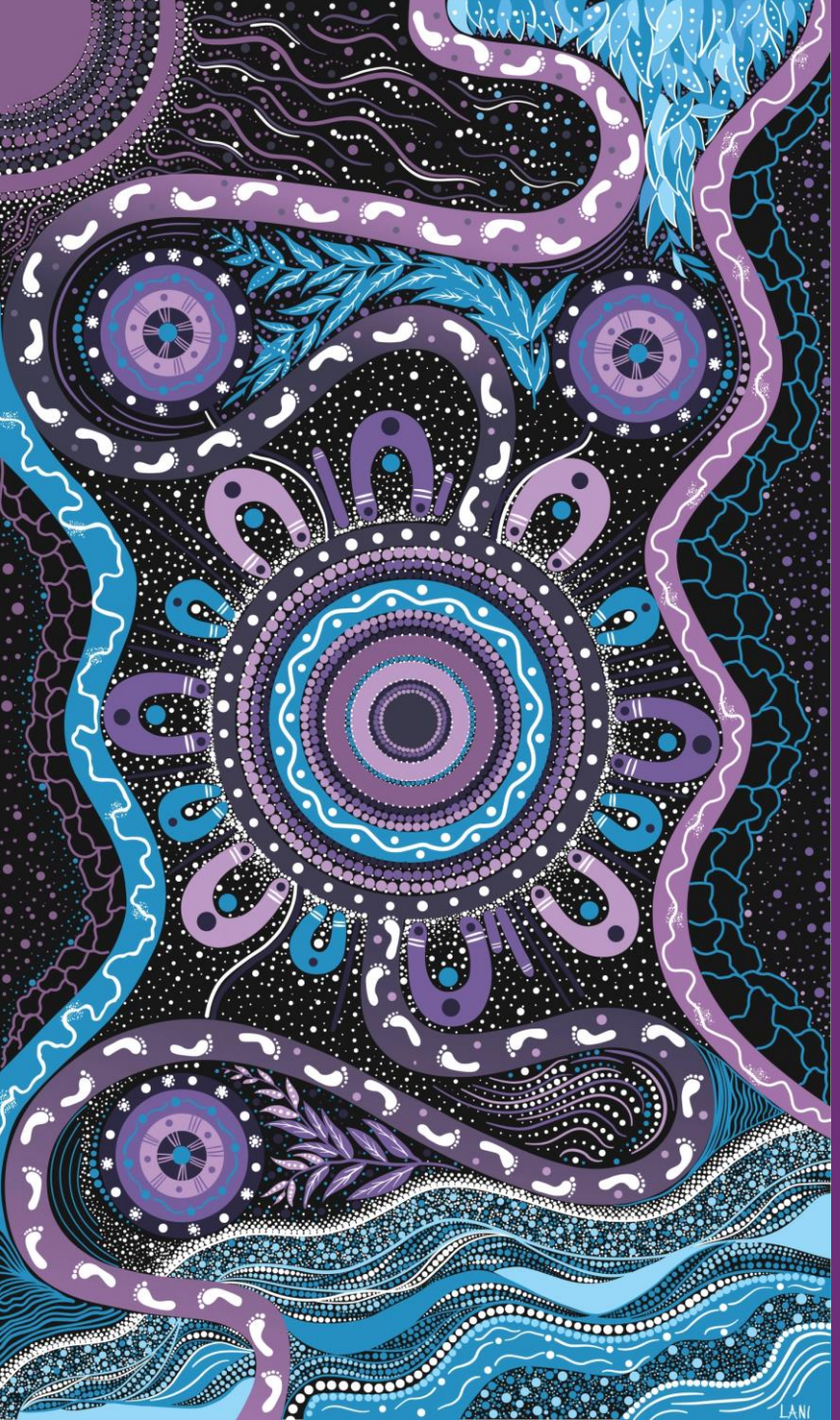
AEMO
AUSTRALIAN ENERGY MARKET OPERATOR

Domain Walkthrough

2025



We acknowledge the Traditional Custodians of the land, seas and waters across Australia. We honour the wisdom of Aboriginal and Torres Strait Islander Elders past and present and embrace future generations.

