Common Cyber Security Requirements for DER

Technical Specification

April 2026

Version 1.1

Ausgrid Endeavour Energy Essential Energy evoenergy SA Power Networks synergy

Contents

1 INTRODUCTION

1.1 Purpose

This document includes technical information relevant to the security requirements of DER solution components within Australia to support emergency backstop requirements and flexible connections.

1.2 Context

The continued growth of distributed energy resources (DER) across Australia's electricity networks is a key element of Australia's path to a more sustainable and decarbonised energy future. With rooftop solar now the single largest generator in both the National Electricity Market (NEM) and the Southwest Interconnected System (SWIS), these generators now form a critical part of the electricity system. Small-scale batteries and other DER, particularly when aggregated into Virtual Power Plants, are also becoming a material component of the energy mix. This means that the correct operation of DER is now a critical factor in the continued safe and reliable operation of the power system. It is, therefore, imperative that DER and the systems that control DER are adequately protected against the risk of cyber-attack.

Utilities seeking to manage this growing risk in a nationally harmonised approach have leveraged existing work in this space to create this document. The document builds on the DER cyber requirements document originally developed by SA Power Networks, with updates to take account of the recent adoption of IEC 62443 as an Australian Standard and the ongoing updates to the Australian Energy Sector Cyber Security Framework (AESCSF).

In the near term, these cyber security requirements are intended to support the use of CSIP-AUS. In the longer term, they are a step towards nationally harmonised cyber requirements that will secure the role of DER in the ongoing decentralisation and decarbonisation of the electricity system and support streamlined entry to the Australian market for DER service providers. In future, this document and the self-assessment process described herein are likely to be superseded by a new national process, e.g. established under the proposed new CER Technical Regulator.

1.3 Scope

These cyber security requirements are applicable to all organisations who are involved in the management and/or control of DER (e.g. manufacturers, technology providers, third-party aggregators), covering their combined people, processes, and technologies that interact with or could otherwise impact on the security of the power system.

The requirements specified in this document have been selected to be applicable to the DER classes of assets and systems. Applicability is to the systems managing the DER notwithstanding the components responsible for integrations between entities on dedicated networks and internet services.

The below diagram is an example of the scope of the requirements. Individual integration methods and supporting systems may vary between each provider.

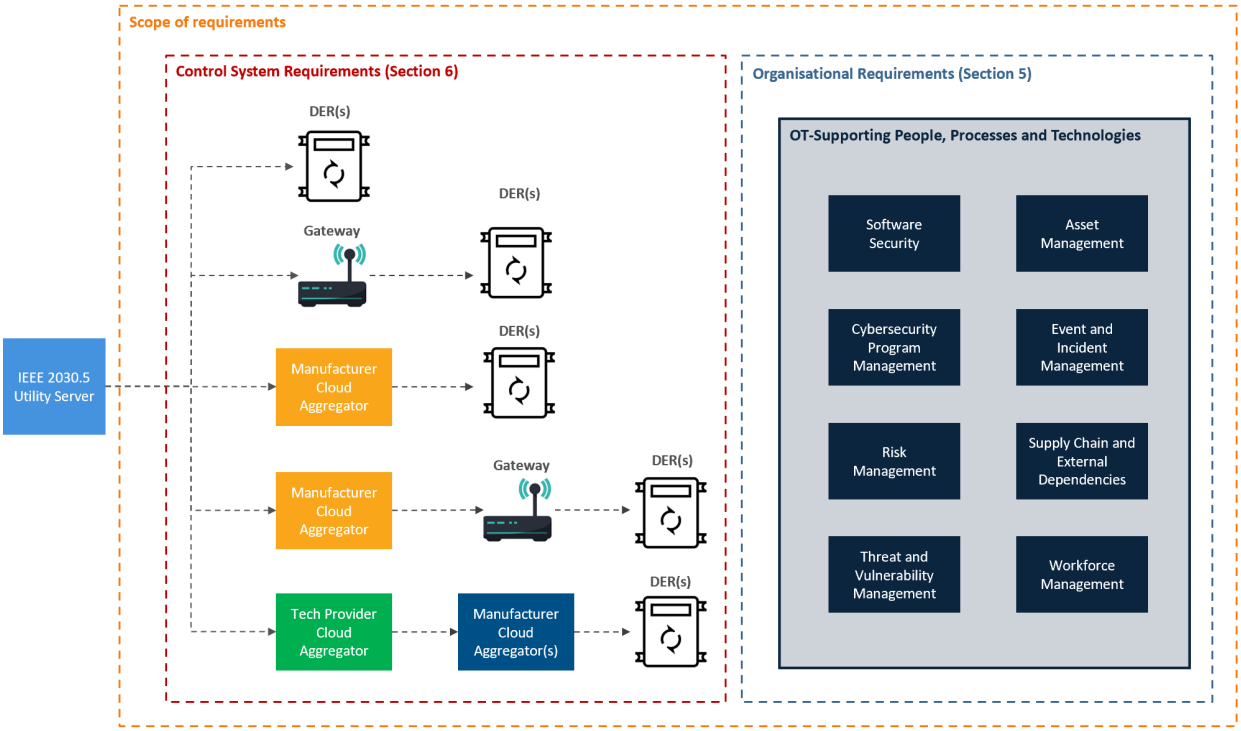

Figure 1: – Sample Scope of Requirements

The requirements applicable to an organisation are tiered based upon its total Capacity Under Management, as per Table 1 below.

Total Capacity Under Management	Tiers
Less than 50 MW	Tier 0
50 to 500 MW	Tier 1
Greater than 500 MW	Tier 2

Table 1 – Capacity Under Management Thresholds

For the purpose of this document, Capacity Under Management is defined as the organisation's total aggregate MW of DER in Australia, as follows:

- For an OEM, it is the total aggregate nameplate capacity in MW of that OEM's inverters installed in Australia
- For an aggregator, it is the total aggregate nameplate capacity in MW of end devices in Australia that are enrolled in the aggregator's control or management system(s) (whether they are managed via CSIP-AUS or some other means)
- DER, in this context, means devices associated with a connection to the distribution network that are currently in operation.

Organisations are required to self-assess their Capacity Under Management to determine which tier their organisation falls into. The method used should be sufficiently accurate to assign the organisation to one of the three tiers, but organisations are not expected to report their exact Capacity Under Management. If requested to do so, the organisation must be able to provide evidence to demonstrate that the method used to determine which tier to self-declare in is reasonable.

This measure is being employed as an interim guide to assess the criticality of the organisation in the context of the Australian power system, and may be superseded in future under a national framework for CER regulation. Similarly, the tiers in Table 1 may be revised in future as the uptake of renewables continues and the criticality of CER control systems increases.

