Australia Energy Sector Cyber Security Framework (AESCSF)

Quick Reference Guide – Domain Overview & Key Terms

Domain		Domain Description
Risk Management	**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	**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	**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	**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**	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.
Threat and Vulnerability Management	**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	**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	**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	**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	**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	**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).

Term	Definition
access	Ability and means to enter a facility, to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions.
ad hoc	In the context of this model, ad hoc (i.e., an ad hoc practice) refers to performing a practice in a manner that depends largely on the initiative and experience of an individual or team (and team leadership), without much in the way of organisational guidance in the form of a prescribed plan (verbal or written), policy, or training. The methods, tools, and techniques used, the priority given a particular instance of the practice, and the quality of the outcome may vary significantly depending on who is performing the practice, when it is performed, and the context of the problem being addressed. With experienced and talented personnel, high-quality outcomes may be achieved even though practices are ad hoc. However, because lessons learned are typically not captured at the organisational level, approaches and outcomes are difficult to repeat or improve across the organisation.
anomalous	Inconsistent with or deviating from what is usual, normal, or expected.
asset	Something of value to the organisation. Assets include many things, including technology, information, roles performed by personnel, and facilities. For the purposes of this model, assets to be considered are IT and OT hardware and software assets, as well as information essential to operating the function.
confidentiality	The preservation of authorised restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. For an information asset, confidentiality is the quality of being accessible only to authorised people, processes, and devices.
controls	The management, operational, and technical methods, policies, and procedures-manual or automated-(i.e., safeguards or countermeasures) prescribed for an IT and ICS to protect the confidentiality, integrity, and availability of the system and its information.
credential	An object or data structure that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a Subscriber.

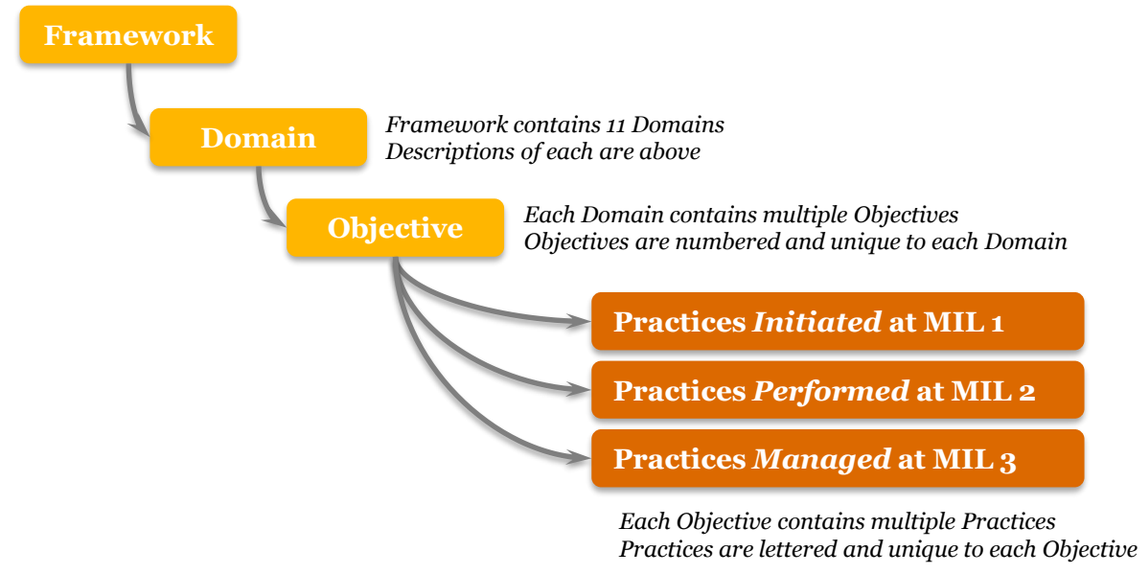
Australia Energy Sector Cyber Security Framework (AESCSF)