We acknowledge that, wherever we work, we do so on Aboriginal and Torres Strait Islander lands. We pay respect to the world's oldest continuing culture and First Nations peoples' deep and continuing connection to Country, and hope that our work can benefit both people and Country.

'Journey of unity: AEMO's Reconciliation Path' by Lani Balzan

AEMO Group is proud to have launched its first Reconciliation Action Plan in May 2024. 'Journey of unity: AEMO's Reconciliation Path' was created by Wiradjuri artist Lani Balzan to visually narrate our ongoing journey towards reconciliation – a collaborative endeavour that honours First Nations cultures, fosters mutual understanding, and paves the way for a brighter, more inclusive future.

Read our RAP

Agenda

Introduction and Overview

Deep Dive into 4 Key Domains

Implementation Tips

Lessons Learned and Key Takeaways

Annual AESCSF Program

Assessment Outcomes & Next Steps

The 11 Domains of AESCSF V2

AESCSF V2 has 11 domains. The domains are logical groupings of cyber security capability. Each domain has an acronym that cross references across the AESCSF Toolkit and Guidance Artefacts.

Enterprise-wide

- Risk Management (RISK)
- Cybersecurity Program Management (PROGRAM)
- Workforce Management (WORKFORCE)

Operating environments

- Identity and Access Management (ACCESS)
- Event and Incident Response, Continuity of Operations (RESPONSE)
- Asset, Change, and Configuration Management (ASSET)
- Situational Awareness (SITUATION)
- Threat and Vulnerability Management (THREAT)
- Australian Privacy Management (APM) *(Australian Specific)*
- Cybersecurity Architecture (ARCHITECTURE)

External parties

- Supply Chain and External Dependencies Management (THIRD-PARTIES)

Scenario: WindGrid

WindGrid is a growing renewable energy operator facing increased cybersecurity challenges as its operations expand across wind and solar assets.

Operations: Manages wind farms and solar installations across regional areas.

Size & Structure: Small-to-mid-sized organisation with centralised IT operations.

Growth: Recently expanded due to green energy subsidies and market demand.

Cybersecurity Gap: Cyber maturity has not kept pace with operational growth.

Third-Party Dependency: Relies on a third-party Managed Service Provider (MSP) for IT and OT management.

Limited OT Visibility: Has minimal oversight and governance across OT environments, including SCADA systems.

Overview | Supply Chain and External Dependencies Management

Domain recognises that a fundamental aspect of an organisation is supply chain. Third-parties should be identified and prioritised based on how critical they are for business functions. This should then be the basis of managing third-party risk.

KEY SUB-DOMAINS

Identify and Prioritise Third Parties	• Identify critical IT and OT third-party dependencies, especially those with access to important assets. • Use a structured and established method to assess third-party risk, with a focus on high-risk vendors. • Regularly update risk prioritisation to proactively address potential disruptions or compromises.	• Mitigates risk of third-party disruption of critical operations or the compromise of sensitive data through. • Enables the focus and prioritisation of high-risk third-party suppliers, ensuring appropriate controls are in place
Manage Third-Party Risk	• Select third-party suppliers and products based on their cybersecurity qualifications and risk profile. • Follow a structured approach to evaluate and mitigate cybersecurity risks associated with third parties. • Require higher-priority suppliers to implement stronger cybersecurity controls. • Include formal cybersecurity requirements in contracts, with periodic attestations from third parties.	• Formalised agreements with third parties maintain consistent security standards and improve risk management across the supply chain • Evaluation of the associated criteria before asset procurement allows for visibility of associated risks in working with specific third parties, ensuring the most optimal choice for supplier is made.

WindGrid uses a **SaaS-based SCADA platform** managed by a third-party vendor, but lacks clear visibility into the vendor's cybersecurity posture, incident response coordination, or data segregation controls. This introduces risk to the availability and integrity of critical operational data and control systems.

‘How To’ | Supply Chain and External Dependencies Management

This domain focuses on identifying, managing, and mitigating cybersecurity risks arising from third-party products, services, and partnerships. It includes assurance mechanisms, contract clauses, and monitoring of vendor security practices — especially for critical systems like SCADA, ICS, or other OT environments.

