Australian Energy Sector Cyber Security Framework (AESCSF)

Framework Overview

Version 2020-21 (Revision 1)

Important Notice

Purpose

This document is made available by The Department of Industry, Science, Energy and Resources (DISER) and The Australian Energy Market Operator (AEMO) to provide information about the 2020-21 Australian Energy Sector Cyber Security Framework (AESCSF) Program.

This document accompanies other general guidance materials made available to Australian energy market Participants in the electricity and gas sub-sectors.

Disclaimer

This document or the information in it may be subsequently updated or amended. This document does not constitute legal or business advice and should not be relied on as a substitute for obtaining detailed advice about any applicable laws, procedures, or policies. DISER has made every effort to ensure the quality of the information in this document but cannot guarantee its accuracy or completeness.

This document might contain information which is provided for explanatory purposes and/or provided by third parties. This information is included “as is” and may not be free from errors or omissions. You should verify and check the accuracy, completeness, reliability, and suitability of this information for any intended use you intend to put it to and seek independent expert advice before using it.

Accordingly, to the maximum extent permitted by law, DISER and its employees and other contributors involved in the preparation of this document:

- Make no representation or warranty, express or implied, as to the currency, accuracy, reliability, or completeness of the information in this document, and;
- Are not liable (whether by reason of negligence or otherwise) for any statements or representations or any omissions from it, or for any use or reliance on the information in it.

Conventions used in this document

For clarity when reading this document, key terms are indicated with a capital letter. Each key term has a specific definition that the reader should consider. An example of this is Participants, as defined above.

Key terms are defined centrally in the AESCSF Glossary which is available separately.

AES | CSF
Australian Energy Sector | Cyber Security Framework

Table of Contents

1. Introduction to the Australian Energy Sector Cyber Security Framework

1.1. Summary

The AESCSF (herein referred to as the Framework) is a cyber security framework that has been developed and tailored to the Australian energy sector. The Framework's purpose is to enable Participants to assess, evaluate, prioritise, and improve their cyber security capability and maturity.

The Framework:

- has been established to address increasing cyber security risks faced by the Australian energy sector, and in response to recommendation 2.10 from the 2017 *Independent Review into the Future Security of the National Electricity Market* [1];
- has been developed through collaboration by industry and government stakeholders, including the:
    - The Australian Energy Market Operator (AEMO);
    - Department of Industry, Science, Energy and Resources (DISER);
    - Australian Cyber Security Centre (ACSC);
    - The Department of Home Affairs (DHA);
    - Critical Infrastructure Centre (CIC); and
    - Cyber Security Industry Working Group (CSIWG)[1].
- leverages existing industry standards that have been adopted internationally, including the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) (version 1.1) [2] and National Institute of Standards and Technology (NIST) Cybersecurity Framework (NIST CSF) (version 1.1) [3], and;
- is tailored for the Australian energy sector to align with existing Australian policy and guidelines, for example, the Australian Privacy Principles and ACSC Essential Eight Strategies to Mitigate Cyber Security Incidents.

The Framework was established in 2018, revised in 2019, and has undergone a review and refresh in this version (version 2020-21). There are no significant changes in version 2020-21 compared to version 2019b. Through the continued collaboration between the above parties, the Framework will continue to evolve – maintaining its relevance to the evolving cyber security threat landscape and the challenges faced by the Australian energy sector.

[1] The CSIWG includes cyber security representatives from Australian energy organisations

1.2. Responding to the challenge of securing the Australian energy sector

In recent years, the security and reliability of the Australian energy sector has fallen under increasing attention due to sophisticated cyber-attacks against critical infrastructure in several global jurisdictions. The consequence of these attacks in Australia may not only impact energy organisations, but have broader impacts to society, public health and safety, and our nation's economy.

The Framework provides a foundation for Participants to assess their current state cyber security capability and maturity in a standardised manner. It empowers Participants to make informed decisions regarding the steps that they need to take to become resilient in the face of a cyber-attack.

