Australian Energy Sector Cyber Security Framework

Frequently Asked Questions

FINAL V1-0

October 2018

Contents

Acronyms and Abbreviations **2**

General and Background **3**

What is the scope of this FAQ? 3

What is the Australian Energy Sector Cyber Security Framework (AESCSF)? 3

Who developed the AESCSF? 3

Why is the AESCSF important for the Australian Energy sector? 3

Is this assessment mandatory for Australian energy market participants? 4

How is data protected? Who has access? How will the data be used? 4

How is the assessment tailored to each energy organisation? 4

What is the deadline for conducting the AESCSF self-assessment? 4

What happens if I miss the submission deadline of 16 November 2018? 5

Is this framework only for Australian energy organisations? 5

Should I complete a single assessment or multiple assessments for an organisation? 5

Why was the ES-C2M2 used as the foundation? 6

Are there any modifications to ES-C2M2 within the AESCSF? 6

Are C2M2 management practices assessed? 6

How does the AESCSF relate to controls frameworks and how do I align my security controls to the AESCSF? 6

What is the Context Assessment Tool (CAT)? 7

What is the AESCSF Australian Privacy Management domain? 7

Will the AESCSF be updated going forward? 8

Preparing for the AESCSF **9**

Which personnel/roles need to be involved in the assessment? 9

How long does it take to complete an assessment? 9

What electricity assets are in scope for the AESCSF assessment? 10

Is the assessment completed at an Asset or Whole of Entity level? 10

How have the Maturity Target States been determined? 10

Does the assessment cover OT and IT? 10

How is the score aggregated if I assess both IT and OT? 11

What are context guidance statements and how do I use them? 11

What are anti-patterns and how do I use them? 11

I am having issues accessing Datapoint, how can I get help? 11

Completing the AESCSF **12**

What does the AESCSF consist of? 12

How do I assess my organisation using the AESCSF? 12

Do I need to substantiate responses with evidence/artefacts for the self-assessment? 14

What notes should I capture in the assessment? 14

How do I submit my AESCSF assessment? 15

How do I submit my Context Assessment Tool (CAT)? 16

How do I use the NIST CSF controls and informative references? 16

What are the Australian references and how do I use them? 16

How is the score aggregated when assessing multiple assets? 17

Can I obtain a NIST CSF score from AESCSF? 18

Acronyms and Abbreviations

AESCSF	Australian Energy Sector Cyber Security Framework
ACSC	Australian Cyber Security Centre
AEMO	Australian Energy Market Operator
CAT	Critical Assessment Tool
CIC	Critical Infrastructure Centre
CSIWG	Cyber Security Industry Working Group
ES-C2M2	Electricity Subsector Cyber Security Capability Maturity Model
IT	Information Technology
MIL	Maturity Level Indicator
NEM	National Energy Market
NIST CSF	National Institute of Standards and Technology Cyber Security Framework
OT	Operational Technology
WEM	Wholesale Electricity Market

General and Background

What is the scope of this FAQ?

The Frequently Asked Questions (FAQ) have been developed as a supporting document for the Australian Energy Sector Cyber Security Framework (AESCSF). It covers both the purpose and use of the AESCSF for the assessment.

Detailed guidance on the related AESCSF Toolkit, and how to complete the assessment on Datapoint, is available from the Welcome and FAQ pages within the platform.

What is the Australian Energy Sector Cyber Security Framework (AESCSF)?

The AESCSF is a cyber security capability maturity model that has been developed and tailored to the Australian energy sector. The AESCSF's purpose is to enable the assessment of cyber security capability and maturity of Australian energy market participants.

The AESCSF:

- Enables organisations to assess, evaluate, prioritise, and improve their cyber security capability
- Leverages existing industry standards that have been adopted globally, including the ES-C2M2 as the foundation and NIST CSF v 1.1
- Is tailored for the Australian energy market and aligns with existing Australian policy and guidelines, for example, the Australian Privacy Principles and ACSC Strategies to Mitigate Cyber Security Incidents

Who developed the AESCSF?

