Australian Energy Sector Cyber Security Framework

Education Workshop

October 2018

Education Workshop - Agenda

Time	Topic
9.30am – 9.50am	1. Project Overview
9.50am – 10.10am	2. Introduction to the Australian Energy Sector Cyber Security Framework (AESCSF)
10.10am – 10.40am	3. Criticality Assessment
10.40am – 10.50am	Morning Break
10.50am – 11.10am	4. AESCSF Structure
11.10am – 11.40am	5. Assessment Scoring Model
11.40am – 12.00pm	6. Assessment Outcome and Next Steps
12.00pm – 12.20pm	AESCSF Toolkit Login and Completion of Initial Scoping Questionnaire
12.20pm – 1.00pm	Lunch Break
1.00pm – 2:00pm	**7. AESCSF Walkthrough Session (Optional)** • Criticality Assessment Tool • AESCSF Assessment • Results – Outcomes and Interpretation

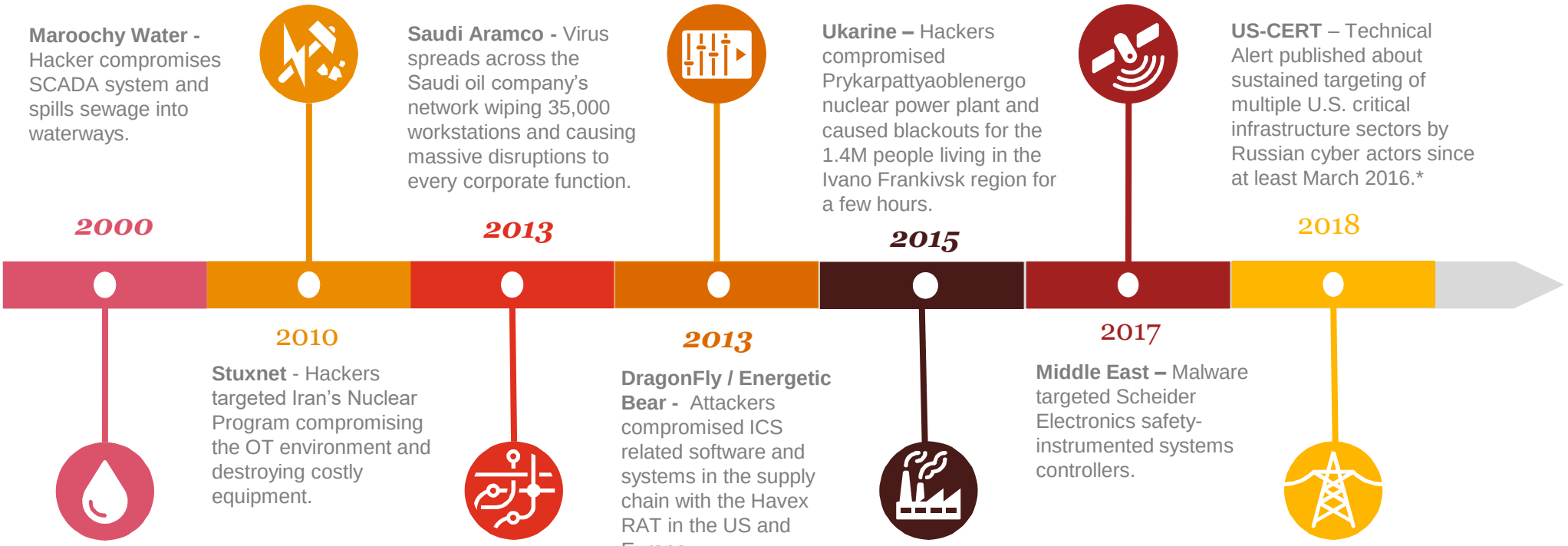
Project Overview

1

Project Overview - Evolution of Critical Infrastructure Threats

The security and reliability of the energy sector has fallen under increasing attention over the last few years due to sophisticated cyber attacks against critical infrastructure in multiple jurisdictions. The consequences of such attacks in Australia may not only impact energy organisations, but have broader impacts to society, public health and safety and our nation's economy.

High profile attacks on critical infrastructure and Industrial Control Systems (ICS) have included:



*Refer to (https://www.us-cert.gov/ncas/alerts/TA18-074A)

Project Overview - Drivers

In response to the increasing threat landscape, AEMO has commissioned a sector wide Cyber Security project. Key considerations underpinning its establishment included:

Project Overview – Guiding Principles

The project has primarily been established to develop a tailored cyber security framework, the Australian Energy Sector Cyber Security Framework (AESCSF), and supporting tools to set the foundation for the future of energy cyber security in Australia.

The guiding principles for the development of the AESCSF include:

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.

Tailored to the Australian Energy Market

Is tailored for the Australian energy market and aligns with existing local policies and guidelines, for example, the Australian Privacy Principles and ACSC Top 37 Mitigation Strategies.

Leverage International Industry Standards

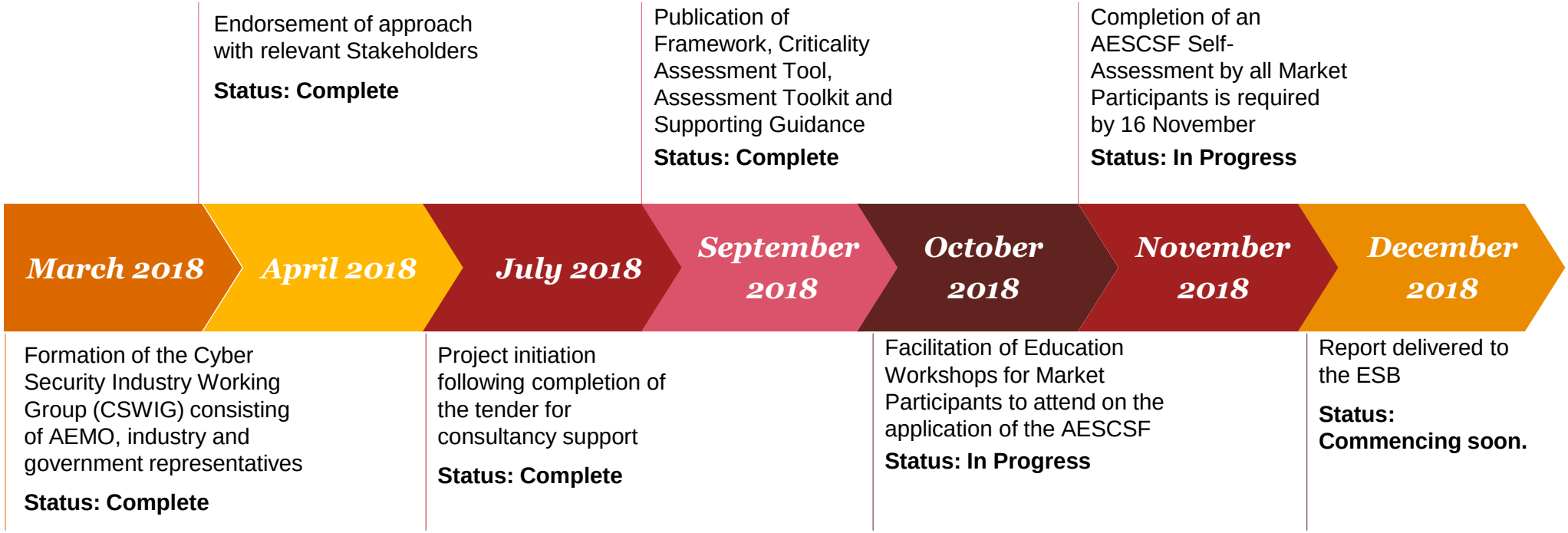
Leverages existing industry standards that have been adopted globally. ES-C2M2* was used as the foundation of the AESCSF, with alignment to the NIST CSF^.

*ES-C2M2 – Electricity Subsector Cyber Security Capability Maturity Model
^NIST CSF – National Institute of Standards and Technology Cyber Security Framework

Project Overview - Timeline

The project must deliver a report to the Australian Energy Security Board (ESB) by EOCY 2018 regarding its "assessment of the cyber maturity of all energy market participants to understand where there are vulnerabilities."[1]

The key milestones in achieving this outcome are:



[1] Finkel Recommendation 2.10

Project Overview - Stakeholder Groups

The key stakeholders including their roles and responsibilities in relation to the development of the AESCSF are summarised below.

