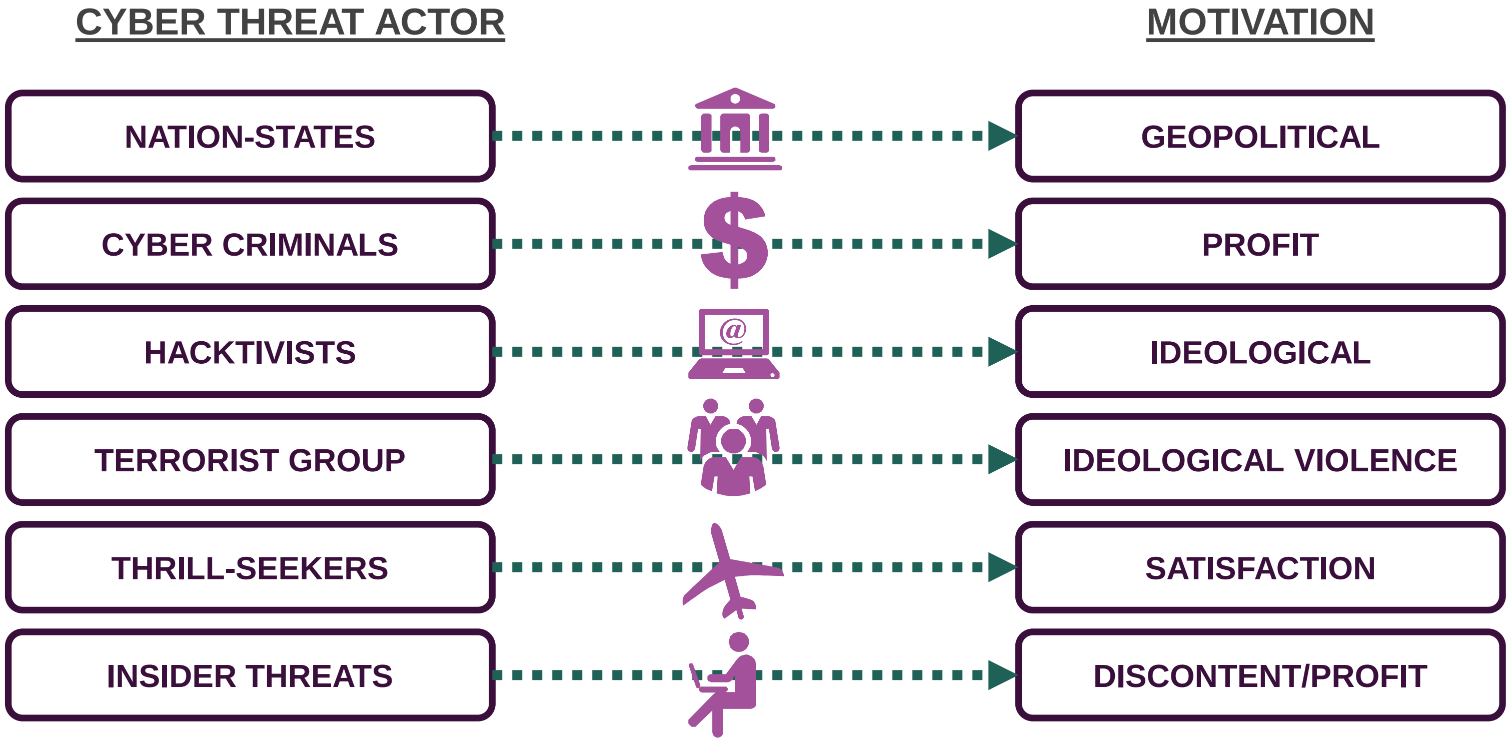
Australia Energy Sector Cyber Security Framework Education Workshop

AEMO
AUSTRALIAN ENERGY MARKET OPERATOR

2023

Background

Background - cyber threat actors and motivations*



CYBER THREAT ACTOR	MOTIVATION
NATION-STATES	GEOPOLITICAL
CYBER CRIMINALS	PROFIT
HACKTIVISTS	IDEOLOGICAL
TERRORIST GROUP	IDEOLOGICAL VIOLENCE
THRILL-SEEKERS	SATISFACTION
INSIDER THREATS	DISCONTENT/PROFIT

Latitude – March 2023

- The Australian personal loan and financial service provider, was affected by a data breach that impacted over **14 million** people from Australia and New Zealand.
- Initial disclosure stated that only 328,000 individual customers were affected, that number quickly grew after further investigation.
- The attack occurred when one set of employee credentials was stolen

Energy One – August 2023

- This wholesale energy software provider revealed certain corporate systems were affected by a cyber-attack
- Whilst the company investigated, it disabled some of the links between its corporate systems and customer-facing systems.
- This supply chain issue impacted energy providers in Australia and the United Kingdom

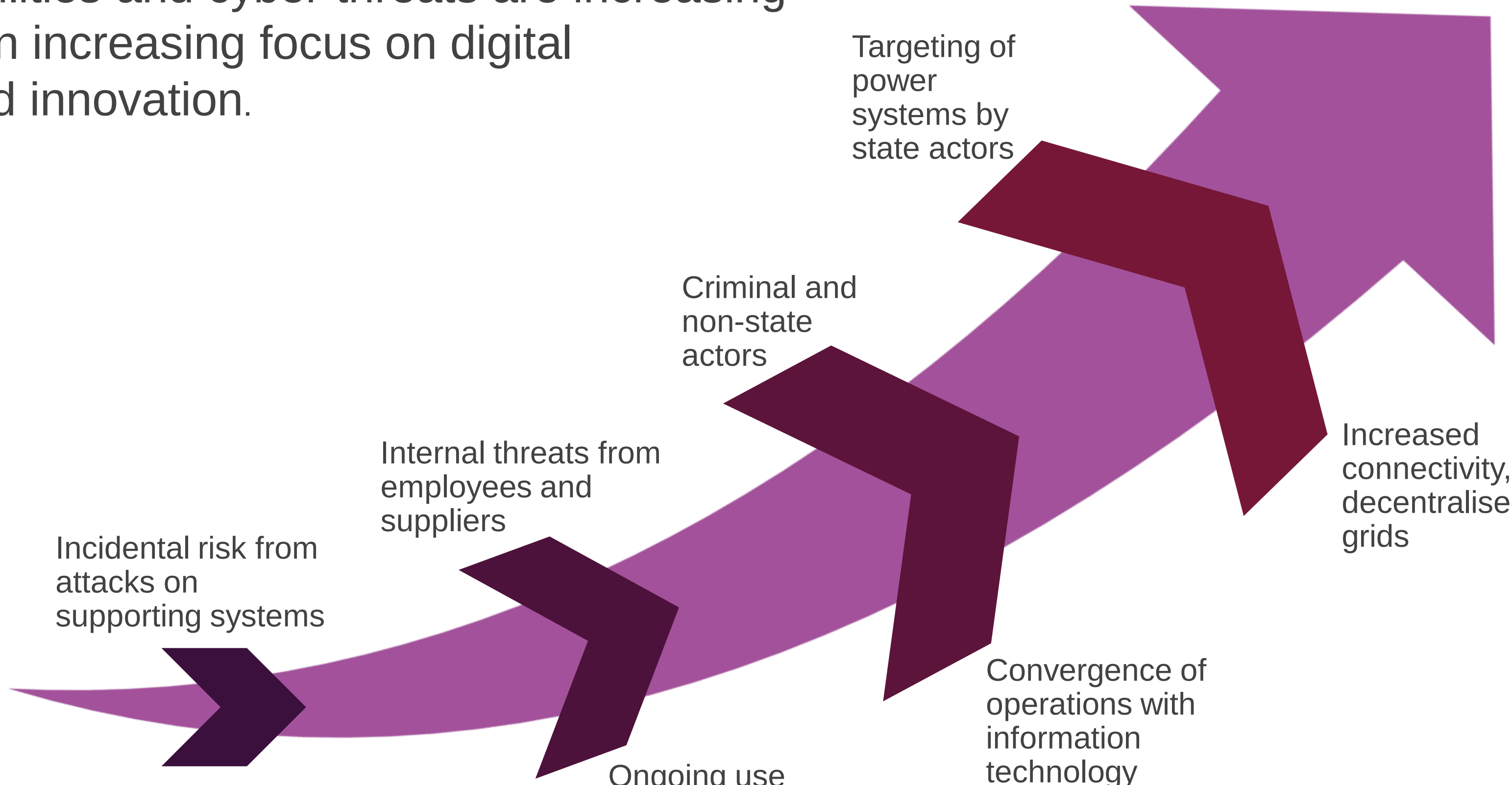
Optus – September 2022

- This Telco had one of the **biggest security breaches** in Australian history.
- State-sponsored cyber criminals are believed to have breached Optus' internal network, compromising personal information and impacting up to **9.8 million** customers, almost 40% of the population.
- It's likely access was gained through an unauthorized API endpoint

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

The cyber security problem

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



Incidental risk from attacks on supporting systems

Digitisation of energy businesses

Internal threats from employees and suppliers

Ongoing use of legacy infrastructure

Criminal and non-state actors

Convergence of operations with information technology

Targeting of power systems by state actors

Increased connectivity, decentralised grids

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 28/03/2023

Unpatched systems continue to be a target.

- Malicious cyber actors exploiting older software vulnerabilities more frequently than recently disclosed vulnerabilities and targeted unpatched, internet-facing systems.

Australian Critical Infrastructure under threat with vulnerabilities exposed in Citrix.

- Successful exploitation attempts against Australian critical infrastructure organisations
- Multiple vulnerabilities in Citrix NetScaler ADC and NetScaler Gateway that may be in use on Australian networks.

Australia faces 'dystopian' future of cyber-attacks targeting fabric of society
Home Affairs Minister, Clare O'Neil (04/04/2023)

https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/serious-vulnerabilities-in-atlassian-products-including-confluence-jira-and-bitbucket
https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/citrix-products-netscaler-adc-and-netscaler-gateway-zero-day-vulnerability
https://minister.homeaffairs.gov.au/ClareONeil/Pages/world-leading-protection-australias-critical-infrastructure.aspx

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 and compliance with SoCI
- 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.

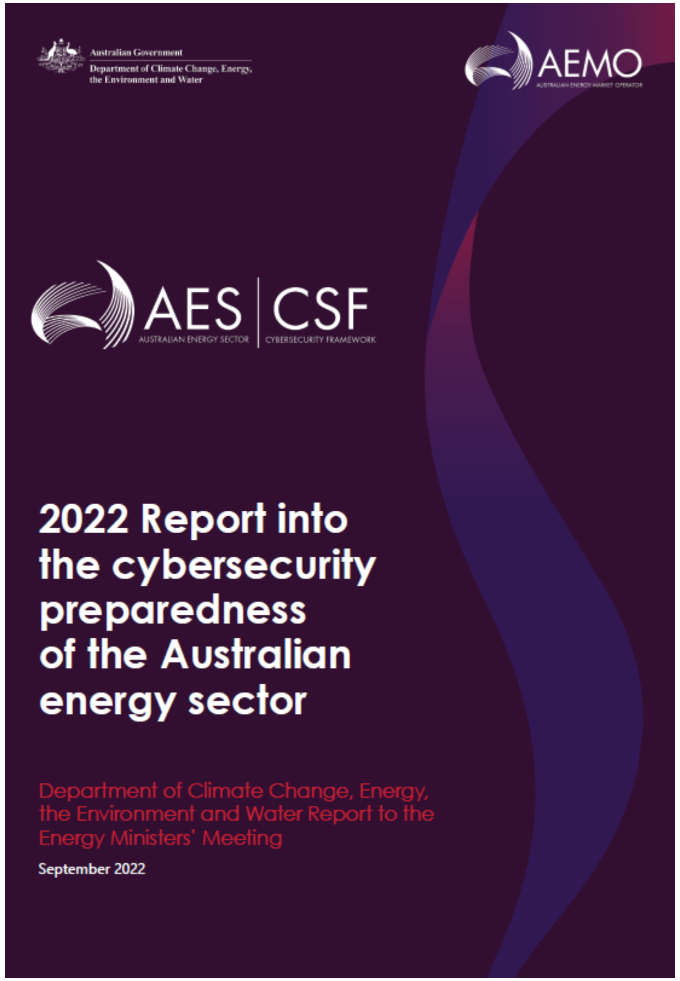
With the 2023 AESCSF being led by AEMO, the drivers for continued uplift are:

- 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.

Outcomes

- The AESCSF is a voluntary cyber security Assessment Framework for Australia's energy sector.
- Australia's energy market participants use the AESCSF Program to assess, benchmark and use the results to inform cyber security maturity uplift programs of work, investment and regulatory compliance.
- 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.

2023 AESCSF Market Coverage			
Electricity (NEM & WEM)	Electricity (Other markets)	Gas	Liquid fuels
✓	✓	✓	✓



Australian Government
Department of Climate Change, Energy, the Environment and Water

AEMO
AUSTRALIAN ENERGY MARKET OPERATOR

AES | CSF
AUSTRALIAN ENERGY SECTOR | CYBERSECURITY FRAMEWORK

2022 Report into the cybersecurity preparedness of the Australian energy sector

Department of Climate Change, Energy, the Environment and Water Report to the Energy Ministers' Meeting

September 2022

Introduction to the AESCSF

Guiding principles of the AESCSF

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.

Designed to evolve with the threat landscape and provide insights into new mitigation strategies.

Tailored to the Australian Energy Sector

Tailored for the Australian energy sector and aligning 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^, ISO 27001, COBIT 5 ISA & NIST SP 800.

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

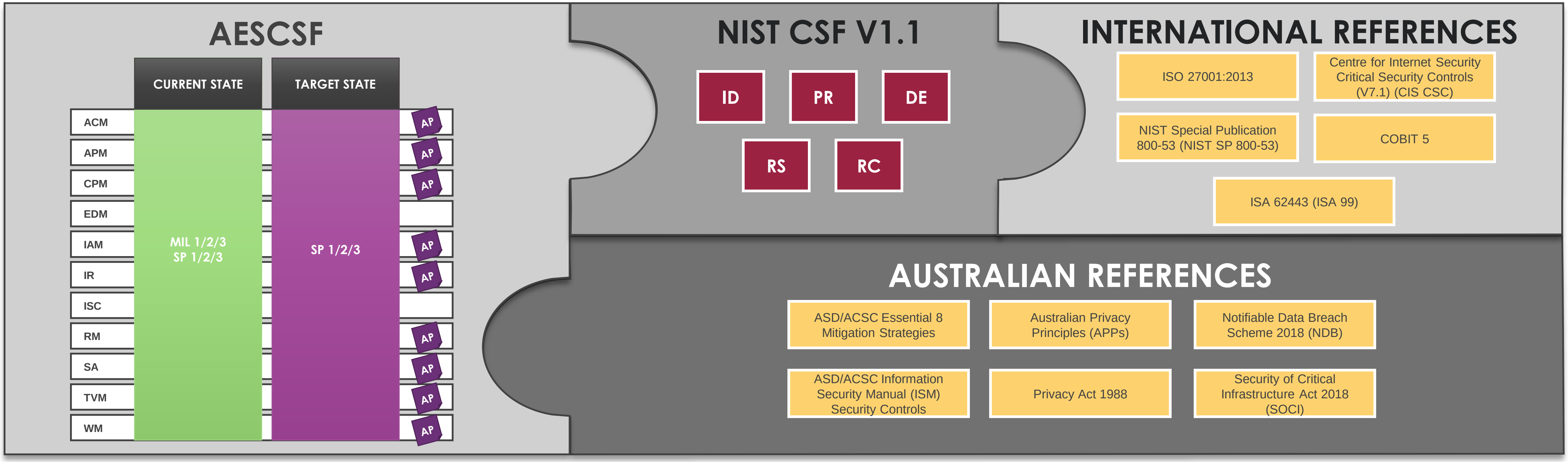
Framework elements

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 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.