WindGrid uses a **SaaS-based SCADA platform** managed by a third-party vendor, but lacks clear visibility into the vendor’s cybersecurity posture, incident response coordination, or data segregation controls. This introduces risk to the availability and integrity of critical operational data and control systems.

No understanding of critical suppliers.

Currently trusts vendors without any external validation.

Contracts with MSP and OT vendors lack any mention of cyber controls.

Has no predefined process to engage MSP or SCADA vendor during cyber incidents.

No current visibility into the MSP or SCADA vendor’s security postures.

No performance tracking linked to vendor security commitments.

‘How To’ | Supply Chain and External Dependencies Management

This domain focuses on identifying, managing, and mitigating cybersecurity risks arising from third-party products, services, and partnerships. It includes assurance mechanisms, contract clauses, and monitoring of vendor security practices — especially for critical systems like SCADA, ICS, or other OT environments.

WindGrid uses a **SaaS-based SCADA platform** managed by a third-party vendor, but lacks clear visibility into the vendor’s cybersecurity posture, incident response coordination, or data segregation controls. This introduces risk to the availability and integrity of critical operational data and control systems.

Action 1: Identify and classify critical third parties

Build a supplier inventory with input from IT, OT, and procurement. Tag vendors as Tier 1 (critical to operations or access), Tier 2 (supporting systems), and Tier 3 (low impact).

Action 2: Define cybersecurity requirements in contracts

Collaborate with legal to update contract templates with mandatory cyber clauses: breach notification timeframes, minimum control expectations (MFA, logging), access control, and audit rights.

Action 3: Perform regular supplier cyber risk assessments

Annually issue security questionnaires or interviews based on AESCSF categories. Prioritise Tier 1 vendors for in-depth reviews.

Action 4: Require independent security certifications or reports

Include a requirement for SOC 2, ISO 27001, or AESCSF self-assessments in agreements. Review these annually and track findings.

Action 5: Develop coordinated incident response plans with vendors

Include third parties in WindGrid’s incident response playbooks. Define escalation contacts, expected response times, and joint testing.

Action 6: Establish vendor performance and compliance tracking

Use a simple dashboard or tracker to monitor KPIs (e.g., response times, control failures, missed patching windows). Include cyber-related penalties or improvement targets.

Overview | Identity and Access Management

Domain recognises that an organisation should focus on establishing access controls across both logical and physical systems. The organisation should ensure secure identification and authentication while also addressing anti-patterns that could affect security.

KEY SUB-DOMAINS

Authentication	• Regularly review user identities and promptly disable or remove those that are inactive or no longer needed. • Apply least privilege access so users only have the permissions required for their role. • Enforce strong passwords and require multi-factor authentication (MFA) for secure access	• Limits the ability of threat actors to move either laterally and vertically through systems. • Removes the vulnerability of unused or old identities being accessed by threat actors.
Logical Access	• Implement and regularly review logical access controls, revoking access when no longer needed. • Define access requirements using least privilege and separation of duties, with approvals from asset owners. • Apply extra scrutiny and monitoring for higher-risk privileges and suspicious activity	• Reduces the likelihood of malicious logical access to systems through poor privilege provisions. • Allows fast detection of any suspicious logical access. • Limits the ability for threat actors to move or access to other systems.
Physical Access	• Implement physical access controls with monitoring and logging of access to sensitive areas. • Regularly review and document access privileges, ensuring they align with the principle of least privilege. • Revoke physical access when no longer required and apply extra scrutiny to higher-risk access and anomalous activity	• Reduces the likelihood of malicious physical access to systems through poor privilege provisions. • Allows fast detection of any suspicious physical access. • Limits the physical ability for threat actors to move or access to other

WindGrid has **shared administrator credentials** between internal staff and the Managed Service Provider (MSP) for both IT and OT systems. There is **no centralised access control**, and audit logs are incomplete or not regularly reviewed, increasing the risk of unauthorised or undetected changes.

