Australian Energy Sector Cyber Security Framework (AESCSF)

Overview

2023 AESCSF Program

Important notice

Purpose

This document is made available by The Australian Energy Market Operator (AEMO) to provide information about the 2023 Australian Energy Sector Cyber Security Framework (AESCSF) Program.

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

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 on the AEMO website.

Table of contents

Tables

Figures

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.**

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.

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.

2. About the Framework

The AESCSF is a cyber security Framework developed and tailored to the Australian energy sector. The purpose of the Framework is to enable energy participants across the electricity, gas and 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 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 Australian Cyber Security Centre’s *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 B: Alignment of the Framework to best practice.

2.1. How the Framework was developed?

It was 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*. Since then, the Framework has 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)
- Department of Climate Change, Energy, the Environment and Water (DCCEEW)
- Australian Cyber Security Centre (ACSC)
- The Department of Home Affairs (DHA)
- Energy market participants

2.2. The Framework's evolution 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
- held 4 meetings
- 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.

Table 1. 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

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 framework.

The table below compares the breakdown of AESCSF v1 and v2 as relevant to the Security Profile (SP) and Maturity Indicator Level (MIL).

Table 2. 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)

As a recognised compliance framework for assessing your cyber maturity to support Risk Management Program regulatory obligations under the SOCI Act the Framework offers extensive benefits to market participants.

AESCSF v2 is currently recognised as an v1 equivalent framework under the SOCI Act. It is expected in future years that AESCSF v2 will replace v1 under the Act, at that time AESCSF v1 will no longer be available as part of the AESCSF program.

Through the 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.

2.3. Why the Framework is important?

The Framework plays a crucial role in improving the cyber security of Australia’s energy sector in a scrutinised, complex, and ever-evolving landscape around data protection. The tailored Australian energy sector Framework has been developed to manage cyber security risk and reduce reputational risk and the potential disruption of 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.
- The 2023 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

2.4. 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 3. Recommended AESCSF participants

Electricity	Gas	Liquid Fuels
• 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

2.5. How the Framework is 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.

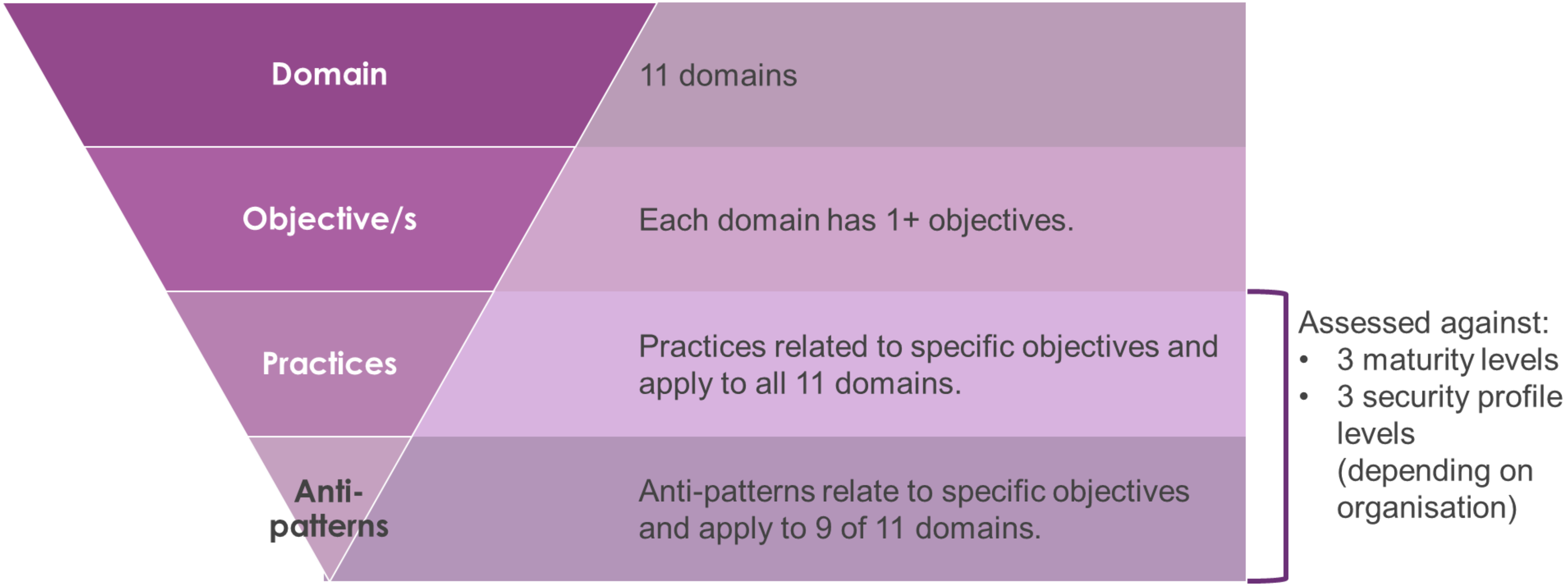
Domain
11 domains
Objective/s
Each domain has 1+ objectives.
Practices
Practices related to specific objectives and apply to all 11 domains.
Anti-patterns
Anti-patterns relate to specific objectives and apply to 9 of 11 domains.
Assessed against:
• 3 maturity levels
• 3 security profile levels (depending on organisation)

Figure 1 How the Framework is structured

2.5.1. 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.