1.3. Structure of the Framework

The Framework includes two key components, including:

- a criticality assessment; and
- a cyber security capability and maturity self-assessment.

1.3.1. The Criticality Assessment Tool

The criticality assessment is conducted through the Criticality Assessment Tool (CAT). The purpose of the assessment tool is to determine the criticality of each Participant relative to their peers.

The CAT has two versions, one each for the electricity and gas sub-sectors respectively:

1. The Electricity CAT (E-CAT) is tailored to assess the following supply chain roles:
    - Generation (E-GEN);
    - Transmission (E-TNSP);
    - Independent Interconnectors (E-IC);
    - Distribution (E-DNSP);
    - Retail (E-RET), and;
    - Market Operations (E-OPS).
2. The Gas CAT (G-CAT) is tailored to assess the following supply chain roles:
    - Production (G-PROD);
    - Transmission (G-TNSP);
    - Bulk Storage (G-STOR);
    - Distribution (G-DNSP);
    - Retail (G-RET), and;
    - Market Operations (G-OPS).

Both the E-CAT and the G-CAT, consider the key attributes of an organisation to determine a criticality rating for each sub-sector.

Overall criticality is determined by taking the highest sub-sector criticality ranking.

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.

1.3.2. Self-assessment

The cyber security capability and maturity self-assessment has been designed to be relevant to all Participants, regardless of their market sub-sector.

The cyber security capability and maturity self-assessment has been adapted into two versions, each with a different use case. These are:

- a Full self-assessment, and;
- a Lite self-assessment.

A Full self-assessment covers all 282 Practices and Anti-Patterns within the Framework. A Lite self-assessment consists of 29 multi-select, easy-to-follow questions. The scope of the Lite self-assessment is intentionally limited to focus on Target State maturity guidance from the ACSC for Low criticality Electricity Participants.

Unless otherwise agreed with the AESCSF Project Team (aescsf@aemo.com.au), a Lite self-assessment should only be completed by Participants who:

- are assessed as Low criticality through the E-CAT or G-CAT, or;
- have extremely limited resources and are completing their first self-assessment in the 2020-21 Program.

Participants with an overall criticality of Medium or High (as per the E-CAT or G-CAT) should complete a Full self-assessment which facilitates comparison of maturity guidance from the ACSC for Participants at all levels of criticality.

PLEASE NOTE

No Participant is restricted from completing a Full self-assessment.

The Framework could be used by any organisation wanting to assess their cyber security maturity and capability; however, it is particularly relevant to those who operate critical infrastructure or operational (OT) assets. Non-energy organisations may not find the CAT relevant as it is based on criteria that are specific to the electricity and gas sub-sectors.

1.3.3. Alignment to the ES-C2M2

The ES-C2M2 was developed in 2012 by the United States Department of Energy [2]. It is a well-established and globally adopted maturity model that empowers energy organisations to assess their cyber security capability and maturity. It covers both IT and OT, and aligns to the NIST CSF [3] (which has cross-sector applicability).

The CSIWG adopted the ES-C2M2 as the foundation for the Framework to ensure that the Australian energy sector remained globally adept, and aligned with best practice.

The Framework has retained the core structure of the ES-C2M2, with the following revisions made in 2018 and 2019:

- A new Domain has been added. This Domain encompasses Australian Privacy Management (APM) concepts (such as managing personal information through its lifecycle) in a manner that is consistent with Australian Privacy Principles and the Office of the Australian Information Commissioner, Privacy Management Framework.
- The institutionalisation of Practices is no longer assessed within a dedicated objective. Management characteristics have been re-integrated, and now explicitly guide self-assessment of Practice implementation.
- Practices that are contained within Maturity Indicator Level 1 (refer to Section 1.4 below) are no longer assessed using a scale of Not, Partially, Largely, and Fully Implemented. The ad-hoc manner in which these Practices may occur supports a simplified scale of Yes and No.
- Integration of Anti-Patterns (refer to Section 1.3.4 below).
- Integration of context and guidance statements for Practices and Anti-Patters (refer to Section 1.3.5 below).
- Integration of Informative References that link the Framework to other sources of good practice (refer to Section 1.3.6 below).