Overview of the AESCSF v1

The AESCSF was developed by the AESCSF Working Group (led by AEMO), energy market participants, the States & Territories and the Federal 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.


AESCSF
CURRENT STATE
TARGET STATE
ACM
APM
CPM
EDM
IAM
IR
ISC
RM
SA
TVM
WM
MIL 1/2/3
SP 1/2/3
SP 1/2/3
AP
NIST CSF V1.1
ID
PR
DE
RS
RC
INTERNATIONAL REFERENCES
ISO 27001:2013
Centre for Internet Security Critical Security Controls (V7.1) (CIS CSC)
NIST Special Publication 800-53 (NIST SP 800-53)
COBIT 5
ISA 62443 (ISA 99)
AUSTRALIAN REFERENCES
ASD/ACSC Essential 8 Mitigation Strategies
Australian Privacy Principles (APPs)
Notifiable Data Breach Scheme 2018 (NDB)
ASD/ACSC Information Security Manual (ISM) Security Controls
Privacy Act 1988
Security of Critical Infrastructure Act 2018 (SOCI)

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

AESCSF Version 2

Updates to 2023 AESCSF Framework

In consultation with industry and governments, AEMO, the ACSC, the Australian Government and industry partners, via a cross sector working group, updated the AESCSF in 2022. Updates align with current international standards and address emerging technologies and the evolving cyber threat landscape - Version 2 (v2) of the AESCSF is now available and is a more comprehensive version of the framework.

- It leverages recognised industry frameworks such as the revised US Department of Energy's Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) and the National Institute of Standards and Technology Cyber Security Framework (NIST CSF) and references global best-practice control standards (e.g. ISO/IEC 27001, NIST SP 800-53, COBIT, etc.)
- It is compatible with new SoCI Act obligations requiring responsible entities of one or more critical infrastructure assets to adopt, comply with, and maintain a critical infrastructure risk management program (CIRMP)
- Revisions to two-thirds of model practices including substantive changes and clarifications along with additions, deletions, and combining of practices (A net total of an additional 72 practices)
- Addition of a Cybersecurity Architecture domain focused on planning, designing, and managing the cyber security control environment
- Refresh of the dependencies domain, now called the Third-Party Risk Management domain, to ensure the model effectively addresses third-party IT and OT cyber security risks, like sensitive data in the cloud and vendors with privileged access, as well as build supply chain security into organisational culture
- Integration of Information Sharing domain activities into the Threat and Vulnerability Management, and Situational Awareness domains

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

- **The AESCSF Overview** - Companion document providing information about the AESCSF and 2023 Assessment Program. Included is a list of frequently asked questions (FAQ) about the AESCSF and assessments.
- **AESCSF v1 – v2 Change Log**

Guidance

- **AESCSF 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 Educational Webinar** - This webinar is designed to assist organisations to understand the AESCSF and the KPMG ConfirmIT Platform
- **ConfirmIT Platform Client User Guide v1** – This document is to assist organisations in using the online platform to complete the AESCSF assessment
- **Glossary –** A document containing key terms used in the AESCSF to provide consistent understanding and clarity.
- **AESCSF Guidance for Low Criticality Organisations** – A guide for smaller organisations getting started on their cyber security uplift journey.

Assessment

- **Criticality Assessment Tool -** Questionnaire used to assess each market participant against a set of predefined criteria to determine their relative criticality to the sector.
- **2023 AESCSF Assessment** - Portal with two modules: (1) ‘Collect’ module used to collect and store Assessment data. (2) ‘Explore’ module to view results against a de-identified AESCSF data set for benchmarking and Year-on-Year analysis.
- **2023 AESCSF Offline Toolkit–** An offline toolkit based in Microsoft Excel that can be used for scenario modelling. Includes both Criticality Assessment Tool and Full Assessment.

Criticality Assessment

Criticality assessment

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.

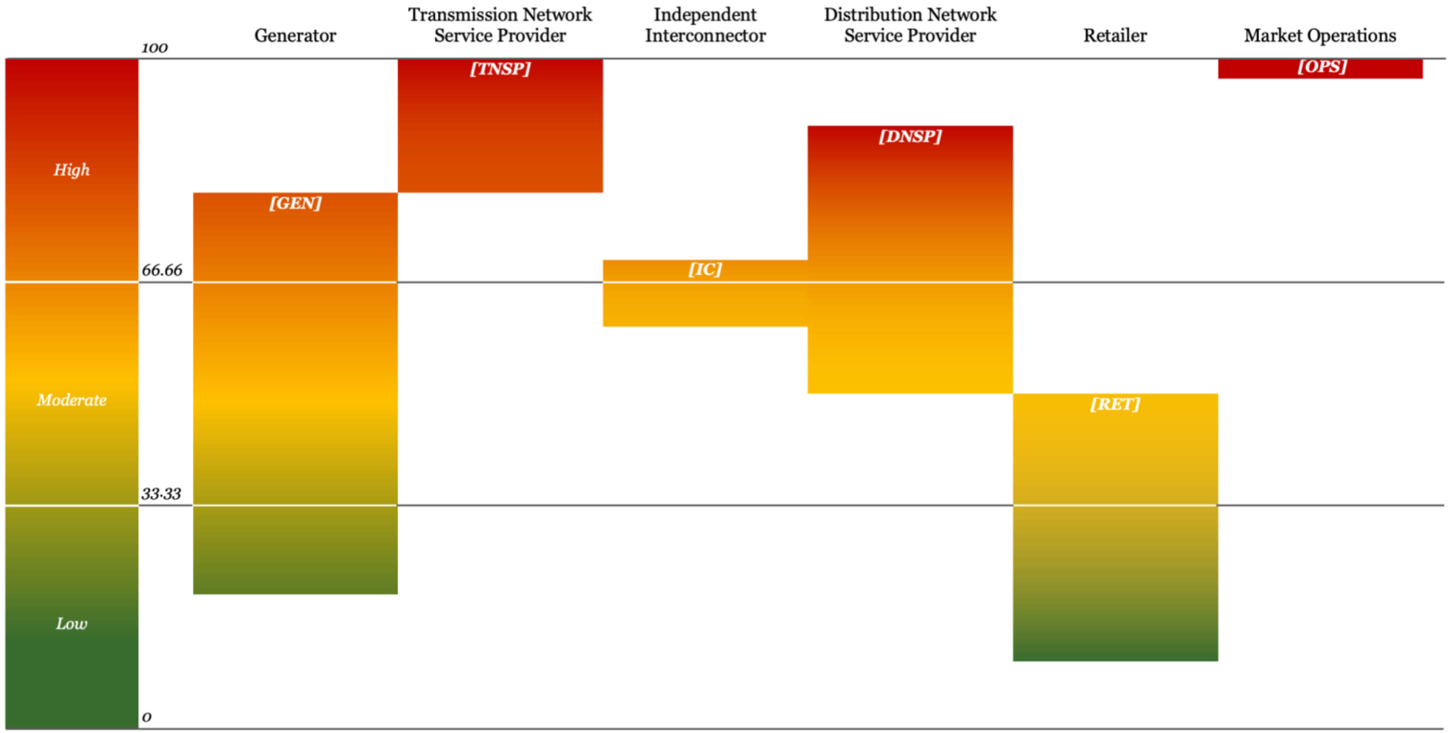
The assessment is **not intended as a comprehensive risk assessment** for each participant – it will not consider likelihood and mitigating controls, but rather **inherent risk of an entity to end user supply** and maximum potential impact (relative to other entities).

Criticality Scale

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

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

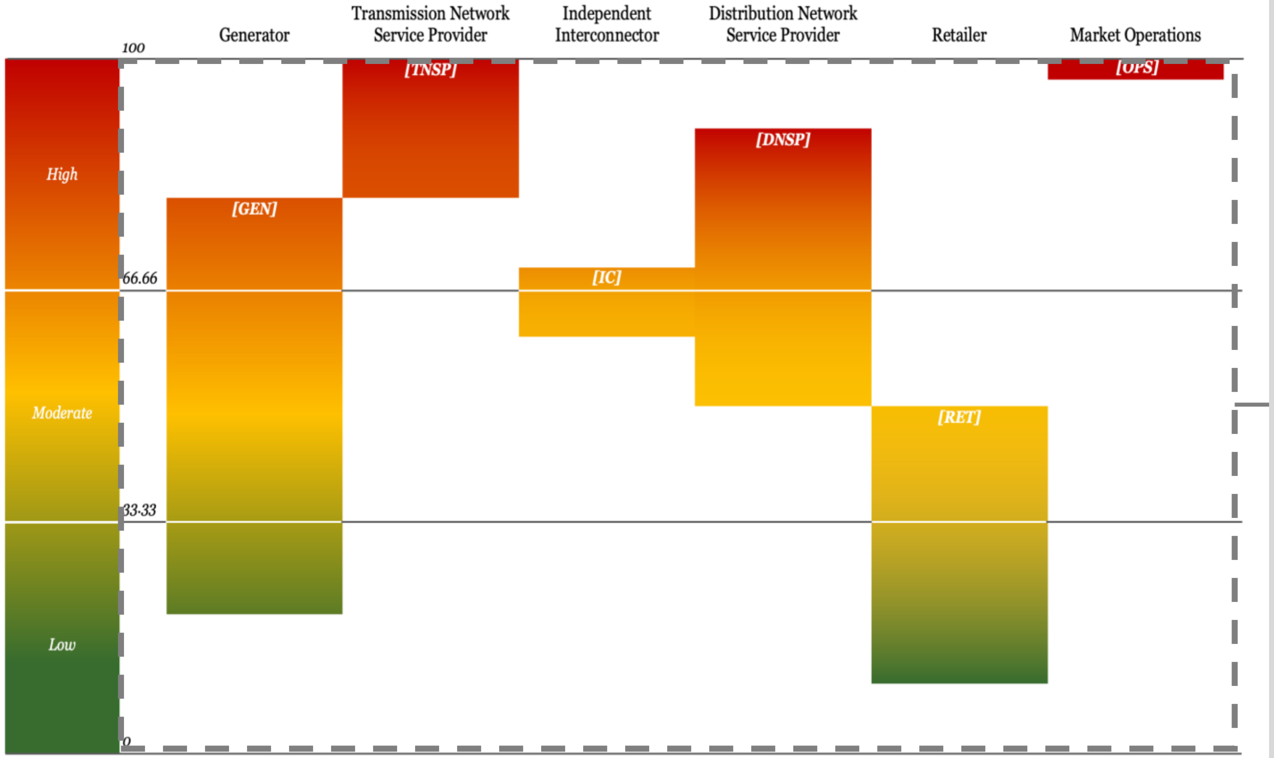
Criticality Assessment Tools (CATs) provide *Key Criticality Indicators* for each market sub-sector have been established to stratify participating entities within the sub-sector criticality bands (CATs apply to both version 1 and version 2 of the AESCSF).



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

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

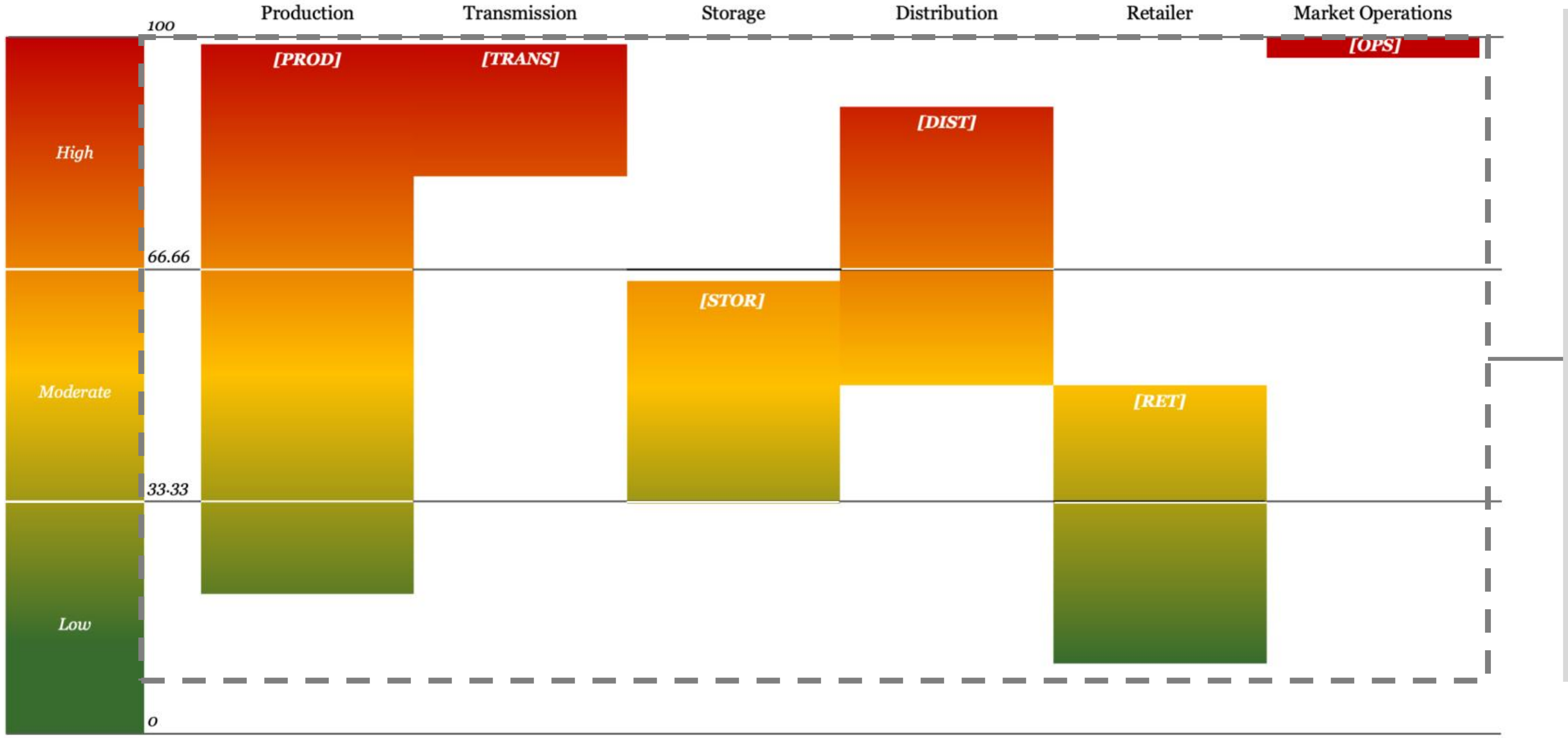
- Number of customers (National Metering Identifiers)
- Connection to Advanced Metering Infrastructure
- Critical and commercial numbers
- Virtual Power Plants
- Retailer of Last Resort
- Sole Retailer for a region