2.5.2. The domains

In both AESCSF v1 and v2 there are 11 domains. The Information Sharing and Communications domain from v1 has been incorporated into other domains as part of v2 while the Cyber Security Architecture domain has been added.

Table 4. Domains and their descriptions

Domain	Acronym	Description
Risk management (RISK)	RM	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)	CPM	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)	ACM	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)	IAM	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.
Information sharing and communications	ISC	**AESCSF v1 Only** Establish and maintain relationships with internal and external entities to collect and provide cybersecurity information, including threats and vulnerabilities, to reduce risks and to increase operational resilience, commensurate with the risk to critical infrastructure and organisational objectives.
Cyber Security Architecture (ARCHITECTURE)		**AESCSF v2 Only** 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.

Domain	Acronym	Description
Threat and vulnerability management (THREAT)	TVM	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)	SA	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)	IR	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)	EDM	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)	WM	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)	APM	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).

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

Table 5. Maturity Indicator Levels (MILs) and their descriptions

Maturity level	Criteria overview
Maturity Indicator Level 1 (MIL 1)	The practice is performed.

Maturity level	Criteria overview
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

2.5.4. 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 Australian Cyber Security Centre, 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).

- Entities only achieve an SP level if all practices and anti-practices indicated for that SP level are present or absent for all domains.
- SPs include identified priority practices. It is recommended that the priority practices be completed first as part of any uplift program.
- SPs were defined by the Australian Cyber Security Centre, in consultation with AEMO and industry representatives.

Table 6. Security Profiles (SPs) and their descriptions

Security Profile	Criteria overview
Security Profile 1	• All SP-1 Practices and Anti-Patterns must be completed to achieve Security Profile 1 • SP1 (v1) is a recognised compliance Framework under the SoCI Act (2018). • All Practices and Anti-Patterns at MIL-1 are included within Security Profile 1 with the addition of select Practices and Anti-Patterns at MIL-2 and MIL-3. • Security Profile 1 contains 20 (AESCSF v1) / 29 (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 2	• All SP-1 & SP-2 Practices and Anti-Patterns must be completed 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 5 (AESCSF v1) / 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 completed to achieve Security Profile 3 • All Practices and Anti-Patterns at MIL-3 are covered in Security Profile 3. • Achieving Security Profile 3 is identical to achieving Maturity Indicator Level (MIL) 3. • Security Profile 3 contains 1 (AESCSF v1) / 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.

2.5.5. How maturity is 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.

Refer to Appendix D: Calculating maturity levels to see how the MILs assessment levels.

2.5.6. Achieving security profiles

Security profiles 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 7. 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 8. 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	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
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 9. Sub-sector organisations who should complete Criticality Assessment Test

Electricity Criticality Assessment Tool (E-CAT)	Gas Criticality Assessment To (G-CAT)	Liquid Fuels Criticality Assessment To (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).

3.2. 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 10. 2023 AESCSF assessment options

AESCSF version 2, full assessment (v2)	
• 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, full assessment (v1)	
• 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) – Australian Cyber Security Centre'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, full assessment (v2 lite)	
• 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.

3.3. 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. That's why AEMO recommends 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 (and in some cases supply chain) 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 11. 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

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.

3.4. Conduct the assessment

3.4.1. 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 of roles that should be involved in contributing to the assessment.

Table 12. Roles that may contribute to an organisation's assessment

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

3.4.2. Take notes

While there is no requirement to upload any evidence/documentation to support your assessment, it is useful 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.

The assessment tool includes free-text fields to support note taking relevant to each practice and anti-pattern. AEMO recommends capturing the following information against each practice:

- 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 2023 AESCSF Program, resources are available for your organisation on the AEMO website.

Appendix A: Frequently Asked Questions

Is completing an Assessment mandatory?

The Assessment is 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 are the results of my AESCSF data used?

Data from AESCSF Self-Assessments are aggregated and anonymised by KPMG to provide 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.

What happens to my data?

Information and data collected will only be used for the purposes of providing anonymised and aggregated benchmarking across the energy sector. As mentioned, this information will then be used to generate the Cyber Security Preparedness of the Australia's Energy Sector Annual Report which will be subsequently presented to government officials and Cyber Ministers.