1.4 Counterparty

For the purpose of this document, the counterparty is the party requiring the organisation to conform to these requirements. Where the document indicates that the organisation may be required to provide information or evidence or take some action, the recipient of the information or the requestor of the action will be the counterparty.

2 DEFINITIONS, REFERENCES AND ABBREVIATIONS

Term	Definition
AESCSF	Australian Energy Sector Cyber Security Framework. This document references version 2 of the AESCSF
Aggregator	Cloud system representing multiple downstream DER as defined in CSIP-AUS, acts as the Software Communications Client for DER. Also used to refer to the commercial entity responsible for same.
Capacity Under Management	The total MW capacity of generation or consumption being managed by an entity. At time of writing this is the sum total of nameplate capacity of managed DER across any and all connected transmission and distribution networks.
Control system	For the purpose of this document 'control system' means the set of software, systems and networks used to or able to monitor and control DER, including the software, systems and networks used to communicate using CSIP-AUS and to give effect to CSIP-AUS controls issued by a CSIP-AUS Utility Server.
CSIP	Common Smart Inverter Profile
CSIP-AUS	Common Smart Inverter Profile – Australia, as defined in Standards Australia SA TS 5573 or any superseding standard
DER	Distributed Energy Resource: rooftop solar systems, home batteries, smart appliances, etc – small-scale resources distributed among homes and businesses that all participate in and contribute to the electricity system. DER owned by consumers/customers is also referred to as CER (Consumer Energy Resources)
End Device	The physical DER device at the premises that is controlled by the CSIP-AUS Software Communications Client, e.g. an inverter.

Term	Definition
IDAM	Identity and Access Management
MFA	Multi-factor Authentication
NEM	National Electricity Market
NEPKI	National PKI
NSP	Network Service Provider
OEM	Original Equipment Manufacturer
PKI	Public Key Infrastructure
SWIS	Southwest Interconnected System
TNSP	Transmission Network Service provider
Utility Server	Server entity as described in CSIP-AUS

3 CONTROL SELECTION

Applicable controls depend on which tier the organisation falls into (refer Table 1):

3.1 Tier 0

- It is anticipated that the controls listed in Section 5 and 6 constitute a baseline of security to establish a protective environment from which to establish greater functionality and continue growth of capacity under management.

3.2 Tier 1

- All Tier 0 Controls as per above
- Due to the anticipated size of the operational technology environment operating these systems, it could be that some controls are bespoke to particular systems, potentially repeated for various components and so not centralised.

3.3 Tier 2

- All Tier 1 Controls as per above
- Control system components related to the integrations being considered in this document might be associated with a larger operational technology environment concerned with other asset classes
- The security control requirements for Tier 2 focus on establishing a more robust and resilient security perimeter for the control system components tasked with operation of load associated with this larger capacity under management.

4 COMPLIANCE

At this time, compliance to the requirements in section 5 and 6 are self-assessed by the organisations in scope. The organisation must be able to provide evidence to support compliance on request, and may also be required to make itself available for the assessment to be undertaken by a third-party.

There is an expectation that those organisations defined in ‘Scope’ will be able to meet these baseline requirements within this document within 12-months from the day the total capacity under management reaches the respective thresholds or when a new version of this document is published.

Compliance to this document does not negate the need for the organisations to meet other legislative obligations; this is an additive expectation.

5 Organisational Requirements

The tables below list the organisational requirements applicable to each tier. Organisations are expected to conform to the practices relevant to their tier. In this section 5, the AESCSF v2 and IEC 62443-2-1:2009 references are to provide guidance but are not intended to be prescriptive as to how the practice is to be demonstrated; organisations should self-assess in the context of their own systems and architecture. For definitions of terms used and further guidance on the intent of each requirement, refer to the referenced requirements in the AESCSF v2 and IEC62443-2-1:2009.

5.1 Secure software development

Ref.	Practice description	Tier 0	Tier 1	Tier 2	AESCSF v2	IEC 62443-2-1:2009 reference
SSD-1	Software developed in-house for deployment on higher priority assets is developed using secure software development practices	Yes	Yes	Yes	ARCHITECTURE-4a	4.3.4.3.8
SSD-2	The selection of procured software for deployment on higher priority assets includes consideration of the vendor's secure software development practices	No	Yes	Yes	ARCHITECTURE-4b	4.3.2.6.4, 4.3.2.6.7
SSD-3	Secure software configurations are required as part of the software deployment process for both procured software and software developed in-house	No	Yes	Yes	ARCHITECTURE-4c	4.3.4.3.3
SSD-4	All software developed in-house is developed using secure software development practices	No	No	Yes	ARCHITECTURE-4d	4.3.4.3.3
SSD-5	The selection of all procured software includes consideration of the vendor's secure software development practices	No	No	Yes	ARCHITECTURE-4e	4.3.2.6.4, 4.3.2.6.7

5.2 Asset Management

Ref.	Practice description	Tier 0	Tier 1	Tier 2	AESCSF v2	IEC 62443-2-1:2009 reference
AM-1	IT and OT assets that are important to the delivery of the organisation's critical functions or services are inventoried, at least in an ad hoc manner	Yes	Yes	Yes	ASSET-1a	4.2.3.4, 4.2.3.6
AM-2	Inventoried IT and OT assets are prioritised based on defined criteria that include importance to the delivery of the organisation's critical functions or services	No	No	Yes	ASSET-1c	4.2.3.6
AM-3	Prioritisation criteria include consideration of the degree to which an asset within the organisation's critical functions or services may be leveraged to achieve a threat objective	No	No	Yes	ASSET-1d	4.2.3.6
AM-4	Information assets that are important to the delivery of the organisation's critical functions or services (for example, SCADA set points and customer information) are inventoried, at least in an ad hoc manner	Yes	Yes	Yes	ASSET-2a	4.2.3.6
AM-5	Inventoried information assets are categorised based on defined criteria that includes importance to the delivery of the organisation's critical functions or services	No	No	Yes	ASSET-2c	4.2.3.6

5.3 Cybersecurity Program Management

Ref.	Practice description	Tier 0	Tier 1	Tier 2	AESCSF v2	IEC 62443-2-1:2009 reference
CPM-1	The organisation has a cybersecurity program strategy, which may be developed and managed in an ad hoc manner	Yes	Yes	Yes	PROGRAM-1a	4.2.2.1, 4.2.3.6
CPM-2	The cybersecurity program strategy identifies any applicable compliance requirements that must be satisfied by the program (for example, NERC CIP, TSA Pipeline Security Guidelines, PCI DSS, ISO, DoD CMMC)	No	No	Yes	PROGRAM-1g	4.4.3.7
CPM-3	Senior management with proper authority provides support for the cybersecurity program, at least in an ad hoc manner	Yes	Yes	Yes	PROGRAM-2a	4.3.2.3.3
CPM-4	The cybersecurity program addresses and enables the achievement of legal and regulatory compliance, as appropriate	No	No	Yes	PROGRAM-2i	4.4.3.7

