Australian Energy Sector Cyber Security Framework

AESCSF Version 2 – Summary of Changes

2023 AESCSF Program

Context and Overview

Developed in 2018, the Australian Energy Sector Cyber Security Framework (AESCSF) is a cyber security Framework tailored to the Australian energy sector. Since the first annual AESCSF Assessment Program commenced in 2018, the AESCSF has had minor annual updates.

In consultation with industry and governments, the Australian Energy Market Operator (AEMO) and the Australian Government Department of Climate Change, Energy, the Environment and Water (DCCEEW) updated the AESCSF in 2022 to align with current international standards and address emerging technologies and the evolving cyber threat landscape.

The AESCSF foundation is based on the US Department of Energy's (DOE) Cybersecurity Capability Maturity Model (C2M2) Version 1.1. The C2M2 has been through a process of updating culminating in the publication of Cybersecurity Capability Maturity Model (C2M2) Version 2.1 (referred to as C2M2 v2.1) in June 2022.

AESCSF v2 incorporates C2M2 v2.1. This will enhance industry cyber security risk management and assist industry with future planning and investment decisions.

This document provides a summary of key changes between the AESCSF (Version 1, referred to as AESCSF v1) and the updated AESCSF that was developed in 2022 (Version 2, referred to as AESCSF v2).

AESCSF Version 2

The update to AESCSF v2 from C2M2 v2.1 has resulted in an increase of 72 practices (i.e., 20 per cent additional practices). A summary of the difference between C2M2 v2.1 and AESCSF v2 is provided in Table 1.

The AESCSF includes additional material when compared to C2M2, tailoring it to the Australian energy sector. The table below summarises the total number of practices and anti-patterns contained in both AESCSF v1 and AESCSF v2. Anti-patterns describe poor cyber security behaviours and activities and were adopted from the UK equivalent of the Australian Cyber Security Centre (ACSC) – the National Cyber Security Centre (NCSC).

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 describe **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

Table 1: C2M2 v2.1 to AESCSF v2 Comparison

AESCSF v2 Update Approach

The practices and anti-patterns in AESCSF v2 have been mapped against those from AESCSF v1 to provide a view on the degree of overlap and change between the two Frameworks. For this mapping exercise, practices were analysed between versions, with each practice being assessed as one of the following based on the strength of the match:

- **Case 1: Match** – The practice wording and / or intention is *effectively the same*.
- **Case 2: Similar intent** – The practice wording and the intention is *similar*, however there are *some differences* in the practice.
- **Case 3: Variation to intent** – The practice wording and intention has *some similarity*, however there is a *significant variation* in the intention of the practice.
- **Case 4: No match / new item** – The practice wording and / or intention is *distinctly different* to practices from AESCSF v1.
- **Case 5: No direct correlation from v1 to v2 –** The practice wording and / or intention from AESCSF v1 could not be mapped to any practices from v2.

A summary of the matching outcomes is provided in Tables 2 and 3. An example of each of the 4 cases can be found in the Appendix.

Additionally:

- Management activities from the C2M2 v2.1 will be integrated in the AESCSF v2 scoring methodology.
- This reduces the overall number of practices co-opt- ed from the C2M2 version v2.1 from 356 to 296.

AESCSF Review Working Group

The AESCSF was updated in consultation with the AESCSF Review Working Group (AESCSF-RWG). The AESCSF-RWG:

- Was convened in early 2022
- Held 4 meetings
- Held 1 working session to review the v2 draft
- Consisted of more than 50 members
- Consisted of more than 40 organisations
- Engaged with the ACSC to determine new Security Profiles (SPs)
- Conducted a detailed review of AESCSF Anti-Pat- terns via an interactive survey
- Conducted a detailed review of the draft AESCSF v2
- Was a key point of engagement between industry and government

AESCSF v1		AESCSF v2	
Framework Core Component	**Number of Practices / Anti-Patterns**	**Framework Core Component**	**Number of Practices / Anti-Patterns**
U.S. C2M2 Version 1.1 Practices*	224	U.S. C2M2 Version 2.1 Practices*	296 (+72)[1]
Australian Privacy Management Domain	16	PRIVACY Domain	16
Anti-Patterns	42	Anti-Patterns	42
Total	**282**	**Total**	**354 (+72)**

Table 2: AESCSF v1 to v2 Comparison

1 Number indicates change from AESCSF v1

Framework Mapping Outcome	Number of Practices / Anti-Patterns	Percentage of Total
Case 1: Match	140	40%
Case 2: Similar intent	53	15%
Case 3: Variation to intent	97	27%
Case 4: No match / new item	64	18%
Case 5: No direct correlation from v1 to v2	50	N/A
Total	**354**	**100%**

Table 3: Mapping outcomes from AESCSF v1 and AESCSF v2

Note: The US DOE published on July 2023 the C2M2 Version 1.1 to Version 2.1 mapping[1].