At the end of the Program the data will either be securely kept by the current vendor (KPMG), or it will be securely transferred to another provider for use in next years' Year-on-Year (YoY) comparison.

KPMG are responsible for collecting personal and business information from Participants. KPMG are responsible for the administration, secure storage, analysis, aggregation, and de-identification of the data collected. AEMO will not have access to your data including individual results. The Assessment vendor will be the custodian.

Please email aescsf@aemo.com.au if you would like to receive the full *AESCSF Assessment Portal Terms and Conditions*.

Will I receive year-on-year comparison data in 2023?

Due to the change in Assessment provider, your year-on-year (YoY) data is not available in 2023. Previous data will be permanently destroyed. In 2022, Participants were provided with a one-month window to download their previous data. Previous data is no longer available for those that did not download it at the time. AEMO also notes that organisations attempting AESCSF v2 for the first time in 2023 will not have prior year data to compare to.

AEMO acknowledges that the lack of YoY organisational comparisons for v1 assessments this year will be disappointing and frustrating to some Participants, however, data that is collected as part of the 2023 Program will be used to perform YoY comparison in 2024. This data will be held by the current vendor (KPMG), or securely transferred to next years' vendor for the purpose of enabling your Year-on-Year (YoY) comparison.

Who has access to my 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 Assessment data.

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

AEMO will not have access to your assessment or data including individual results. The Assessment vendor, KPMG, will be the custodian.

I can't complete the Assessment during the program period. Can I still do the AESCSF assessment?

The AESCSF assessment is available year-round through the Offline Toolkits available on the AESCSF webpage (Available once the 2023 Program has been completed - expected December 2023 – the Offline Tool Kits will also be made available on the Trusted Information Sharing Network (TISN) Teams Site at this time). You can complete the assessment anytime, however to be able to benchmark your organisation against energy sector peers or have your aggregated and de-identified data included in the final report you would need to submit your AESCSF assessment on the Portal during the program period. **Can my organisation complete a Framework Assessment if they are not a participant?**

All Australian energy organisations are encouraged to complete an Assessment to evaluate and improve their cyber security capability and maturity. However, if you are not a market participant, your results will not be included in the *Cyber Security Preparedness of the Australia's Energy Sector Annual Report* to Australia's Energy Ministers.

How do I access the AESCSF Assessment?

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

How do I participate in the AESCSF Program?

To participate in the AESCSF program contacts (e.g. CEO/CISO) will receive a welcome email containing registration details at the beginning of the program period. If you are expecting to be invited to participate in the program and have not received the welcome email, please contact the AESCSF Project Team (aescsf@aemo.com.au).

What are the differences between AESCSF v1 and v2?

For a summary of changes, please refer to Appendix E of this document and 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 going to do a Lite Assessment. Is this included in the benchmarking results?

Dashboards will be available at the completion of the Lite assessment for organisations to review their results, however benchmarking against other organisations is not available for Lite assessments. If a Lite Assessment is completed, the toolkit will transfer responses into a full Assessment to enable benchmarking. This process will not be visible to Participants but will enable transition to full Assessments in subsequent years.

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 Framework 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.

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 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.
- 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.

How do I assess practice implementation as per the Framework?

Error! Reference source not found.table below provides example of how to assess and respond to a practice for Identity and Access Management Practices:

Table 13. Example responses for Framework Assessment

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

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

Do I need to get sign off on the results?

Once you have completed the Assessment, you will be prompted to indicate that you have:

- Briefed the appropriate management structures of the entities you are completing this Assessment for and;
- Permission to submit the Assessment on behalf of the organisation.

The option is available to upload a CEO attestation and is encouraged but not mandatory.

This process replaces the old process of CEO attestation.

Appendix B: 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 Australian Cyber Security Centre'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 C: 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 14. 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	-	-

Table 15. 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 D: Calculating maturity levels

Table 16. Calculating Maturity Levels

MIL	Implementation response	The practice is performed	The practice is documented	Stakeholders of the practice are identified and involved.	Adequate resources are provided to support the practice (people, funding, and tools).	Standards and/or guidelines have been identified to guide the implementation of the practice	Activities are guided by policies (or other organisational directives) and governance	Personnel performing the practice have adequate skills and knowledge	Policies include compliance requirements for specified standards and/or guidelines	Responsibility and authority for performing the practice is assigned to personnel	Activities are periodically reviewed to ensure they conform to policy
MIL1	No										
	Yes	✓									
MIL 2	Partially	✓	✓								
	Largely	✓	✓	✓	✓						
	Fully	✓	✓	✓	✓	✓					
MIL 3	Partially	✓	✓	✓	✓	✓	✓	✓			
	Largely	✓	✓	✓	✓	✓	✓	✓	✓	✓	
	Fully	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Appendix E: 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 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.
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”

Reference	Document	Change description
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.
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

Reference	Document	Change description
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 • 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 inline with AESCSF Overview document