To address increasing cyber risks, and in response to the Finkel Review recommendation 2.10, the AESCSF has been developed through the collaboration of a number of industry and government stakeholders, including the AEMO, ACSC, CIC, and CSIWG which includes representatives from Australian energy organisations. The first version of the AESCSF was established in 2018, and it will continue to evolve to maintain relevance to the evolving cyber security threat and energy security landscape within Australia.

Why is the AESCSF important for the Australian Energy sector?

In recent years the security and reliability of the 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 AESCSF provides a foundation for Australian energy market participants to assess their current state capability in a standardised manner, and enable participants to make informed decisions on the required steps to strengthen resilience against cyber-attacks.

Is this assessment mandatory for Australian energy market participants?

This assessment is not currently mandatory but is considered critical input into the establishment of a sector-wide understanding of current state cyber security capability. AEMO will draw on the data and insights from these assessments to issue a report to the Energy Security Board before the end of 2018.

The Energy Security Board is mandated by the Finkel Review Recommendation 2.10 to report the cyber security preparedness of the NEM.

How is data protected? Who has access? How will the data be used?

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.

The AESCSF project team will have access to all data collected for the purpose of reporting to the Energy Security Board as per Finkel Review Recommendation 2.10. 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.

How is the assessment tailored to each energy organisation?

There are two main components to the AESCSF: 1) the Context Assessment Tool (CAT), and 2) the AESCSF assessment. Both components are required to be completed by your organisation.

1) The CAT will be tailored to energy industry subsectors: generation, transmission, distribution, and retail and identifies the key attributes of an organisation to determine their overall criticality in the delivery of electricity to the Australian Energy Market.

2) The AESCSF assessment is designed to apply to all energy industry sub-sectors. The cyber security practices within the AESCSF are based on ES-C2M2, and are relevant to organisations of various types, structures and sizes. The AESCSF is accompanied by supporting artefacts to drive clarity and consistent understanding of the assessment.

What is the deadline for conducting the AESCSF self-assessment?

For the purpose of the 2018 report to the Energy Security Board, the response cut-off deadline for self-assessments is 16th November 2018.

What happens if I miss the submission deadline of 16 November 2018?

If you miss the submission deadline the data from your assessment will not be incorporated into the sector-wide report published to the ESB. Organisations can still use the assessment tool beyond this date for their internal purposes.

Is this framework only for Australian energy organisations?

Whilst designed for Australian energy organisations, the AESCSF is based on existing globally adopted standards such as the NIST CSF and ES-C2M2 that have broader applicability. The AESCSF could be used by any organisation wishing to assess their cyber security maturity capability, particularly those who operate critical infrastructure or OT environments. For non-energy organisations, the CAT may not be relevant as this is based on criteria specific to the energy sector.

Should I complete a single assessment or multiple assessments for an organisation?

In most cases, only one assessment is to be completed per entity as the AESCSF assessment considers all assets that are critical to your operations. Example include infrastructure required for the generation, transmission, and distribution of electricity, and other related infrastructure you control such as mine sites or gas pipelines.

If your entity meets the criteria below, please complete multiple assessments by sub entity.

Criteria:

Please select "Multiple assessments by sub-entity" only if **all** the following conditions are met:

- The entities in question have no common in-house network infrastructure
- The entities in question have no network integration/connectivity
- Those responsible for management of information technology and operational technology of the entities in question are completely separate.

If one or more of the conditions are not met please group those entities together and complete a single assessment for those combined entities. Please note: If you have three entities (entity A, entity B and entity C) but only one of those entities (entity B) meets the conditions above you should still select the Multiple entities. When defining the access rights to the assessments below you should group entities A and C into a single entity and define the user's who should have access and separately define the user requiring access to entity B.

Why was the ES-C2M2 used as the foundation?