1.3.4. Anti-Patterns

Specific indicators of bad practice were defined during the development of the Framework. These are referred to as Anti-Patterns, and they are assessed similarly to Practices.

Most Domains contain a dedicated Objective that consists of Anti-Patterns. Each Anti-Pattern is assessed as either:

- present; or
- not present.

Where an Anti-Pattern is present, it prevents the Participant from achieving the associated maturity measure (refer to Section 1.4 for more information).

1.3.5. Context and Guidance

Accompanying each Practice and Anti-Pattern is additional context and guidance to drive consistency, clarity, and a shared understanding across the energy sector. The context and guidance:

- can support facilitators who are less familiar with Practice statements;
- establishes a consistent view of the Practice or Anti-Pattern intent, and;
- can support Participants who are completing a self-assessment for the first time.

1.3.6. Informative References and Controls

The Framework is focussed on cyber security maturity and is therefore not prescriptive in relation to security controls. It describes *what* your organisation should strive to achieve, but not *how* they should achieve it.

However, to support organisations seeking control suggestions or recommendation, the Framework has a selection of Australian and global informative references mapped to each Practice. These informative references include:

- the ACSC Essential Eight;
- specific controls from the Australian Government Information Security Manual (ISM);
- the Australian Privacy Principles (APPs);
- the NIST Cybersecurity Framework (version 1.1) (NIST CSF 1.1);
- Control Objectives for Information and Related Technology (COBIT) Revision 5;
- Centre for Internet Security Critical Security Controls (CIS CSC) Version 7.1;
- NIST Special Publication 800-53 (NIST SP 800-53) Revision 5;
- NIST Special Publication 800-150 (NIST SP 800-150);
- Industrial Automation and Control System Security (ISA) 99 (ISA 99) also known as International Electrotechnical Commission (IEC) 62443 series, and;
- International Organisation for Standardisation (ISO) 27001:2013.

PLEASE NOTE

The informative references integrated into the Framework are not intended to be self-assessed – they are sources of guidance and further information, not mandatory requirements.

1.4. Measuring cyber security capability and maturity

There are two measures for cyber security capability and maturity in the Framework. They are:

- Maturity Indicator Level (MIL), and;
- Security Profile (SP).

1.4.1. Maturity Indicator Level

The Framework leverages the MILs established within the ES-C2M2 [2]. An overview of how the MIL measure is used within Framework is detailed below.

There are four MILs, MIL-0 through MIL-3, that apply across all the Domains in the Framework. MIL-0 through MIL-3 define the maturity progression in the Framework. Each Practice and Anti-Pattern has been assigned a MIL that indicates its maturity relative to other Practices.

The following concepts are important in understanding and correctly applying the Framework:

- The MILs apply independently to each Domain. As a result, a Participant using the Framework may receive different MIL ratings for different Domains. For example, a Participant could be functioning at MIL-1 in one Domain, MIL-2 in another Domain, and MIL-3 in a third Domain. The overall MIL achieved is the lowest MIL achieved across all Domains.
- The MILs are cumulative within each Domain; to earn a MIL in a given Domain, an organisation must perform all of the Practices, and not exhibit any of the Anti-Patterns, in that MIL and any preceding MILs. For example, a Participant must perform all of the Practices, and not exhibit any of the Anti-Patterns, in that Domain at MIL-1 and MIL-2 to achieve MIL-2 in the Domain. Similarly, the Participant would have to perform all Practices, and not exhibit any of the Anti-Patterns, in MIL-1, MIL-2, and MIL-3 to achieve MIL-3.