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

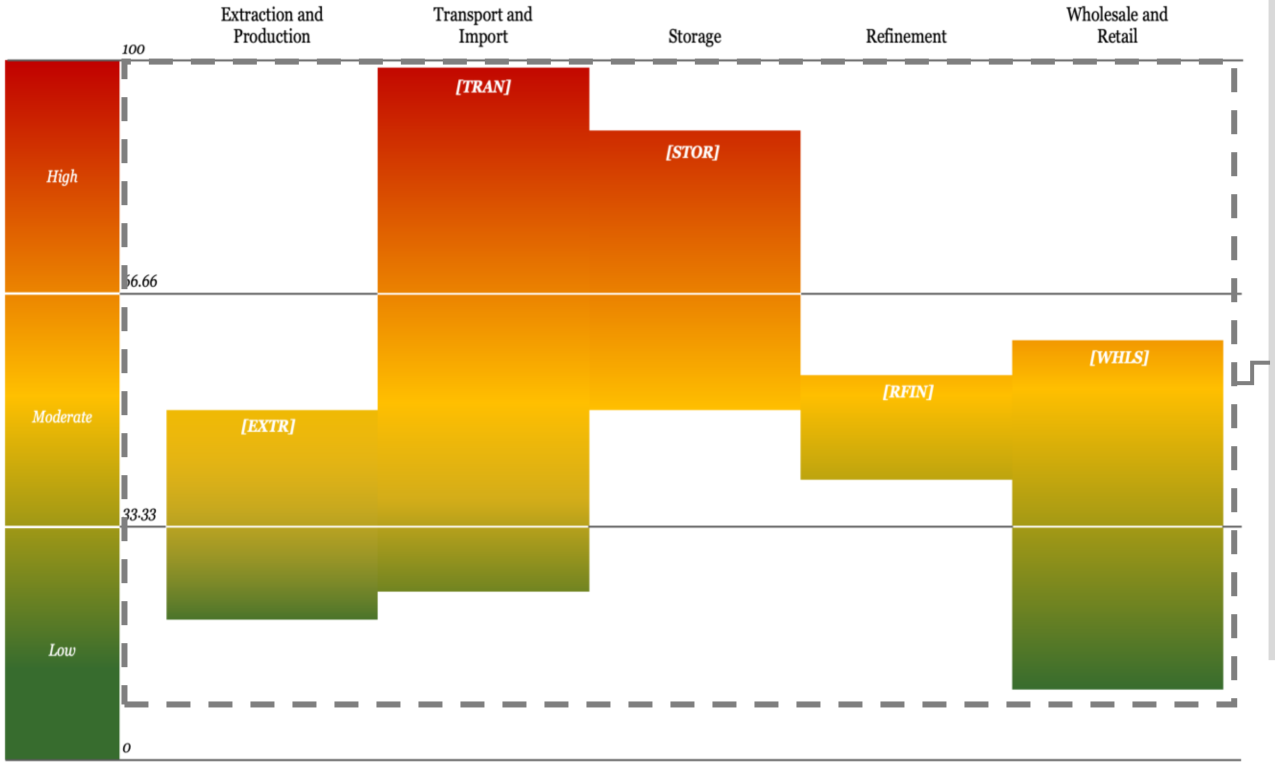
- Number of customers (National Metering Identifiers)
- Number of Critical and Commercial entities

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

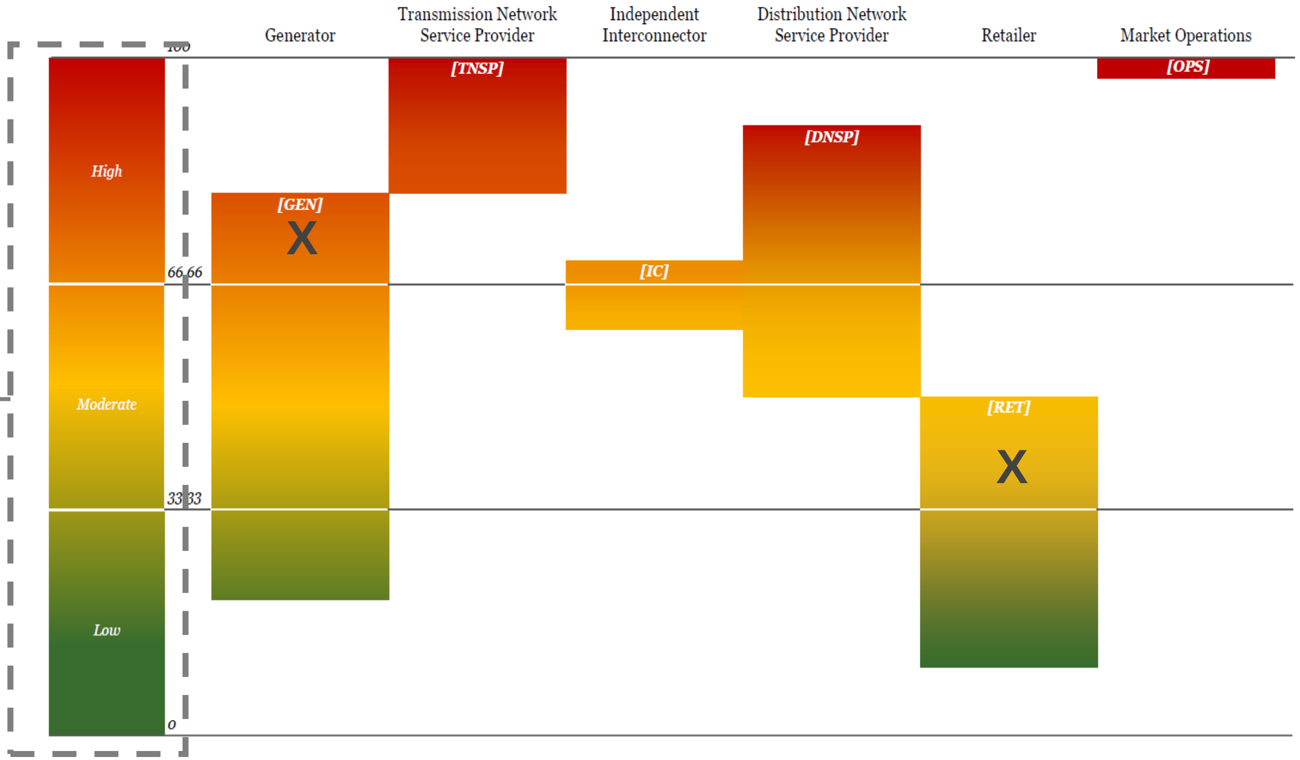
The Criticality Scale score of each entity will determine their cyber-security capability maturity target state.

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.

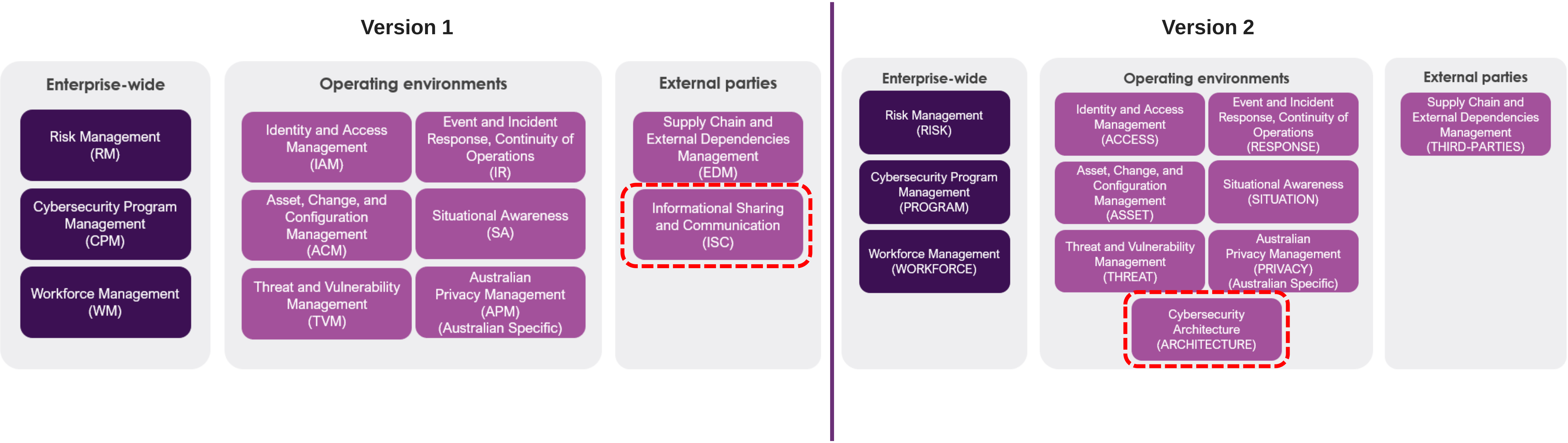
Framework structure

Domains (v1 and v2)

The framework comprises 11 domains, ten from the underlying United States Department of Energy Cyber Security Capability Maturity Model (C2M2) and one added Australian Privacy domain. Each domain has at least one objective.

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

Note: from version 1 to version 2 of the framework, Information Sharing & Communication (ISC) was integrated into Threat and Vulnerability Management, and Situational Awareness domains. Also, Cybersecurity Architecture has been added as a new domain



Version 1

Enterprise-wide
- Risk Management (RM)
- Cybersecurity Program Management (CPM)
- Workforce Management (WM)

Operating environments
- Identity and Access Management (IAM)
- Event and Incident Response, Continuity of Operations (IR)
- Asset, Change, and Configuration Management (ACM)
- Situational Awareness (SA)
- Threat and Vulnerability Management (TVM)
- Australian Privacy Management (APM) (Australian Specific)

External parties
- Supply Chain and External Dependencies Management (EDM)
- Informational Sharing and Communication (ISC)

Version 2

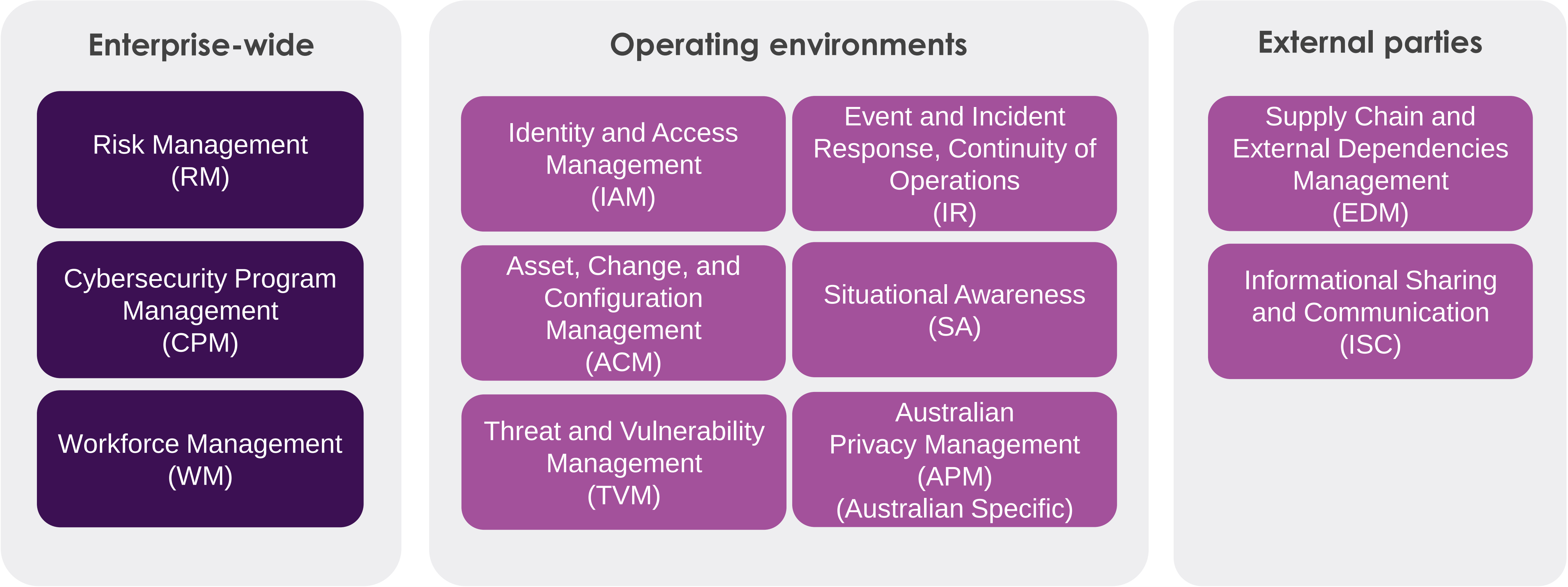
Enterprise-wide
- Risk Management (RISK)
- Cybersecurity Program Management (PROGRAM)
- Workforce Management (WORKFORCE)

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 (PRIVACY) (Australian Specific)
- Cybersecurity Architecture (ARCHITECTURE)

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

AESCSF v1 domains

11 domains: 10 C2M2 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.



Enterprise-wide

Risk Management (RM)

Cybersecurity Program Management (CPM)

Workforce Management (WM)

Operating environments

Identity and Access Management (IAM)

Event and Incident Response, Continuity of Operations (IR)

Asset, Change, and Configuration Management (ACM)

Situational Awareness (SA)

Threat and Vulnerability Management (TVM)

Australian Privacy Management (APM) (Australian Specific)

External parties

Supply Chain and External Dependencies Management (EDM)

Informational Sharing and Communication (ISC)

AESCSF v2 domains

11 domains: 10 C2M2 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.

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 (PRIVACY) (Australian Specific)
- Cybersecurity Architecture (ARCHITECTURE)

External parties

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

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 (v1)

PRIVACY (v2)

- 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.

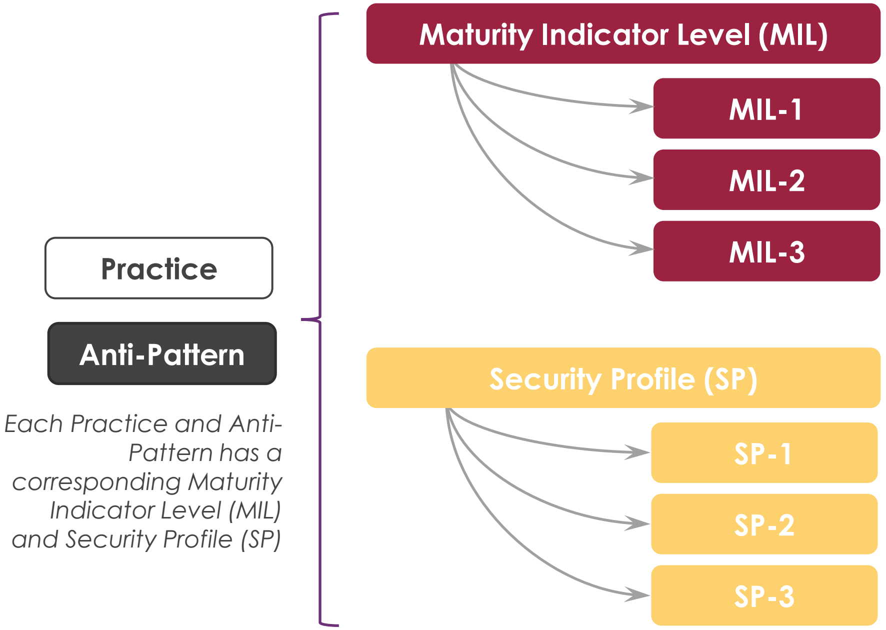
- *AEMO and the project team do not act as an authority on privacy law compliance to participants at any stage of the AESCSF.*