Stakeholders	Key Personnel	Responsibilities
Australian Signals Directorate (ASD) Home Affairs (Critical Infrastructure Centre)	Head of Australian Cyber Security Centre + Head of Critical Infrastructure Centre	• Review the AESCSF, any associated artefacts and standards as they are developed.
System and Market Operator (AEMO)	AEMO CEO & CDTO	• Endorse recommendations from CSIWG • Provide strategic advice to the ASD and CIC on grid and market cyber security related matters • Report annually to the ESB and other government agencies on the status of cyber security resilience
Cyber Security Industry Working Group (CSIWG) + Sub-Working Groups	Government, AEMO and participant SME representatives	• Advise on detailed framework selection and adoption • Meet monthly • Progress technical and operational cyber related improvements including threat and information sharing • Engage with other participant types in a prioritised manner
Market Participants	Key Executives and Cyber Security Manager	• Active engagement in education workshops, AESCSF assessments, development of cyber security uplift plans and information sharing to collectively uplift Industry Maturity.

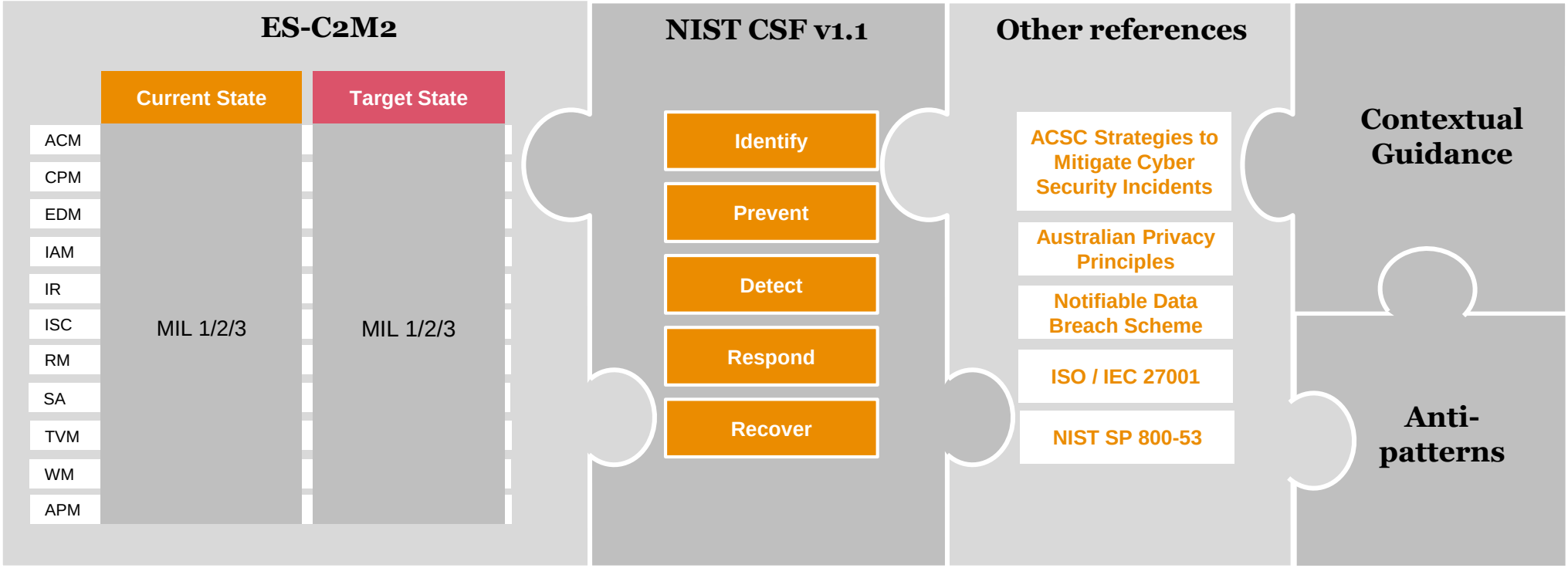
Introduction to the AESCSF

2

Overview of the AESCSF

The AESCSF is based on well-established and globally adopted frameworks – namely ES-C2M2 and the NIST CSF. The AESCSF augments areas where ES-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 CSIWG. This provides the depth and breadth of coverage necessary for Australian market participants.

Australian Energy Sector Cyber Security Framework "Master Data"



AESCSF Augmentation Elements

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

Key Project Artefacts

The following suite of artefacts is designed to complement and enable organisations to optimally utilise 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 ES-C2M2 practices to NIST CSF, Contextual Guidance, Anti-Patterns, International and Australian informative references.
- **Criticality Assessment Tool -** Questionnaire used to assess each market participant against a set of predefined criteria to determine their relative criticality to the sector.

Guidance

- **AESCSF FAQ**- A documented list of questions and answers to support an organisation's understanding of how the AESCSF operates.
- **AESCSF Quick Reference Guide -** A quick reference guide on how to use the assessment scoring model.
- **Education Training Workshop Pack –** A PowerPoint pack designed to assist organisations to understand the AESCSF, and to use as a template when training staff on the AESCSF.
- **Glossary –** A document containing the terms used in the AESCSF to ensure consistent understanding and clarity.
- **AESCSF Toolkit User Guide -** Documented guidance on how to use the AESCSF Toolkit.

Toolkit

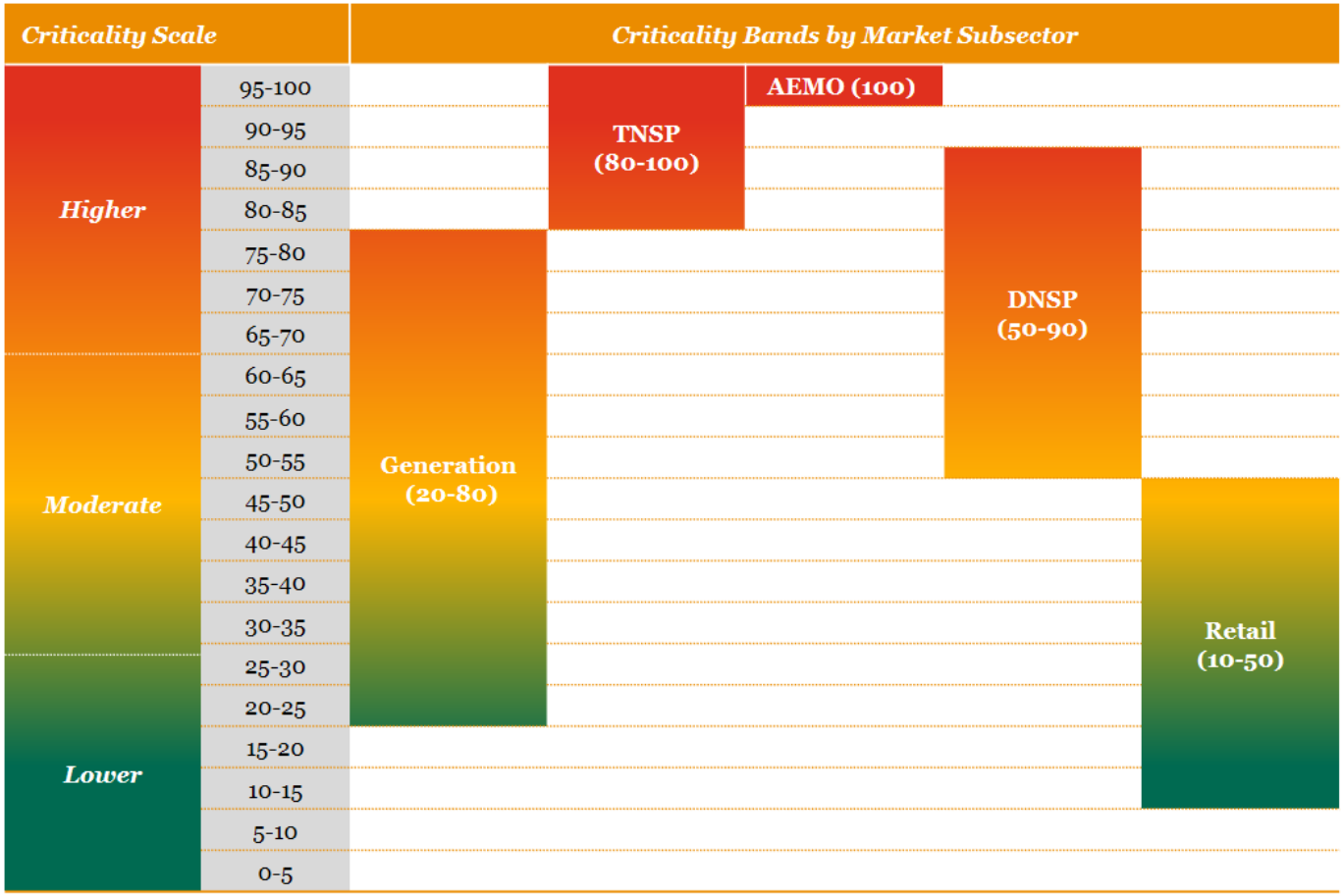
- **Web-enabled AESCSF Toolkit** - A web-based platform (Datapoint) is used to collect and store assessment data. Participants are able to download their assessment results from the platform. Once the assessment period is closed, participants will be given access to the 'Explore' Module to view their results against a de-identified AESCSF data set for benchmarking purposes.