1.4.2. Security Profile

In addition to the MIL, the Framework has three alternate groupings of Practices referred to as Security Profiles (SPs). The SPs have been defined by the ACSC, in consultation with AEMO and the CSIWG, as a measure of target state maturity. They also respond to the current threat landscape. The target state maturity SP that a Participant in the electricity sub-sector[2] should achieve is determined based on their overall criticality result (per the E-CAT).

The Practices and Anti-Patterns grouped within the SPs are at differing MILs. This has been done deliberately to target higher levels of maturity across certain cyber security activities and behaviours.

PLEASE NOTE

Unlike MILs, SPs cannot be applied independently to each Domain. To achieve an SP, Participants must be performing all the Practices, and not exhibiting any of the Anti-Patterns within that SP, and any preceding SPs, across all Domains.

The cumulative nature of MILs continues to apply to SPs (i.e., SP-2 can only be achieved if SP-1 is also achieved).

[2] Guidance for Participants in the gas sub-sector has not been determined as of this writing.

1.5. Identifying and achieving a target state maturity

SPs introduce a flexible mechanism that can be used to drive uplift in targeted cyber security activities and behaviours, to address evolving threats. For example, if greater maturity around situation awareness is required to respond to an evolving threat landscape, Practices at higher MILs can be moved into lower SPs to drive this uplift. As such, the target state maturity SPs should be expected to evolve over time.

Table 1 indicates which SP an organisation in the electricity sub-sector should achieve based on their criticality (as determined by the E-CAT).

Security Profile (SP)	Participant criticality	Practices and anti-patterns			Total required to achieve SP
		MIL-1	MIL-2	MIL-3	
Security Profile 1 (SP-1)	Low	57	27	4	88
Security Profile 2 (SP-2)	Medium	2	92	18	200 (112+88 from SP1)
Security Profile 3 (SP-3)	High	0	0	82	282 (82+200 from SP2)

Table 1: Target State Maturity and Security Profiles

To assist organisations in defining roadmaps to uplift maturity and reach their target state, the ACSC included guidance on “Priority Practices” within each SP. It is recommended that the Priority Practices be completed first as part of any uplift program.

Refer to Appendix 3.1 for the list of Priority Practices within each SP.

1.6. Framework Change Management

The U.S. DOE released a draft of the ES-C2M2 version 2.0 on 14 August 2019 seeking comments and information from the public.

As of the 2020-21 Program, the ES-C2M2 version 2.0 remains in draft.

The AESCSF Project team, in consultation with the CSIWG and other stakeholders, will agree on the integration process for ES-C2M2 version 2.0 as part of a future AESCSF program, where appropriate.

To address Participant feedback from prior programs, and to accommodate the expansion to additional grids and markets, some changes were made to the Framework and supporting artefacts in the 2020-21 Program. Refer to Appendix 3.2 for a register of changes made.

2. 2020-21 Self-Assessment Program

This section has been structured in a question-and-answer style in order to provide responses to common questions related to the 2020-21 Self-Assessment Program.

2.1. Preparing for a Framework Self-Assessment

2.1.1. Is completing a Framework self-assessment mandatory?

The Framework self-assessment is **not** mandatory; however, it is considered a critical input into the establishment of a sector-wide understanding of current state cyber security capability and maturity. Consistent with the 2018 and 2019 Programs, DISER will draw insights from self-assessments to issue a report to the Energy Ministers' Meeting (EMM) in the second half of 2021 (herein referred to as the EMM Report).

It is expected that the Program will continue to operate on an annual cycle.

PLEASE NOTE

Participants who do not complete and submit their Framework self-assessment by the deadline will not have their aggregated and de-identified data included in the EMM Report. Additionally, no access to the industry benchmarking portal will be provided to these Participants.

2.1.2. Can my organisation complete a Framework self-assessment if they are not a Participant?

Any Australian energy organisation that is outside of the scope (see How should I determine the scope of my Framework self-assessment? below) is encouraged to complete a self-assessment to evaluate and improve their cyber security capability and maturity; however, these results will not be included in the EMM Report.

