Australian Energy Sector Cyber Security Framework (AESCSF)

Overview

AEMO
AUSTRALIAN ENERGY MARKET OPERATOR

Important notice

Purpose

This document is made available by The Australian Energy Market Operator (AEMO) to provide information about the Australian Energy Sector Cyber Security Framework (AESCSF).

This document accompanies other general guidance materials made available to Australian energy organisations in the electricity, gas, and liquid fuels sub-sectors.

Disclaimer

This document or the information in it may be subsequently updated or amended. This document does not constitute legal or organisation-specific advice and should not be relied on as a substitute for obtaining detailed advice about any applicable laws, procedures, or policies. AEMO have 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, AEMO 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

Each key term has a specific definition that the reader should consider. Key terms are defined centrally in the AESCSF Glossary which is available separately on the AEMO website.

Table of contents

Tables

1. Cybersecurity in Australia's energy industry

The global energy sector and Australia in particular has undergone an unprecedented transformation over the last decade, with continuously evolving and emerging interconnected technologies. The increased digitisation and interconnectedness of Australia's energy system, creates and amplifies the risks to the system, to industry participants, and ultimately, to Australia's sovereignty and Australians' way of life. The threat is real. Worldwide, critical infrastructure networks are increasingly targeted. Both state actors and cybercriminals view critical infrastructure as an attractive target. Successful attacks on Australia's critical energy infrastructure could put essential services at risk. **That's why cyber security and reinforcing our energy resilience is a national priority.**

It is therefore essential that all energy industry participants seek clarity on their cyber defences and what they need to remain secure and take steps to address their vulnerabilities. The Australian Energy Sector Cyber Security Framework (AESCSF) supports participants in the Australian energy sector to do this.

Energy system evolution and technological advancement means that the energy sector is more integrated and automated than ever and is continuing to become even more so.

2. About the Framework

The AESCSF is a cyber security framework developed and tailored to the Australian energy sector. The purpose of the AESCSF (the 'Framework') is to enable market and non-market participants across the electricity (including distributed and consumer energy resources), gas, liquid fuels sub-sectors to assess, evaluate, prioritise, and improve their cyber security capability and maturity. It comprises a set of security practices relevant to Australia's energy sector and a methodology for organisations (where applicable) to assess their criticality with respect to the Australian energy system and their maturity against the security practices. The Framework is focused on cyber security maturity and describes *what* your organisation should strive to achieve, not *how* it should be achieved.

The Framework was developed in consultation with industry and government in 2018 (AESCSF Version 1) and updated in 2022 (AESCSF Version 2) to align with current international standards and address emerging technologies and the evolving cyber threat landscape.

The foundation of the AESCSF is based on the US Department of Energy's (DOE) Cybersecurity Capability Maturity Model (C2M2) Version 1.1. The C2M2 has been updated, culminating in the publication of C2M2 Version 2.1 in June 2022. AESCSF V2 incorporates C2M2 V2.1 enhancements to cyber security risk management and assist industry with future planning and investment decisions.

The Framework also aligns with existing Australian policy and guidelines, including the Australian Privacy Principles and the Australia Signals Directorate's Australian Cyber Security Centre's (ACSC) *Strategies to Mitigate Cyber Security Incidents* and with the *Security of Critical Infrastructure Act 2018* (SOCI Act).

A list of other Australian and global informative references that are mapped to each practice for additional guidance is available at Appendix E: Alignment of the Framework to best practice.

2.1. How was the Framework developed?

Initially developed in 2018 in response to a recommendation from the 2017 *Independent Review into the Future Security of the National Electricity Market - Blueprint for the Future*, otherwise known as 'The Finkel Review'. Since then, the Framework had minor revisions in 2019 and 2021 to ensure it reflects the evolution of cyber and technology advances.

The Framework was developed with industry representatives and government stakeholders, including:

- The Australian Energy Market Operator (AEMO)
- Australian Signal Directorate's Australian Cyber Security Centre (ACSC)
- Energy market participants
- Department of Climate Change, Energy, the Environment and Water (DCCEEW)
- The Department of Home Affairs (DHA)

2.2. How did the Framework's evolve from Version 1 to Version 2?

In 2022, following the release of the revised C2M2 2.1, the Framework was reviewed to align with current international standards and address emerging technologies and the evolving cyber threat landscape. To complete this review the AESCSF Review Working Group (AESCSF-RWG) was established.