5.4 Event and Incident Response, Continuity of Operations

Ref.	Practice description	Tier 0	Tier 1	Tier 2	AESCSF v2	IEC 62443-2-1:2009 reference
IR-1	Detected cybersecurity events are reported to a specified person or role and documented, at least in an ad hoc manner	Yes	Yes	Yes	RESPONSE-1a	4.3.4.5.5
IR-2	Criteria are established for cybersecurity event detection (for example, what constitutes a cybersecurity event, where to look for cybersecurity events)	No	Yes	Yes	RESPONSE-1b	4.3.4.5.6, 4.4.3.2
IR-3	Criteria for declaring cybersecurity incidents are established, at least in an ad hoc manner	Yes	Yes	Yes	RESPONSE-2a	4.2.3.10, 4.3.4.5.6
IR-4	Cybersecurity incident response personnel are identified, and roles are assigned, at least in an ad hoc manner	Yes	Yes	Yes	RESPONSE-3a	4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4
IR-5	Responses to cybersecurity incidents are executed, at least in an ad hoc manner, to limit impact to the function and restore normal operations	Yes	Yes	Yes	RESPONSE-3b	4.3.4.5.10, 4.3.4.5.6
IR-6	Reporting of incidents is performed (for example, internal reporting, ICS-CERT, relevant ISACs), at least in an ad hoc manner	Yes	Yes	Yes	RESPONSE-3c	4.3.4.5.9
IR-7	Continuity plans are developed to sustain and restore operation of the function if a cybersecurity event or incident occurs, at least in an ad hoc manner	Yes	Yes	Yes	RESPONSE-4a	4.3.2.5.3, 4.3.4.5.1

5.5 Risk Management

Ref.	Practice description	Tier 0	Tier 1	Tier 2	AESCSF v2	IEC 62443-2-1:2009 reference
RM-1	The organisation has a strategy for cyber risk management, which may be developed and managed in an ad hoc manner	Yes	Yes	Yes	RISK-1a	4.3.4.2
RM-2	Cyber risks are identified, at least in an ad hoc manner	Yes	Yes	Yes	RISK-2a	4.2.3.1, 4.2.3.11, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.3.2.4.3, 4.3.2.6.3, 4.3.4.2
RM-3	Identified cyber risks are consolidated into categories (for example, data breaches, insider mistakes, ransomware, OT control takeover) to facilitate management at the category level	No	No	Yes	RISK-2d	4.2.3, 4.2.3.1, 4.2.3.11, 4.2.3.12, 4.2.3.3, 4.2.3.7, 4.2.3.8, 4.2.3.9, 4.3.2.4.3, 4.3.2.6.3, 4.3.2.6.5, 4.3.4.2
RM-4	Defined criteria are used to prioritise cyber risks (for example, impact to the organisation, impact to the community, likelihood, susceptibility, risk tolerance)	No	No	Yes	RISK-3b	4.2.3, 4.2.3.1, 4.2.3.11, 4.2.3.12, 4.2.3.3, 4.2.3.7, 4.2.3.8, 4.2.3.9, 4.3.2.4.3, 4.3.2.6.3, 4.3.2.6.5, 4.3.4.2
RM-5	Risk responses (such as mitigate, accept, avoid, or transfer) are implemented to address cyber risks, at least in an ad hoc manner	Yes	Yes	Yes	RISK-4a	4.2.3.1, 4.2.3.11, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.3.2.4.3, 4.3.2.6.3, 4.3.4.2

5.6 Supply Chain and External Dependencies Management

Ref.	Practice description	Tier 0	Tier 1	Tier 2	AESCSF v2	IEC 62443-2-1:2009 reference
TP-1	Third parties that have access to, control of, or custody of any IT, OT, or information assets that are important to the delivery of the organisation's critical functions or services are identified, at least in an ad hoc manner	Yes	Yes	Yes	THIRD-PARTIES-1b	None identified.
TP-2	The selection of suppliers and other third parties includes consideration of their cybersecurity qualifications, at least in an ad hoc manner	Yes	Yes	Yes	THIRD-PARTIES-2a	4.2.3.1, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.3.2.6.7, 4.3.4.2
TP-3	The selection of products and services includes consideration of their cybersecurity capabilities, at least in an ad hoc manner	Yes	Yes	Yes	THIRD-PARTIES-2b	4.2.3.1, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.3.2.6.4, 4.3.2.6.7, 4.3.4.2
TP-4	Cybersecurity requirements (for example, vulnerability notification, incident-related SLA requirements) are formalised in agreements with suppliers and other third parties	No	No	Yes	THIRD-PARTIES-2f	4.3.2.6.4, 4.3.2.6.7
TP-5	Suppliers and other third parties periodically attest to their ability to meet cybersecurity requirements	No	No	Yes	THIRD-PARTIES-2g	4.3.2.6.7
TP-6	Cybersecurity requirements for suppliers and other third parties include secure software and secure product development requirements where appropriate	No	No	Yes	THIRD-PARTIES-2h	4.3.2.6.4, 4.3.2.6.7

5.7 Threat and vulnerability management

Ref.	Practice description	Tier 0	Tier 1	Tier 2	AESCSF v2	IEC 62443-2-1:2009 reference
TVM-1	Information sources to support cybersecurity vulnerability discovery are identified, at least in an ad hoc manner	Yes	Yes	Yes	THREAT-1a	4.2.3, 4.2.3.12, 4.2.3.7, 4.2.3.9
TVM-2	Cybersecurity vulnerability information is gathered and interpreted for the organisation's critical functions or services, at least in an ad hoc manner	Yes	Yes	Yes	THREAT-1b	4.2.3, 4.2.3.12, 4.2.3.7, 4.2.3.9
TVM-3	Cybersecurity vulnerability assessments are performed, at least in an ad hoc manner	Yes	Yes	Yes	THREAT-1c	4.2.3, 4.2.3.1, 4.2.3.12, 4.2.3.7, 4.2.3.9
TVM-4	Cybersecurity vulnerabilities that are relevant to the organisation's critical functions or services, are mitigated, at least in an ad hoc manner	Yes	Yes	Yes	THREAT-1d	None identified for this practice
TVM-5	Cybersecurity vulnerability information sources that collectively address higher priority assets are monitored	No	Yes	Yes	THREAT-1e	4.2.3, 4.2.3.12, 4.2.3.7, 4.2.3.9
TVM-6	Cybersecurity vulnerability assessments are performed periodically and according to defined triggers, such as system changes and external events	No	Yes	Yes	THREAT-1f	4.2.3, 4.2.3.1, 4.2.3.12, 4.2.3.7, 4.2.3.9
TVM-7	Identified cybersecurity vulnerabilities are analysed and prioritised, and are addressed accordingly	No	Yes	Yes	THREAT-1g	4.2.3, 4.2.3.12, 4.2.3.7, 4.2.3.9
TVM-8	Internal and external information sources to support threat management activities are identified, at least in an ad hoc manner	Yes	Yes	Yes	THREAT-2a	4.2.3, 4.2.3.12, 4.2.3.9
TVM-9	Information about cybersecurity threats is gathered and interpreted for the organisation's critical functions or services, at least in an ad hoc manner	Yes	Yes	Yes	THREAT-2b	4.2.3, 4.2.3.12, 4.2.3.9
TVM-10	Threat objectives for the organisation's critical functions or services are identified, at least in an ad hoc manner	Yes	Yes	Yes	THREAT-2c	4.2.3, 4.2.3.12, 4.2.3.9