Criticality Assessment

3

Criticality Assessment Overview

The purpose of the Criticality Assessment Tool (CAT) is to determine the criticality of the entity, to rank entities within their industry sub sector, and to assist in the determination of the target maturity state for the entity.



The CAT was developed through consultation with AEMO, the CSIWG, and energy market participants.

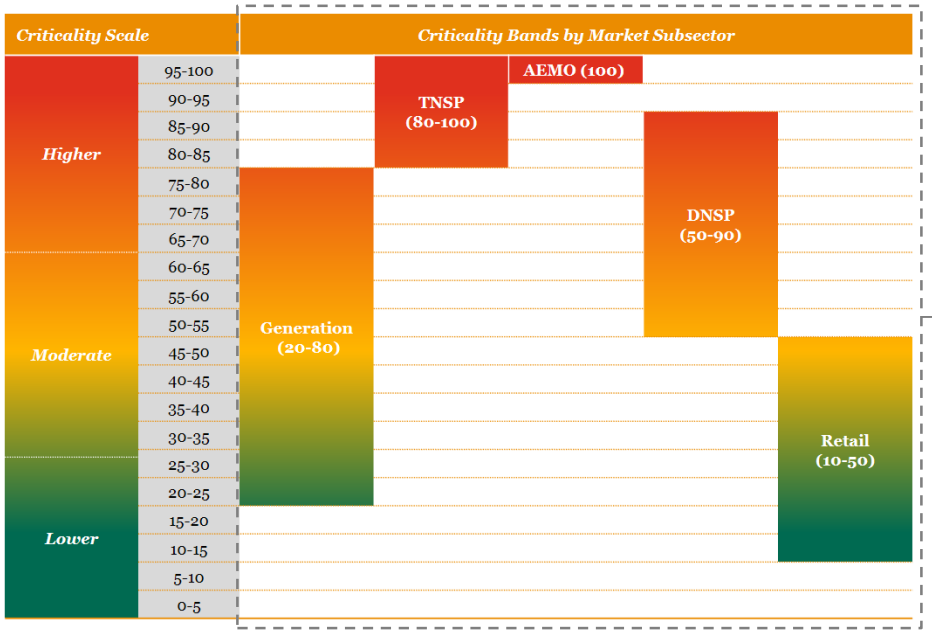
Based on consultation, each market subsector has been assigned a band on the criticality scale within which all energy market participants will be mapped.

Within each subsector criticality band, a set of criticality attributes are used to stratify the participants.

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 and maximum potential impact.

Criticality Bands by Market Subsector

The CAT stratifies all participants across a single criticality scale based on a questionnaire designed to focus on an entity's context within the subsector(s).



Criticality Bands by Market Subsector

- The CAT scopes which subsector an entity operates in, entities can operate in more than one subsector – TNSP, DNSP, Generator, Retailer, Interconnector, and System/ Market Operator (AEMO).
- The scope determines the criticality band and starting score, as well as the set of criticality questions an entity is required to answer.
- The questionnaire contain the relevant focus areas of criticality for each subsector, and a weighting is assigned to each. The weighting assigned to each questions was determined in collaboration with AEMO and the CSIWG.
- Organisations may find their response to some questions in the CAT will differ by region. In these situations please respond based on a whole of Market perspective (ie aggregated view across both NEM and WEM).

Criticality Bands by Market Subsector (cont.)

Each subsector questionnaire has *'criticality attributes'* which determine the most crucial components of an entity's operating environment. Weighting of *'criticality attributes'* were determined in collaboration with the CSIWG.

Criticality Attributes for each Subsector

Generation

- Maximum dispatchable capacity
- Actual dispatchable capacity
- Availability of dispatchable capacity
- Regional criticality
- Synchronous generation
- Ancillary services
- Network Support Agreements

Transmission

- Electricity transported
- Interconnector capacity

Interconnector

- Nominal Capacity
- Regional criticality*

* Independently operated interconnectors only.

Distribution

- Electricity transported
- Number of customers (National Metering Identifiers)
- Number of critical and commercial customers

Retail

- Number of customers (National Metering Identifiers)
- Use of Smart Meters
- Number of critical and commercial customers
- Virtual Power Plants
- Retailer of Last Resort
- Sole Retailer for a region

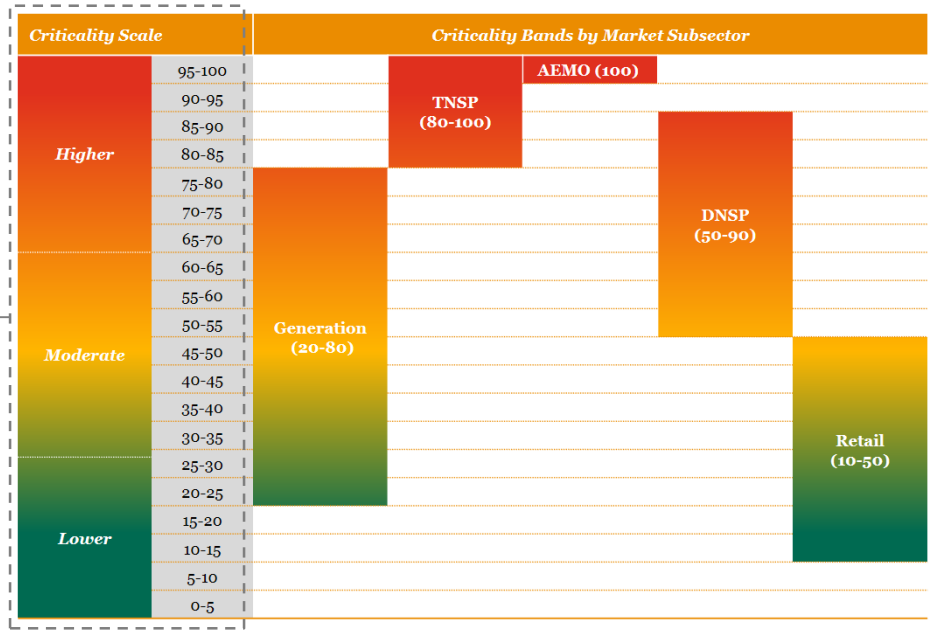
System/market Operator – If the entity is a system/market operator, it automatically is assigned the highest criticality band

Criticality Scale & Target Maturity State

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

Criticality Scale

- The responses to the questionnaire will provided an overall category score of High, Medium or Low by subsector.
- If an entity operates across multiple subsectors, the CAT will use the higher criticality band.
- This is an indication of the potential impact to the Australian energy market in the event of a cyber incident at the particular organisation.



Target State

A consultation process is underway with stakeholders from relevant Government departments and industry working groups to define the initial Target Maturity States for the Australian energy industry. Consideration is being given to:

a) The criticality of organisations;
b) The timeframes organisations are provided to achieve the relevant Target Maturity State; and
c) The related assurance requirements.

Further information on Target Maturity States will be communicated on completion of the consultation period.

Framework Structure

4

AESCSF Domains

The AESCSF is divided into 11 domains - 10 C2M2 domains and the Australia 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.

RM Risk Management	ACM Asset, Change, and Configuration Management	IAM Identity and Access Management	TVM Threat and Vulnerability Management
SA Situational Awareness	ISC Information Sharing and Communications	IR Event and Incident Response, Continuity of Operations	EDM Supply Chain and External Dependencies Management
WM Workforce Management	CPM Cybersecurity Program Management	APM Australian Privacy Management	

APM is an Australian specific domain to enable organisations to manage personal identifiable information through its lifecycle.

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 - collection, storage, use and disclosure, and disposal (including de-identification) by reduce privacy related risks, and respond to personal information data breaches.