The AESCSF-RWG:

- was convened in early 2022
- consisted of more than 50 members and 40 organisations across Australia's energy sectors
- conducted a detailed review of the draft AESCSF V2
- engaged with the ACSC to determine the updated Security Profiles (SPs)
- conducted a detailed review of AESCSF Anti-Patterns via an interactive survey
- was a key point of engagement between industry and government.

The update to AESCSF V2 from C2M2 V2.1 resulted in a further 72 practices, creating a more mature Framework for the energy industry, reflecting the evolving cyber risk landscape.

AESCSF V2 builds on the strong foundations developed in V1 improving the comprehensiveness of cyber security activities, clarification of language, and improved consistency of concepts across the Framework.

The AEMO Framework and Resources tab details the background, history, and evolution of the AESCSF with comprehensive guidance materials to support AESCSF V1 users.

2.1. Is the AESCSF Framework's SOCI compliant?

Both AESCSF versions are recognised compliance frameworks for assessing your cyber maturity to support Risk Management Program regulatory obligations under the SOCI Act. Through continued collaboration, 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.

This Overview document support application of Version 2, for the historic Version 1 supporting materials AEMO | AESCSF framework and resources.

2.2. Why the Framework is important?

The Framework plays a crucial role in improving the cyber security of Australia's energy sector in a complex, and ever-evolving landscape. The tailored Framework has been developed to manage cyber security risk, reduce reputational risk, and prevent potential disruption to energy services in Australia.

The Framework will allow participants to realise the following:

- Participants can **use the self-assessment results to inform actions, priorities, and investments,** to deliver a consistent risk-based approach, embedding cyber security responsibilities in the first line of defence to build organisational operational resilience.
- Participants will be able to **benchmark their organisation against energy sector peers**.
- Participants can **use the Program to assess their cyber maturity to support their Risk Management Plan (RMP)** regulatory obligations under the SOCI Act (where applicable).
- The aggregated and anonymised **AESCSF self-assessment data provides data-driven insights** that are used for the **benchmarking tool** (available for participants) and **informs content for the Cyber Security Preparedness of the Australia's Energy Sector Annual Report**. In turn this information informs sector policies to improve cyber security and operational resilience in the Energy sector.
- The AESCSF allows Australian energy market participants to speak a common cyber language and to work collaboratively in a community of users.

2.3. Who the Framework is for?

The Framework was developed for energy organisations with Operational Technology (OT) assets and Information Technology (IT) assets. This is because 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.

It is recommended all energy industry participants complete the assessment, including:

Table 1. Recommended AESCSF participants

Electricity	Gas	Liquid Fuels	DER/CER
• Generation • Transmission • Independent Interconnectors • Distribution • Retail • Market operations	• Production • Transmission • Bulk Storage • Distribution • Retail • Market operations	• Extraction and production • Transport and import • Storage • Refinement • Wholesale and retail	• Wind Farms • Solar Farms • Batteries • Meting Agents • Microgrids • Virtual Power Plans (VPPs)

2.1. What is the AESCSF Lite?

The AESCSF Lite Framework offers a tailored approach for smaller, emerging, or resource-constrained organisations—including those within the Distributed Energy Resources (DER) and Consumer Energy Resources (CER) ecosystems. These organisations play a critical role in the broader energy landscape and are increasingly interconnected with critical energy systems. As such, it is important to ensure foundational cyber capabilities are assessed and uplifted in a proportionate and scalable manner.

The AESCSF Lite Framework is deliberately agnostic to organisational size, scale, or maturity, making it especially suitable for DER/CER participants who may not have dedicated cybersecurity teams or mature security programs. The framework simplifies engagement without compromising on core cybersecurity principles and enables organisations to:

- Establish a baseline understanding of their cybersecurity posture.
- Identify and address key gaps based on risk-informed priorities.
- Leverage industry-aligned practices that are scaled to operational reality.

In conjunction with the AESCSF Priority Practices and supporting DER/CER-specific guidance material, the Lite Framework enables a consistent and practical approach for uplifting cybersecurity resilience across all parts of the energy ecosystem. DER/CER organisations are encouraged to use the framework as both a self-assessment tool and a foundation for further engagement with energy sector partners and regulators.

2.2. How is the Framework structured?

The Framework comprises practices and anti-patterns that are grouped within domains and which relate to an objective relevant to that domain. Accompanying each practice and anti-pattern is context and guidance to provide clarity about the intent of the practice or anti-pattern, encourage consistency in their application and support participants to understand the requirement.