2.1.3. Are previous ES-C2M2 assessment results comparable to the Framework?

Whilst not directly comparable, each result set can be similarly explored. The score that accompanies your Framework self-assessment is specific to the AESCSF; however, if your organisation would like to compare this score to previous ES-C2M2 results, please contact the AESCSF Project Team (aescsf@aemo.com.au).

2.1.4. How do I access the Framework self-assessment toolkit?

Program contacts (e.g., CEO, Managing Director, Cyber Security) will receive a welcome email containing registration and login details prior to the commencement of the 2020-21 self-assessment period. If you are expecting access to the toolkit and have not received the welcome email, please contact the AESCSF Project Team (aescsf@aemo.com.au).

2.1.5. How long does it take to complete a Framework self-assessment?

Full self-assessment: Depending on the size of your organisation and the number of stakeholders required, an assessment could take anywhere from a few hours to a few days. The time it takes to complete all responses in the tool is minimal - the greater investment of effort is collecting the necessary information and resources to undertake the assessment.

Lite self-assessment: The length of time required to complete the assessment will vary - if responses to all questions are known, the survey can be filled in around 15-20 minutes. However, some clarification with specialists and outsourced providers may be required to answer the questions accurately, in which case the total time to complete the assessment will increase.

2.1.6. How should I determine the scope of my Framework self-assessment?

The scope of Framework self-assessments should be determined based on the following principles:

- Framework self-assessments should be completed by the ultimate Australian legal entity (Parent Company) that controls Participants in the electricity or gas sub-sector.
- The Parent Company should complete a single Framework self-assessment, including in scope the operations of all controlled Participants, unless each of the following apply:
    - there exists no common in-house network infrastructure
    - there is no inter-network integration and (or) connectivity
    - there are no common parties responsible for the management of IT and OT.
- If operations and maintenance are performed by a third party (e.g., an operations and maintenance (O&M) Provider), the Parent Company must either:
    - integrate information from the O&M Provider into their assessment, or;
    - exclude the relevant assets from scope and ensure the O&M Provider completes a Framework self-assessment on their behalf for those assets.

Where a Participant:

- has the trading rights to the output from an electricity generation asset or gas processing facility, but does not own and/or operate the asset, the Participant must notify the relevant O&M Provider of the need to complete an AESCSF self-assessment for that facility/asset. Additionally, the Participant must also advise the AESCSF Project Team (aescsf@aemo.com.au).
- is an O&M Provider, and also a Participant in their own right; they should engage with each Parent Company who has outsourced to them, to ensure clear agreement on scoping according to the above principles.
- is an electricity generator, they must ensure that the scope of their self-assessment considers operations as far down the supply chain for an asset as they reasonably control.

Where a Parent Company:

- controls Participants in both the electricity and gas sub-sectors, that Parent Company will be required to complete two separate self-assessments; one for electricity, and one for gas.
- controls and operates a gas pipeline as well as a facility that feeds a gas fired power generator (that they also control and operate), the gas self-assessment should consider all operations up to the gas feed into the electricity generator. Additionally:
    - operations related to the electricity generator itself should be considered as part of the electricity self-assessment.

PLEASE NOTE

The scoping principles above must be considered in conjunction with, and defer to, any licencing requirements, particularly those related to ring fencing requirements as determined by the Australian Energy Regulator (AER).

Where unique circumstances exist that prevent scoping per the above guidance, please engage directly with the AESCSF Project Team (aescsf@aemo.com.au) to clarify and agree an alternative scoping approach.

The agreed scope is to be applied when completing all areas of the Framework self-assessment.

2.2. Framework Self-Assessment

2.2.1. Can I transition from a Lite Framework self-assessment to a Full Framework self-assessment?

If a Lite Framework self-assessment is completed, the toolkit will transpose responses into a Full self-assessment to enable benchmarking. This process will not be visible to Participants, but will enable transition to Full self-assessments in subsequent years. There is no automated capability to transpose a Full self-assessment to a Lite self-assessment.