APM

Australian Privacy Management

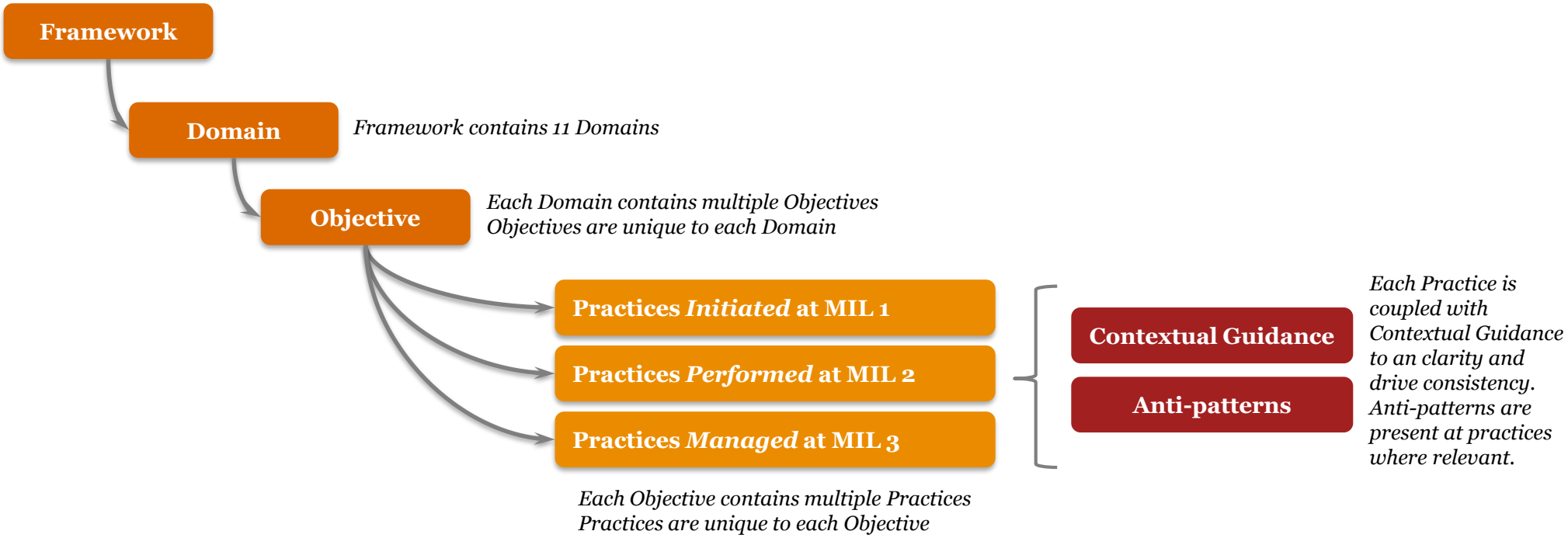
- The APM domain focuses on matters that intersect with or provide an indication of cyber security maturity.
- The development of the APM domain leveraged the Australian Privacy Principles and the Office of the Australian Information Commissioner, Privacy Management Framework. Privacy related elements of international 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 does 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 on the recommendation of Cyber Security Industry Working Group, 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

The practices within a domain are grouped by objective – target achievements that support the domain. Within each objective, the practices are ordered by MIL – Maturity Indicator Level.



Four aspects of the Maturity Level Indicators

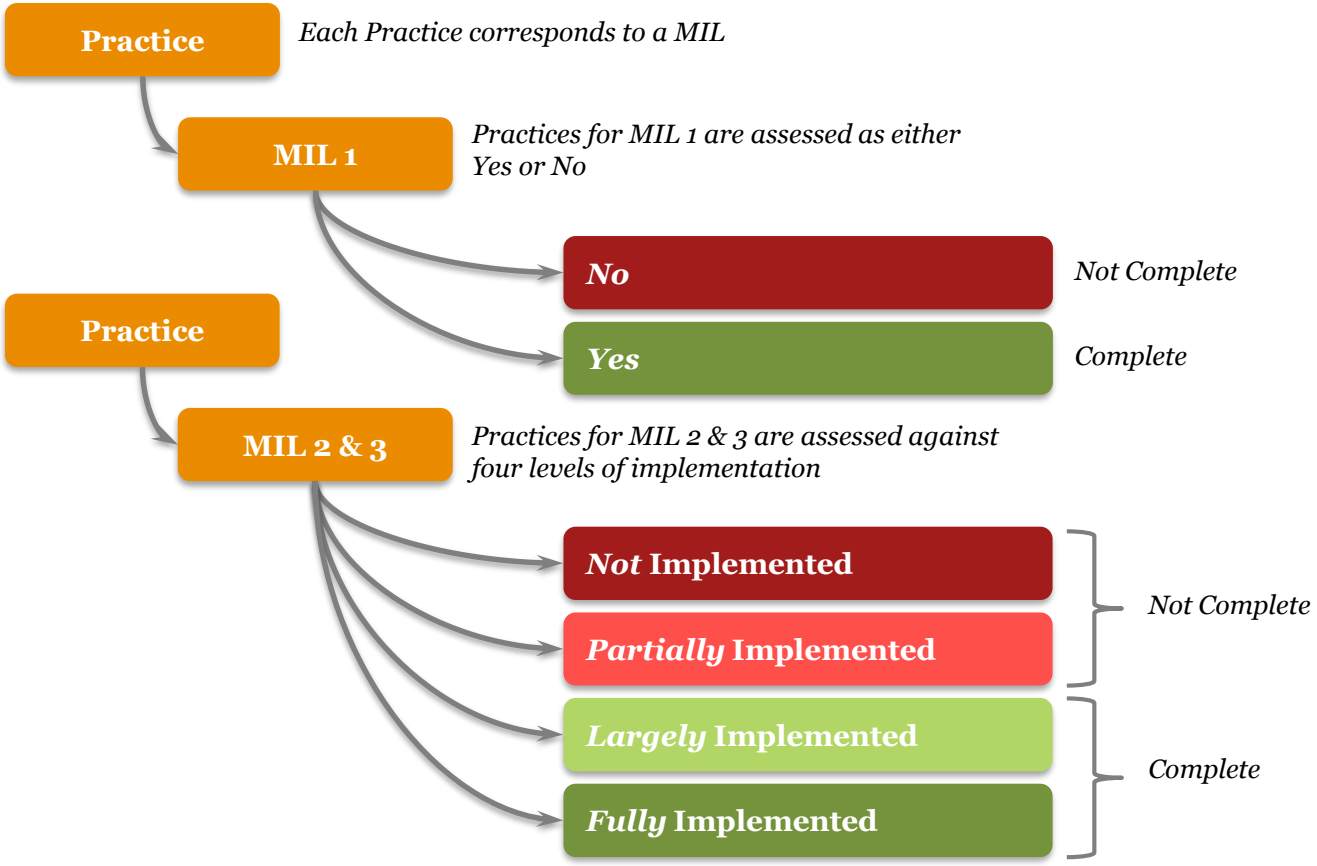
1. MILs apply independently to each domain. As a result, entity's may be operating at different MIL rating for different domains.
2. The MILs are cumulative within each domain; to earn a MIL in a given domain, an organisation must perform all of the practices in that level and its predecessor level(s).
3. Establishing a target MIL for each domain is an effective strategy for using the model to guide cyber security program improvement.
4. Practice performance and MIL achievement need to align with business objectives, risk appetite and the organisation's cyber security strategy. Achieving the highest MIL in all domains may not be an optimal strategy for all organisations.

Assessment Scoring Model

5

Assessment Scoring Model Key Features

The AESCSF uses a revised ES-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 Implementation

MIL 1

Practice

&

Figure 1

Practices *Initiated* at MIL 1	
No activities that evidence the practice are visible within the function	*No*
Some activities that evidence the practice are visible within the function. These activities are ad-hoc, and vary in frequency, accuracy, and completeness, based on the skills and tools of the personnel completing the activities	*Yes*

*Where an **Anti-Pattern** is present within the organisation, the practice must be assessed as No (at MIL 1) and either Not or Partially Implemented (at MIL 2 or 3)*

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

MIL 2

Practice

&

Figure 2

Practices *Performed* at MIL 2			
1	*Practices are **documented***	*Partially*	
2	***Stakeholders** of the practice are identified and involved*	*Largely*	
3	*Adequate **resources** are provided to support the process (people, funding, and tools)*		
4	***Standards** and/or guidelines have been identified to guide the implementation of the practices*	*Fully*	

MIL 3

Practice

&

Figure 3

Practices *Managed* at MIL 3			
1 2 3	*Practices at **MIL 3 must also** exhibit **complete** (that is, Largely or Fully Implemented) **Management Characteristics from MIL 2.***	*Partially*	
5	*Activities are guided by **policies** (or other organisational directives) and governance*		
6	*Personnel performing the practices have adequate **skills and knowledge***		
7	*Policies include **compliance** requirements for specified standards and/or guidelines*	*Largely*	
8	***Responsibility and authority** for performing the practices are assigned to personnel*		
9	*Activities are **periodically reviewed** to ensure they conform to policy*	*Fully*	

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 Energy Electric Company 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, so he responds to this practice with “Yes”

ID	Practice	MIL	Self Assessment 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. less...	MIL-1	Yes	Configuration baselines exist and they cover the majority of assets.

Assessment Scoring Model - Worked Example 1 (Cont.)

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

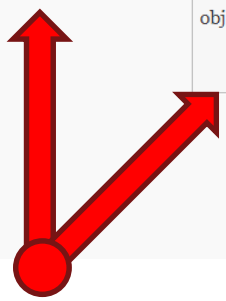
Assessment Scenario:

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 Energy Electric Company, 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 with many systems, one of which is Service Now (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 (Characteristic 2). 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), so he assesses the organisation as Largely Implemented.