Table 2. Framework Structure

Section	Description
Domain	• Logical grouping of cyber capability • The AESCSF contains 11 domains.
Objective	• Target achievements to support domains • Objectives are numbered and unique to each Domain.
Practices	• Positive security pattern, task or activity • Each Objective contains multiple Practices. • Practices are lettered and unique to each Objective • 354 Practices and Anti-Patterns across 11 domains
Anti-Patterns	• Outlines negative security patterns that shouldn't be present. • 9 of the 11 domains contain Anti-Patterns. • Applicable Anti-Patterns for each domain are contained in their own Objective.

2.2.1. What are the AESCSF Domains?

Table 3. Domains and their descriptions

Domain	Description
Risk management (RISK)	Establish, operate, and maintain an enterprise cybersecurity risk management program to identify, analyse, and mitigate cybersecurity risk to the organisation, including its business units, subsidiaries, related interconnected infrastructure, and stakeholders.
Cybersecurity program management (PROGRAM)	Establish and maintain an enterprise cybersecurity program that provides governance, strategic planning, and sponsorship for the organisation's cybersecurity activities in a manner that aligns cybersecurity objectives with the organisation's strategic objectives and the risk to critical infrastructure.
Asset, change, and configuration management (ASSET)	Manage the organisation's operations technology (OT) and information technology (IT) assets, including both hardware and software, commensurate with the risk to critical infrastructure and organisational objectives.
Identify and access management (ACCESS)	Create and manage identities for entities that may be granted logical or physical access to the organisation's assets. Control access to the organisation's assets, commensurate with the risk to critical infrastructure and organisation objectives.
Cyber Security Architecture (ARCHITECTURE)	Establish and maintain clear mapping of your IT and OT assets and a plan as to where and how controls should be implemented to protect your environment in the event of a cybersecurity attack.
Threat and vulnerability management (THREAT)	Establish and maintain plans, procedures, and technologies to detect, identify, analyse, manage and respond to cybersecurity threats and vulnerabilities, commensurate with the organisation's infrastructure (e.g., critical, IT, operational) and organisational objectives.
Situational awareness (SITUATION)	Establish and maintain activities and technologies to collect, analyse, alarm, present, and use operational and cybersecurity information, including status and summary information from the other model domains, to form a common operating picture (COP).
Event and Incident Response, Continuity of Operations (RESPONSE)	Establish and maintain plans, procedures, and technologies to detect, analyse, and respond to cybersecurity events and to sustain operations throughout a cybersecurity event, commensurate with the risk to critical infrastructure and organisational objectives.
Supply chain and external dependencies management (THIRD-PARTIES)	Establish and maintain controls to manage the cybersecurity risks associated with services and assets that are dependent on external entities, commensurate with the risk to critical infrastructure and organisational objectives.
Workforce management (WORKFORCE)	Establish and maintain plans, procedures, technologies, and controls a culture of cybersecurity and to ensure that ongoing suitability and competence of personnel, commensurate with the risk to critical infrastructure and organisational objectives.
Australian privacy management (PRIVACY)	Establish and maintain plans, procedures, and technologies to reduce privacy related risks, and manage personally identifiable information through its lifecycle - collection, storage, use and disclosure, and disposal (including de-identification).

2.2.2. What are Anti-patterns?

Anti-patterns describe issues and problem statements that increase cyber risk. They are intended to be the 'opposite' of good practice. If an anti-pattern exists, it will impact an organisation's ability to achieve the associated maturity level.

In essence, anti-patterns are 'bad 'activities that undermine the effectiveness of a cyber security capability. Therefore, additional focus is given to them to encourage organisations to fix these behaviours.

Anti-patterns were developed in consultation with AEMO, industry and government stakeholders.

2.2.3. What are Maturity Indicator levels?

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

- All practices, must be attained and anti-practices absent, for an MIL within a domain, to achieve that level for the domain.
- Apply independently to each domain i.e. entities may have different MILs for different domains.
- An organisation's overall MIL reflects the lowest MIL obtained in any domain.

Table 4. Maturity Indicator Levels (MILs) and their descriptions

Maturity level	Criteria overview
Maturity Indicator Level 1 (MIL 1)	The practice is performed.
Maturity Indicator Level 2 (MIL 2)	• The practice is performed. • The practice is documented. • Stakeholders of the practice are identified and involved. • Adequate resources are provided to support the practice (people, funding, and tools). • Standards and/or guidelines have been identified to guide the implementation of the practice
Maturity Indicator Level 3 (MIL 3)	• Practices meet MIL 2 • Activities are guided by policies (or other organisational directives) and governance • Personnel performing the practice have adequate skills and knowledge • Policies include compliance requirements for specified standards and/or guidelines • Responsibility and authority for performing the practice is assigned to personnel • Activities are periodically reviewed to ensure they conform to policy

2.2.4. How is maturity calculated?

MILs are calculated for each domain based on response for each practice and anti-pattern. The extent to which the MIL applies to each domain is assessed as:

- Partially implemented
- Largely implemented or
- Fully implemented.