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

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



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

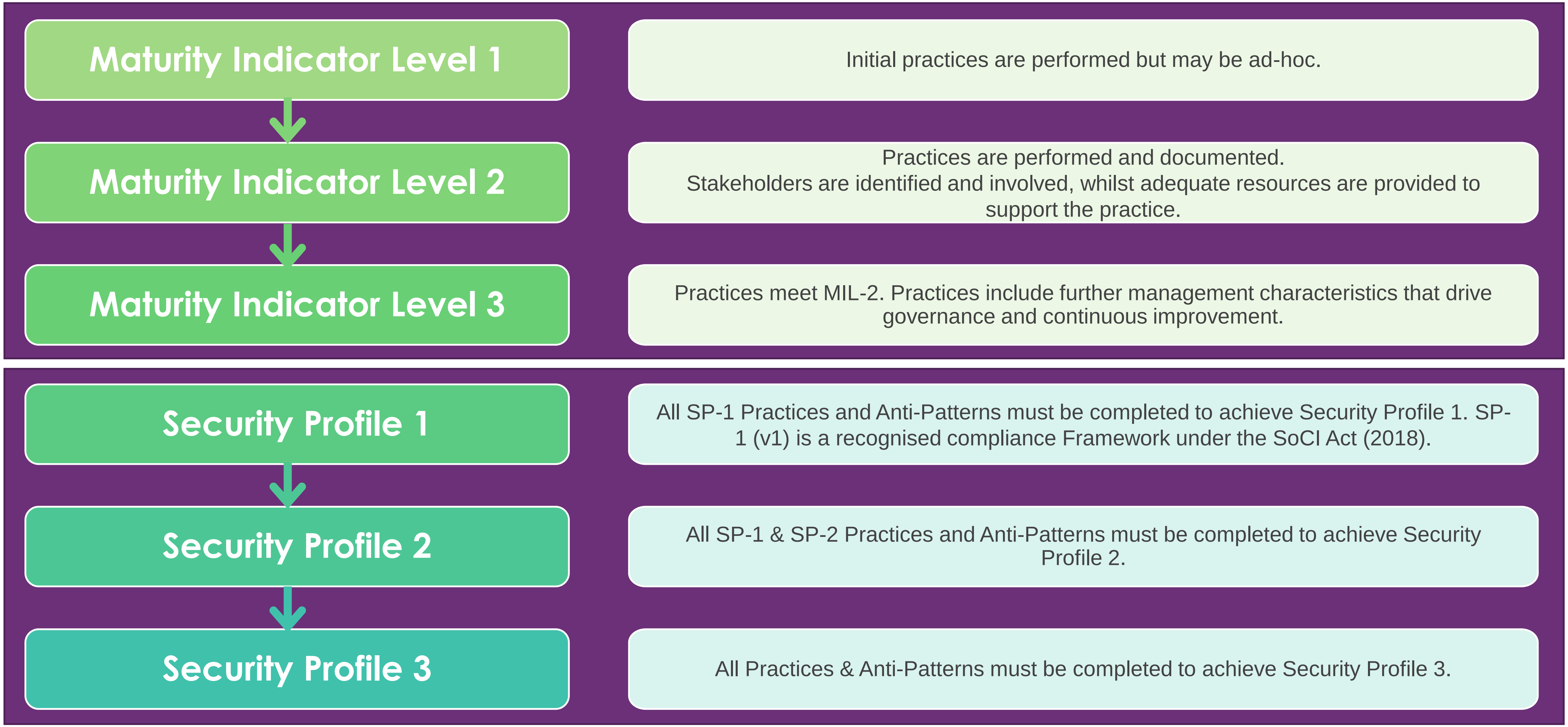
Maturity Indicator Levels:
Each Practice and Anti-Pattern has been assigned a MIL (MIL-1, MIL-2 or MIL-3) that indicates its maturity relative to other Practices. Each MIL has specific characteristics which impact assessment for Practices (See later slides on scoring model).

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).

Key aspects of MILs and SPs

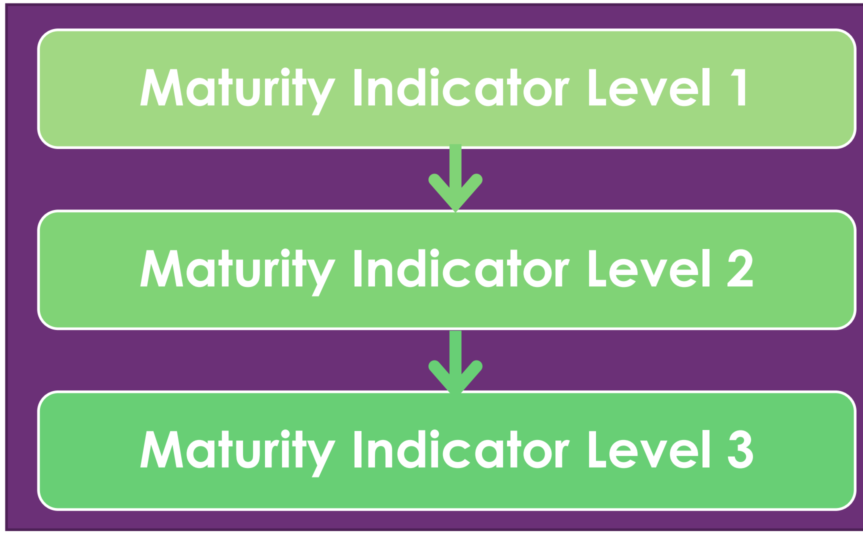
1. MILs apply independently to each domain. As a result, entities may be operating at different MIL ratings for different Domains.
2. SPs apply collectively across all Domains. As a result, entities only achieve a SP if they have completed all Practices in the SP across all Domains.
3. The MILs and SPs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

Maturity levels and security profiles



Maturity Indicator Level 1	Initial practices are performed but may be ad-hoc.
Maturity Indicator Level 2	Practices are performed and documented. Stakeholders are identified and involved, whilst adequate resources are provided to support the practice.
Maturity Indicator Level 3	Practices meet MIL-2. Practices include further management characteristics that drive governance and continuous improvement.
Security Profile 1	All SP-1 Practices and Anti-Patterns must be completed to achieve Security Profile 1. SP-1 (v1) is a recognised compliance Framework under the SoCI Act (2018).
Security Profile 2	All SP-1 & SP-2 Practices and Anti-Patterns must be completed to achieve Security Profile 2.
Security Profile 3	All Practices & Anti-Patterns must be completed to achieve Security Profile 3.

Maturity levels and security profiles - application



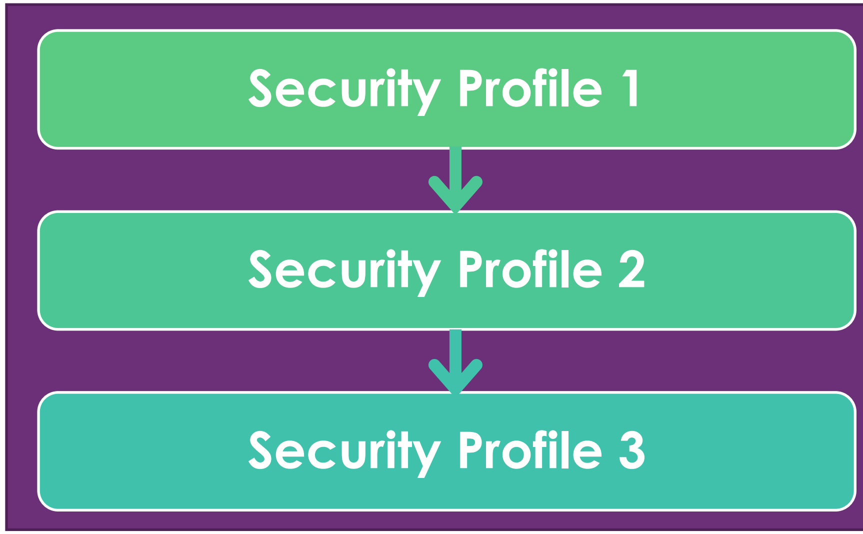
Maturity Indicator Level 1

Maturity Indicator Level 2

Maturity Indicator Level 3

Maturity Indicator Levels (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.
- Apply independently to each domain i.e. entities may have different MILs for different domains.
- An organisation's overall MIL reflects the lowest MIL obtained in any domain.



Security Profile 1

Security Profile 2

Security Profile 3

Security Profiles (SPs)

- Apply to each Practice.
- Entities only achieve an SP level if they have in place all practices for that SP level for all domains.

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
- Anti-patterns relate to specific objectives and apply to 9 of 11 domains

Priority practices

The Australian Cyber Security Centre and AEMO have selected practices within each SP that should be completed as a priority as key practices for cyber security best practice. The tables below provide further detail on the practices for both version 1 and 2 of the AESCSF. When prioritising practices, those listed in Security Profile 1 (SP1) should be completed prior to any in SP2 or SP3.

Version 1

Domain (v1)	SP1	SP2	SP3
ACM	1A, 1B	1F	2D
APM	1B		
CPM	2A, 2B	3B	
EDM	1A, 2A	2L	
IAM	1F, 2F	2I	
IR	3C, 4A, 4B		
ISC	1C		
RM	2A, 2B		
SA	1B		
TVM	1C, 2G	2E	
WM	2A, 2B		
Total	**20**	**5**	**1**

Version 2

Domain (v2)	SP1	SP2	SP3
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	
ACCESS	ACCESS-1B ACCESS-1F ACCESS-2G ACCESS-3H	ACCESS-2I ACCESS-3J	
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**

Changes to the framework

(Summary of Practices and Anti-Patterns per Security Profile: version 1 to version 2)

Version 1					
Security Profile	**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	74	14	0	0	88
SP-2	90	22	74	14	200 (112+88 from SP1)
SP-3	76	6	164	36	282 (82+200 from SP2)

Version 2					
Security Profile	**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	109	14	0	0	123
SP-2	130	22	109	14	275 (152+123 from SP1)
SP-3	73	6	275	36	354 (79+275 from SP2)

AESCSF Full Assessment Scoring Model

Key features of the assessment scoring model

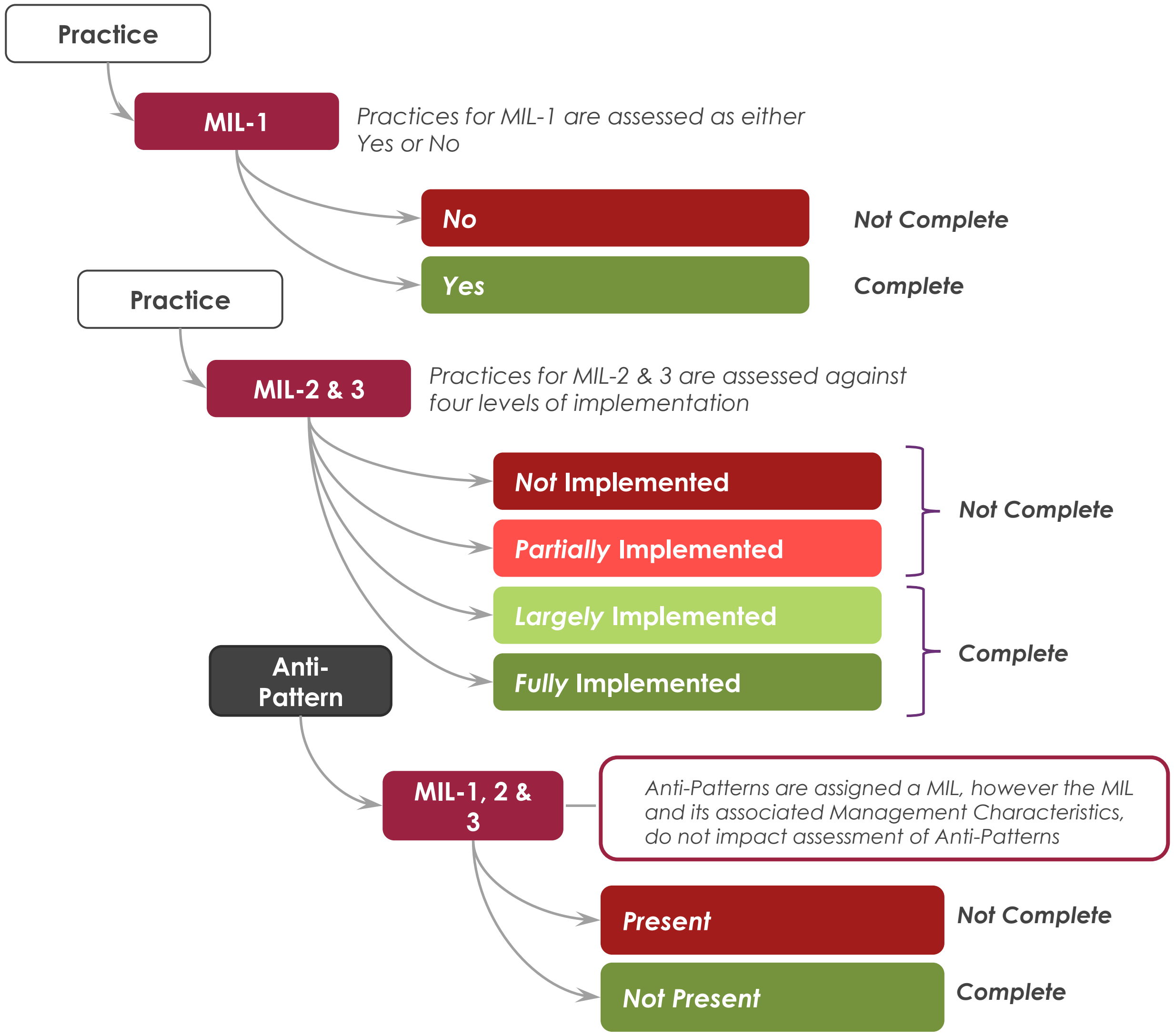
The AESCSF uses a revised version of the C2M2 scoring model to drive consistency and clarity.

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.



Practice

MIL-1

Practices for MIL-1 are assessed as either Yes or No

No — ***Not Complete***

Yes — ***Complete***

Practice

MIL-2 & 3

Practices for MIL-2 & 3 are assessed against four levels of implementation

***Not* Implemented**

***Partially* Implemented**

***Largely* Implemented**

***Fully* Implemented**

Not Complete

Complete

Anti-Pattern

MIL-1, 2 & 3

Anti-Patterns are assigned a MIL, however the MIL and its associated Management Characteristics, do not impact assessment of Anti-Patterns

Present — ***Not Complete***

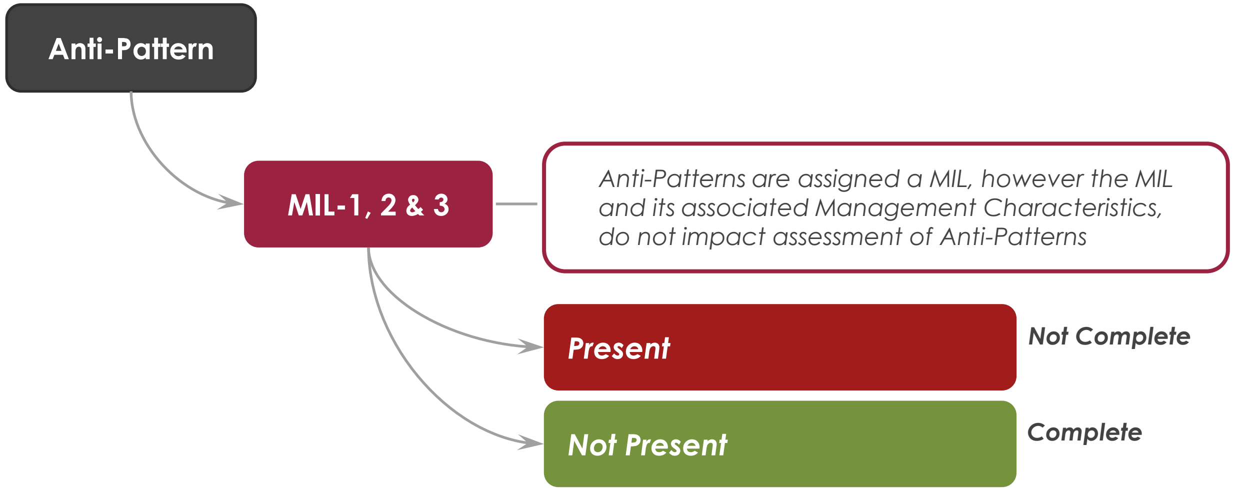
Not Present — ***Complete***

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.