The ES-C2M2 developed by the U.S Department of Energy is a well-established and globally adopted framework that allows energy organisations to assess their cyber security capability maturity. It covers both IT and OT in scope and aligns to the NIST CSF v 1.1, which has cross-sector applicability. The decision to adopt ES-C2M2 as the foundation for the AESCSF was made in collaboration by the stakeholders listed above in question 'Who developed the AESCSF?'

Please click here to be directed to the Department of Energy, Electricity Subsector Cyber Security Capability Maturity Model (ES-C2M2).

(https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0-1)

Are there any modifications to ES-C2M2 within the AESCSF?

The AESCSF has not made any material changes to the original ES-C2M2 objectives and practices but does include a new Australian Privacy Management domain to enable organisations to manage personal identifiable information through its lifecycle - collection, storage, use and disclosure, and disposal (including de-identification) aligned with Australian privacy guidelines.

One minor change has been made to the assessment approach, with the ES-C2M2 Management Objectives (institutional characteristics) being integrated into the Level of Implementation to drive clarity and consistency during assessments. Organisations need to consider these institutional characteristics when evaluating the Level of Implementation, from Not Implemented through to Fully Implemented.

Please refer to FAQ 'How do I assess my organisation in the AESCSF?' for the explanation of how management objectives are integrated and how to use Level of Implementation.

Are C2M2 management practices assessed?

The characteristics of the C2M2 management practices are integrated into the AESCSF scoring model to drive consistency and clarity. They are not separately assessed as per the vanilla C2M2 model.

The AESCSF assessment does not assess management activities, so the AESCSF score is independent and is not directly comparative to the vanilla C2M2 results. If your organisation wishes to obtain an AESCSF score comparative to the C2M2 results, please contact the AESCSF project team.

How does the AESCSF relate to controls frameworks and how do I align my security controls to the AESCSF?

The AESCSF is a cyber security capability maturity model based on the ES-C2M2 and is not prescriptive with regards to security controls - it describes *what* organisations should strive to achieve, but not exactly *how* they should achieve it. To support organisations seeking this additional detail, the AESCSF has

mapped Informative References to each practice, which are sources of other technical standards and controls frameworks. The AESCSF has also mapped Australian specific guidelines, such as the ACSC Top 37 Strategies to Mitigate Cyber Security Incidents, to provide a view of good-practice controls that have been developed for Australian organisations to mitigate cyber risks.

Many organisations may have defined their own hybrid control frameworks or controls libraries. Assuming these have been based on well-established security frameworks such as ISO27001/2 or NIST CSF, the Informative References should allow you to map such controls to the designated ES-C2M2 practice.

What is the Context Assessment Tool (CAT)?

The CAT is the first component to be completed in the AESCSF. The purpose of the CAT is to determine the criticality of the entity, to rank entities within their industry subsector and to assist in the determination of the target state of maturity for the entity. The CAT determines the criticality context of each organisation.

The Criticality context aims to identify the key attributes of an organisation to determine their criticality in the delivery of electricity to the Australian Energy Markets. These attributes have been assigned weightings in collaboration with AEMO, the CIC and CSIWG, to classify organisations into different bands of criticality (High, Medium, Low). The CAT tool provides further detail on how different organisations are classified across the energy sub-sectors.

Organisations may find their response to some questions in the CAT will differ by region within the NEM. In these situations please respond based on a whole of NEM perspective (eg. if you only have Network Support Agreements in one region please respond in the affirmative that you have Network Support Agreements in place).

What is the AESCSF Australian Privacy Management domain?

The AESCSF includes a domain with a focus on privacy and security of personal identifiable information, an area of increasing focus and regulation within Australia. This ensures the AESCSF remains as relevant to energy organisations dealing with significant volumes of customer data and those who operate critical infrastructure.

The objective of the Australian Privacy Management domain is to enable organisations to manage personal identifiable information through its lifecycle - collection, storage, use and disclosure, and disposal (including de-identification). The Australian Privacy Management domain aligns with the ES-C2M2 maturity level indicators, MIL 0 through MIL 3, which apply independently to each domain. As an organisation progresses from one MIL to the next, it will have more completed or advanced implementations of core activities in the domain. The Australian Privacy Management domain MIL 1 objective focuses on identifying an organisation's privacy obligations. The MIL 2 objective focuses on defined and established policy, practices, and processes to foster a foundation for good privacy governance. The MIL 3 objective focuses on performance measurement and continuous improvement.