5.8 Workforce management

Ref.	Practice description	Tier 0	Tier 1	Tier 2	AESCSF v2	IEC 62443-2-1:2009 reference
WM-1	Personnel vetting (for example, background checks, drug tests) is performed at hire, at least in an ad hoc manner	Yes	Yes	Yes	WORKFORCE-1a	4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3
WM-2	Personnel separation procedures address cybersecurity, at least in an ad hoc manner	Yes	Yes	Yes	WORKFORCE-1b	4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3
WM-3	Cybersecurity awareness activities occur, at least in an ad hoc manner	Yes	Yes	Yes	WORKFORCE-2a	4.3.2.4.2
WM-4	Cybersecurity awareness activities are conducted periodically	No	Yes	Yes	WORKFORCE-2d	4.3.2.4.2
WM-5	Cybersecurity responsibilities are identified, at least in an ad hoc manner	Yes	Yes	Yes	WORKFORCE-3a	4.3.2.3.3, 4.3.2.4.2, 4.3.2.4.3, 4.4.3.1
WM-6	Cybersecurity responsibilities are assigned to specific people, at least in an ad hoc manner	Yes	Yes	Yes	WORKFORCE-3b	4.3.2.3.3, 4.3.2.4.2, 4.3.2.4.3
WM-7	Cybersecurity responsibilities are assigned to specific roles, including external service providers	No	No	Yes	WORKFORCE-3c	4.3.2.3.3, 4.3.2.4.2, 4.3.2.4.3
WM-8	Cybersecurity training is made available to personnel with assigned cybersecurity responsibilities, at least in an ad hoc manner	Yes	Yes	Yes	WORKFORCE-4a	4.3.2.4.2

6 Control System Requirements

The tables below list the control system requirements applicable to each tier. Organisations are expected to conform to the practices relevant to their tier. In this section 6, the AESCSF v2 and IEC 62443-3-3:2013 references are to provide guidance but are not intended to be prescriptive as to how the control is to be implemented; organisations should self-assess in the context of their own systems and architecture. For definitions of terms used and further guidance on the intent of each requirement, refer to the referenced requirements in the AESCSF v2 and IEC62443-3-3:2013.

6.1 Identity Management

Identity management and, more generally, Identity and Access Management (IDAM), provides an important suite of controls to protect the integrated control system components between each entity and the respective NSP.

Note: as of April 2026, work is underway to establish a National PKI service (NEPKI) for DER.

Ref	Control Description	Tier 0	Tier 1	Tier 2	Rationale	AESCSF v2 Domains	IEC 62443-3-3:2013
IDAM-1	Solution should be managed by identified users.	Yes	Yes	Yes	Standard identity management control capability.	ACCESS, ARCHITECTURE	SR 1.1
IDAM-2	Identified users should be unique	No	Yes	Yes	Key aspect of IDAM is to ensure actions are attributable to someone or thing.	ACCESS, ARCHITECTURE	SR 1.1 RE 1
IDAM-3	If coming from untrusted network multiple MFA should form basis of authentication process.	No	No	Yes	For more critical systems, providing added security by employing MFA is a powerful control to resist common cyber attack techniques.	ACCESS, ARCHITECTURE	SR 1.1 RE 2
IDAM-4	Provide means to ensure processes and devices can be identified, such as IP, process ID, user, port, signature, certificate, API or schema	Yes	Yes	Yes	To support whitelisting of communications, processes, actions and non-repudiation it is important to be able to identify processes and devices within the control system solution.	ACCESS, ARCHITECTURE	SR 1.2
IDAM-5	Using these controls uniquely identify all software and devices.	No	No	Yes	For more critical systems, it is especially beneficial to be able to identify every discrete process or device uniquely to ensure only vetted actions can be performed by authorised components.	ACCESS, ARCHITECTURE	SR 1.2 RE 1
IDAM-6	There should be a means employed to ensure user access to environment can be administered.	Yes	Yes	Yes	The control system should either represent its own security domain or be within an appropriate security domain. While this includes numerous other controls to ensure the security from known threats, having a dedicated means of managing IDAM for the control system components is a powerful security control.	ACCESS, ARCHITECTURE	SR 1.3

Ref	Control Description	Tier 0	Tier 1	Tier 2	Rationale	AESCSF v2 Domains	IEC 62443-3-3:2013
IDAM-7	Management of the authentication controls within the solution to protect from exposure.	Yes	Yes	Yes	There is a need to ensure no default passwords are employed during the build and commissioning of a control system and its components. There must be processes to ensure the authentication systems work and are secure.	ACCESS, ARCHITECTURE	SR 1.5
IDAM-8	Extension of the requirement whereby the authenticators for processes and devices is handled by hardware controls.	No	No	Yes	This enhancement suggests the use of hardware security appliances to manage and protect the authentication system for processes and devices.	ACCESS, ARCHITECTURE	SR 1.5 RE 1
IDAM-9	Password policy can be established and enforced.	Yes	Yes	Yes	Standard and basic password policy to reduce exposure and vulnerabilities associated with password spraying.	ACCESS, ARCHITECTURE	SR 1.7
IDAM-10	Password policy can include re-use and lifetime restrictions to human users.	No	No	Yes	Additional password policy requirements to reduce risks associated with password re-use or neglect.	ACCESS, ARCHITECTURE	SR 1.7 RE 1
IDAM-11	The solution shall provide for the use of PKI certificates either internally generated or from an existing PKI. This includes the process to have certificates issued for use.	Yes	Yes	Yes	General requirement to ensure the control system solution can handle X.509 certificates and is able to resolve associated names and establish trust.	ACCESS, ARCHITECTURE	SR 1.8
IDAM-12	Utilisation of certificates for client identification of any kind ensuring validation processes are employed.	Yes	Yes	Yes	This enhancement requires end points be issued certificates and more rigorous capabilities relating to validation and protection of private keys.	ACCESS, ARCHITECTURE	SR 1.9
IDAM-13	Private keys employed for the solution's PKI capability are protected by hardware security modules.	No	No	Yes	Hardware security modules represent industry best practice in the protection of private keys and secrets more generally. This is a very high bar and one that might be challenging for some proponents. Physically managed offline root private keys whilst not best practice is able to provide a significant level of protection for smaller entities.	ACCESS, ARCHITECTURE	SR 1.9 RE 1
IDAM-14	Ability to monitor and control access to the system from untrusted networks.	Yes	Yes	Yes	This is an important control to protect the control system solution components from compromise from less trusted environments such as ICT or the internet.	ACCESS, ARCHITECTURE	SR 1.13
IDAM-15	Ensure the ability to support segregation of duties and least privilege exists.	Yes	Yes	Yes	This control aligns with guidance to separate control system administration out from normal IT systems. Segregation of duties at an identity and authorisation level can help resist attacks relating to identity.	ACCESS, ARCHITECTURE	SR 2.1