An organisation's overall assessment rating is based on the lowest MIL achieved for any domain. This is because cyber criminals will usually take advantage of the weakest security link to achieve their objective and so an organisation's security is only as strong as its weakest link.

2.2.1. What are Security Profiles?

The AESCSF has three alternate groupings of Practices and Anti-Patterns referred to as Security Profiles (SPs). The SPs have been defined by the ACSC, in consultation with AEMO and industry representatives, as a risk-based approach to maturity. The target state maturity SP a participant should pursue is determined based on their overall criticality result (per the CAT for those market participants who completed one).

- Entities only achieve an SP level if all practices are attained and anti-practices are absent as identified for that SP level.
- SPs include identified priority practices. It is recommended that the priority practices be attained first as part of any uplift program.

Table 5. Security Profiles (SPs) and their descriptions

Security Profile	Criteria overview
Security Profile 1	• All SP-1 Practices and Anti-Patterns must be attained to achieve Security Profile 1 • All Practices and Anti-Patterns at MIL-1 are included within Security Profile 1 with the addition of select Practices and Anti-Patterns from MIL-2 and MIL-3. • Security Profile 1 in Version 2 contains 29 Practices that have been identified by the ACSC as a priority for completion. These Practices should be considered when sequencing Practice remediation activities
Security Profile 2	• All SP-1 & SP-2 Practices and Anti-Patterns must be attained to achieve Security Profile 2 • All Practices and Anti-Patterns at MIL-2 are included in Security Profile 2 with the addition of select Practices and Anti-Patterns at MIL-3. • Security Profile 2 contains 28 (AESCSF V2) Practices that have been identified by the ACSC as a priority for completion. These Practices should be considered when sequencing Practice remediation activities.
Security Profile 3	• All Practices and Anti-Patterns must be attained to achieve Security Profile 3

Security Profile	Criteria overview
	• All Practices and Anti-Patterns at MIL-3 are covered in Security Profile 3. • Achieving Security Profile 3 is identical to achieving Maturity Indicator Level (MIL) 3. • Security Profile 3 contains 13 (AESCSF V2) Practice that have been identified by the ACSC as a priority for completion. This Practice should be considered when sequencing Practice remediation activities.

Security Profiles introduce a 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 6. Security profiles for AESCSF V2

Security Profile (SP)	Practices and Anti-Patterns			Total required to achieve SP
	MIL-1	MIL-2	MIL-3	
Security Profile 1 (SP-1)	62 (+5)	57 (+30)	4 (0)	123 (+35)
Security Profile 2 (SP-2)	0	123 (+29)	29 (+11)	275 (152+123 from SP-1) (+40)
Security Profile 3 (SP-3)	0	0	79 (-3)	354 (79+275 from SP-2) (-3)

3. How to use the Framework

There are four key steps to using the Framework:

1. Assess your organisation's criticality (where applicable)
2. Select the appropriate assessment model
3. Determine the assets in scope for the assessment
4. Complete the assessment

3.1. Assess your organisation's criticality

An organisation's criticality to the energy sub-sector/s (electricity, gas and liquid fuels) in which they operate, should determine which assessment model (full or lite version) they complete. The criticality assessment tools between each sub-sector are not comparable and thus an organisation should use their highest criticality ranking (if they operate in more than one sub-sector) as their overall level of criticality. Overall criticality is determined by taking the highest sub-sector criticality ranking.

Please note, the criticality assessment does not align to the criticality parameters outlined in the *SOCI Act* and a criticality rating of X or above does not necessarily indicate that an entity has obligations under, or is compliant with applicable Commonwealth legislation, such as the SOCI Act.

Table 7. Sub-sector organisations who should complete Criticality Assessment Tool

Electricity Criticality Assessment Tool (E-CAT)	Gas Criticality Assessment Tool (G-CAT)	Liquid Fuels Criticality Assessment Tool (L-CAT)
• Generation (E-GEN) • Transmission (E-TNSP) • Independent interconnectors (E-IC) • Distribution (E-DNSP) • Retail (E-RET) • Market operations (E-OPS).	• Production (G-PROD) • Transmission (G-TNSP) • Bulk storage (G-STOR) • Distribution (G-DNSP) • Retail (G-RET) • Market operations (G-OPS).	• Extraction and production (L-EXTR) • Transport and import (L-TRAN) • Storage (L-STOR) • Refinement (L-RFIN) • Wholesale and retail (L-WHLS).