The development of the Privacy Management 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 also mapped to the privacy practices to assist organisations to achieve implementation of practices.

Will the AESCSF be updated going forward?

Yes. The AESCSF is intended to continually evolve to ensure sustainability for the future and adaptability to changes in the cyber threat landscape and regulatory requirements. The modular design of the AESCSF provides flexibility for updates to future versions. The use of the AESCSF by Australian energy organisations will also provide valuable feedback and lessons learnt for integration into future versions. Updates may also occur when supporting references undergo updates, such as revisions to the ES-C2M2 or NIST CSF, or the enactment of new legislation such as the Australian Treasury Laws Amendment (Consumer Data Right) Bill 2018.

Preparing for the AESCSF

Which personnel/roles need to be involved in the assessment?

Depending on your organisational structure, type, and size, you can anticipate input from the below resources to complete the assessment. A proposed/template agenda pack is available to assist organisations through the self-assessment process.

To access the agenda pack, please use the following links to the AEMO Market Websites: NEM - Cyber Security and WEM - Cyber Security.

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 • 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

How long does it take to complete an 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.

What electricity assets are in scope for the AESCSF assessment?

All assets of entities operating under the NEM and the WEM are in scope for the AESCSF assessment. The assessment is currently not mandatory but is considered critical input into the establishment of a sector-wide understanding of the current state cyber security capability of Australia.

Any Australian electricity entity outside of the scope is still encouraged to complete a self-assessment to evaluate and improve their cyber security capability. The AESCSF leverages international standards and Australian guidelines and requirements to enable organisations to assess their current cyber security capability state and prioritise remediation effort.

Is the assessment completed at an Asset or Whole of Entity level?

The assessment is completed at an entity level to ensure a comprehensive evaluation of cyber security capability across an entire 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 at the entity level taking an aggregate view across these assets. For example, if security monitoring/logging is only performed on some assets and not others, this would not be scored as 'Fully Implemented' at the entity level for that related practice. 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.

How have the Maturity Target States been determined?

Maturity Target States will be driven by the criticality of the organisation and will be set based on input from the ACSC. The criticality of organisations is determined through the evaluation of the Criticality Assessment Tool. The Maturity Target State definitions will be continuously updated to: address changes in the underlying framework, ensure future sustainability, and safeguard the reliability of the Australian energy market.

A consultation process is underway with stakeholders from relevant Government departments and industry working groups to define the initial Maturity Target 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 Maturity Target State and (c) the related assurance requirements. Further information on the target state will be communicated on completion of the consultation period.

Does the assessment cover OT and IT?

Yes. The AESCSF was developed to apply to energy organisations operating critical infrastructure and OT environments, as well as IT/corporate environments. It is important to assess overall cyber security capability holistically, as an organisation's ability to protect OT environments will often depend on security technologies, people and processes across the IT environment. This has been demonstrated in recent cyber attacks on critical energy infrastructure that took advantage of security weaknesses across both the IT and OT domains. Some of the Informative References within the AESCSF are specific to OT environments, such as NIST 800-82 and ISA/IEC 62443.

How is the score aggregated if I assess both IT and OT?

If OT environments are applicable for your organisation, you will have the opportunity to assess scores for IT and OT separately. This may be useful, for example, to indicate that you have higher-maturity practices within the IT environment compared to the OT environment. The assessment tool will take the minimum level of implementation for the aggregated score. For example, if IT was rated as 'Largely Implemented' and OT was rated 'Partially Implemented', the tool will take the minimum level of implementation, 'Partially Implemented', as the aggregated score for that objective and/or domain. The reasoning for this lowest common denominator approach is driven by the nature of cyber threats, which will usually take advantage of the weakest security link to achieve their objective.