Anti-Patterns are assigned a MIL, however the MIL and its associated Management Characteristics, do not impact assessment of Anti-Patterns

Assessing implementation of practices and Anti-Patterns

MIL-1 Practice

Practices performed at **MIL-1**		Implementation Response
	*The Practice is **NOT** performed*	**No**
	*The Practice **IS** performed* *Note: For MIL-1 this can be ad-hoc, and may therefore vary in frequency, accuracy, and completeness, based on the skills and tools of the personnel completing the activities*	**Yes**

MIL-2 Practice

Practices performed at **MIL-2**				Implementation Response
	*The Practice **IS NOT** performed*			***Not***
	*The Practice **IS** performed*			***Partially***
	Management Characteristics	**1**	*The Practice is **documented***	
		2	***Stakeholders** of the Practice are identified and involved*	***Largely***
		3	*Adequate **resources** are provided to support the Practice (people, funding, and tools)*	
		4	***Standards** and/or guidelines have been identified to guide the implementation of the Practice*	***Fully***

MIL-3 Practice

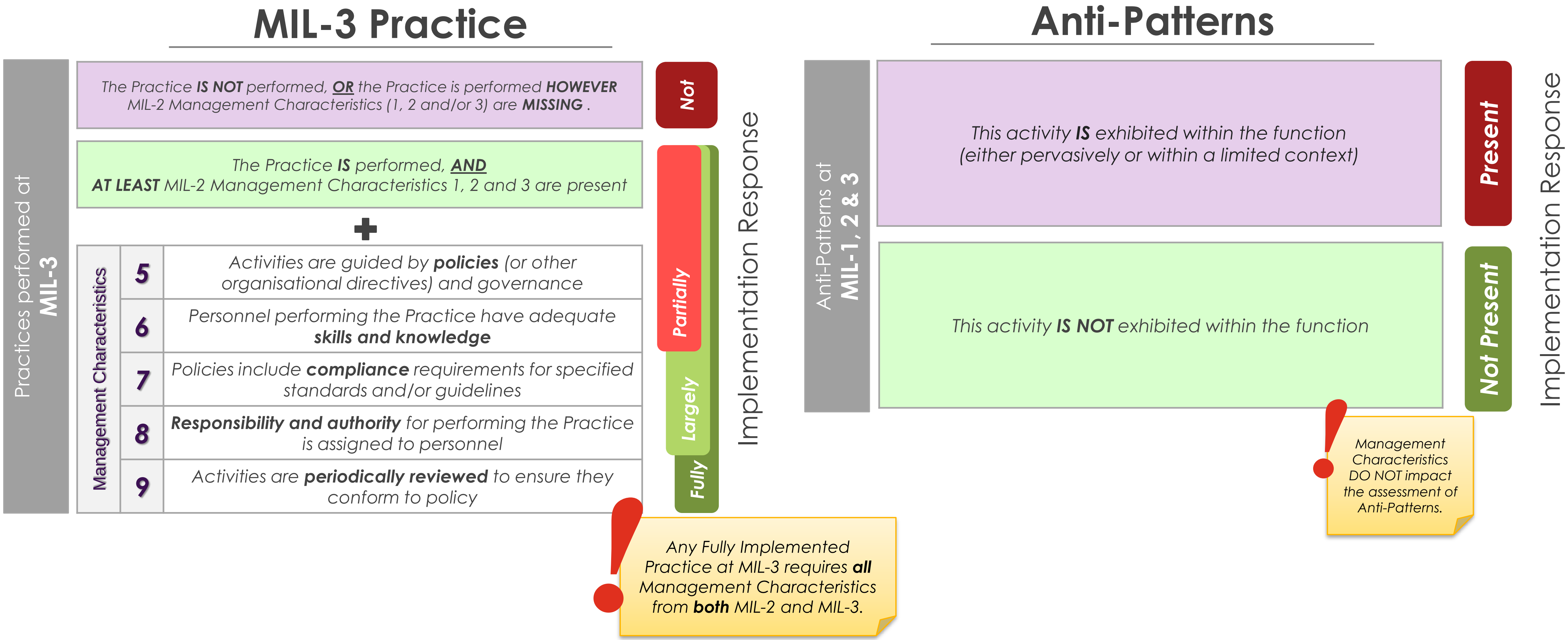
Practices performed at **MIL-3**				Implementation Response
	*The Practice **IS NOT** performed, **OR** the Practice is performed **HOWEVER** MIL-2 Management Characteristics (1, 2 and/or 3) are **MISSING** .*			***Not***
	*The Practice **IS** performed, **AND*** ***AT LEAST** MIL-2 Management Characteristics 1, 2 and 3 are present*			***Partially***
	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*	***Largely***
		8	***Responsibility and authority** for performing the Practice is assigned to personnel*	
		9	*Activities are **periodically reviewed** to ensure they conform to policy*	***Fully***

Anti-Patterns

Anti-Patterns at **MIL-1, 2 & 3**		Implementation Response
	*This activity **IS** exhibited within the function (either pervasively or within a limited context)*	***Present***
	*This activity **IS NOT** exhibited within the function*	***Not Present***

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

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*

Not

Partially

Largely

Fully

Implementation Response

*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)*

Present

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

Not Present

Implementation Response

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

Assessment outcomes against MILs

Characteristics	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
MIIL 1	No										
	Yes	✓									
MIL 2	Partially Implemented	✓	✓								
	Largely Implemented	✓	✓	✓	✓						
	Fully Implemented	✓	✓	✓	✓	✓					
MIL 3	Partially Implemented	✓	✓	✓	✓	✓	✓	✓			
	Largely Implemented	✓	✓	✓	✓	✓	✓	✓	✓	✓	
	Fully Implemented	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

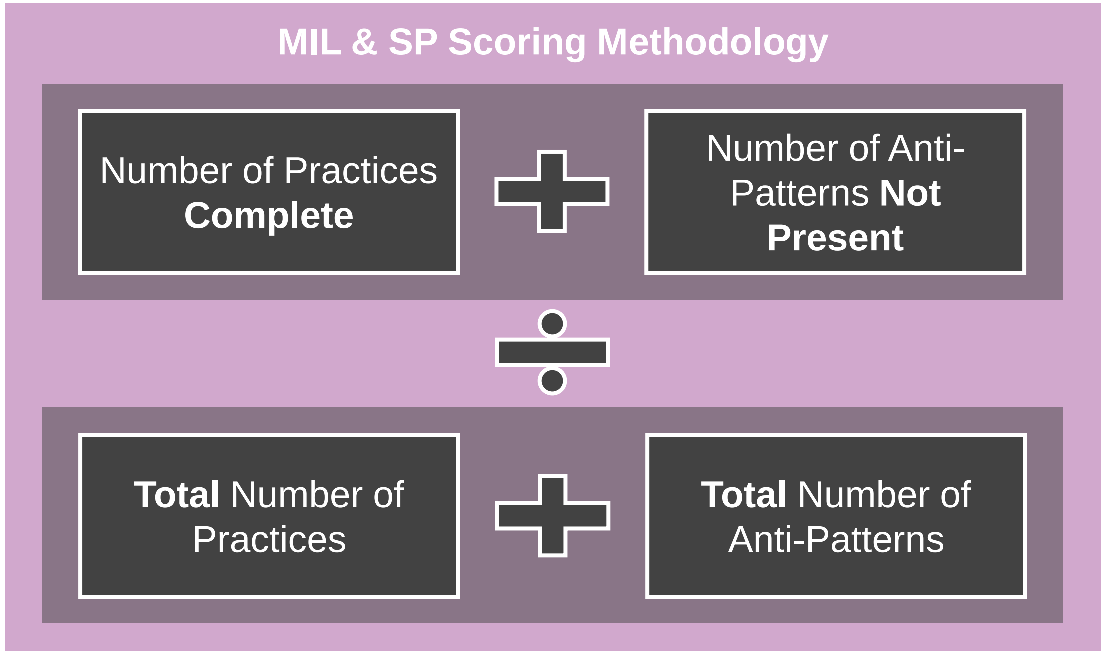
Assessment scoring methods

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.



MIL & SP Scoring Methodology

Number of Practices **Complete** + Number of Anti-Patterns **Not Present**

÷

Total Number of Practices + **Total** Number of Anti-Patterns

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.

Assessment scoring model – Worked example 1

AESCSF Practice:

ACM-2A (MIL-1): “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

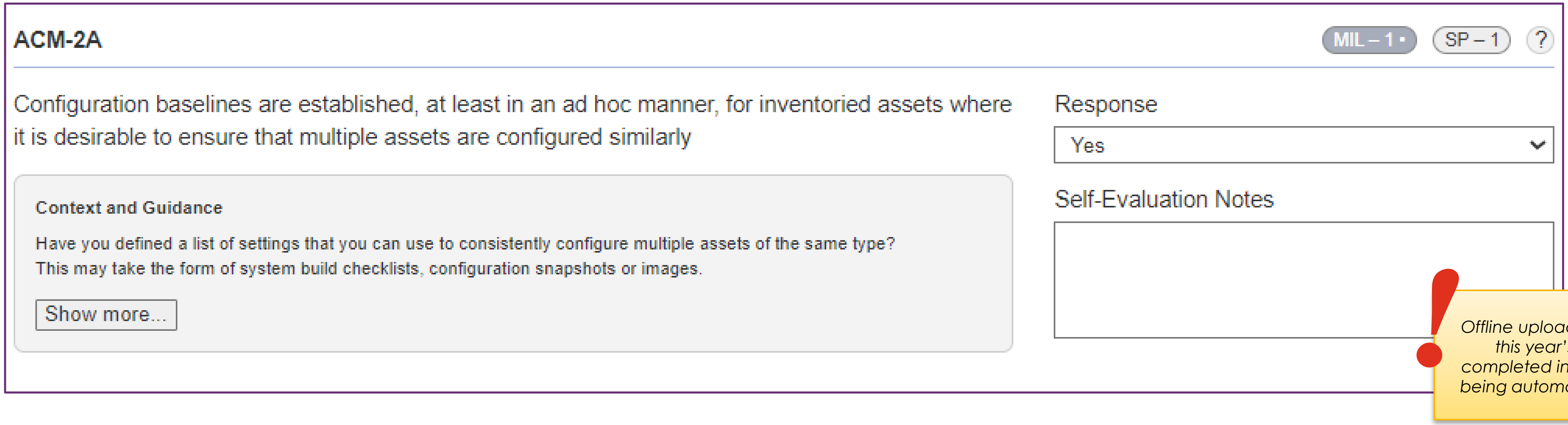
Assessment Scenario:

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, at least in an ad hoc manner, 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.**



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

Response: Yes

Self-Evaluation Notes:

Context and 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.

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

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 cyber security 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

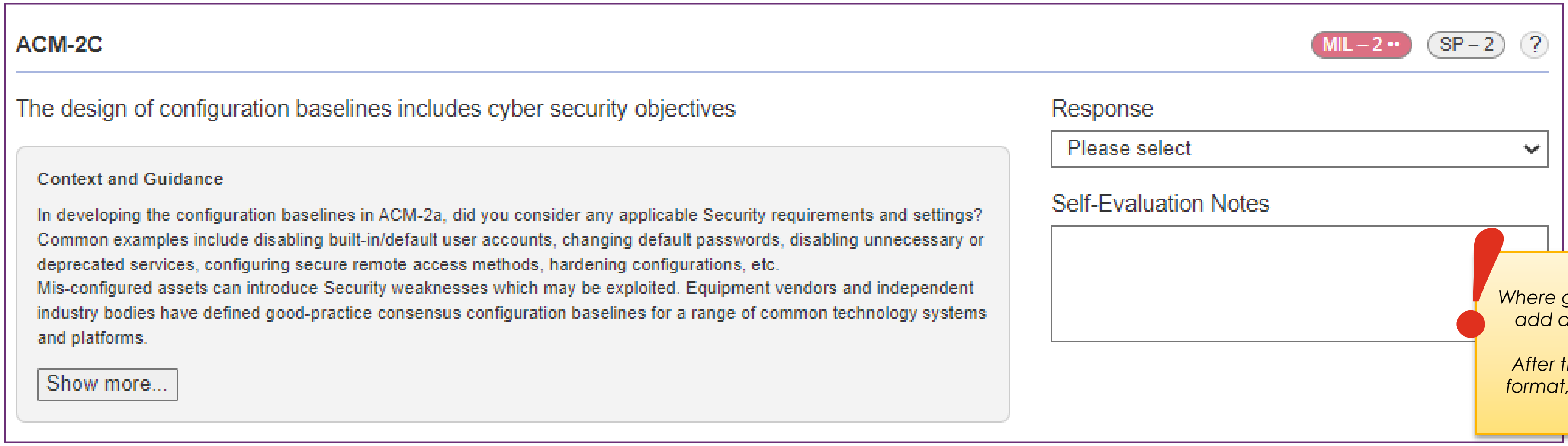
AESCSF Practice: ACM-2C (MIL-2): “The design of configuration baselines includes Cyber Security objectives”.

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 cyber security 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).**



The design of configuration baselines includes cyber security objectives

Context and Guidance

In developing the configuration baselines in ACM-2a, did you consider any applicable Security requirements and settings? Common examples include disabling built-in/default user accounts, changing default passwords, disabling unnecessary or deprecated services, configuring secure remote access methods, hardening configurations, etc.
Mis-configured assets can introduce Security weaknesses which may be exploited. Equipment vendors and independent industry bodies have defined good-practice consensus configuration baselines for a range of common technology systems and platforms.

Response: Please select

Self-Evaluation Notes

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 pdf format, and filtering can be performed to extract a list of all known gaps against the AESCSF.

Assessment scoring model – Worked example 1

AESCSF Practice:

ACM-2E (MIL-3): “Configuration baselines are reviewed and updated at an organisationally-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.

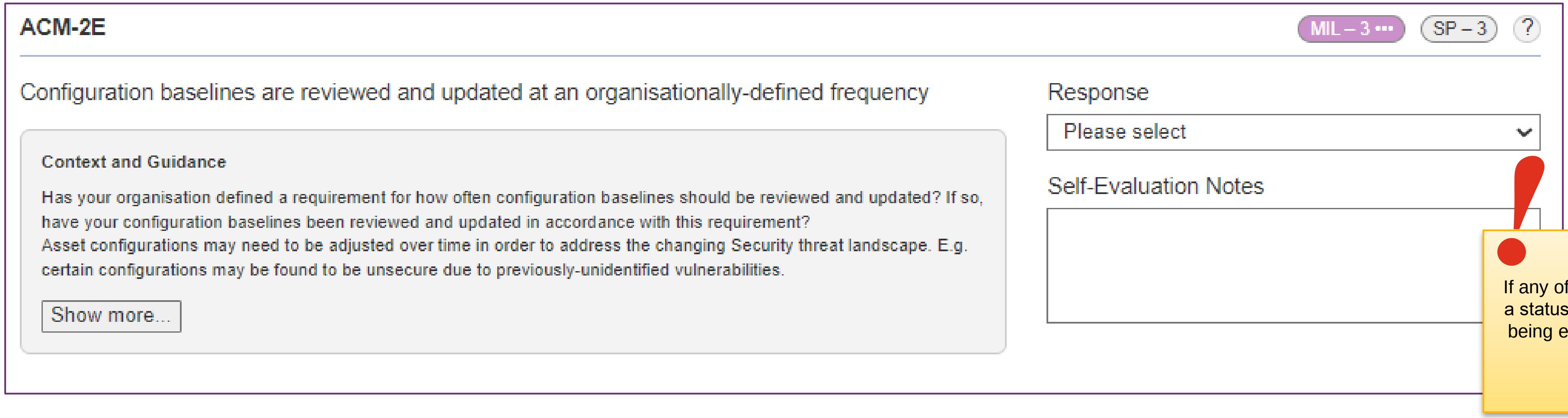
Assessment scoring model – Worked example 1

AESCSF Practice: ACM-2E (MIL-3): “Configuration baselines are reviewed and updated at an organisationally-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).**



ACM-2E

Configuration baselines are reviewed and updated at an organisationally-defined frequency

Context and Guidance

Has your organisation defined a requirement for how often configuration baselines should be reviewed and updated? If so, have your configuration baselines been reviewed and updated in accordance with this requirement?
Asset configurations may need to be adjusted over time in order to address the changing Security threat landscape. E.g. certain configurations may be found to be unsecure due to previously-unidentified vulnerabilities.