DER/CER organisations are best suited to use the AESCSF Lite Framework, which is scalable and accessible for smaller or emerging participants. They are always welcome to adopt the full framework if appropriate, but the Criticality Assessment Tool (CAT) may not be required unless the organisation is a AEMO registered participant. The Lite version, supported by priority practices and DER/CER-specific guidance, offers a practical path to uplift cybersecurity resilience.Select the appropriate assessment model

There are three versions of the AESCSF which participants can select based on their criticality to the energy sub-sectors in which they operate:

Table 8. AESCSF assessment options

AESCSF Version 2 (V2) Full Assessment	

Description
• Established 2023.
• 354 practices and Anti-Patterns across 11 domains.
• Aligns with all of the same control references as V1 and also:
  ○ the US Department of Energy's Cybersecurity Capability Maturity Model version 2.1
  ○ Security of Critical Infrastructure Critical Infrastructure Risk Program (CIRMP) obligations.
	Best suited to …
	Best suited to medium and high criticality organisations and lower criticality organisations who are experienced with the AESCSF assessment and those with the resources to support the assessment.
	
	Time commitment
	Depending on the size of your organisation and the number of stakeholders required, it could take anywhere from a few hours to a few days to collect the necessary information and resources for the assessment.

AESCSF Version 1 (V1) Full Assessment	

Description
• Established 2018.
• 282 practices and Anti-Patterns across 11 domains.
• Aligns with Australian-specific and international control references, including:
  ○ Security of Critical Infrastructure Act 2018 (SOCI Act)
  ○ ACSC's Essential Eight
  ○ Australian Privacy Principles
  ○ Notifiable Data Breaches scheme
  ○ US Department of Energy's Electricity Subsector Cybersecurity Capability Maturity Model
  ○ National Institute of Standards and Technology Cyber Security Framework
	Best suited to …
	This is the minimum standard for medium and high criticality organisations. May also suit lower criticality organisations that are still maturing or that don't have the resources to complete the V2 assessment.
	
	Time commitment
	Depending on the size of your organisation and the number of stakeholders required, it could take anywhere from a few hours to a few days to collect the necessary information and resources for the assessment.

AESCSF Version 2 (V2) Lite	
Description • Established 2023 (replaces V1 lite). • 28 multi-select, easy-to-follow questions	**Best suited to …** This is the minimum standard for medium and high criticality organisations. May also suit lower criticality organisations that are still maturing or that don't have the resources to complete the V2 assessment. **Time commitment** If responses to all questions are known, the survey should take around 15-20 minutes. However, some clarification with specialists and outsourced providers may be required to answer the questions accurately, which would increase the completion time.

3.2. Determine the assets in scope for the assessment

Cyber security capability may vary across an organisation's energy assets and cyber criminals will usually take advantage of the weakest security link. Recommendation that organisations include all assets in their assessment collectively (rather than asset by asset), to get an aggregate view across the assets and organisation. This provides a more accurate view of an organisation's overall security posture.

Where an organisation has assets in more than one energy sub-category (electricity, gas, liquid fuels), an assessment should be conducted across the assets for each sub-category in which the organisation participates.

When determining what assets to include in the assessment, consider these principles:

- the assessment should be completed by the ultimate Australian legal entity (parent company) that controls participants in the electricity, gas or liquid fuels sub-sector
- the parent company should complete a single assessment, including in scope all operations, unless each of the following apply:
  - there is 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 assessment on their behalf for those assets.

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

Table 9. Guide to determining assessment scope, in particular circumstances

Participant status	Scope of assessment	Responsible for assessment
Participant with trading rights to the output from a generation asset, gas processing, or liquid fuels handling facility	Facility/asset	O&M provider
O&M provider and also a participant in their own right	Agree scope, according to the above principles	All relevant parent companies who have outsourced to them
Electricity generator	Operations as far along the supply chain for an asset as they reasonably control.	Electricity generator
Company with participants in more than one of electricity, gas, and liquid fuels sub-sectors	An assessment for each of the relevant subsectors in which the participant operates.	Parent company
Parent company that controls and operates a gas pipeline, as well as a facility that feeds a gas fired power generator (that they also control and operate).	All operations up to the gas feed into the electricity generator.	Parent Company
Parent company that produces or supplies liquid fuel products.	Any and all infrastructure used for the handling of product for the Australian domestic market.	Parent Company

3.3. Conduct the assessment

3.3.1. Involve the right people

The people required to help the coordinator conduct an assessment will vary based on the size and structure of each organisation. However, the table **Error! Reference source not found.**, indicates the type o f roles that should be involved in contributing to the assessment.