Practice Updates Originating from the C2M2 Version 2.1

As outlined by the US DOE, while the overall structure of the C2M2 model remains the same, Version 2.1 reflects several key updates since the last major release of version 1.1 in 2014 [2], including:

- **Revisions to two-thirds of model practices** - including substantive changes and clarifications - along with additions, deletions, and combining of practices.
- **Addition of a cyber security architecture domain** focused on planning, designing, and managing the cyber security control environment.
- **Significant updates to 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.

Several key updates were made between C2M2 version 2.0 and C2M2 Version 2.1 (the current version) based on industry and government feedback:

- **Addition** of practices to improve the comprehensiveness of cyber security activities addressed by the model.
- **Addition** of practices to form a closer alignment with the National Institute of Standards and Technology (NIST) Cybersecurity Framework[3]
- **Reordering and revision** of practices to improve practice progression across maturity indicator levels and within objective areas.
- **Clarification of language** and improved consistency of concepts across the model.

Note: Following the successful introduction of 'Context and Guidance' in AESCSF v1 (2018), Version 2.0 (2021) and 2.1 (2022) of the C2M2 includes similar 'Help Text'. This provides additional detail, interpretation, and guidance for assessment of the practice.

1 https://c2m2.doe.gov/resources
2 https://www.energy.gov/ceser/articles/department-energy-releases-version-21-update-cybersecurity-capability-maturity-model
3 Between C2M2 version 2.0 and 2.1, reference to a C2M2 to NIST CSF mapping appear to have been removed. The AESCSF project team has contacted the DOE for clarification.

Table 4 compares the breakdown of AESCSF v1 and v2 as relevant to the Security Profile (SP) and Maturity Indicator Level (MIL).

SP / MIL	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 4: AESCSF v2 Security Profile (SP) and Maturity Indicator Level (MIL) Comparative Summary

Security Profile Updates

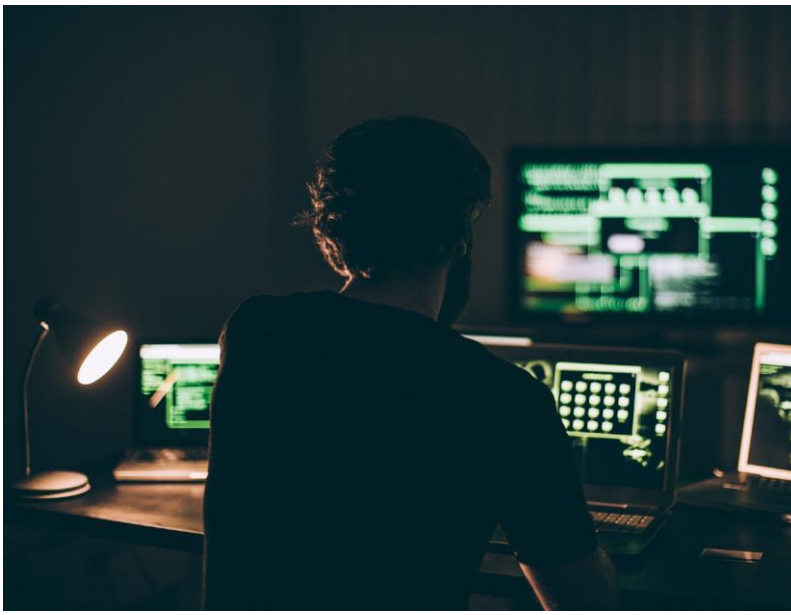
The cyber security threat landscape evolves quickly, and the Australian Cyber Security Centre (ACSC) has provided updated Security Profile guidance for AESCSF v2. This guidance is based on their analysis of current threat activity both within Australia and globally. In summary:

- 123 practices would be required to achieve Security Profile 1 (SP-1).
- This is an increase of 35 (29 per cent) from the 88 required in AESCSF v1.

A summary of the total number of practices / anti-patterns across each Maturity Indicator Level (MIL) that are included at each Security Profile are outlined in Table 4.

Australian Privacy Management (PRIVACY) Domain Updates

For consistency with the naming of domains in the C2M2, the Australian Privacy Domain (APM) was renamed to PRIVACY. Minor updates were made to the context and guidance of 4 of the practices in this domain (1A, 1C, 1H and 1M).