Response

Please select

Self-Evaluation Notes

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.

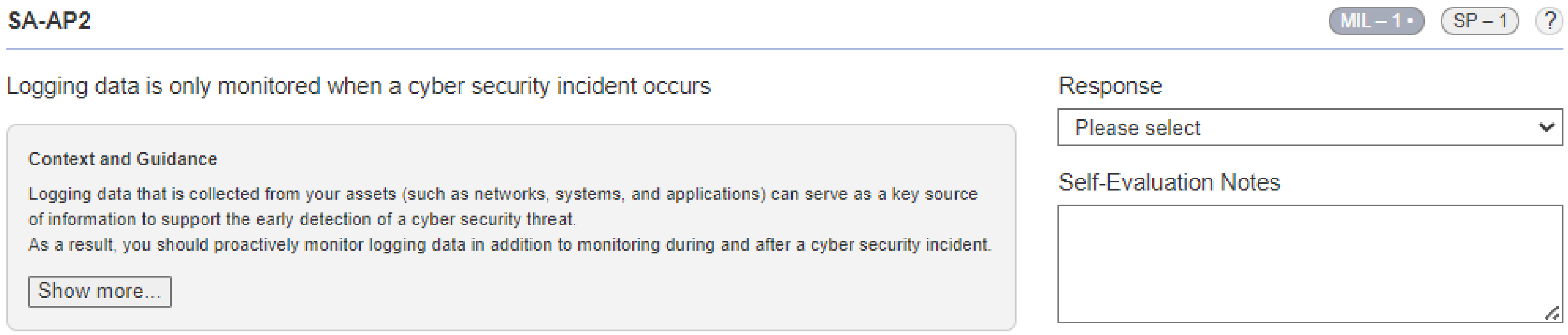
Assessment Scoring Model – Anti-Pattern Worked Example 2

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.



Logging data is only monitored when a cyber security incident occurs

Context and Guidance

Logging data that is collected from your assets (such as networks, systems, and applications) can serve as a key source of information to support the early detection of a cyber security threat.
As a result, you should proactively monitor logging data in addition to monitoring during and after a cyber security incident.

AESCSF v2 Lite Assessment

AESCSF v2 Lite – Overview

The AESCSF Lite framework has been developed to facilitate Assessment against the AESCSF by lower-criticality market entities, and those with limited time and security resources; the Lite Framework is **only available in Version 2 and via the annual assessment program (No offline version)**.

The version 2 assessment consists of 29 multi-select easy to follow questions written in plain English. Simply select as many responses as possible that are applicable to your organisation. If none of responses apply, select ‘None of the above’.

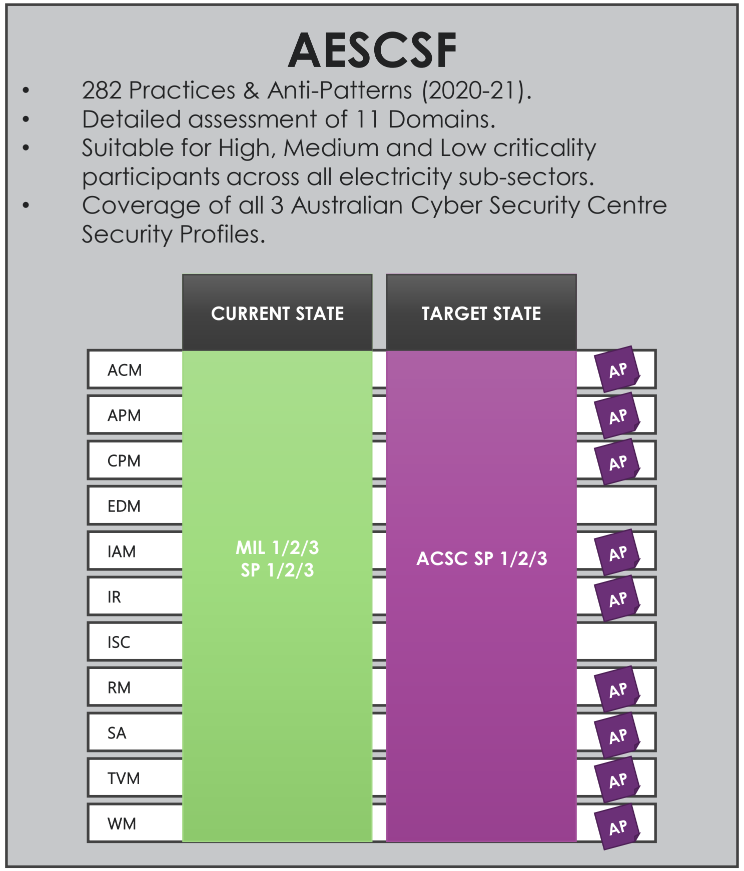
Completing the Lite Assessment

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.

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.

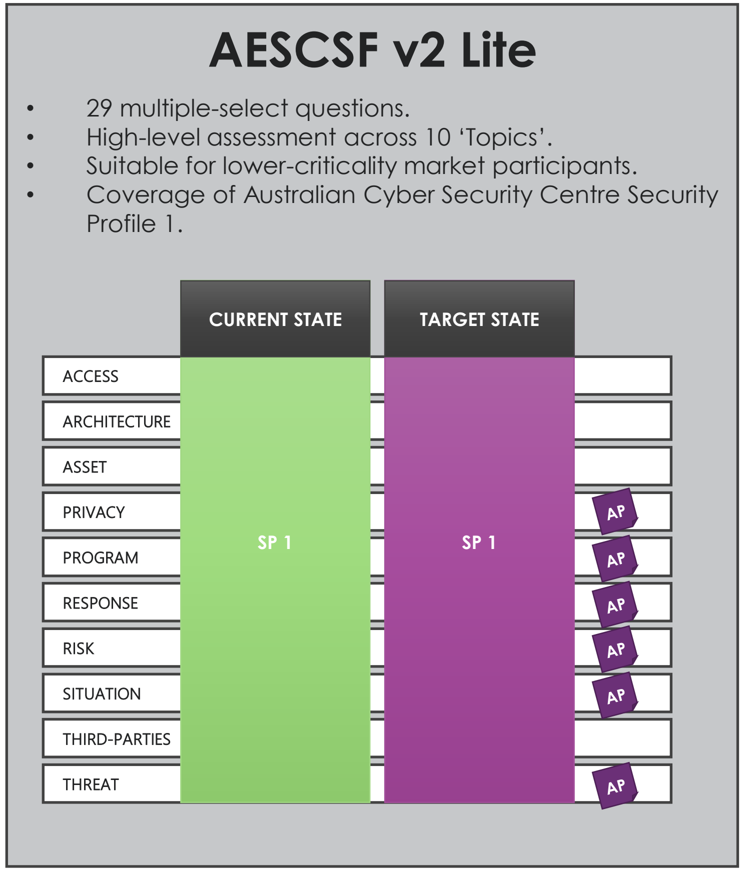
Results from the assessment can be transposed into a full Framework Assessment based on a mapping of Lite questions to AESCSF Practices.

Refer to the AESCSF Guidance Material for Low Criticality Organisations for further support.



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.

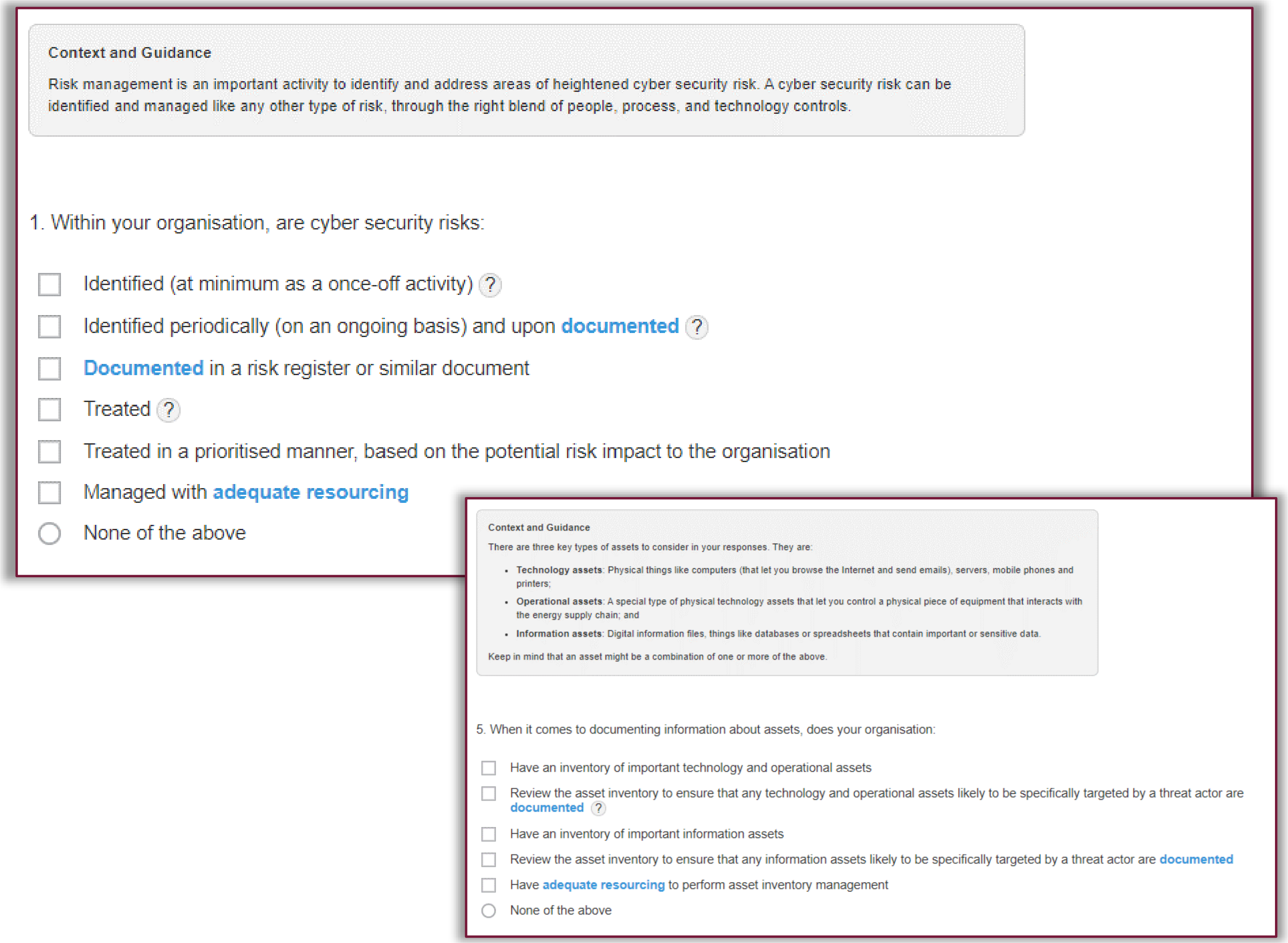


AESCSF v2 Lite

- 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.

AESCSF Lite – Assessment Examples

- 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 Assessment can be transposed into a full Framework Assessment based on a mapping of Lite questions to AESCSF Practices.



Context and Guidance

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.

1. Within your organisation, are cyber security risks:

□ Identified (at minimum as a once-off activity) ?

□ Identified periodically (on an ongoing basis) and upon **documented** ?

□ **Documented** in a risk register or similar document

□ Treated ?

□ Treated in a prioritised manner, based on the potential risk impact to the organisation

□ Managed with **adequate resourcing**

○ None of the above

Context and Guidance

There are three key types of assets to consider in your responses. They are:

- **Technology assets**: Physical things like computers (that let you browse the Internet and send emails), servers, mobile phones and printers;
- **Operational assets**: A special type of physical technology assets that let you control a physical piece of equipment that interacts with the energy supply chain; and
- **Information assets**: Digital information files, things like databases or spreadsheets that contain important or sensitive data.

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

5. When it comes to documenting information about assets, does your organisation:

□ Have an inventory of important technology and operational assets

□ Review the asset inventory to ensure that any technology and operational assets likely to be specifically targeted by a threat actor are **documented** ?

□ Have an inventory of important information assets

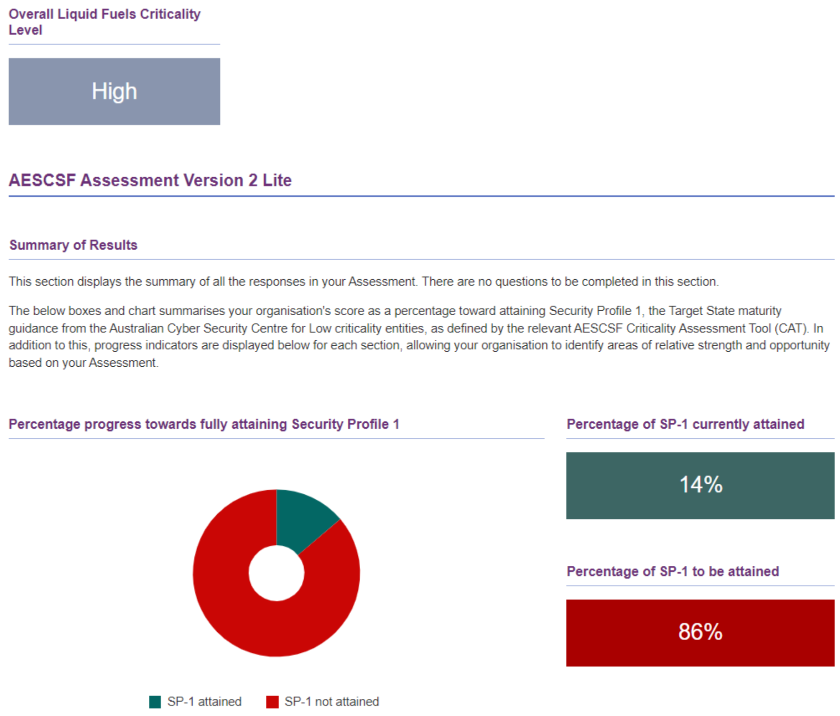
□ Review the asset inventory to ensure that any information assets likely to be specifically targeted by a threat actor are **documented**

□ Have **adequate resourcing** to perform asset inventory management

○ None of the above

AESCSF Lite – Results Example

- The below boxes and chart summarises your organisation's score as a percentage toward attaining Security Profile 1, the Target State maturity guidance from the Australian Cyber Security Centre for Low criticality entities, as defined by the relevant AESCSF Criticality Assessment Tool (CAT). In addition to this, progress indicators are displayed below for each section, allowing your organisation to identify areas of relative strength and opportunity based on your Assessment.
- 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 in Image 2 with the associated ratio of ‘Complete’ responses on the right.
- ‘Complete’ response options correspond to the entity exhibiting desired cyber security capabilities.