Table 10. Roles that may contribute to an organisation's assessment

Business Unit	Roles
Organisational Management	• Executive/Board
Information and Communications Technology (ICT) or Information Technology (IT)	• Chief Information Security Officer (CISO) • Security Manager • Enterprise Architect • Security Architect • Operations Manager • Support Manager • Specialist Operational Teams - Identify and Access, Networks etc • Security Specialist/Practitioner
Operational Technology or Engineering	• Control Systems Engineer • SCADA Engineer • Substations (Field Engineering) • Telecommunications Engineer (where applicable) • Security Specialist
Shared Services	• Executive/Board • 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

3.3.2. Take notes

It is recommended to keep notes about your assessment and make reference to key documents (e.g. policies, processes, reports) and practices that substantiate your assessment rating for your own benefit. This will make the process easier in subsequent years and help you be more specific about what actions you need to take to uplift your security posture. Examples may include:

- evidence that 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 will enable you to filter to aggregate these 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.

4. Related resources

If you would like any additional support or information on the AESCSF, resources are available for your organisation on the AEMO website.

Appendix A: Frequently Asked Questions

Is completing an assessment mandatory?

The assessment is recommended but not mandatory; **however**, participants can use the Framework to assess their cyber maturity to support their Risk Management Program (RMP) regulatory obligations under the SOCI Act. Participants can also use the self-assessment results to inform actions, priorities, and investments, to deliver a consistent risk-based approach, embedding cyber security responsibilities in the first line of defence to build organisational operational resilience.

How do I access the AESCSF assessment?

You can access the AESCSF assessment by visiting the AESCSF Resources webpage.

What are the differences between AESCSF V1 and V2?

For a summary of changes and supporting V1 materials, please refer to the AESCSF V2 Summary of Changes on the AESCSF website.

Does AESCSF V2 adhere to the Security of Critical Infrastructure Act 2018 (SOCI Act)?

AESCSF V2 is recognised as an equivalent Framework and compatible with new SOCI Critical Infrastructure Risk Program (CIRMP) obligations.

How long does it take to complete an assessment?

Full 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 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.

Can I transition from a lite assessment to a full assessment?

Yes, you can. Organisations are encouraged to complete the full assessment for greater visibility of their security practices and gaps, regardless of your organisation's critical rating.

I am time poor. My organisation has previously done full assessments – can I do a lite assessment due to time pressure?

If your organisation has previously completed a full assessment, it is recommended that your organisation continues to do the full assessment each year to receive the full benefit.

Can separate assessments be completed by asset if maturity varies greatly?

While capability may vary across energy assets, assessments should cover all relevant assets and operations to identify 'the weakest link' and ensure a comprehensive evaluation of cyber security capability across the organisation. Undertaking the assessment at an asset level could misrepresent the overall security posture of the organisation, leaving your organisation, your customers and Australia's energy system exposed.

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

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

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.

Appendix B: Priority practices by Security Profile

To assist organisations in defining its maturity roadmap 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.

Table 11. Priority practices by security profile for AESCSF V2

Domain	Priority practices and Anti-Patterns		
	Security Profile 1	**Security Profile 2**	**Security Profile 3**
ASSET	ASSET-1A ASSET-2A ASSET-3A ASSET-4D	ASSET-1G ASSET-2G ASSET-3D ASSET-4G	ASSET-1F ASSET-2F ASSET-3E
PRIVACY	PRIVACY-1B	PRIVACY-1I	PRIVACY-1M
PROGRAM	PROGRAM-2A	PROGRAM-2E	PROGRAM-1H
THIRD-PARTIES	THIRD-PARTIES-1A THIRD-PARTIES-1B THIRD-PARTIES-2A THIRD-PARTIES-2B	THIRD-PARTIES-1C THIRD-PARTIES-2F THIRD-PARTIES-2M	-
ACCESS	ACCESS-1B ACCESS-1F ACCESS-2G ACCESS-3H	ACCESS-2I ACCESS-3J	-
RESPONSE	RESPONSE-2G RESPONSE-3C RESPONSE-4E	RESPONSE-1F RESPONSE-3L RESPONSE-2D	RESPONSE-3J
ARCHITECTURE	ARCHITECTURE-2B ARCHITECTURE-2C ARCHITECTURE-3A	ARCHITECTURE-1C ARCHITECTURE-3F ARCHITECTURE-3G ARCHITECTURE-3I ARCHITECTURE-3H	ARCHITECTURE-1I ARCHITECTURE-4G
RISK	RISK-2A RISK-3A RISK-4A	RISK-1F RISK-2F RISK-2M RISK-3D	RISK-3G RISK-4E
SITUATION	SITUATION-1A	SITUATION-1B	SITUATION-1F
THREAT	THREAT-2D THREAT-2H	THREAT-1G THREAT-2G	THREAT-2I
WORKFORCE	WORKFORCE-1A WORKFORCE-1B WORKFORCE-1E	WORKFORCE-1F WORKFORCE-3C WORKFORCE-3E	WORKFORCE-2G