‘How To’ | Identity and Access Management

This domain ensures that only authorised individuals or systems can access assets, data, and operations — and that their access is granted based on the principle of least privilege. It includes account management, authentication mechanisms, and monitoring of access activity across IT and OT environments.

WindGrid has **shared administrator credentials** between internal staff and the Managed Service Provider (MSP) for both IT and OT systems. There is **no centralised access control**, and audit logs are incomplete or not regularly reviewed, increasing the risk of unauthorised or undetected changes.

Shared OT admin accounts still used by MSP and field teams.

No recertification process in place, especially for MSP access.

No formal roles; access often granted on request without review.

MSP has persistent access across systems without visibility.

Expansion has increased remote access needs, but MFA is not consistently applied.

Departed contractors still had access months after offboarding.

‘How To’ | Identity and Access Management

This domain ensures that only authorised individuals or systems can access assets, data, and operations — and that their access is granted based on the principle of least privilege. It includes account management, authentication mechanisms, and monitoring of access activity across IT and OT environments.

WindGrid has **shared administrator credentials** between internal staff and the Managed Service Provider (MSP) for both IT and OT systems. There is **no centralised access control**, and audit logs are incomplete or not regularly reviewed, increasing the risk of unauthorised or undetected changes.

Action 1: Remove shared and orphaned accounts

Conduct a full review of user accounts across all systems. Disable unused accounts and replace shared ones with named accounts linked to individuals.

Action 2: Implement role-based access control (RBAC)

Define standard roles for employees, contractors, and vendors. Map each role to the minimum access needed. Configure these roles in Active Directory and SCADA systems.

Action 3: Enforce multi-factor authentication (MFA)

Enable MFA for all remote access, privileged IT accounts, and OT interfaces that support it. Select a common MFA provider and roll out in phases.

Action 4: Implement quarterly access reviews

Assign system owners to verify who has access, whether it's appropriate, and revoke outdated privileges. Use IAM tools or spreadsheets to support this process.

Action 5: Monitor and control third-party access

Require third parties (e.g., MSP) to request time-bound access via a formal approval workflow. Log all sessions and actions taken.

Action 6: Establish an identity governance lifecycle

Define access workflows for onboarding, role changes, and offboarding. Link these to HR processes and system provisioning.

Overview | Cybersecurity Architecture

Domain recognises that cyber resilience starts at the design stage, how systems are interconnected, how access is controlled across zones, and how the network is isolated to contain breaches

KEY SUB-DOMAINS

Strategy and Program	• Align cybersecurity architecture and strategy with business goals and the threat landscape across IT and OT. • Conduct regular reviews with senior leadership involvement. • Define cybersecurity requirements and assess conformance to operational standards	• Ensures cybersecurity architecture is relevant to organisation goals • Allows for continuous improvement and addressing of current and emerging threats.
Network Protections	• Implement risk-based network protections with segmentation across IT, OT, assets, and networks. • Enforce least privilege, network monitoring, and strict access controls. • Restrict access to authorised devices and isolate compromised assets when necessary	• Ensures that lateral movement is limited, reducing the number of impacted systems • Enhances security posture and stops unauthorised access to critical systems
IT and OT Asset Security	• Enforce access controls, secure configurations, and endpoint protections for critical assets, with stricter controls for high-priority systems. • Manage the use of removable media and firmware to reduce risk. • Prevent unauthorised code execution through defined security measures	• Reduces the attack surface and ability for unauthorised access on critical assets • Reduces likelihood of asset tampering
Software Security	• Apply secure development practices for both in-house and third-party software, including validation of authenticity and secure configuration. • Perform regular security testing, with a focus on key changes or updates to systems and applications.	• Reduces vulnerabilities by ensuring security standards in third-party or self developed software. • Identifies and mitigates risks early through regular testing
Data Security	• Protect sensitive data using encryption, cryptographic controls, and key management, along with data loss prevention measures. • Safeguard against unauthorised changes to software, firmware, and data, and prevent data exfiltration	• Ensures that data is secure at rest or during transit. • Maintains the integrity of data and assets by protecting against tampering.

Due to recent growth, WindGrid has rapidly onboarded new wind and solar sites but **reused legacy flat network architecture** with **limited IT/OT segmentation**, increasing the attack surface and risk of lateral movement from IT into OT environments.