Ref	Control Description	Tier 0	Tier 1	Tier 2	Rationale	AESCSF v2 Domains	IEC 62443-3-3:2013
IDAM-16	Extend the ability to enforce authorisations to all users, be it human, process or device	No	No	Yes	Restrict the permissions available to automated processes and devices to ensure they cannot compromise the system due to maloperation or malfunction.	ACCESS, ARCHITECTURE	SR 2.1 RE 1
IDAM-17	Map authorisations to roles and enforce them.	No	No	Yes	A slightly more mature approach to authorisations where the restrictions of authorisation is formalised into roles.	ACCESS, ARCHITECTURE	SR 2.1 RE 2
IDAM-18	Ability to limit number of concurrent sessions for all use classes/types.	No	No	Yes	This control is compelling in that it helps to defeat MiM and impersonation.	ACCESS, ARCHITECTURE	SR 2.7
IDAM-19	Control system components should have the ability to create audit logs relating to security.	Yes	Yes	Yes	This control is required for both incident detection but also forensics and fault resolution.	RESPONSE, SITUATION	SR 2.8
IDAM-20	Audit log storage capacity must remain sufficient to ensure it can be used purposefully.	Yes	Yes	Yes	Ensure availability of the audit log store by ensuring capacity.	RESPONSE, SITUATION	SR 2.9
IDAM-21	Alerting should be put in place to ensure audit log capacity is not exhausted.	No	No	Yes	A simple monitor to ensure that the audit logs store does not fill up and thus hindering the monitoring of the system.	RESPONSE, SITUATION	SR 2.9 RE 1
IDAM-22	Alerting and relevant response personnel must be in place to prevent loss of control system functionality.	Yes	Yes	Yes	Incident response from automated log monitoring must include the associated staffing to ensure the control system can be protected or recovery procedures actioned as quickly as possible.	RESPONSE, SITUATION	SR 2.10
IDAM-23	Ensure clocks are accurate and aligned across the control system components	Yes	Yes	Yes	The timestamps for events can be a key data point in establishing what actions have taken place within the control system environment.	RESPONSE, SITUATION	SR 2.11
IDAM-24	The system components will update and align time at designated intervals	No	No	Yes	To ensure time does not drift or diverge across the control system and its integrated components. The clocks should be updated at predefined intervals.	RESPONSE, SITUATION	SR 2.11 RE 1
IDAM-25	The system should be able to identify what actions were taken by a particular human user.	Yes	Yes	Yes	Human actions to administer or operate the system must be associated with a particular human user.	RESPONSE, SITUATION	SR 2.12
IDAM-26	The system should be able to identify what actions were taken by any user of the system human or otherwise.	No	No	Yes	Any actions to administer or operate the system must be associated with that particular human, process or device.	RESPONSE, SITUATION	SR 2.12 RE 1

6.2 System Security

These controls are primarily focused on the integrity and confidentiality of the integrated control system and its components.

Ref	Control Description	Tier 0	Tier 1	Tier 2	Rationale	AESCSF v2 Domains	IEC62443-3-3:2013
SS-1	The system should protect the integrity of transmitted information.	Yes	Yes	Yes	With a preference for physical over logical protection controls, ensure the communications paths are secure and free from threats to the integrity of the information being used within the control system.	ARCHITECTURE, SITUATION, THREAT	SR 3.1
SS-2	Employ cryptographic controls to establish assurances of integrity of transmitted information.	No	No	Yes	The use of cryptographic controls, where appropriate, to protect information transmissions and detect anomalies. There are some scenarios where this control may present as a threat the availability of certain functions.	ARCHITECTURE, SITUATION, THREAT	SR 3.1 RE 1
SS-3	Malware detection and protection is deployed within the control system and updated as required.	Yes	Yes	Yes	Given the prevalence of COTS products within control systems of today, malware prevention and detection is becoming more important.	ARCHITECTURE, SITUATION, THREAT	SR 3.2
SS-4	Malware detection and protection is deployed explicitly at points of entry and exit from the control system environment.	No	Yes	Yes	The deployment of anti-malware capability at the points of ingress and egress provides a first line of defence for the control system environment.	ARCHITECTURE, SITUATION, THREAT	SR 3.2 RE 1
SS-5	Anti-malware capability is centrally managed.	No	No	Yes	The anti-malware capabilities of the environment is managed centrally to ensure conformity and alerting is consistent.	ARCHITECTURE, SITUATION, THREAT	SR 3.2 RE 2
SS-6	Security controls are tested prior to and at commissioning.	Yes	Yes	Yes	In order to ensure security controls behave as expected and provide the expected level of assurance, they must be tested.	ARCHITECTURE, RESPONSE, SITUATION, THREAT	SR 3.3
SS-7	Security control testing is automated.	No	No	Yes	The testing of security controls is automated by way of scripting or otherwise to ensure it can be verified and validated throughout the lifecycle of the environment.	ARCHITECTURE, RESPONSE, SITUATION, THREAT	SR 3.3 RE 1
SS-8	The system must have the ability to detect unauthorised changes to software and data	Yes	Yes	Yes	In order to ensure the expected behaviour is observed the control system should not be modified unless under an authorised change.	ARCHITECTURE, SITUATION, THREAT	SR 3.4
SS-9	Any unauthorised changes should trigger an alert that is actioned.	No	No	Yes	A timely automated detection and response to detections of unauthorised changes to the control system should align with the criticality of the system impacted.	ARCHITECTURE, SITUATION, THREAT	SR 3.4 RE 1
SS-10	Input to the control system is validated to protect operation of the control system components	Yes	Yes	Yes	Any data that is being employed to manage or direct the operation of the system, should be filtered or checked to ensure there is no departure from expected behaviour	ARCHITECTURE	SR 3.5