If you completed the Full Framework self-assessment in 2019, it is recommended that your organisation continue to complete the Full self-assessment each year to enable your organisation to get the full benefit of year-on-year result comparison and industry benchmarking.

2.2.2. Can separate Framework self-assessments be completed by asset if maturity varies greatly?

Self-assessments should be scoped according to the principles outlined in 2.1.6 above. We ask that self-assessments be completed considering all relevant assets and operations to ensure a comprehensive evaluation of cyber security capability across the organisation.

Whilst capability may be different across various energy assets (i.e., some have more mature security processes than others) the assessment needs to be performed by taking an aggregate view across these assets.

For example, if security logging and monitoring is performed on some assets but not others, this should be scored as 'Partially Implemented' or 'Largely Implemented' (depending on the extent of the gaps). Cyber-attacks will usually take advantage of the weakest security link, and therefore undertaking the assessment at an asset level could misrepresent the overall security posture of the organisation.

2.2.3. Does the assessment cover Operational Technology and Information Technology?

The Framework was developed to apply to energy organisations with Operational Technology (OT) assets as well as Information Technology (IT) assets. It is important to assess cyber security capability and maturity holistically, as an organisation's ability to secure and protect OT assets will often depend on processes maintained by personnel within IT functions.

2.2.4. Can I assess the maturity of Operational Technology and Information Technology separately?

If your organisation has OT assets, you will have the opportunity to assess maturity for OT and IT separately. Capturing your self-assessment with this additional level of granularity can help when utilising results to plan and prioritise remediation and uplift efforts.

2.2.5. How is my organisation's overall maturity determined if Operational Technology and Information Technology are assessed separately?

The toolkit will consider the lowest level of maturity in any area (regardless of whether that is OT or IT) when aggregating your organisation's overall score. For example, if IT was rated as 'Largely Implemented' and OT was rated 'Partially Implemented', the toolkit will take the lower level of implementation, 'Partially Implemented', as the aggregated score for that Practice. This approach is driven by the nature of cyber threats, which will usually take advantage of the weakest security link to achieve their objective.

2.2.6. Who should be involved in a Full Framework self-assessment?

The personnel required for a Framework self-assessment will vary based on the size and shape of a given organisation. Table 2 below details the personnel that should be involved, and may be adjusted to suit the roles that your organisation employs.

Function	Roles
Information and Communications Technology (ICT) or Information Technology (IT)	• Chief Information Security Officer (CISO) • Security Manager • Enterprise Architect • Security Architect • Operations Manager • Support Manager • Security Specialist
Operational Technology or Engineering	• Control Systems Engineer • SCADA Engineer • Substations (Field Engineering) • Telecommunications Engineer (where applicable) • Security Specialist
Shared Services	• Risk and Compliance Officer • Physical Security Manager • Buildings and Facilities Manager • Human Resources Manager • Vendor/Contract Manager • Legal Counsel • Privacy Officer • Personnel Security Manager • Training Coordinator • Emergency Manager

Table 2: Who should be involved in a Framework self-assessment

2.2.7. How do I assess practice implementation the Framework?

Please refer to the AESCSF Quick Reference Guide and Education and Training resources on the AEMO website.

2.2.8. Do I need to provide evidence for any Framework self-assessment responses?

It is expected that the self-assessment process will involve discussion with key stakeholders in your organisation as well as review of relevant documentation (e.g., policies, procedures, reports).

Within the AESCSF tool there are free-text fields where organisations can make references to key documents or artefacts that substantiate the assessment rating, i.e., referencing the name of a security policy or procedure document and its version number.

As of this writing, there is no requirement to upload any evidence/documentation.