	Measure			
PracticeId	Clarity	Reasonableness	Threat relevance	Grand Total
TVM-AP2	60	59	60	179
IR-AP2	57	59	59	175
IR-AP1	55	60	59	174
TVM-AP3	58	56	59	173
IR-AP3	58	60	55	173
RM-AP1	58	57	56	171
SA-AP7	60	56	54	170
SA-AP5	60	56	54	170
TVM-AP1	57	55	57	169
SA-AP10	55	56	58	169
RM-AP4	58	57	54	169
ACM-AP1	55	57	57	169
SA-AP11	58	54	56	168
SA-AP1	59	53	56	168
SA-AP8	56	54	57	167
WM-AP1	57	53	56	166
SA-AP2	58	52	56	166
CPM-AP2	54	54	58	166
SA-AP9	57	54	54	165
RM-AP3	57	54	54	165
IAM-AP5	56	54	55	165
SA-AP4	57	53	54	164
WM-AP3	55	55	53	163
CPM-AP1	53	54	56	163
ACM-AP3	59	50	52	161
IAM-AP8	55	48	57	160
IAM-AP4	56	49	55	160
RM-AP2	51	52	56	159
IAM-AP1	53	55	51	159
IAM-AP2	54	50	54	158
SA-AP6	54	51	52	157
IAM-AP7	56	49	52	157
IAM-AP10	54	50	52	156
WM-AP2	49	54	52	155
SA-AP3	52	50	52	154
CPM-AP3	50	49	54	153
APM-AP1	54	51	48	153
IAM-AP11	52	50	50	152
IAM-AP9	51	48	50	149
IAM-AP6	50	48	50	148
IAM-AP3	46	49	46	141
ACM-AP2	45	43	43	131

Anti-Pattern Updates

Anti-patterns complement the 'good-practice' capabilities described by the practices and provide the 'bad-practice' indicators of 'cyber insecurity'. The presence of an anti-pattern typically circumvents key cyber security controls, and subsequently, presents a heightened level of cyber security risk to an organisation. The Australian energy sector, via the AESCSF-RWG, was consulted on the 42 anti-patterns in the AESCSF v2.

Feedback identified 10 anti-patterns that could be improved. This has been determined by a score of less than 50 points on any of the three key feedback metrics.

The three key feedback metrics are:

1. Clarity
2. Reasonableness
3. Threat relevance

The 10 anti-patterns that were identified for improvement were:

1. IAM-AP8 (reasonableness)
2. IAM-AP4 (reasonableness)
3. IAM-AP7 (reasonableness)
4. WM-AP2 (clarity)
5. CPM-AP3 (reasonableness)
6. APM-AP1 (threat relevance)
7. IAM-AP9 (reasonableness)
8. IAM-AP6 (reasonableness)
9. IAM-AP3 (clarity, reasonableness, threat relevance)
10. ACM-AP2 (clarity, reasonableness, threat relevance)

Based on this information, the AESCSF Project Team made minor, targeted adjustments to each of the 10 anti-patterns, based on the low-scoring metric(s). The MIL and SP of each anti-pattern has remained the same.

Australian References Updates

The AESCSF includes references to key Australian frameworks and legislation, including the Information Security Manual (ISM) and the Essential Eight (E8). AESCSF v2 practices and anti-patterns were mapped against these Frameworks in 2022. The outcomes of this are included under the Australian References column in the AESCSF v2 Framework Core.

Additional Notes for AESCSF v2

Supporting materials to the AESCSF Core v2, e.g., the Lite Framework, designation of 'Priority Practices', and education material are available on the AEMO website.

The AESCSF Lite is purpose-built to enable organisations to assess against Security Profile 1 (SP-1), asking multiple-choice questions instead of the full Framework's practices and anti-patterns. The new AESCSF Lite v2 has superseded the original Lite Framework.

The Priority Practices within AESCSF v1 were designated by the ACSC, to guide organisations that are seeking to prioritise the basics. A similar designation for AESCSF v2 has been completed and published on the AEMO website.

Appendix

An example of each case type from the AESCSF v2 update approach is below.

Case 1: Match

- V1 practice: ACM-1a "There is an inventory of OT and IT assets that are important to the delivery of the function; management of the inventory may be ad hoc".
- V2 practice: ASSET-1a "IT and OT assets that are important to the delivery of the function are inventoried, at least in an ad hoc manner".

Case 2: Similar intent

- V1 practice: ACM-1d "Inventoried assets are prioritised based on their importance to the delivery of the function".
- V2 practice: ASSET-1c "Inventoried IT and OT assets are prioritized based on defined criteria that include importance to the delivery of the function".

Case 3: Variation to intent

- V1 practice: ACM-1e "There is an inventory for all connected IT and OT assets related to the delivery of the function".
- V2 practice: ASSET-1b "The IT and OT asset inventory includes assets within the function that may be leveraged to achieve a threat objective".

Case 4: No match / new item

- V2 practice: ASSET-1h "Data is destroyed or securely removed from IT and OT assets prior to redeployment and at end of life".

Case 5: No direct correlation from v1 to v2

- V1 practice: CPM-1F "The Cyber Security Program strategy is approved by senior management"
- V2 practice: Many of the practices in v2 refer to senior management sponsorship of a cyber security program strategy, as well as involvement in the development, maintenance, and enforcement of the strategy and its policies. Although a direct correlation to another practice cannot be made the intent has been maintained through one or more other practices in v2.