Ref	Control Description	Tier 0	Tier 1	Tier 2	Rationale	AESCSF v2 Domains	IEC62443-3-3:2013
SS-11	The system must be able to protect the integrity of all sessions.	Yes	Yes	Yes	Provide protection against man in the middle attacks and ensure sessions remain under the control of the initiating parties.	ARCHITECTURE, SITUATION, THREAT	SR 3.8
SS-12	Invalidate sessions once terminated.	No	No	Yes	Prevent the reuse of session identifiers to ensure accesses or privileges associated with terminated sessions cannot be exploited.	ARCHITECTURE, SITUATION, THREAT	SR 3.8 RE 1
SS-13	All session IDs are unique	No	No	Yes	Not only are session IDs unique, but managed in a way that unknown IDs are rejected.	ARCHITECTURE, SITUATION, THREAT	SR 3.8 RE 2
SS-14	Session IDs are seen as random and cannot be guessed	No	No	Yes	To avoid attack related to impersonation, the session IDs are random.	ARCHITECTURE, SITUATION, THREAT	SR 3.8 RE 3
SS-15	Audit log information is secured to avoid manipulation or deletion.	No	Yes	Yes	Audit log information and the associated system are protected to ensure they are secure and persistent.	RESPONSE	SR 3.9
SS-16	Ensure the confidentiality of the control system information.	Yes	Yes	Yes	Only those authorised users are allowed read access to the information whether at rest or in transit.	ARCHITECTURE, THREAT	SR 4.1
SS-17	Ensure confidentiality for information at rest and in transit via untrusted networks.	No	No	Yes	Ensure the control system information is remains confidential across untrusted networks. Untrusted networks are any networks outside the control system.	ARCHITECTURE, THREAT	SR 4.1 RE 1
SS-18	Ensure confidentiality is protected across zone boundaries.	No	No	Yes	Confidentiality is protected even within the control system across all zone boundaries.	ARCHITECTURE, THREAT	SR 4.1 RE 2
SS-19	If cryptography is required, it will be to a relevant appropriate standard	Yes	Yes	Yes	Apply industry best practice to the use of cryptographic controls.	ARCHITECTURE	SR 4.3

6.3 Network Security

The controls listed here are focused on establishing and maintaining a robust boundary around the control system components and those tasked with integration with NSPs.

Ref	Control Description	Tier 0	Tier 1	Tier 2	Rationale	AESCSF v2 Domains	IEC62443-3-3:2013
NS-1	Logically segment control system networks from non-control system networks.	Yes	Yes	Yes	Ensure that systems that are not related to the control system function or purpose are able to be segmented logically.	ARCHITECTURE, RESPONSE	SR 5.1

Ref	Control Description	Tier 0	Tier 1	Tier 2	Rationale	AESCSF v2 Domains	IEC62443-3-3:2013
NS-2	Where possible, physically segment control system components from non-control system and physically segment critical systems from remainder of control system.	No	Yes	Yes	Best practice is to physically segment the control system from non-control system networks and then ensure critical control system component networks are also physically segmented from the rest of the control system. The extent to which this can be achieved will depend on system architecture.	ARCHITECTURE, RESPONSE	SR 5.1 RE 1
NS-3	Ensure the control system can operate without requiring services from non-control system networks.	No	No	Yes	Design the control system and its networks in such a way that all necessary critical supporting services are contained within the control system to ensure they are also protected.	ARCHITECTURE, RESPONSE	SR 5.1 RE 2
NS-4	The ability to inspect and control communications at zone boundaries.	Yes	Yes	Yes	In alignment with the malware related controls, this is the ability to inspect traffic and protect the control system at boundary interfaces.	ARCHITECTURE, PROGRAM, RESPONSE, THREAT	SR 5.2
NS-5	Ensure firewall rules are authored as whitelists.	No	Yes	Yes	Ensure boundary protections are established and the default behaviour is to deny all traffic unless identified as required.	ARCHITECTURE, PROGRAM, RESPONSE, THREAT	SR 5.2 RE 1
NS-6	There must be an ability to island/isolate the control system when required	No	No	Yes	This is an important control aligned with the above, SR 5.2 & RE 1, whereby the control system may need to be disconnected from a network where a threat is present or an anomaly has been detected that is likely a threat.	ARCHITECTURE, PROGRAM, RESPONSE, THREAT	SR 5.2 RE 2
NS-7	The system will fail in such as way as to not allow traffic through a control system boundary when there is a failure.	No	No	Yes	Establish network flow controls and boundary protection such that if there is a failure in these devices that traffic will also be stopped. That is ensure that devices are non-bypassable and routing is not dynamic.	ARCHITECTURE, PROGRAM, RESPONSE, THREAT	SR 5.2 RE 3
NS-8	Design the control system to support partitioning of the workloads and functionality in a way conducive to zoning of the networks.	Yes	Yes	Yes	In addition to the normal physical and logical segmentation of workload to ensure a performant control system and its associated services, also consider the segmentation of the workloads to support the security requirements.	RESPONSE	SR 5.4

6.4 Security Monitoring

The controls listed in the table below are focused on ensuring the integrated control system components are monitored and are within scope of a security monitoring regimen within the entity's organisation.

Ref	Control Description	Tier 0	Tier 1	Tier 2	Rationale	AESCSF v2 Domains	IEC62443-3-3:2013
SM-1	Ensure authorised humans and tools can access audit logs in read-only.	Yes	Yes	Yes	With an audit log store established for the control system, provide read-only access as required to these logs to both humans and relevant tooling.	RESPONSE, SITUATION, THIRD-PARTIES, THREAT	SR 6.1
SM-2	Deploy services to provide appropriate security monitoring and alerting capabilities.	No	Yes	Yes	Commensurate with the criticality of the control system, develop monitoring, alerting and response capabilities.	ARCHITECTURE, SITUATION	SR 6.2

6.5 System Assurance

The security controls in the below table support the availability of the integrated control system solution.

Ref	Control Description	Tier 0	Tier 1	Tier 2	Rationale	AESCSF v2 Domains	IEC62443-3-3:2013
SA-1	Continue to operate, even if degraded during DoS event.	Yes	Yes	Yes	The solution should be designed to be able to function while be resource constrained due to a denial of service (DoS) event.	ARCHITECTURE, PROGRAM, THREAT	SR 7.1
SA-2	Ability to rate limit communications to protect against DoS	No	Yes	Yes	In addition to other resource management and segmentation controls, ensure communications bandwidth and other resources cannot be exhausted.	ARCHITECTURE, PROGRAM, THREAT	SR 7.1 RE 1
SA-3	Ability to restrict the communications within the control system due to all users to protect from DoS events.	No	No	Yes	Design the control system in order to protect from the control system itself creating a Denial of Service (DoS) within itself.	ARCHITECTURE, PROGRAM, THREAT	SR 7.1 RE 2
SA-4	Ensure security control resources do not impact on control system itself.	Yes	Yes	Yes	The operation of security tools and systems within the control system should not present as a threat to the resource requirements of the control system itself.	PROGRAM, THREAT	SR 7.2

APPENDIX A - Declaration

Part A. Company details

Entity name	
Australian Business Number (ABN)	
Is your organisation declaring as Tier 0, Tier 1 or Tier 2 (refer Table 1)?	
Primary country where your DER control system is hosted	

Part B. Declaration

Please use tables B.1 and B.2 to record your level of conformance against the cyber requirements herein. Note that you are only required to conform to the requirements that are applicable to the Tier that you have nominated for your business in Part A above. In the conformance column in each table, please indicate one of the following:

- Y = Yes, fully conform to all requirements in this category relevant to my Tier
- N = No, do not conform to requirements in this category relevant to my Tier
- P = Partial, conform to requirements in this category relevant to my Tier other than the specific exceptions listed

Tables B.1 and B.2 are included below and may be completed in this document, or can be provided and completed in spreadsheet form if preferred.