Appendix C: Management Characteristics

Table 12. The Management Characteristics

MIL	MIL 1		MIL 2			MIL 3		
Implementation Response	No	Yes	Partially Implemented	Largely Implemented	Fully Implemented	Partially Implemented	Largely Implemented	Fully Implemented
The practice is performed		✓	✓	✓	✓	✓	✓	✓
The practice is documented			✓	✓	✓	✓	✓	✓
Stakeholders of the practice are identified and involved.				✓	✓	✓	✓	✓
Adequate resources are provided to support the practice (people, funding, and tools).				✓	✓	✓	✓	✓
Standards and/or guidelines have been identified to guide the implementation of the practice					✓	✓	✓	✓
Activities are guided by policies (or other organisational directives) and governance						✓	✓	✓
Personnel performing the practice have adequate skills and knowledge						✓	✓	✓
Policies include compliance requirements for specified standards and/or guidelines							✓	✓
Responsibility and authority for performing the practice is assigned to personnel							✓	✓
Activities are periodically reviewed to ensure they conform to policy								✓

Appendix D: Alignment of the Framework to best practice

The AESCSF is based on the United States' Department of Energy's Cybersecurity Capability Maturity Model (C2M2 V1.1) as the foundation for the AESCSF to ensure that the Australian energy sector remained globally adept and aligned with best practice. The C2M2 was developed in 2012 before going through a complete process of updating culminating in the publication of C2M2 V2.1 in June 2022 and is a well-established and globally adopted maturity model that empowers energy organisations to assess their cyber security capability and maturity.

The AESCSF covers both IT and operations and aligns to the National Institute of Standards and Technology (NIST) Cybersecurity Framework (NIST CSF), which applies across sectors.

The Framework also aligns with existing Australian policy and guidelines, including the Australian Privacy Principles and ACSC's *Strategies to Mitigate Cyber Security Incidents* and with the Security of Critical Infrastructure Risk Management Program (CIRMP) rules which came into effect as of February 2023, under the *Security of Critical Infrastructure Act 2018* (SOCI Act).

The Framework also has a number of Australian and global informative references mapped to each practice for additional guidance. These 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.

Appendix E: How does the AESCSF differ from the C2M2?

The AESCF retains the core structure of the C2M2, with the following revisions:

- the addition of a domain for Australian Privacy Management (APM) concepts, such as managing personal information in a way that is consistent with Australian Privacy Principles and the Office of the Australian Information Commissioner's privacy management Framework.
- the integration of management practices within other domains, rather than as a separate domain
- the simplification of the assessment of practices within Maturity Indicator Level 1 (refer to Section **Error! Reference source not found.** below) are assessed using yes or no and no longer assessed u sing 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.
- the integration of Anti-Patterns.
- the integration of context and guidance statements for practices and Anti-Patterns.
- The integration of informative references that link the Framework to other sources of good practice.
- the integration of 'security profiles' to guide target state implementation, as provided by the ACSC.