2.2.9. What notes should I capture in the Framework self-assessment?

Below are some tips on the suggested type of notes you should capture against each practice within the assessment:

- Evidence which supports your response of the practice on IT/OT level or entity level;
- Details of particular assets which may require remediation;
- Areas of opportunity. We recommend flagging these using a consistent term (such as “GAP:”) which can then be for filtering by your organisation at the conclusion of the assessment to quickly identify areas of improvement required to uplift maturity ratings
- Presence of management characteristics, and;
- Why (or why not) a practice is important to your organisation’s cyber security capability.

Table 3 provides example responses for Identity and Access Management Practices:

MIL	Practice ID	Practice Description	IT Response	OT Response	Notes
Establish and Maintain Identities					
1	IAM-1A	Identities are provisioned, at least in an ad hoc manner, for personnel and other entities (e.g., services, devices) who require access to assets (note that this does not preclude shared identities)	Yes	Yes	Identity Management is present in multiple forms across entity. Identities are captured in SAP and Active Directory. Personnel have unique identifiable accounts.
….					
2	IAM-1F	Identities are deprovisioned within organisationally defined time thresholds when no longer required	Largely Implemented	Not Implemented	IT - time period has been defined in process e.g.: when personnel leaves business, identity is deactivated within 14 days. OT – GAP: No defined interval to reclaim physical keys. Identified as area of opportunity

Table 3: Example Responses for Framework Self-Assessment

2.2.10. What is the purpose of the results attestation?

A nominated contact (e.g., CEO, Managing Director, Executive) is required to attest to the accuracy and completeness of self-assessment results prior to final submission.

Attestation is **mandatory** and must be provided in the toolkit before final submission of a self-assessment is processed. The attestation process is guided and will take 5 - 10 minutes once logged-in.

Additional instructions on how to complete and submit the assessment can be found in the toolkit user guide.

2.2.11. How do I use the Informative References?

Once your organisation has identified cyber security capability and maturity gaps, they can refer to the Informative References (including the NIST CSF and Australian references) for guidance on how to remediate gaps and uplift capability.

Refer to Section 1.3.6 for a list of Informative References mapped into the Framework.

2.3. Self-Assessment Results

2.3.1. Who has access to my self-assessment and what will the results be used for?

Security has been established as a fundamental, and non-negotiable requirement for all tools used to collect and aggregate any Participant's self-assessment data.

The security of the toolkit has been reviewed by DISER, AEMO, and the CSIWG; and a security statement is available upon request, should a Participant or Parent Company wish to understand the security controls in place.

2.3.2. Can I obtain NIST CSF results from my Framework Self-Assessment?

Participants who complete a Full Framework self-assessment will have their results transposed into a score that is aligned to the categories and functions of the NIST CSF (version 1.1). The score is between 0 and 3.9, and is aligned to the Capability Maturity Model Integration (CMMI) established by the CMMI Institute [4].

Please refer to the Framework Core for mapping of NIST CSF (version 1.1) to Framework practices.

PLEASE NOTE

Whilst the Framework maps to the NIST CSF, there are subtle differences between the two frameworks regarding several areas of focus. If an organisation requires a comprehensive assessment of their capability and maturity that is aligned to the NIST CSF, it is recommended this is completed independently of any Full Framework self-assessment.

3. Appendices

3.1. Priority Practices[3]

Domain	Security Profile 1	Security Profile 2	Security Profile 3
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

Table 4: Priority Practices by Security Profile

[3] As at May 2021. Priority Practices are subject to change.