ID	Practice	MIL	Self Assessment Response	Notes
ACM-2C	**The design of configuration baselines includes cybersecurity objectives** **Context & 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.	MIL-2	Largely Implemented	Configuration baselines are created for new assets when they are procured. Security team is responsible and creates the baselines in alignment with the cybersecurity objectives. Majority are documented with Service Now.



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 (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 Service Now (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) (Characteristic 2). 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). Taking this into account, John feels that the practice is incomplete, and Partially Implemented.

ID	Practice	MIL	Self Assessment Response	Notes
ACM-2E	**Configuration baselines are reviewed and updated at an organisationally-defined frequency** **Context & Guidance :** Has your organisation defined a requirement for how often configuration baselines should be reviewed and upda… If so, have your configuration baselines been reviewed and updated in accordance with this requirement? Asset configurations… …ndscape. E.g. certain configur… less...	MIL-3	Partially Implemented	Baselines are reviewed annually as a part of the cyber security calendar. Documentation of the baselines and the review performed is retained in Service Now. Reviews are conducted by the Security Team however there is no policy is place to govern this activity. Baselines have never been reviewed by a third party or anyone outside the security team.

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

Assessment Scoring Model - Worked Example 2

AESCSF Practice:

SA-1B “Logging requirements have been defined for all assets important to the function (e.g., scope of activity and coverage of assets, cybersecurity requirements [confidentiality, integrity, availability])

Anti-Pattern: “Third party vendors or services have privileged access that is not logged.”

Assessment Scenario:

John has completed his assessment of SA-1A and determined that logging is occurring for key IT and OT assets where possible and, as such, has responded to that practice with “Yes”.

Now John reads practice SA-1B and considers the logging being conducted across the IT and OT environments. He knows that all logging is configured in accordance with an established log management standard (Characteristic 4) by the security team (Characteristic 2). The security team has two staff (Characteristic 3), responsible for managing the organisations Security Information and Event Management (SIEM) solution, who have documented the operational logging requirements (events and logging verbosity) that assets must be configured in accordance with (Characteristic 1). However, he knows that privileged activities for some environments are only logged via a privileged session management tool which is not used by the third party vendor supporting elements of the OT environment. Instead support is provided via remote sessions which directly connect to the OT environment without logging enabled.

Whilst acknowledging the gap around privileged access logging for a limited number of OT systems, John feels the Management Characteristics are met and the practice is therefore “Largely Implemented”. However as the organisation exhibits the Anti-Pattern he must revise his assessment down to “Partially Implemented”.

ID	Practice	MIL	Self Assessment Response	Notes
SA-1B	**Logging requirements have been defined for all assets important to the function (e.g., scope of activity and coverage of assets, cybersecurity requirements [confidentiality, integrity, availability])** **Anti-Pattern :** Third party vendors or services have privileged access that is not logged. **Context & Guidance :** Has the organisation defined specific requirements for systems and devices that support the organisation's critical business functions to generate Security event logs? Such requirements may be documented in a Security Logging & Monitoring Standard, and should specify: - The type of events that are required to be logged for each type of system/device; - The information to be captured in event logs; - Requirements for aggregating and protecting event logs from unauthorised access, modification and deletion. less...	MIL-2	Partially Implemented	All logging is configured in accordance with an established log management standard. Operational logging requirements (events and logging verbosity) have been defined for all assets. Privileged activities for some environments are only logged via a privileged session management tool which is not used by the third party vendor supporting elements of the OT environment. All logs are piped directly to the SIEM.

Assessment Scoring Model - Worked Example 2 (Cont.)

AESCSF Practice:

SA-1B "Logging requirements have been defined for all assets important to the function (e.g., scope of activity and coverage of assets, cybersecurity requirements [confidentiality, integrity, availability])

Anti-Pattern: "Third party vendors or services have privileged access that is not logged."

Anti-Pattern Assessment:

John now proceeds to the Anti-Pattern assessment tab. Recognising the organisation exhibits the SA-1B Anti-Pattern, John documents that "Yes" the Anti-Pattern is present. He then proceeds to consider the reasons why, and reflects that:

- the security team has been trying to mandate all privileged access be via the privileged session management tool to enhance controls, include logging capabilities.
- the third party vendor does not operate a support model, and requires utilities, that are not compatible with the use of the privileged session management tool.
- the vendors will only move to the required support model and upgrade the utilities to ensure compatibility if changes are made to the support contract (Other Dependencies Inhibitor).
- management are supportive of the move to enhance controls but are reluctant to make the contractual changes given the limited number of systems, reducing risk exposure well below other security uplift priorities (Competing Priorities Inhibitor).
- additionally, there is a shortage of people in the market with the required skills should the vendor seek to implement the changes required (Skill Shortage Inhibitor).

Situational Awareness - Anti-Pattern

Anti-Patterns	ID	Practice	MIL	Anti-Pattern Present	Funding	Skills Shortage	Headcount	Management Support	Competing Priorities	Other Dependencies	Notes
Third party vendors or services have privileged access that is not logged.	SA-1B	Logging requirements have been defined for all assets important to the function (e.g., scope of activity and coverage of assets, Cyber Security requirements [confidentiality, integrity, availability])	MIL-2	Yes	☐	☑	☐	☐	☑	☑	Dependent on changes to vendor support contract. Uplift has been de-prioritised due to limited number of systems exposed. Remediation requires additional in-house skills which are not currently available.

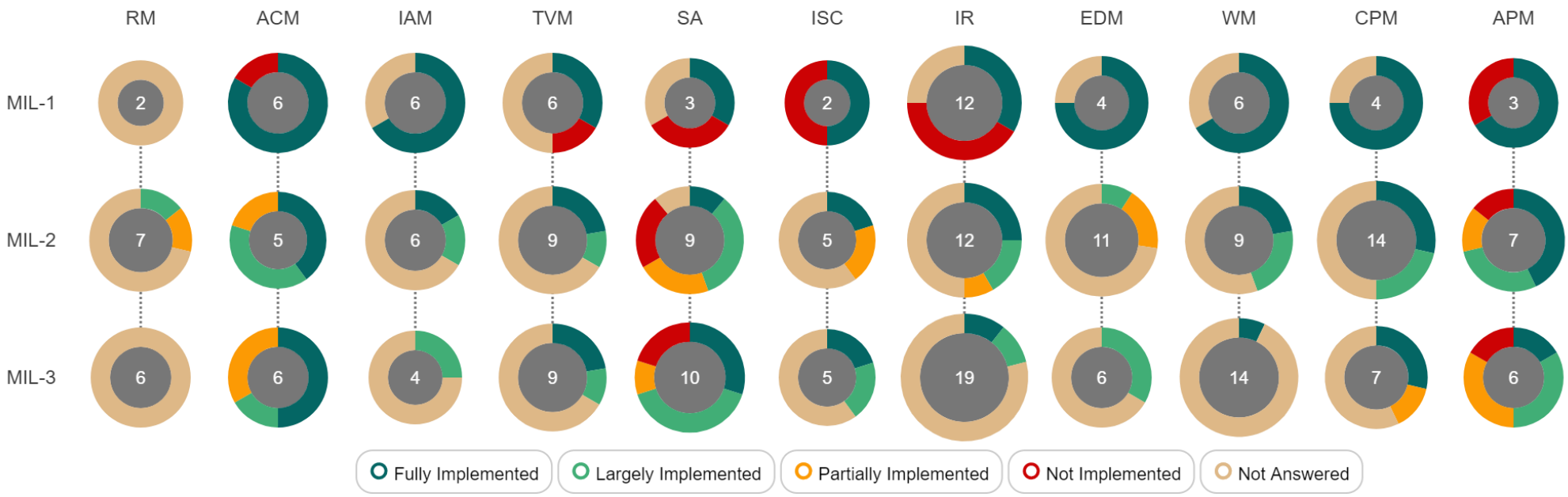
Assessment Outcomes & Next Steps

6

Overview of Assessment Results & Reporting

Below is an example of the live Summary of Results by Domain you will be able to extract from Datapoint.

Summary of Results by Domain



- The results show 11 domains 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 organisations must complete all of the practices in a given MIL as well a all practices from predecessor MIL(s) in order to consider it complete.
- Organisation’s will have the ability to export chart above and a .csv file of responses including notes.
- Energy participant results will be de-identified and aggregated to report to the Energy Security Board by EOCY 2018

Next Steps & Support

The next steps for energy market participants are:

1. Complete the AESCSF Toolkit

2. Submit your completed AESCSF assessment by ***16th November 2018.*** This will need to be accompanied by your CEO's attestation response letter. The CEO's attestation response letter template can be downloaded from AESCSF 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**
For any Datapoint website related queries, please email **datapoint@au.pwc.com**

Alternatively, you can call us on **1800 982 125**
*If you require assistance with the AESCSF Toolkit (Datapoint), 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.***

Australian Government
Australian Signals Directorate

ACSC
Australian Cyber Security Centre

AEMO
AUSTRALIAN ENERGY MARKET OPERATOR

National Energy Cyber Security Readiness and Resilience Program in 2019

including a

National Energy Cyber Security Exercise (GridEx V) in November 2019

for

Australia's energy sector

Program and GridEx V Overview, October 2018

Program and GridEx V Overview

Overarching Aim

- To **build and propagate a best practice approach** for the energy sector to **prevent, detect, respond and recover** from cyber security incidents, and to **strengthen response and recovery arrangements at a jurisdictional and national level** to effect a coordinated and swift management of incidents to reduce impacts and maintain community confidence.

