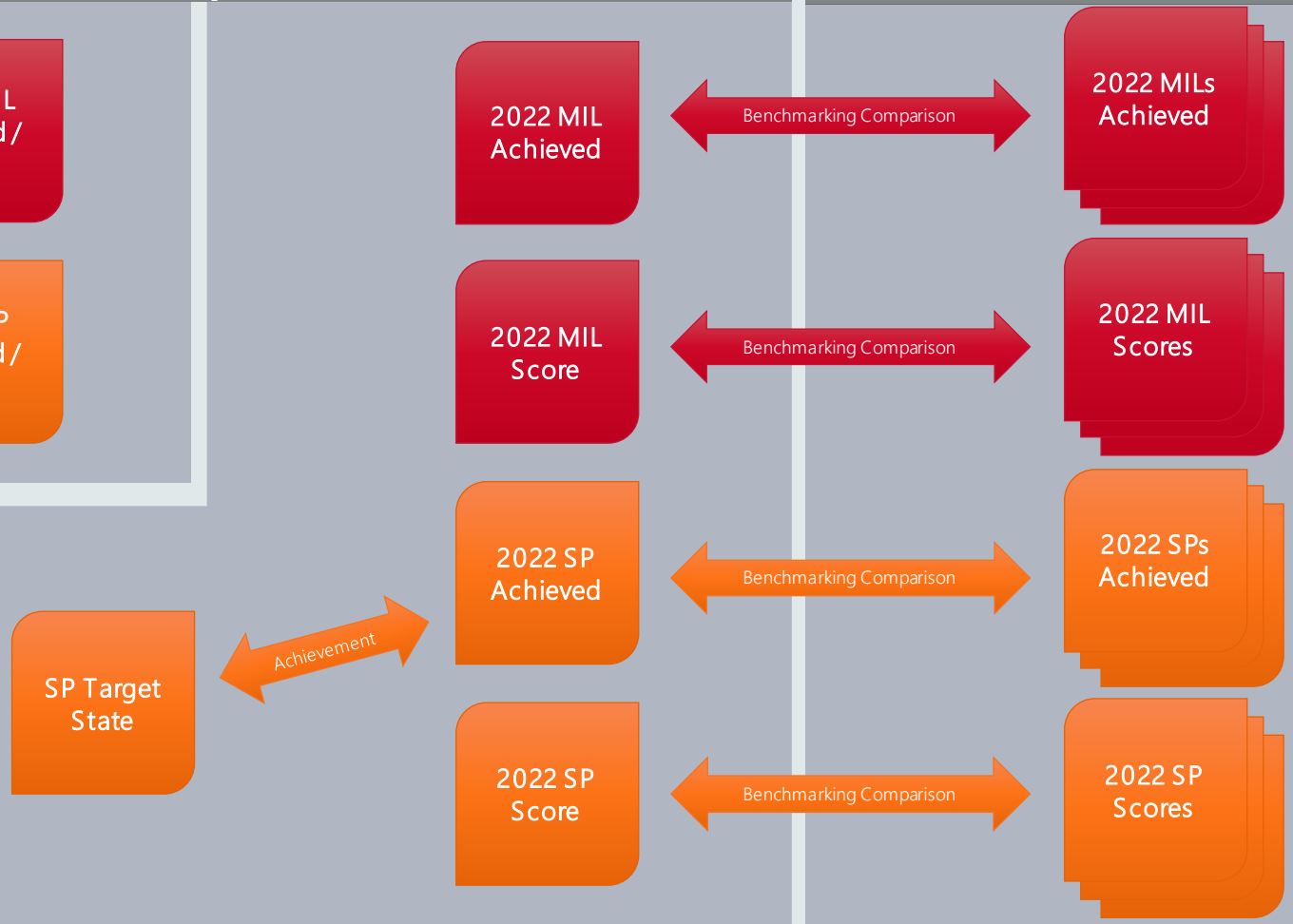
2020-21 Entity Assessment

2022 Entity Assessment



Sector Benchmarking

All 2022 Assessments



All entities who submit a 2022 self-assessment will have access to the AESCSF 2022 Benchmarking Portal. If entities consent to their 2020-21 assessment results being available, year on year comparison of results will be displayed. In addition, entities will see how they compare to deidentified industry benchmarks based on the population of 2022 assessments submitted.

AES | CSF
Australian Energy Sector | Cyber Security Framework

Next Steps & Support

The next steps for energy sector participants are:

1 Please complete your organisation's assessment – which was launched on **Monday 28th of March 2022.** The portal will remain open until the **30th of June 2022** to complete the self-assessment. For organisations wanting to commence their self-assessment prior to the portal opening, the 2022 Framework Core has been uploaded to AEMO's website and can be used to record your self-assessment in the interim, with results able to be copied into the portal once launched.

2 The specific closure date of the self-assessment portal will be **30th of June 2022**. Your submission will need to be accompanied by your CEO's attestation response letter for full AESCSF assessments. The CEO's attestation response letter template can be downloaded from the Online Toolkit and will need to be completed and signed before uploading as part of your submission.

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

Alternatively, you can call us on **1800 982 125**
*If you require assistance with the AESCSF Toolkit, please **press 1***
*If you have a question about the AESCSF, including clarifications on how to complete your organisation's self-assessment, please **press 2***

AES | CSF
Australian Energy Sector | Cyber Security Framework

AESCSF Timeline for Engagement and Assessment Completion

AESCSF 2022 Timeline

The project will deliver the '2022 Annual Report into the cyber security preparedness of the Australian energy sector' for the Australian Energy Ministers Meeting by end of calendar year 2022.

The key milestones to achieve this outcome are:

March 2022

- Launch email sent to 2022 AESCSF program participants.
- Self-assessment data collection portal opened 28 March 2022

April – June 2022

- Education workshops held via videoconference.
- New training and educational material published on AEMO website.
- Self-assessment results submitted (alongside management attestation).
- Self-assessment period closed.

July – September 2022

- Data collation, aggregation and analysis completed.
- Self-assessment benchmarking portal opened (to participants who completed a self-assessment).
- 2022 Report into the Cyber Security Preparedness of the Australian Energy Sector submitted to Energy Ministers.