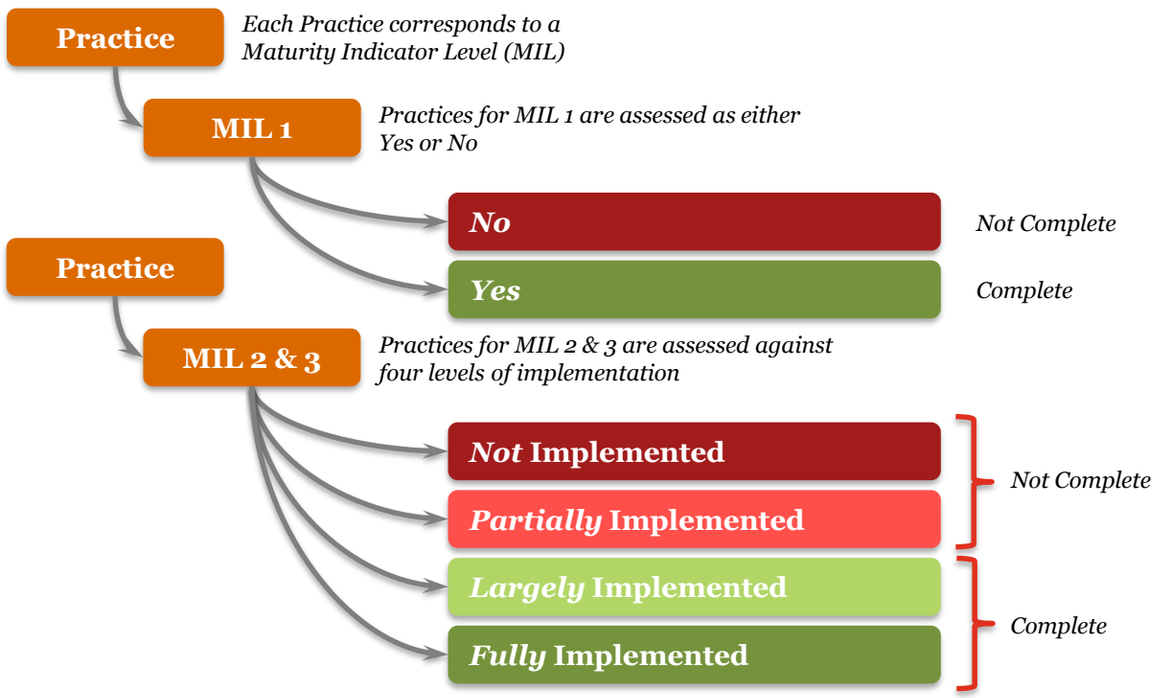
Quick Reference Guide – Key Terms (continued)

Term	Definition
current	Updated at an organisation-defined frequency (e.g., as in the asset inventory is kept 'current') that is selected such that the risks to critical infrastructure and organisation objectives associated with being out-of-date by the maximum interval between updates are acceptable to the organisation and its stakeholders.
establish and maintain	The development and maintenance of the object of the practice (such as a program). For example, 'Establish and maintain identities' means that not only must identities be provisioned, but they also must be documented, have assigned ownership, and be maintained relative to corrective actions, changes in requirements, or improvements.
event	Any observable occurrence in a system or network. Depending on their potential impact, some events need to be escalated for response. To ensure consistency, criteria for response should align with the organisation's risk criteria.
function	The high-level electricity system activity or set of activities performed by the utility to which the model is being applied. Generally, the function will be generation, transmission, distribution, and/or markets. When using the AESCSF evaluation survey, the function is the organisational line-of-business (generation, transmission, distribution, or markets) that is being evaluated by completing the model.
governance	An organisational process of providing strategic direction for the organisation while ensuring that it meets its obligations, appropriately manages risk, and efficiently uses financial and human resources. Governance also typically includes the concepts of sponsorship (setting the managerial tone), compliance (ensuring that the organisation is meeting its compliance obligations), and alignment (ensuring that processes such as those for cybersecurity program management align with strategic objectives).
guidelines	A set of recommended practices produced by a recognised authoritative source representing subject matter experts and community consensus, or internally by an organisation. See standard.
identity	The set of attribute values (i.e., characteristics) by which an entity is recognisable and that, within the scope of an identity manager's responsibility, is sufficient to distinguish that entity from any other entity.
incident	An event (or series of events) that significantly affects (or has the potential to significantly affect) critical infrastructure and/or organisational assets and services and requires the organisation (and possibly other stakeholders) to respond in some way to prevent or limit adverse impacts. See also computer security incident and event.
institutionalisation	The extent to which a practice or activity is ingrained into the way an organisation operates. The more an activity becomes part of how an organisation operates, the more likely it is that the activity will continue to be performed over time, with a consistently high level of quality. ('Incorporated into the ingrained way of doing business that an organisation follows routinely as part of its corporate culture.' - CERT RMM). See also maturity indicator level.
logging	Logging typically refers to automated recordkeeping (by elements of an IT or OT system) of system, network, or user activity. Logging may also refer to keeping a manual record (e.g., a sign-in sheet) of physical access by personnel to a protected asset or restricted area, although automated logging of physical access activity is commonplace. Regular review and audit of logs (manually or by automated tools) is a critical monitoring activity that is essential for situational awareness (e.g., through the detection of cybersecurity events or weaknesses).
monitoring	Collecting, recording, and distributing information about the behaviour and activities of systems and persons to support the continuous process of identifying and analysing risks to organisational assets and critical infrastructure that could adversely affect the operation and delivery of services.
periodic review/activity	A review or activity that occurs at specified, regular time intervals, where the organisation-defined frequency is commensurate with risks to organisational objectives and critical infrastructure.
personnel	Employees of the organisation. This includes full time, part time, and contracted employees.
risk	A measure of the extent to which an organisation is threatened by a potential circumstance or event, and typically a function of (1) the adverse impacts that would arise if the circumstance or event occurs and (2) the likelihood of occurrence.
stakeholder	An external organisation or an internal or external person or group that has a vested interest in the organisation or function (that is being evaluated using this model) and its practices. Stakeholders involved in performing a given practice (or who oversee, benefit from, or are dependent upon the quality with which the practice is performed) could include those from within the function, from across the organisation, or from outside the organisation.
threat	Any circumstance or event with the potential to adversely impact organisational operations (including mission, functions, image, or reputation), resources, and other organisations through IT, OT, or communications infrastructure via unauthorised access, destruction, disclosure, modification of information, and/or denial of service.
vulnerability	A cybersecurity vulnerability is a weakness or flaw in IT, OT, or communications systems or devices, system procedures, internal controls, or implementation that could be exploited by a threat source. A vulnerability class is a grouping of common vulnerabilities.