What are context guidance statements and how do I use them?

The ES-C2M2 content is presented at a high level of abstraction so it can be interpreted by organisations of various types, structures, and size. Accompanying each practice is additional context guidance to drive consistency, clarity, and a shared understanding across the energy sector. The context guidance does not make any material changes to the ES-C2M2. It is consider additional supporting guidance to enable facilitators to effectively and efficiently guide self-assessment activities, and to drive a more accurate assessment outcome.

What are anti-patterns and how do I use them?

The ACSC and CSIWG identified a set of anti-patterns which describe issues and problem statements that may increase cyber security risk. They are intended to be the opposite of 'good practice', and will impact an organisation's ability to achieve a certain maturity level.

These anti-patterns have been mapped to specific practices within the Framework. When conducting an assessment, if it is determined that an anti-pattern is present, the practice cannot be assessed as complete, i.e. either 'Largely Implemented' or 'Fully Implemented'. If the organisation is taking action to achieve this practice, the practice may be assessed as 'Partially Implemented'.

I am having issues accessing Datapoint, how can I get help?

For any AESCSF related queries, please email the Project Team via aescsf@aemo.com.au
For any Datapoint website related queries, please reply to the welcome email you received from the platform.

Alternatively, you can call us on 1800 982 125.
If you require assistance with the 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.*

Completing the AESCSF

What does the AESCSF consist of?

The AESCSF consists of the following components:

- AESCSF documentation - contains the design concepts and principles, the purpose of the AESCSF and how the AESCSF can assist organisations assess their cyber security capabilities
- AESCSF mapping - including the ES-C2M2 practices, mapped to NIST CSF, Australia references, informative references and supporting artefacts such as context guidance and anti-patterns.
- FAQ - collection of questions that have been frequently asked about the AESCSF.
- Datapoint - The AESCSF toolkit is implemented within a web-based platform called Datapoint.

Energy market participants will complete the AESCSF using Datapoint, which includes the CAT and AESCSF Assessment.

How do I assess my organisation using the AESCSF?

A design goal of the AESCSF is to drive consistency and objectivity to enable organisations to complete the assessment with a common understanding of the domain-specific objectives and practices. The AESCSF is divided into 11 domains, 10 existing ES-C2M2 domains and the new Australian Privacy Management Domain developed to tailor to the Australian privacy requirements.

The practices within each domain are organised into objectives. For Example, the Threat and Vulnerability domain comprises of two objectives:

- Identify and Respond to Threats
- Reduce Cyber Security Vulnerabilities

You will assess your organisation by evaluating the Level of Implementation for every practice in the assessment, and considering the appropriate MIL and Management Characteristics.

The table below shows the mapping of the level of implementation to the management characteristics required for progression against MIL 2 and MIL 3. MIL 1 practices are assessed in a binary approach, either Yes or No.

Completion Status	Level of Implementation	Criteria for answering MIL2 practices	Criteria for answering MIL3 practices
Not Complete	Not Implemented	Should no Management Characteristics be present, this practice is Not Implemented	Should no MIL 3 Management Characteristics be present, this practice is Not Implemented
	Partially Implemented	1. Practices are documented	At least all Largely Implemented Management Characteristics at MIL 2 must be present, as well as the following MIL 3 Characteristics: 5. Activities are guided by policies (or other organizational directives) and governance, and; 6. Personnel performing the practices have adequate skills and knowledge.
Complete	Largely Implemented	1. Practices are documented; 2. Stakeholders of the practice are identified and involved; 3. Adequate resources are provided to support the process (people, funding, and tools).	At least all Largely Implemented Management Characteristics at MIL 2 must be present, as well as the following MIL 3 Characteristics: 5. Activities are guided by policies (or other organizational directives) and governance; 6. Personnel performing the practice have adequate skills and knowledge; 7. Policies include compliance requirements for specified standards and/or guidelines, and; 8. Responsibility and authority for performing the practices are assigned to personnel.
	Fully Implemented	1. Practices are documented; 2. Stakeholders of the practice are identified and involved; 3. Adequate resources are provided to support the process (people, funding, and tools), and; 4. Standards and/or guidelines have been identified to guide the implementation of the practices.	At least all Largely Implemented Management Characteristics at MIL 2 must be present, as well as the following MIL 3 Characteristics: 5. Activities are guided by policies (or other organizational directives) and governance; 6. Personnel performing the practices have adequate skills and knowledge; 7. Policies include compliance requirements for specified standards and/or guidelines; 8. Responsibility and authority for performing the practices are assigned to personnel, and; 9. Activities are periodically reviewed to ensure they conform to policy.