Part C. Authorised representative

The declaration, including the conformance tables, must be completed by an authorised representative of your business. Please provide their name below.

Name of authorised representative	

Declaration table B.1: Organisational requirements:

Ref	Practice Description	Tier			Conform Y/N/P	List any exceptions
		0	1	2		
SSD-1	Software developed in-house for deployment on higher priority assets is developed using secure software development practices	X	X	X		
SSD-2	The selection of procured software for deployment on higher priority assets includes consideration of the vendor's secure software development practices		X	X		
SSD-3	Secure software configurations are required as part of the software deployment process for both procured software and software developed in-house		X	X		
SSD-4	All software developed in-house is developed using secure software development practices		X	X		
SSD-5	The selection of all procured software includes consideration of the vendor's secure software development practices			X		
AM-1	IT and OT assets that are important to the delivery of the organisation's critical functions or services are inventoried, at least in an ad hoc manner	X	X	X		
AM-2	Inventoried IT and OT assets are prioritised based on defined criteria that include importance to the delivery of the organisation's critical functions or services			X		
AM-3	Prioritisation criteria include consideration of the degree to which an asset within the organisation's critical functions or services may be leveraged to achieve a threat objective			X		
AM-4	Information assets that are important to the delivery of the organisation's critical functions or services (for example, SCADA set points and customer information) are inventoried, at least in an ad hoc manner	X	X	X		
AM-5	Inventoried information assets are categorised based on defined criteria that includes importance to the delivery of the organisation's critical functions or services			X		
CPM-1	The organisation has a cybersecurity program strategy, which may be developed and managed in an ad hoc manner	X	X	X		
CPM-2	The cybersecurity program strategy identifies any applicable compliance requirements that must be satisfied			X		

Ref	Practice Description	Tier			Conform Y/N/P	List any exceptions
		0	1	2		
	by the program (for example, NERC CIP, TSA Pipeline Security Guidelines, PCI DSS, ISO, DoD CMMC)					
CPM-3	Senior management with proper authority provides support for the cybersecurity program, at least in an ad hoc manner	X	X	X		
CPM-4	The cybersecurity program addresses and enables the achievement of legal and regulatory compliance, as appropriate			X		
IR-1	Detected cybersecurity events are reported to a specified person or role and documented, at least in an ad hoc manner	X	X	X		
IR-2	Criteria are established for cybersecurity event detection (for example, what constitutes a cybersecurity event, where to look for cybersecurity events)		X	X		
IR-3	Criteria for declaring cybersecurity incidents are established, at least in an ad hoc manner	X	X	X		
IR-4	Cybersecurity incident response personnel are identified, and roles are assigned, at least in an ad hoc manner	X	X	X		
IR-5	Responses to cybersecurity incidents are executed, at least in an ad hoc manner, to limit impact to the function and restore normal operations	X	X	X		
IR-6	Reporting of incidents is performed (for example, internal reporting, ICS-CERT, relevant ISACs), at least in an ad hoc manner	X	X	X		
IR-7	Continuity plans are developed to sustain and restore operation of the function if a cybersecurity event or incident occurs, at least in an ad hoc manner	X	X	X		
RM-1	The organisation has a strategy for cyber risk management, which may be developed and managed in an ad hoc manner	X	X	X		
RM-2	Cyber risks are identified, at least in an ad hoc manner	X	X	X		
RM-3	Identified cyber risks are consolidated into categories (for example, data breaches, insider mistakes, ransomware, OT control takeover) to facilitate management at the category level			X		
RM-4	Defined criteria are used to prioritise cyber risks (for example, impact to the organisation, impact to the community, likelihood, susceptibility, risk tolerance)			X		
RM-5	Risk responses (such as mitigate, accept, avoid, or transfer) are	X	X	X		

Ref	Practice Description	Tier			Conform Y/N/P	List any exceptions
		0	1	2		
	implemented to address cyber risks, at least in an ad hoc manner					
TP-1	Third parties that have access to, control of, or custody of any IT, OT, or information assets that are important to the delivery of the organisation's critical functions or services are identified, at least in an ad hoc manner	X	X	X		
TP-2	The selection of suppliers and other third parties includes consideration of their cybersecurity qualifications, at least in an ad hoc manner	X	X	X		
TP-3	The selection of products and services includes consideration of their cybersecurity capabilities, at least in an ad hoc manner	X	X	X		
TP-4	Cybersecurity requirements (for example, vulnerability notification, incident-related SLA requirements) are formalised in agreements with suppliers and other third parties			X		
TP-5	Suppliers and other third parties periodically attest to their ability to meet cybersecurity requirements			X		
TP-6	Cybersecurity requirements for suppliers and other third parties include secure software and secure product development requirements where appropriate			X		
TVM-1	Information sources to support cybersecurity vulnerability discovery are identified, at least in an ad hoc manner	X	X	X		
TVM-2	Cybersecurity vulnerability information is gathered and interpreted for the organisation's critical functions or services, at least in an ad hoc manner	X	X	X		
TVM-3	Cybersecurity vulnerability assessments are performed, at least in an ad hoc manner	X	X	X		
TVM-4	Cybersecurity vulnerabilities that are relevant to the organisation's critical functions or services, are mitigated, at least in an ad hoc manner	X	X	X		
TVM-5	Cybersecurity vulnerability information sources that collectively address higher priority assets are monitored		X	X		
TVM-6	Cybersecurity vulnerability assessments are performed periodically and according to defined triggers, such as system changes and external events		X	X		