Australia Energy Sector Cyber Security Framework (AESCSF)

Quick Reference Guide – Framework Structure





*Where an **Anti-Pattern** is present within the organisation, the practice must be assessed as No (at MIL 1) and either Not or Partially Implemented (at MIL 2 or 3)*

How Do I Assess Implementation?

Quick Reference Guide – Management Characteristics

MIL 1

Practice

&

Figure 1

Practices *Initiated* at MIL 1	
	No activities that evidence the practice are visible within the function
	Some activities that evidence the practice are visible within the function. These activities are ad-hoc, and vary in frequency, accuracy, and completeness, based on the skills and tools of the personnel completing the activities

No

Yes

*Where an **Anti-Pattern** is present within the organisation, the practice must be assessed as No (at MIL 1) and either Not or Partially Implemented (at MIL 2 or 3)*

*Any **Fully Implemented** practice at **MIL 3 requires all Management Characteristics** from both MIL 2 and MIL 3.*

MIL 2

Practice

&

Figure 2

Practices *Performed* at MIL 2		
1	*Practices are **documented***	*Partially*
2	***Stakeholders** of the practice are identified and involved*	
3	*Adequate **resources** are provided to support the process (people, funding, and tools)*	*Largely*
4	***Standards** and/or guidelines have been identified to guide the implementation of the practices*	*Fully*

MIL 3

Practice

&

Figure 3

Practices *Managed* at MIL 3		
1 2 3	*Practices at **MIL 3 must also** exhibit **complete** (that is, Largely or Fully Implemented) **Management Characteristics from MIL 2.***	*Partially*
5	*Activities are guided by **policies** (or other organisational directives) and governance*	*Largely*
6	*Personnel performing the practices have adequate **skills and knowledge***	
7	*Policies include **compliance** requirements for specified standards and/or guidelines*	
8	***Responsibility and authority** for performing the practices are assigned to personnel*	
9	*Activities are **periodically reviewed** to ensure they conform to policy*	*Fully*

How Do I Assess Implementation?

Quick Reference Guide – Worked Example

*Where **Management Characteristics** are **absent**, you must lower your self-assessment response.*

Asset Change and Configuration Management

Manage Asset Configuration

ACM-2a establishes whether the function (or organisation) creates configuration baselines for information and operations technology.

- At MIL 1, this would be answered as Yes or No, acknowledging that activities at MIL 1 can be performed in an ad-hoc manner (Figure 1)

MIL 1

ACM-2c establishes whether the function (or organisation) designs the configuration baselines from ACM-2a with conscious consideration of cybersecurity objectives.

- At MIL 2, this would be answered against one of four levels of implementation: Not, Partially, Largely, or Fully.
- Implementation is assessed against the Management Characteristics in Figure 2. **For ACM-2a to be assessed as Largely Implemented, it must be;**
    1. documented;
    2. the stakeholders of the practice should be identified and involved, and;
    3. adequate resources (people, funding, and tools) should be provided to support the practice.

MIL 2

ACM-2e establishes whether the function (or organisation) reviews and updates the configuration baselines (created in ACM-2a, and aligned with cybersecurity objectives in ACM-2c) at a defined and regular interval.

- At MIL 3, this would be answered against one of four levels of implementation, Not, Partially, Largely, or Fully.
- Implementation is assessed against the Management Characteristics in Figure 2 and Figure 3. For ACM-2e to be assessed as Partially Implemented, the first three Management Characteristics at MIL 2 must also be present.
- **For ACM-2e to be assessed as Partially Implemented, it must be;**
    1. documented;
    2. the stakeholders of the practice should be identified and involved;
    3. adequate resources (people, tools, and funding) should be provided to support the practice;
    5. the practice should be guided by an organisational directive or governance, and;
    6. personnel performing the practice should have adequate skills and knowledge.

MIL 3