National Energy Cyber Security Readiness and Resilience Program in 2019

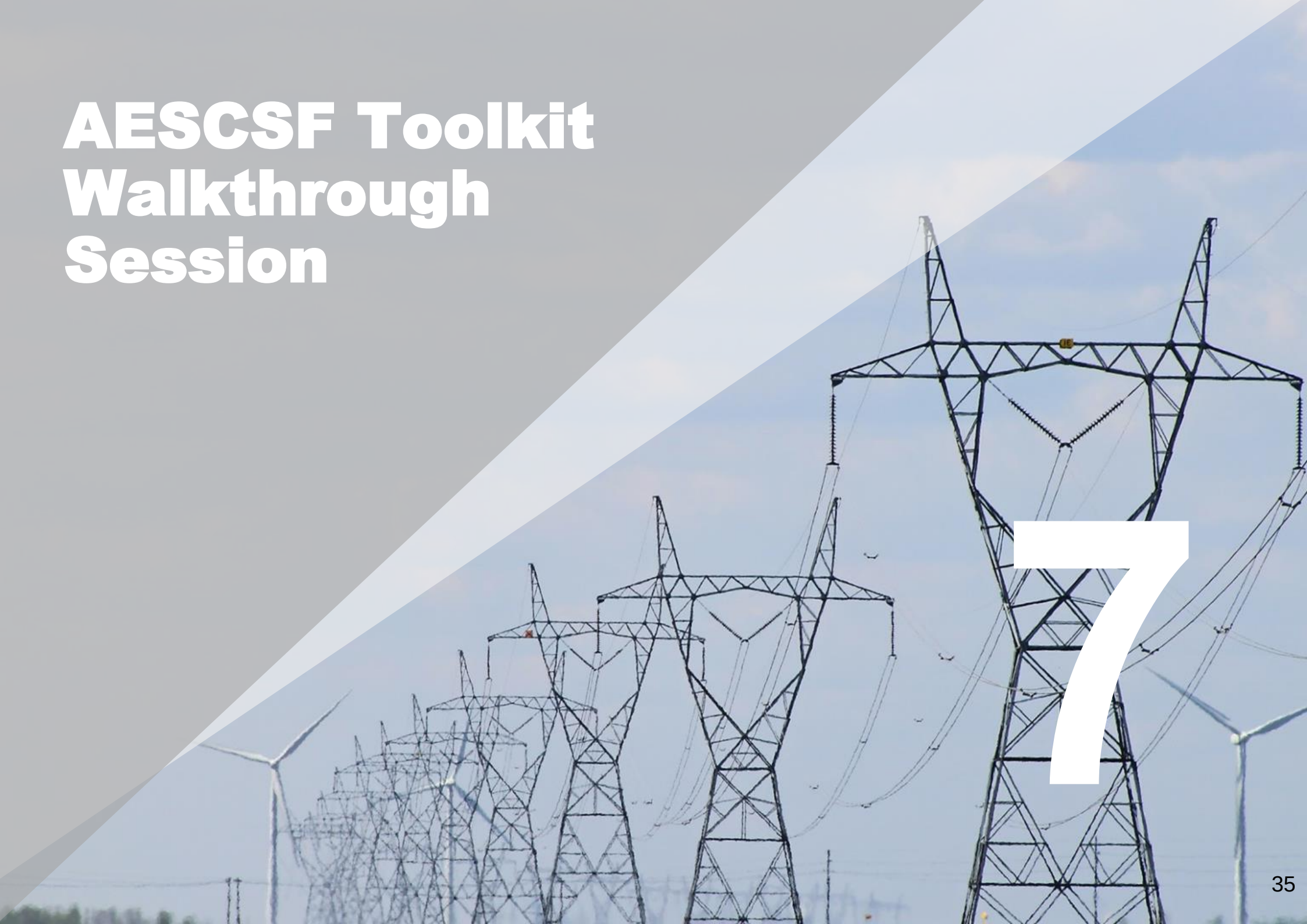
- Program to be designed by an industry and government working group
- All Australian energy sector and applicable government agencies invited to participate
  - Whole energy supply chain
- Series of activities between January to October 2019
  - Information sharing sessions on threats, vulnerabilities and mitigations
  - Workshops to develop new protocols
  - Smaller exercises to practise protocols
  - Workshops to learn how to design, conduct and evaluate functional exercises (e.g. writing Master Schedule of Events – MSEs)

National Energy Cyber Security Exercise (GridEx V) in November 2019

- 2 day functional exercise
  - All Australian energy sector and applicable government agencies invited to participate
  - Organisations to design own MSEs from a central MSE
- 1 day Executive Tabletop
  - Limited to a smaller number of participants

More information coming soon

AESCSF Toolkit Walkthrough Session



7

AESCSF Toolkit (Datapoint) - Security Overview

Recognising the sensitivity of the data being collected via this project, data security is at the core of the tools and methodology used to developed the AESCSF.

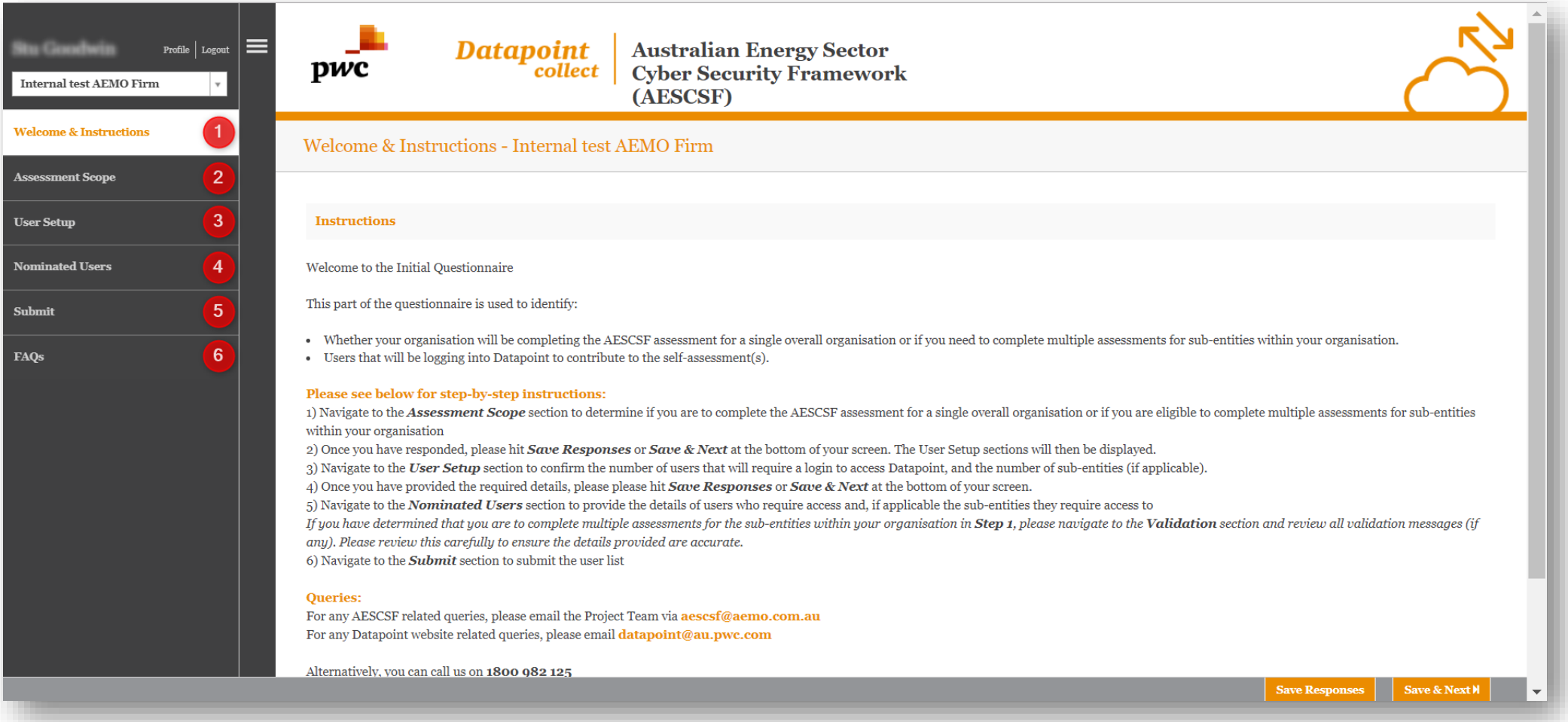
The security of the tools been used to collect, analyse, and report on assessment results has been reviewed by members of the CSIWG and AEMO.