Do I need to substantiate responses with evidence/artefacts for the self-assessment?

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 artifacts that substantiate the assessment rating, i.e. referencing the name of a security policy or procedure document and its version number. At this time, there is no requirement to upload any documentation.

What notes should I capture in the 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
- Areas of opportunity
- Note whether anti-pattern(s) exist
- Presence or lack of management characteristics
- Why/why not a practice is important to your organisation's cyber security capability

The table below provides some explains of notes taken against Identity and Access Management domain practices:

MIL	Practice ID	Practice Description	IT Assessment Response	OT Assessment Response	Notes
1. 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) *Anti-pattern: Identities and accounts are created for people without first checking if there is a genuine need for them to be able to access systems within your technology environments.*	Yes	Yes	Identity Management is present in multiple forms across entity. Identities are captured in SAP and Active Directory. Personnel have unique identifiable accounts. Anti-pattern not present in either environment.
....					
2	IAM-1f	Identities are deprovisioned within organizationally defined time thresholds when no longer required	Largely Implemented	Not Implemented	IT - time period has been defined in process eg: when personnel leaves business, identity is deactivated within 14

					days. OT - No defined interval to reclaim physical keys. Identified as area of opportunity
....					
2. Control Access					
....					
2	IAM-2d	Access requirements incorporate least privilege and separation of duties principles *Anti-Pattern: People are given administrator access to systems by default. A common example is end users being local administrators on their corporate laptop/workstation.* *There are known instances where people have access which breaches a segregation of duties requirement (e.g. being able to both create and approve a request).*	Partially Implemented	Partially Implemented	Occurs in some places. Different tiers of access are applied. Secondary system teams have no local admin. Anti-pattern not present in either environment.
....					
2	IAM-2f	Root privileges, administrative access, emergency access, and shared accounts receive additional scrutiny and monitoring *Anti-Pattern: A complete and current register of identities with privileged access is not maintained.*	Not Implemented	Not Implemented	IT - occurs in an ad-hoc manner. OT - no additional scrutiny and monitoring for emergency access or shared accounts. Anti-pattern not present in either environment.

How do I submit my AESCSF assessment?

Assessments are submitted using the AESCSF Toolkit hosted on Datapoint. Datapoint will allow you to review your responses before submission. Your organisation's CEO or nominated executive sponsor is required to attest to the accuracy and completeness of the assessment before the final submission. A CEO attestation response letter addressed to AEMO CEO and Head of the Australia Cyber Security Centre is **mandatory** and must be uploaded to Datapoint before final submission of assessment.

The submission results from energy market participants will be collectively analysed and benchmarked. Insights and analysis of results will be made available to energy market participants once energy industry assessments are completed.

Further detailed instructions on how to complete and submit the assessment can be found in the AESCSF Toolkit User Guide available within the Datapoint platform.

How do I submit my Context Assessment Tool (CAT)?

The CAT is submitted within Datapoint, and can be submitted separately from the AESCSF assessment. Datapoint will allow you to review your responses before submission.

The review page will show your organisation's criticality per subsector in three buckets: High, Medium, Low.

Further detailed instructions on how to complete and submit the assessment can be found in the AESCSF Toolkit User Guide available within the Datapoint platform.

How do I use the NIST CSF controls and informative references?

Once your organisation has identified cyber security capability gaps, your organisation can refer to NIST CSF controls and informative references (including Australia-specific references) for guidance on how to remediate gaps and uplift capability.