3.2. Changes made to the AESCSF

3.2.1. AESCSF Artefact Changes Log

The following changes have been incorporated into the Framework and its supporting artefacts:

Reference	AESCSF Artefact	Change Description
2019-1	Framework Core	Anti-Patterns detached from Practices and reintegrated into the Framework as line items (equivalent to Practices) under a new Anti-Pattern Objective within relevant Domains. This has resulted in the Anti-Pattern column being removed from the Framework Core. Anti-Patterns will now be assessed independently from Practices to reduce confusion.
2019-2	Framework Core	Context and Guidance developed for Anti-Patterns.
2019-3	Framework Core	Security Profiles integrated per guidance from the Australian Cyber Security Centre (ACSC).
2019-4	Framework Core	Australian References updated to • reflect deprecation of the ASD/ACSC Top 37 Strategies. • incorporate relevant controls from the Australian Government Information Security Manual (ISM).
2019-5	Framework Core	Informative References from the Center for Internet Security Critical Security Controls (CIS CSC) updated from version 6 to 7.1.

Reference	AESCSF Artefact	Change Description
2019-6	FAQ Document	Restructured document to overview the Framework using a narrative rather than question and answer format. Content duplicated in Education Workshop Pack and AESCSF Toolkit User Guide removed and referenced. Document retitled to “Framework and 2020-21 Assessment Overview Document”
2019-7	CAT	Revised wording of DNSP.3 and RET.3 from “How many Critical Customers does your entity serve?” to “How many Critical and Commercial Customers does your entity serve?”. Definition of Critical Customer and Commercial Customer clarified within Glossary. Change made to address feedback regarding how these terms were being interpreted differently by Participants.
2019-8	CAT	Context and Guidance developed for all questions.
2020-21-1	Framework Core	Minor revisions to informative references. Further detail is provided in the Framework Core version 2020-21
2020-21-2	CAT	Revision of the Criticality Assessment Tool (CAT) to specify its applicability to the electricity sub-sector. Document retitled to "Electricity Criticality Assessment Tool (E-CAT)" Addition of a Gas Criticality Assessment Tool (G-CAT) to support the inclusion of the gas sub-sector in the 2020-21 Program.

Reference	AESCSF Artefact	Change Description
2020-21-3	Glossary	Added new terms and definitions. Further detail is provided in the Glossary version 2020-21.
2020-21-4	Lite Framework	Minor graphical updates to Lite Framework document.
2020-21-5	Education Workshop Presentation	Revision of the Education Workshop Presentation to reflect the changes in this document.

Table 5: AESCSF Artefact Change Log

3.2.2. Changes to Practices, Anti-Patterns and Context and Guidance implemented in 2019

Reference	Content Changed	Change Description
IAM-2A	Practice Guidance	Updated to explicitly reference physical security considerations.
IAM-2C	Practice Guidance	Updated to explicitly reference physical security considerations.
CPM-AP3	Anti-Pattern	Anti-Pattern 'The organisation is unable to isolate critical Operational Technology systems from the Internet and still maintain continuity of operations.' has been deprecated due to duplicate intent with CPM-AP3: 'Critical assets cannot be isolated from non-critical assets in response to a cyber security threat or incident'.
SA-AP1	Anti-Pattern	Anti-Pattern 'Logging is only used to support operational performance monitoring and not Security monitoring.' has been deprecated due to duplicate intent with SA-AP1: 'Operational assets are monitored only for performance and not for cyber security events'.
IR-AP2	Anti-Pattern	The Anti-Pattern 'The organisation has not identified which assets support the delivery of critical functions.' has been deprecated due to duplicate intent with IR-AP2: 'Services and assets that support the delivery of critical functions have not been identified (IR-AP1)'.

Table 6: Practice and Anti-Pattern Change Log

3.3. Table of Figures

4. References

[1] A. Finkel, K. Moses, C. Munro, T. Effeney and M. O'Kane, "Independent Review into the Future Security of the National Electricity Market - Blueprint for the Future," Commonwealth of Australia, 2017.

[2] U.S. DOE, "ELECTRICITY SUBSECTOR CYBERSECURITY CAPABILITY MATURITY MODEL (ES-C2M2)," 2014. [Online]. Available: https://www.energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf.

[3] NIST, "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1," 16 April 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[4] CMMI Institute, "Introducing CMMI V2.0," 2019. [Online]. Available: https://cmmiinstitute.com/cmmi.