Ref	Practice Description	Tier			Conform Y/N/P	List any exceptions
		0	1	2		
TVM-7	Identified cybersecurity vulnerabilities are analysed and prioritised, and are addressed accordingly		X	X		
TVM-8	Internal and external information sources to support threat management activities are identified, at least in an ad hoc manner	X	X	X		
TVM-9	Information about cybersecurity threats is gathered and interpreted for the organisation's critical functions or services, at least in an ad hoc manner	X	X	X		
TVM-10	Threat objectives for the organisation's critical functions or services are identified, at least in an ad hoc manner	X	X	X		
WM-1	Personnel vetting (for example, background checks, drug tests) is performed at hire, at least in an ad hoc manner	X	X	X		
WM-2	Personnel separation procedures address cybersecurity, at least in an ad hoc manner	X	X	X		
WM-3	Cybersecurity awareness activities occur, at least in an ad hoc manner	X	X	X		
WM-4	Cybersecurity awareness activities are conducted periodically		X	X		
WM-5	Cybersecurity responsibilities are identified, at least in an ad hoc manner	X	X	X		
WM-6	Cybersecurity responsibilities are assigned to specific people, at least in an ad hoc manner	X	X	X		
WM-7	Cybersecurity responsibilities are assigned to specific roles, including external service providers			X		
WM-8	Cybersecurity training is made available to personnel with assigned cybersecurity responsibilities, at least in an ad hoc manner	X	X	X		

Declaration table B.2: Operational systems controls:

Ref	Control Description	Tier			Conform Y/N/P	List any exceptions
		0	1	2		
IDAM-1	Solution should be managed by identified users.	X	X	X		
IDAM-2	Identified users should be unique		X	X		
IDAM-3	If coming from untrusted network multiple MFA should form basis of authentication process.			X		
IDAM-4	Provide means to ensure processes and devices can be identified, such as IP, process ID, user, port, signature, certificate, API or schema	X	X	X		
IDAM-5	Using these controls uniquely identify all software and devices.			X		
IDAM-6	There should be a means employed to ensure user access to environment can be administered.	X	X	X		
IDAM-7	Management of the authentication controls within the solution to protect from exposure.	X	X	X		
IDAM-8	Extension of the requirement whereby the authenticators for processes and devices is handled by hardware controls.			X		
IDAM-9	Password policy can be established and enforced.	X	X	X		
IDAM-10	Password policy can include re-use and lifetime restrictions to human users.			X		
IDAM-11	The solution shall provide for the use of PKI certificates either internally generated or from an existing PKI. This includes the process to have certificates issued for use.	X	X	X		
IDAM-12	Utilisation of certificates for client identification of any kind ensuring validation processes are employed.	X	X	X		
IDAM-13	Private keys employed for the solution's PKI capability are protected by hardware security modules.			X		
IDAM-14	Ability to monitor and control access to the system from untrusted networks.	X	X	X		

Ref	Control Description	Tier			Conform Y/N/P	List any exceptions
		0	1	2		
IDAM-15	Ensure the ability to support segregation of duties and least privilege exists.	X	X	X		
IDAM-16	Extend the ability to enforce authorisations to all users, be it human, process or device			X		
IDAM-17	Map authorisations to roles and enforce them.			X		
IDAM-18	Ability to limit number of concurrent sessions for all use classes/types.			X		
IDAM-19	Control system components should have the ability to create audit logs relating to security.	X	X	X		
IDAM-20	Audit log storage capacity must remain sufficient to ensure it can be used purposefully.	X	X	X		
IDAM-21	Alerting should be put in place to ensure audit log capacity is not exhausted.			X		
IDAM-22	Alerting and relevant response personnel must be in place to prevent loss of control system functionality.	X	X	X		
IDAM-23	Ensure clocks are accurate and aligned across the control system components	X	X	X		
IDAM-24	The system components will update and align time at designated intervals			X		
IDAM-25	The system should be able to identify what actions were taken by a particular human user.	X	X	X		
IDAM-26	The system should be able to identify what actions were taken by any user of the system human or otherwise.			X		
SS-1	The system should protect the integrity of transmitted information.	X	X	X		
SS-2	Employ cryptographic controls to establish assurances of integrity of transmitted information.			X		
SS-3	Malware detection and protection is deployed within the control system and updated as required.	X	X	X		
SS-4	Malware detection and protection is deployed explicitly at points of entry and exit from the control system environment.		X	X		

Ref	Control Description	Tier			Conform Y/N/P	List any exceptions
		0	1	2		
SS-5	Anti-malware capability is centrally managed.			X		
SS-6	Security controls are tested prior to and at commissioning.	X	X	X		
SS-7	Security control testing is automated.			X		
SS-8	The system must have the ability to detect unauthorised changes to software and data	X	X	X		
SS-9	Any unauthorised changes should trigger an alert that is actioned.			X		
SS-10	Input to the control system is validated to protect operation of the control system components	X	X	X		
SS-11	The system must be able to protect the integrity of all sessions.	X	X	X		
SS-12	Invalidate sessions once terminated.			X		
SS-13	All session IDs are unique			X		
SS-14	Session IDs are seen as random and cannot be guessed			X		
SS-15	Audit log information is secured to avoid manipulation or deletion.		X	X		
SS-16	Ensure the confidentiality of the control system information.	X	X	X		
SS-17	Ensure confidentiality for information at rest and in transit via untrusted networks.			X		
SS-18	Ensure confidentiality is protected across zone boundaries.			X		

Ref	Control Description	Tier			Conform Y/N/P	List any exceptions
		0	1	2		
SS-19	If cryptography is required, it will be to a relevant appropriate standard	X	X	X		
NS-1	Logically segment control system networks from non-control system networks.	X	X	X		
NS-2	Physically segment control system components from non-control system and physically segment critical systems from remainder of control system.		X	X		
NS-3	Ensure the control system can operate without requiring services from non-control system networks.			X		
NS-4	The ability to inspect and control communications at zone boundaries.	X	X	X		
NS-5	Ensure firewall rules are authored as whitelists.		X	X		
NS-6	There must be an ability to island/isolate the control system when required			X		
NS-7	The system will fail in such as way as to not allow traffic through a control system boundary when there is a failure.			X		
NS-8	Design the control system to support partitioning of the workloads and functionality in a way conducive to zoning of the networks.	X	X	X		
SM-1	Ensure authorised humans and tools can access audit logs in read-only.	X	X	X		
SM-2	Deploy services to provide appropriate security monitoring and alerting capabilities.		X	X		
SA-1	Continue to operate, even if degraded during DoS event.	X	X	X		
SA-2	Ability to rate limit communications to protect against DoS		X	X		
SA-3	Ability to restrict the communications within the control system due to all users to protect from DoS events.			X		

Ref	Control Description	Tier			Conform Y/N/P	List any exceptions
		0	1	2		
SA-4	Ensure security control resources do not impact on control system itself.	X	X	X		

APPENDIX B – Change log

Version	Date	Notes
1.0	November 2025	Initial version
1.1	April 2026	Added definition of 'control system' Clarified referenced versions of IEC 62443-2-1:2009 and IEC 62443-3-3:2013, aligned with versions referenced in AESCSF v2 Revised requirement NS-2 Updated Appendix A part C to replace electronic signature with name of authorised representative Added Appendix B (Change log)