Table 13. Comparison between C2M2 V2.1 and AESCSF V2

C2M2 V2.1		AESCSF V2	
Component	**Description**	**Component**	**Description**
C2M2 Domains	The C2M2 has 10 domains	**AESCSF Domains**	The AESCSF has 11 domains
Coverage of 'Privacy' as a Concept	The C2M2 **implicitly** covers 'Privacy' as a concept	**Coverage of 'Privacy' as a Concept**	The AESCSF **explicitly** covers 'Privacy' as a concept, with its own Australian Privacy Management domain
C2M2 Practice Groupings	1 available; the Maturity Indicator Level (MIL)	**AESCSF Practice Groupings**	2 available; the MIL and the Security Profile (SP)
Nature of C2M2 Subject Matter	All C2M2 activities describe **good** behaviour (i.e., Practices)	**Nature of AESCSF Subject Matter**	Most AESCSF activities describes **good** behaviour (i.e., Practices), some describe **bad** behaviour. These are 'Anti-Patterns' and considered the non-negotiables of cyber.
C2M2 Practice Guidance	The C2M2 contains 'Help Text' as of V2.0 in 2021	**AESCSF Practice Guidance**	The AESCSF contains 'Context and Guidance' as of V1.0 in 2018

Appendix F: V1 Information

The following tables provides a high-level introduction to the AESCSF V1, for more details, please review the historical supporting materials and guidance on the AEMO website.

Table 14. AESCSF V1 SP and MIL practices comparison to AESCSF V2

	AESCSF V1				AESCSF V2			
	MIL-1	MIL-2	MIL-3	TOTAL	MIL-1	MIL-2	MIL-3	TOTAL
SP-1	57	27	4	88	62 (+5)	57 (+30)	4 (0)	123 (+35)
SP-2	0	94	18	200 (112+88)	0	123 (+29)	29 (+11)	275 (152+123) (+40)
SP-3	0	0	82	282 (82+200)	0	0	79 (-3)	354 (79+275) (-3)

Table 15. Security Profiles for AESCSF V1

Security Profile (SP)	Practices and Anti-Patterns			Total required to achieve SP
	MIL-1	MIL-2	MIL-3	
Security Profile 1 (SP-1)	57	27	4	88
Security Profile 2 (SP-2)	0	94	18	200 (112+88 from SP-1)
Security Profile 3 (SP-3)	0	0	82	282 (82+200 from SP-2)

Table 16. Priority practices by security profile for AESCSF V1

Domain	Priority practices and Anti-Patterns		
	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	-	-

Appendix G: Framework change management

To address participant feedback from prior programs and to accommodate the expansion to additional sub-sectors, some changes were made to the Framework and supporting artefacts.

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

Table 17. AESCSF artefact change log

Reference	Document	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 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.
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?”.

Reference	Document	Change description
		• 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.
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.
2022-1	CAT	• Addition of a Liquid Fuels Criticality Assessment Tool (L-CAT) to support the inclusion of the liquid fuels sub-sector in the 2022 Program.
2022-2	Glossary	• Added new terms and definitions. Further detail is provided in the Glossary version 2022.
2022-3	Education Workshop Presentation	• Revision of the Education Workshop Presentation to reflect the changes in this document.
2022-3	Guidance material for low criticality organisations	• Guidance material to assist organisations in getting started on their uplift journey
2023	Framework Core (AESCSF V2)	• Increase of 72 practices (total 354 practices) – *Refer to AESCSF Core Change Log guide for full details* • Revisions to two-thirds of model practices including substantive changes and clarifications along with additions, deletions, and combining of practices

Reference	Document	Change description
		• Addition of a Cybersecurity Architecture **domain** focused on planning, designing, and managing the cybersecurity control environment • Significant updates of the Risk Management domain to incorporate leading risk management practices and enhance coordination between cyber and enterprise risk management • Refresh of the Dependencies domain, now called the Third-Party Risk Management domain**,** to ensure the model effectively addresses third-party IT and OT cyber security risks, like sensitive data in the cloud and vendors with privileged access, as well as build supply chain security into organisational culture • Integration of Information Sharing domain activities into the Threat and Vulnerability Management and Situational Awareness domains • Addition of help text for each practice to improve clarity and consistency in how practices are applied • Increase in number of Priority Practices (70)
2023	Lite Framework	• AESCSF V1 discontinued and replaced with V2
2023	AESCSF Overview Document	• Inclusion of AESCSF V2 • CRIMP obligations under SOCI • Updated ACSC Security Profiles • Format revisions
2023	Guidance material for low criticality organisations	• Inclusion of AESCSF V2 • CRIMP obligations under SOCI • Updated ACSC Security Profiles
2023	Education Workshop Presentation	• Updates in line with AESCSF Overview document
2025	Guidance material for DER/CER organisations	• Updated Guidance material for low criticality organisations to accommodate focus on DER/CER organisations
2025	Education Presentation Pack	• Refreshed Education Workshop Presentation
2025	AESCSF Overview Document	• Reduced focus on AESCSF V1 • Separation of AESCSF Program supporting references • Format revisions