Overall Liquid Fuels Criticality Level

High

AESCSF Assessment Version 2 Lite

Summary of Results

This section displays the summary of all the responses in your Assessment. There are no questions to be completed in this section.

The below boxes and chart summarises your organisation's score as a percentage toward attaining Security Profile 1, the Target State maturity guidance from the Australian Cyber Security Centre for Low criticality entities, as defined by the relevant AESCSF Criticality Assessment Tool (CAT). In addition to this, progress indicators are displayed below for each section, allowing your organisation to identify areas of relative strength and opportunity based on your Assessment.

Percentage progress towards fully attaining Security Profile 1

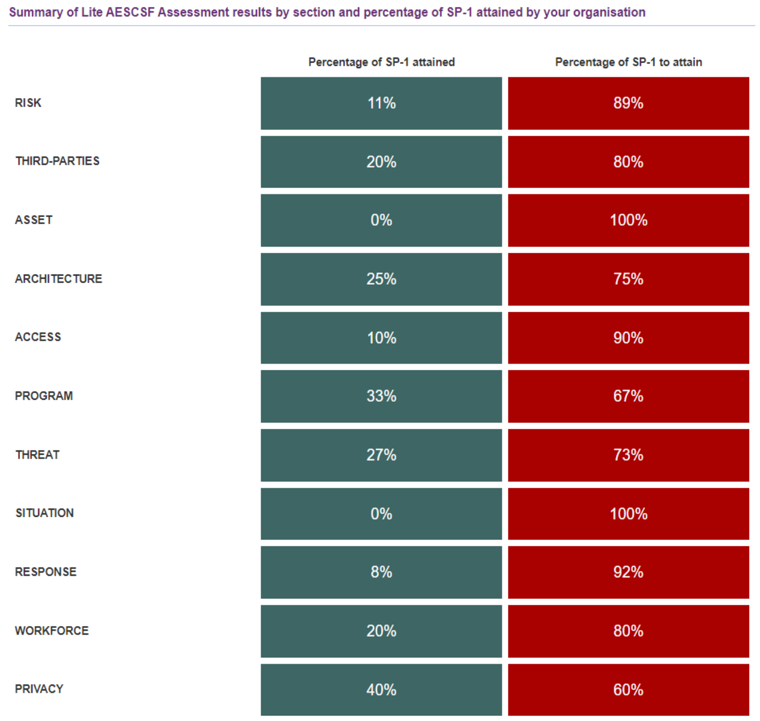
Percentage of SP-1 currently attained

14%

Percentage of SP-1 to be attained

86%

Image 1.



Summary of Lite AESCSF Assessment results by section and percentage of SP-1 attained by your organisation

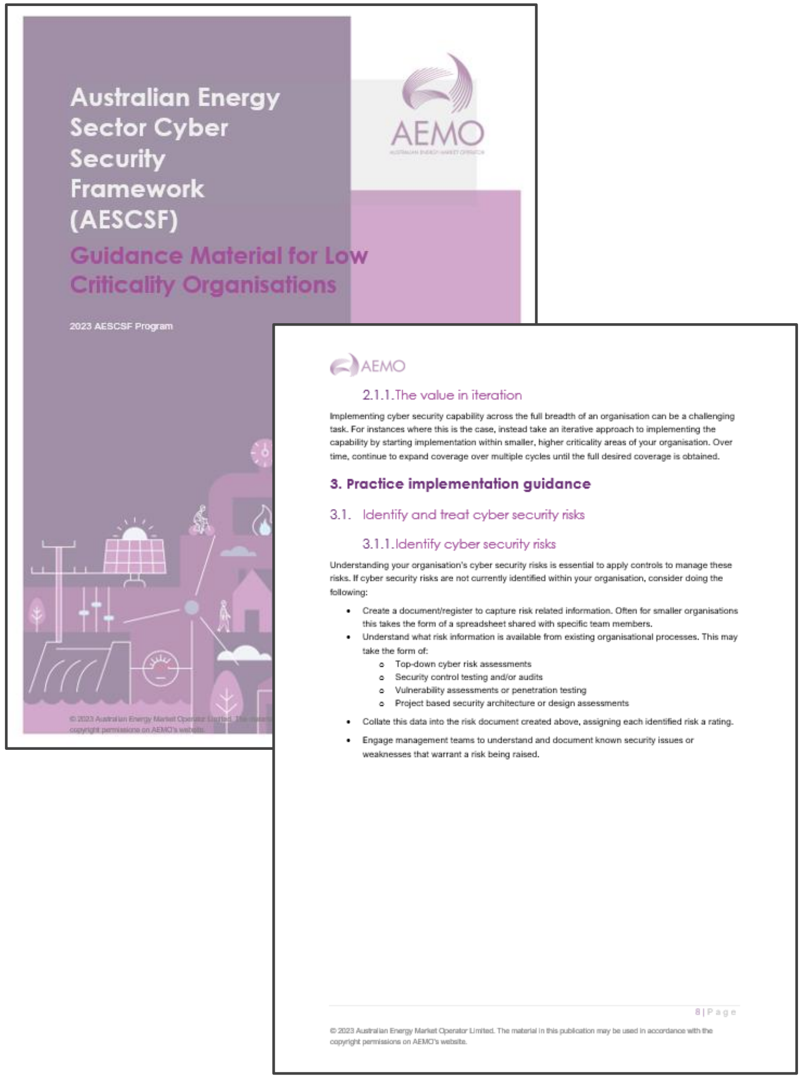
	Percentage of SP-1 attained	Percentage of SP-1 to attain
RISK	11%	89%
THIRD-PARTIES	20%	80%
ASSET	0%	100%
ARCHITECTURE	25%	75%
ACCESS	10%	90%
PROGRAM	33%	67%
THREAT	27%	73%
SITUATION	0%	100%
RESPONSE	8%	92%
WORKFORCE	20%	80%
PRIVACY	40%	60%

Image 2.

AESCSF Guidance for Low Criticality 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 (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

2023 AESCSF Program

© 2023 Australian Energy Market Operator Limited. The materia
copyright permissions on AEMO's website.

2.1.1.The value in iteration

Implementing cyber security capability across the full breadth of an organisation can be a challenging task. For instances where this is the case, instead take an iterative approach to implementing the capability by starting implementation within smaller, higher criticality areas of your organisation. Over time, continue to expand coverage over multiple cycles until the full desired coverage is obtained.

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.

8 | Page

© 2023 Australian Energy Market Operator Limited. The material in this publication may be used in accordance with the copyright permissions on AEMO's website.

Security Profiles

AESCSF Version 1

AESCSF v1 Security Profile 1

In 2019, the Australian Cyber Security Centre, in consultation with the AEMO and the AESCSF Working Group, defined three 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 threshold SoCI compliance.**
- 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).

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

AESCSF v1 Security Profile 2

- 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.

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 v1 Security Profile 3

- **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.

AESCSF v1

Summary of Practices and Anti-Patterns per Security Profile					
Security Profile	**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	74	14	0	0	88
SP-2	90	22	74	14	200 (112+88 from SP1)
SP-3	76	6	164	36	282 (82+200 from SP2)

Security Profiles

AESCSF Version 2

AESCSF v2 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 v2 Security Profile 2

- 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 v2
Security Profile 3

- **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 has been identified by the ACSC as a priority for completion. This Practice should be considered when sequencing Practice remediation activities.

AESCSF v2

Summary of Practices and Anti-Patterns per Security Profile					
Security Profile	**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	109	14	0	0	123
SP-2	130	22	109	14	275 (152+123 from SP1)
SP-3	73	6	275	36	354 (79+275 from SP2)

AESCSF Priority Practices

AESCSF v1 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
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**

AESCSF v2 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.

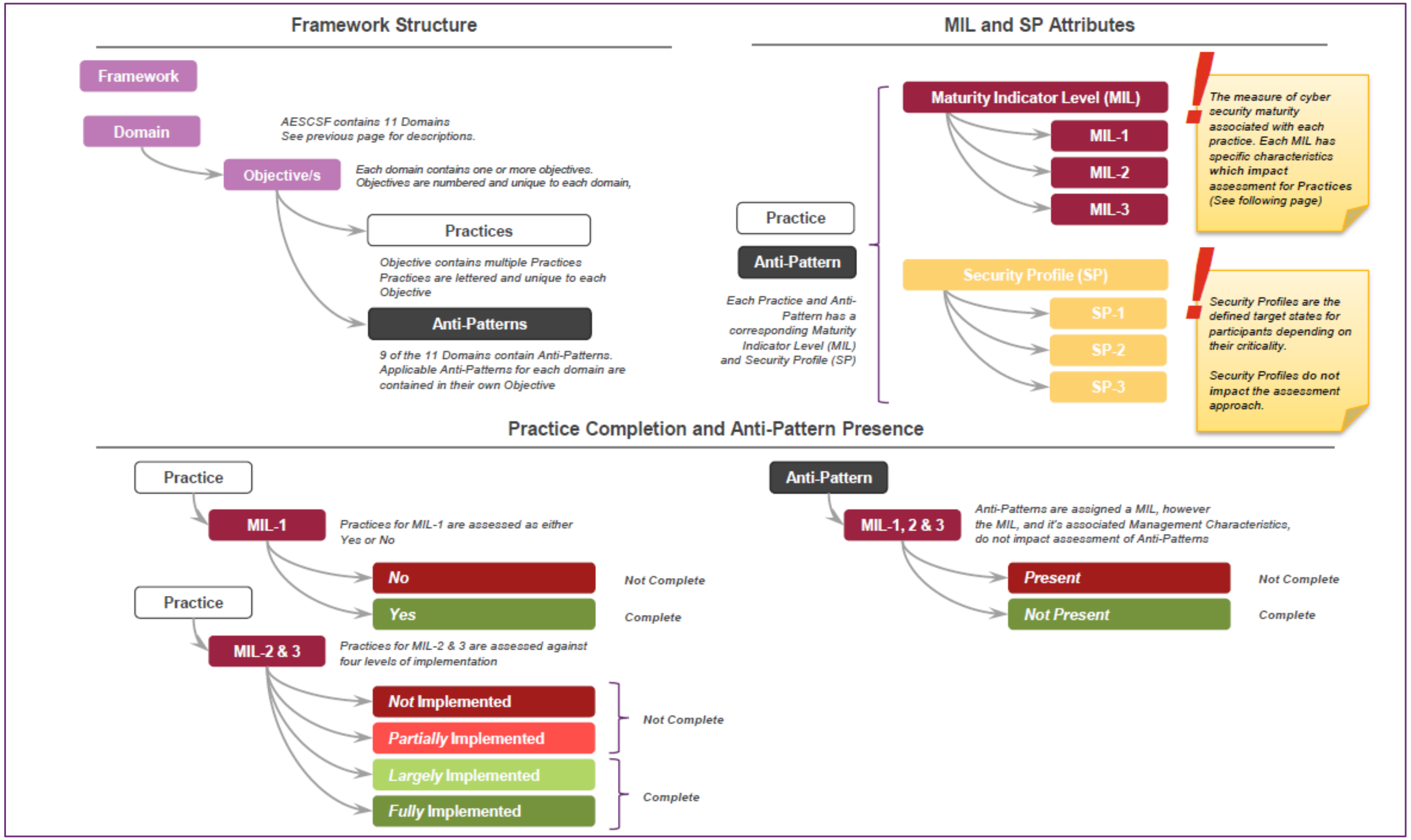
When prioritising Practices, the first priority is to complete Practices in any preceding Security Practices (i.e. Practices in Security Profile 1 should be prioritised over Priority Practices in Security Profile 2).

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**

Where to go for further information

Further information on the framework, including the structure and how to use MILs and SPs, is provided in the AESCSF v2 Quick Reference guide (here). The guide offers additional explanation (shown below) as to how elements of the framework fit together and enable organisations to gauge their cyber security maturity.



Framework Structure

AESCSF contains 11 Domains
See previous page for descriptions.

Each domain contains one or more objectives.
Objectives are numbered and unique to each domain,

Objective contains multiple Practices
Practices are lettered and unique to each Objective

9 of the 11 Domains contain Anti-Patterns.
Applicable Anti-Patterns for each domain are contained in their own Objective

MIL and SP Attributes

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

The measure of cyber security maturity associated with each practice. Each MIL has specific characteristics which impact assessment for Practices (See following page)

Security Profiles are the defined target states for participants depending on their criticality.

Security Profiles do not impact the assessment approach.

Practice Completion and Anti-Pattern Presence

Practices for MIL-1 are assessed as either Yes or No

Practices for MIL-2 & 3 are assessed against four levels of implementation

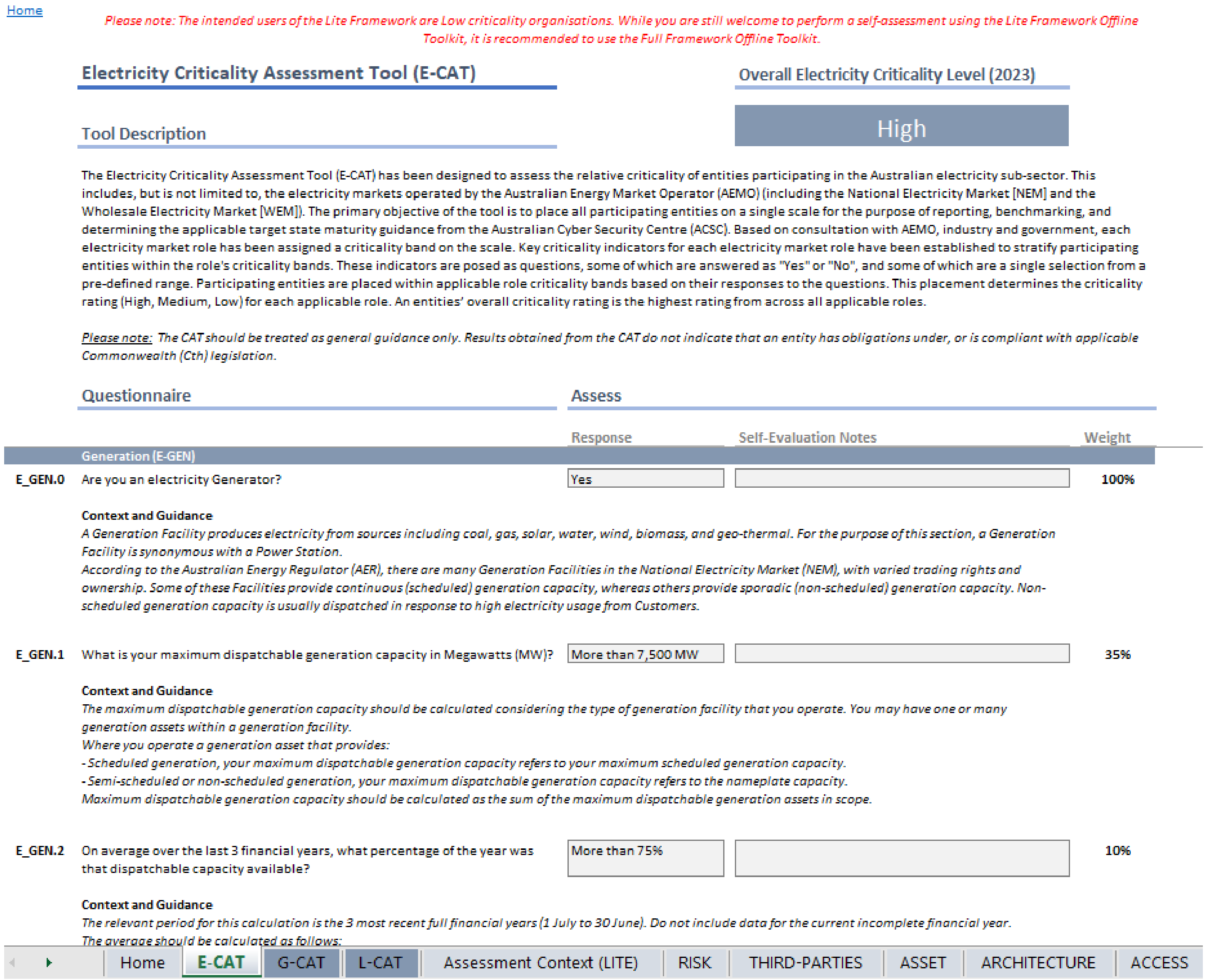
Anti-Patterns are assigned a MIL, however the MIL, and it's associated Management Characteristics, do not impact assessment of Anti-Patterns

Offline Toolkit

AESCSF Offline Toolkit

Criticality Assessment Tool

- To support your ongoing cyber maturity journey and SoCI compliance, both versions of the of the framework are available via the AMEO website as an offline toolkit that produces your CAT, overall score (MIL & SP) & domains doughnuts
- Download the toolkit and complete your appropriate CAT to confirm your overall criticality score.