A security statement is available upon request, should you wish to understand the nature of the security controls in place.

Any data used to facilitate industry benchmarking will be de-identified and controls exist with Datapoint to restrict the ability to filter benchmarking data such that it may allow an entities data to be derived.

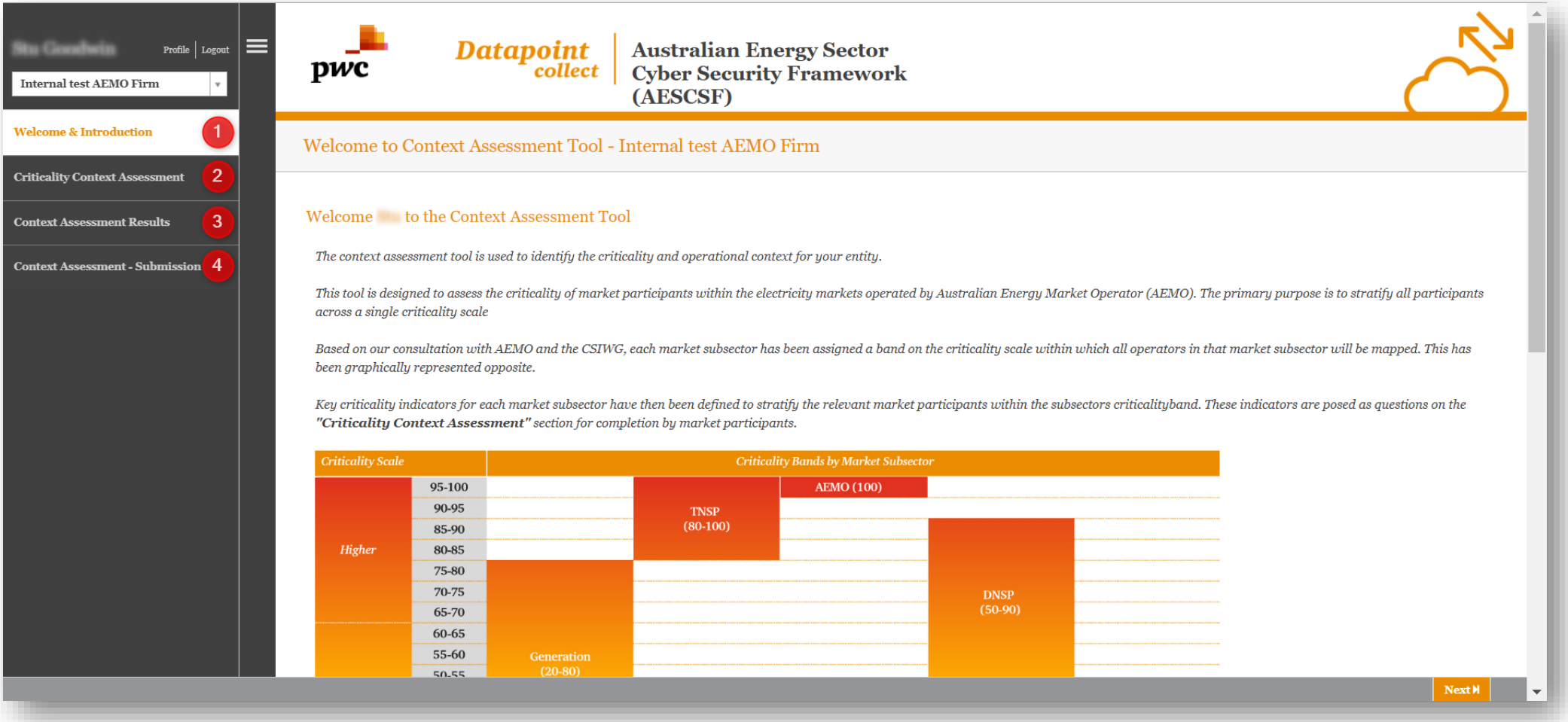
The AESCSF Toolkit is hosted in Australia and all development and support team members are also located in Australia. This includes all application, database and operating system administration activities.

AESCSF Toolkit (Datapoint) - Initial Questionnaire



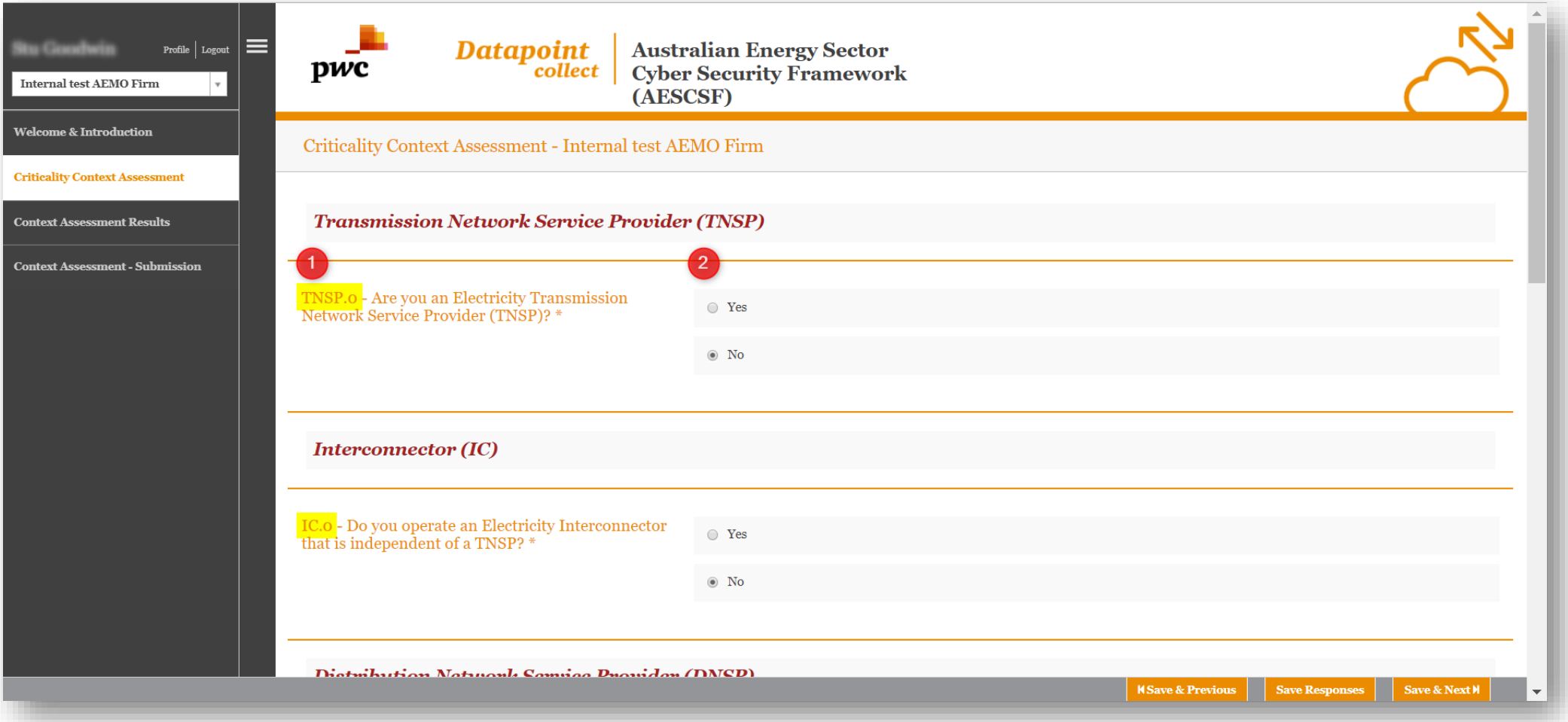
1	This tab takes you to an overview of the **Initial Scoping** activity. Contact information for the Datapoint & AESCSF teams lives here.	3	This tab takes you to the **User Setup** activity. Here you will select whether you will be the only user of Datapoint, or more are required.	5	This tab takes you to the **Submit** activity. Here you confirm and submit the information entered on the previous tabs.
2	This tab takes you to the **Assessment Scope** activity. Here you will select how you intend to complete the Framework Assessment.	4	This tab takes you to the **Nominated Users** activity. **Note:** this tab appears only when multiple users are selected in **User Setup**	6	This tab takes you to the **Frequently Asked Questions (FAQ)**. Here you can find guidance on common Datapoint questions.