Some practices without NIST CSF controls have informative references mapped directly to the ES-C2M2 practices. This approach ensures a relationship between ES-C2M2 practices and informative references to support the evaluation, prioritisation and improvement of cyber security capabilities.

The international informative references are:

- National Institute of Standards and Technology Cyber Security Framework (NIST CSF v 1.1)
- Center for Internet Security Controls v7
- International Organization for Standardization/International Electrotechnical Commission (ISO/IEC 27001:2013)
- National Institute of Standards and Technology Special Publication revision 4 (NIST SP 800-53 r4)
- Control Objectives for Information and Related Technologies (COBIT v5)
- International Society of Automation/International Electrotechnical Commission (ISA/IEC 62443)

What are the Australian references and how do I use them?

The AESCSF integrates Australian specific requirements and guidelines to provide greater relevance and local context to Australian energy market participants. The AESCSF links the ES-C2M2 maturity indicator levels to more granular requirements from the ACSC Strategies to Mitigate Cyber Security Incidents, Australian Privacy Principles, and Notifiable Data Breaches. The Australian references integrated into the AESCSF are not prescriptive and are not intended to be part of the assessment - they are sources of guidance and further information, not mandatory requirements.

How is the score aggregated when assessing multiple assets?

The lowest common response will be used as the aggregated score for assessments completed on multiple assets, including IT and OT assets. Participants are recommended to make notes in the space provided to provide further detail on the assets assessed.

The following two example illustrates the application of the scoring aggregation.

Example 1: Company A assesses *Cyber Security Program Management domain, objective 2: Establish and Maintain Cyber security Architecture*. Company A identifies an Industrial Control System is administered by the Engineering team (OT) and is supported by an IT Control Data Network team (IT).

The assessment identified that IT is more mature than OT. The scoring model would aggregate the scoring and determine the minimum response as "Partially Implemented" as the overall score for this objective. The table below lists example responses.

Practice	**IT response**	**OT response**	**Practice results**
CPM-3a - A strategy to architecturally isolate the organisation's IT's system from OT system is implemented	Fully Implemented	Largely Implemented	Largely Implemented
CPM-3b - A cybersecurity architecture is in place to enable segmentation, isolation, and other requirements that support the cybersecurity strategy	Largely Implemented	Partially Implemented	Partially Implemented
CPM-3c - Architecturally segmentation and isolation is maintained according to a documented plan	Largely Implemented	Largely Implemented	Largely Implemented
CPM-3d - Cyber security architecture is updated at an organisation- defined frequency to keep it current	Partially Implemented	Partially Implemented	Partially Implemented

Refer to 'Does the assessment cover Operational Technology (OT) and Information Technology (IT)?' and 'How do I assess my organisation using the AESCSF?' for details on how the scoring model works in AESCSF' for further information.

Example 2: Company A assesses *Identity and Access Management* practices and has a critical OT process which relies on an IT hosted authentication service. The OT system relies on an IT authentication repository to identify 'Super users' accounts . There is no defined process on how 'Super user' accounts are flagged.

Practice	**IT response**	**OT response**	**Practice results**
IAM-2d - Access requirements incorporate least privilege and separation of duties principles	Partially Implemented	Fully Implemented	Partially Implemented

The practice result for IAM-2d is Partially Implemented as it is the lowest common response.

Can I obtain a NIST CSF score from AESCSF?

Yes. Participants will be able to derive a NIST CSF score on a category level, across four levels between 0-3, Not Implemented to Fully Implemented. Please refer to the Framework Core for mapping of NIST CSF to AESCSF practices. The Framework Core is available for download via the following links to the AEMO Market Websites: NEM - Cyber Security and WEM - Cyber Security.

Please note, whilst the AESCSF maps to the NIST CSF, there are subtle differences between the two frameworks in regards to areas of focus. If an organisation requires a comprehensive assessment against the NIST CSF, it is recommended this is completed independently of the AESCSF assessment.