Please note: The intended users of the Lite Framework are Low criticality organisations. While you are still welcome to perform a self-assessment using the Lite Framework Offline Toolkit, it is recommended to use the Full Framework Offline Toolkit.

Electricity Criticality Assessment Tool (E-CAT)

Overall Electricity Criticality Level (2023)

High

Tool Description

The Electricity Criticality Assessment Tool (E-CAT) has been designed to assess the relative criticality of entities participating in the Australian electricity sub-sector. This includes, but is not limited to, the electricity markets operated by the Australian Energy Market Operator (AEMO) (including the National Electricity Market [NEM] and the Wholesale Electricity Market [WEM]). The primary objective of the tool is to place all participating entities on a single scale for the purpose of reporting, benchmarking, and determining the applicable target state maturity guidance from the Australian Cyber Security Centre (ACSC). Based on consultation with AEMO, industry and government, each electricity market role has been assigned a criticality band on the scale. Key criticality indicators for each electricity market role have been established to stratify participating entities within the role's criticality bands. These indicators are posed as questions, some of which are answered as "Yes" or "No", and some of which are a single selection from a pre-defined range. Participating entities are placed within applicable role criticality bands based on their responses to the questions. This placement determines the criticality rating (High, Medium, Low) for each applicable role. An entities' overall criticality rating is the highest rating from across all applicable roles.

Please note: *The CAT should be treated as general guidance only. Results obtained from the CAT do not indicate that an entity has obligations under, or is compliant with applicable Commonwealth (Cth) legislation.*

Questionnaire

Assess

		Response	Self-Evaluation Notes	Weight
	Generation (E-GEN)			
E_GEN.0	Are you an electricity Generator?	Yes		100%
E_GEN.1	What is your maximum dispatchable generation capacity in Megawatts (MW)?	More than 7,500 MW		35%
E_GEN.2	On average over the last 3 financial years, what percentage of the year was that dispatchable capacity available?	More than 75%		10%

E_GEN.0 – **Context and Guidance**

A Generation Facility produces electricity from sources including coal, gas, solar, water, wind, biomass, and geo-thermal. For the purpose of this section, a Generation Facility is synonymous with a Power Station.

According to the Australian Energy Regulator (AER), there are many Generation Facilities in the National Electricity Market (NEM), with varied trading rights and ownership. Some of these Facilities provide continuous (scheduled) generation capacity, whereas others provide sporadic (non-scheduled) generation capacity. Non-scheduled generation capacity is usually dispatched in response to high electricity usage from Customers.

E_GEN.1 – **Context and Guidance**

The maximum dispatchable generation capacity should be calculated considering the type of generation facility that you operate. You may have one or many generation assets within a generation facility.

Where you operate a generation asset that provides:

- Scheduled generation, your maximum dispatchable generation capacity refers to your maximum scheduled generation capacity.

- Semi-scheduled or non-scheduled generation, your maximum dispatchable generation capacity refers to the nameplate capacity.

Maximum dispatchable generation capacity should be calculated as the sum of the maximum dispatchable generation assets in scope.

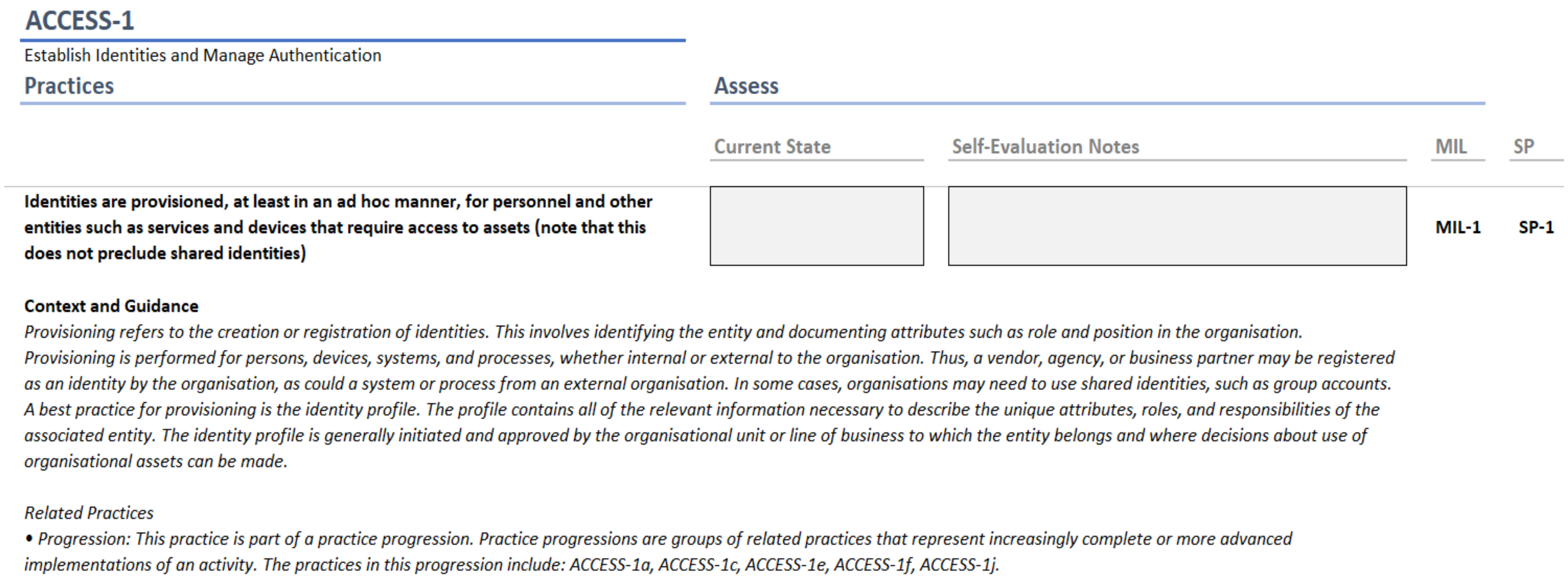
E_GEN.2 – **Context and Guidance**

The relevant period for this calculation is the 3 most recent full financial years (1 July to 30 June). Do not include data for the current incomplete financial year.

The average should be calculated as follows:

AESCSF Offline Toolkit

- Make your way through the tab's at the bottom of the screen for each domain, choosing an option for each practice from the drop down box. You can include additional comments for your own records in the *self-evaluation notes*.



ACCESS-1

Establish Identities and Manage Authentication

Practices	Assess			
	Current State	Self-Evaluation Notes	MIL	SP
Identities are provisioned, at least in an ad hoc manner, for personnel and other entities such as services and devices that require access to assets (note that this does not preclude shared identities)			MIL-1	SP-1

Context and Guidance

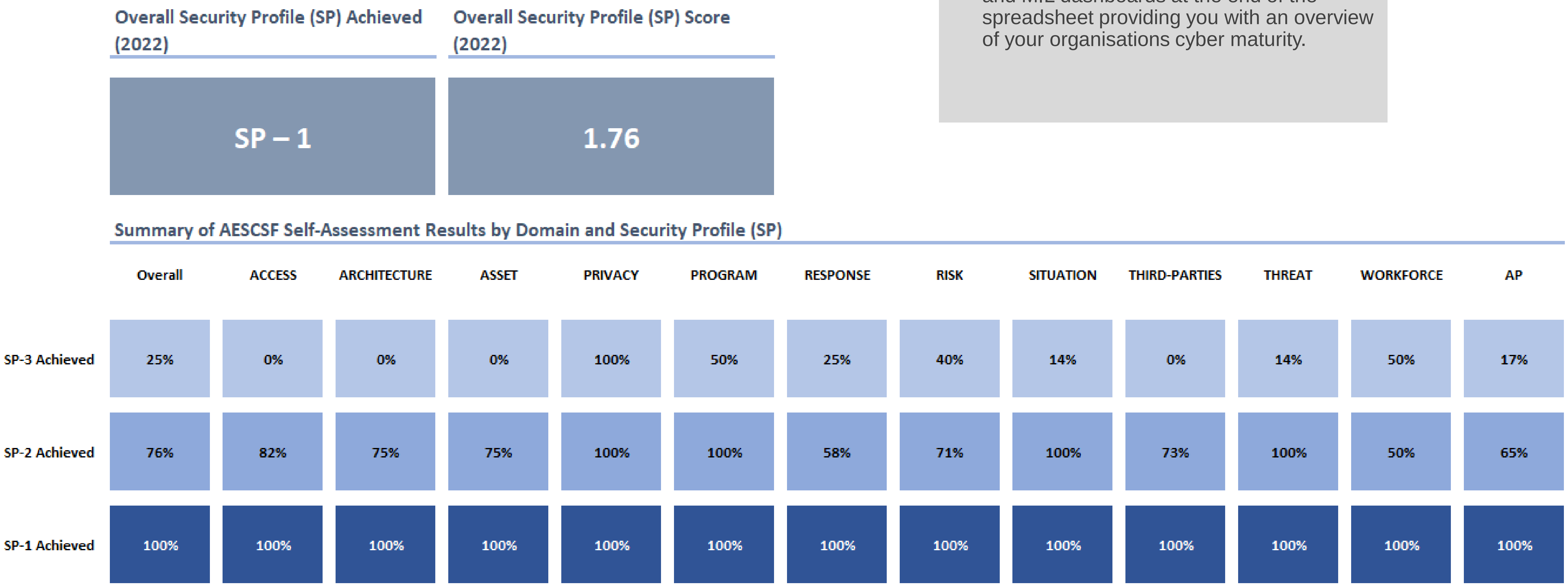
Provisioning refers to the creation or registration of identities. This involves identifying the entity and documenting attributes such as role and position in the organisation. Provisioning is performed for persons, devices, systems, and processes, whether internal or external to the organisation. Thus, a vendor, agency, or business partner may be registered as an identity by the organisation, as could a system or process from an external organisation. In some cases, organisations may need to use shared identities, such as group accounts. A best practice for provisioning is the identity profile. The profile contains all of the relevant information necessary to describe the unique attributes, roles, and responsibilities of the associated entity. The identity profile is generally initiated and approved by the organisational unit or line of business to which the entity belongs and where decisions about use of organisational assets can be made.

Related Practices

- *Progression: This practice is part of a practice progression. Practice progressions are groups of related practices that represent increasingly complete or more advanced implementations of an activity. The practices in this progression include: ACCESS-1a, ACCESS-1c, ACCESS-1e, ACCESS-1f, ACCESS-1j.*

AESCSF Dashboards

- As you complete the assessment your results are updated in the Security Profile and MIL dashboards at the end of the spreadsheet providing you with an overview of your organisations cyber maturity.



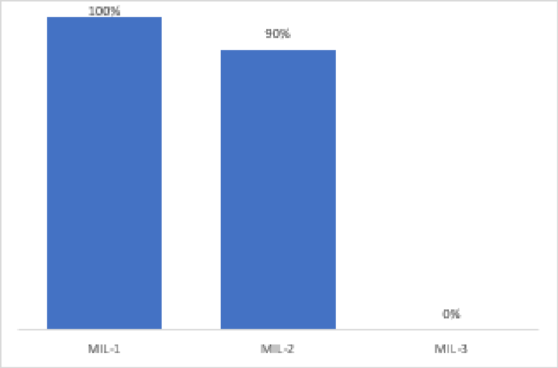
Overall Security Profile (SP) Achieved (2022)	Overall Security Profile (SP) Score (2022)
SP – 1	1.76

Summary of AESCSF Self-Assessment Results by Domain and Security Profile (SP)

	Overall	ACCESS	ARCHITECTURE	ASSET	PRIVACY	PROGRAM	RESPONSE	RISK	SITUATION	THIRD-PARTIES	THREAT	WORKFORCE	AP
SP-3 Achieved	25%	0%	0%	0%	100%	50%	25%	40%	14%	0%	14%	50%	17%
SP-2 Achieved	76%	82%	75%	75%	100%	100%	58%	71%	100%	73%	100%	50%	65%
SP-1 Achieved	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%

AESCSF Dashboards

Summary of AESCSF Self-Assessment Results by Percentage Completion of Maturity Indicator Level (MIL)



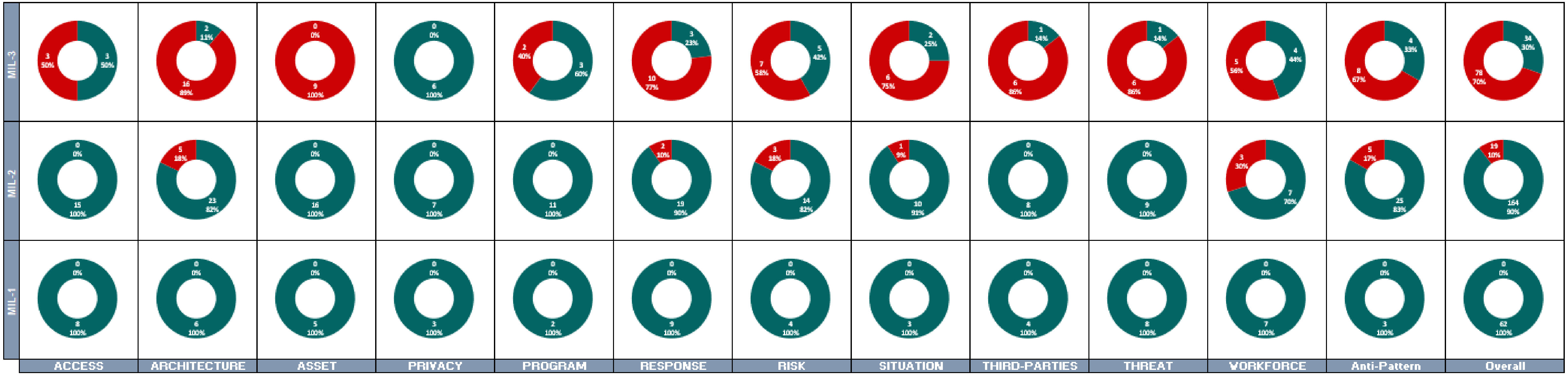
Overall Maturity Indicator Level (MIL) Achieved (2022)

MIL – 1

Overall Maturity Score (2022)

1.90

Summary of AESCSF Self-Assessment Results by Domain and Maturity Indicator Level (MIL)


MIL-3
MIL-2
MIL-1
ACCESS
ARCHITECTURE
ASSET
PRIVACY
PROGRAM
RESPONSE
RISK
SITUATION
THIRD-PARTIES
THREAT
WORKFORCE
Anti-Pattern
Overall