AESCSF Toolkit (Datapoint) - Criticality Assessment Tool



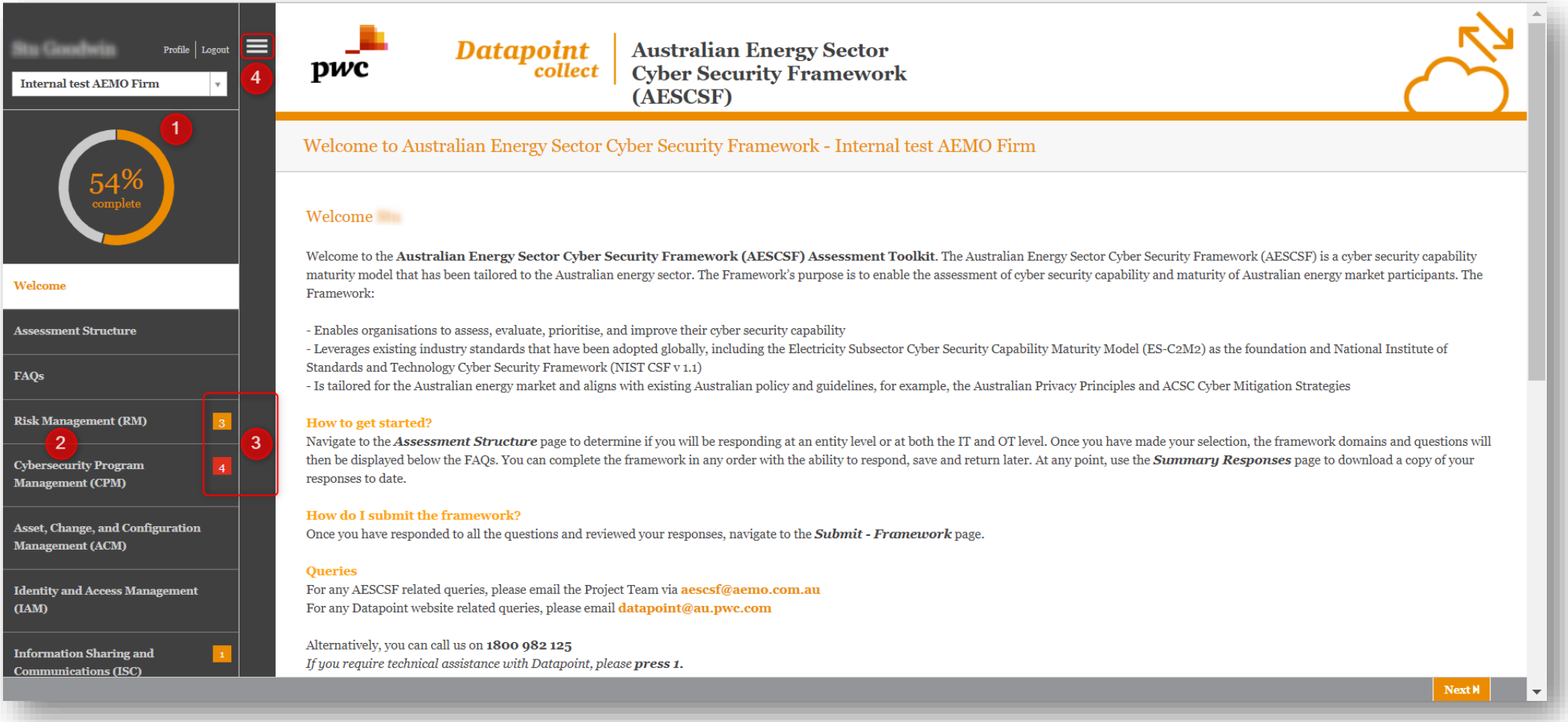
1	This tab takes you to an overview of the **Criticality Assessment Tool**. Here you will find the Criticality Bands by Market Subsector.	**3**	This tab takes you to the **Results** of your Criticality Assessment. Here you will find a breakdown of your criticality by market subsector.
2	This tab takes you to the **Criticality Assessment Tool** questionnaire. Here you will find the questions that assess your market criticality.	**4**	This tab takes you to the **Submit** activity. Here you confirm and submit the information entered on the previous tabs.

AESCSF Toolkit (Datapoint) - Criticality Assessment Tool



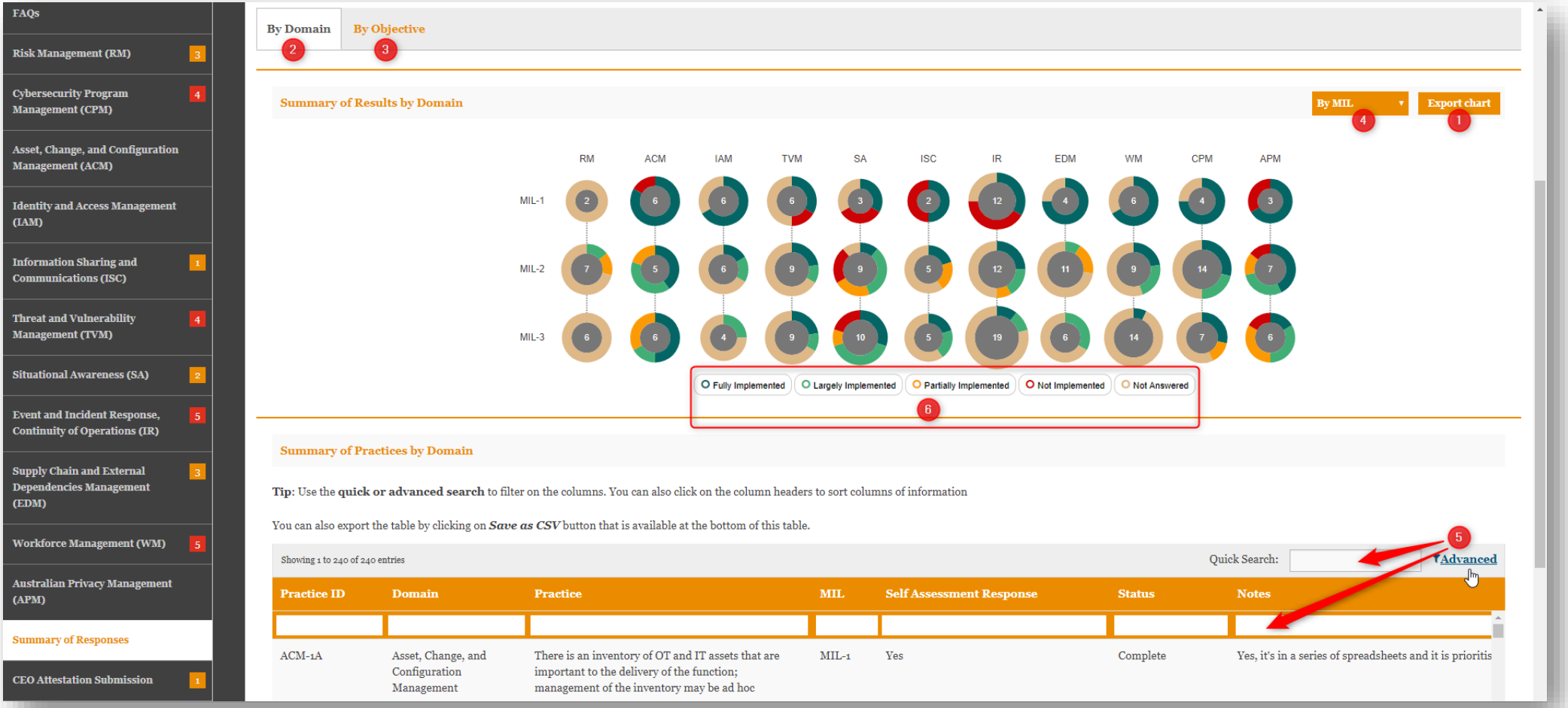
1	This section contains the **Criticality Assessment question**. Each question has a unique identifier to make it distinct, as some questions are similar.
2	This section contains the response options for the question in **Section 1**.

AESCSF Toolkit (Datapoint) - Framework Assessment



1	This donut shows your completion of responses within the assessment.	3	Areas of the assessment that have no response are highlighted like this (e.g. Risk Management requires 3 additional responses).
2	Each domain within the framework has a tab in the left-hand menu bar (e.g. Risk Management).	4	This button hides and shows the left-hand menu bar.

AESCSF Toolkit (Datapoint) - Summary of Responses



1	Use the **Export Chart** button to save an image of the current summary results view. **Note:** selected areas of the chart are shown in the saved image.	3	Use this tab to show the **Summary of Results by Objective.**	5	Toggle the **Advanced** option to search and filter responses in the table. A text box will appear before the first row allowing text to be searched.
2	Use this tab to show the **Summary of Results by Domain**.	4	Use this drop down menu to change the Summary of Results by Domain from a **standalone score** to a **cumulative score** of MIL.	6	Use these buttons to change the **Summary of Results by Domain** view. Click once to show as a percentage, and again to show the count.

Thank you