‘How To’ | Cybersecurity Architecture

This domain assesses the design and segmentation of IT/OT environments to ensure they are secure-by-design, resilient, and able to withstand threats. It includes the application of zoning principles, network segregation, and secure system baselines.

Due to recent growth, WindGrid has rapidly onboarded new wind and solar sites but **reused legacy flat network architecture** with **limited IT/OT segmentation**, increasing the attack surface and risk of lateral movement from IT into OT environments.

Flat network allows compromise to spread between SCADA and IT.

Has no accurate view of which systems are connected or exposed.

MSP accesses OT remotely with no standard controls or monitoring.

Recent sites were brought online rapidly with no cyber review.

Legacy systems onboarded quickly with default settings.

OT changes sometimes made directly by vendors with no review.

‘How To’ | Cybersecurity Architecture

This domain assesses the design and segmentation of IT/OT environments to ensure they are secure-by-design, resilient, and able to withstand threats. It includes the application of zoning principles, network segregation, and secure system baselines.

Due to recent growth, WindGrid has rapidly onboarded new wind and solar sites but **reused legacy flat network architecture** with **limited IT/OT segmentation**, increasing the attack surface and risk of lateral movement from IT into OT environments.

Action 1: Segment IT and OT networks

Introduce firewalls and VLANs to separate OT systems (e.g., SCADA) from corporate IT. Use jump servers or demilitarised zones (DMZs) for controlled access.

Action 2: Implement secure remote access architecture

Use VPN gateways with MFA and logging for all external or vendor access to SCADA. Only allow access from trusted devices.

Action 3: Harden all systems and apply baselines

Use CIS Benchmarks to configure OS and devices securely. Maintain “gold images” for common configurations.

Action 4: Maintain up-to-date architecture and asset diagrams

Create and maintain network diagrams, data flow maps, and asset inventories. Store them in a shared repository and review after any change.

Action 5: Embed cybersecurity into new site rollouts

Include security requirements in planning, procurement, and commissioning checklists for new wind/solar sites. Assign a security SME.

Action 6: Apply secure change management processes

Implement formal change request workflows for SCADA and network changes, with cyber review steps.

Overview | Situational Awareness

This domain ensures organisations can effectively detect, understand, and respond to cybersecurity events by collecting, monitoring, analysing, and communicating relevant information across IT and OT environments.

KEY SUB-DOMAINS

Perform Logging	Enables logging for the early identification of threats across critical IT and OT assets, including high-risk systems and infrastructure	• Captures system events and access activity to support detection, investigation, and forensic analysis
Perform Monitoring	Reviews and analyses logs and monitoring data for anomalies or signs of attack	• Enables early detection of incidents and unusual behaviour to prevent escalation
Maintain Awareness	Aggregates and shares cybersecurity status internally and externally, using predefined reporting and response processes	• Improves coordination, response decisions, and preparedness during events or threats

WindGrid has **limited monitoring capabilities** across OT assets and **relies on the MSP** for incident detection — but there's **no clear escalation workflow** or visibility into telemetry from critical systems like SCADA, making it difficult to detect anomalies or confirm system integrity.

‘How To’ | Situational Awareness

This domain is about the ability to detect, understand, and respond to cyber threats in real-time or near-real-time. It covers security monitoring, logging, alerting, threat intelligence, and operational visibility across both IT and OT systems.

WindGrid has **limited monitoring capabilities** across OT assets and **relies on the MSP** for incident detection — but there’s **no clear escalation workflow** or visibility into telemetry from critical systems like SCADA, making it difficult to detect anomalies or confirm system integrity.

Logs are fragmented across IT and MSP platforms with no integration.

Currently relies entirely on reactive alerts from the MSP.

No defined use cases or detection logic tied to OT.

No prior OT-focused incident simulations have been conducted.

No formal agreement on who detects/responds to incidents.

Execs currently lack visibility into overall cyber posture.

‘How To’ | Situational Awareness

This domain is about the ability to detect, understand, and respond to cyber threats in real-time or near-real-time. It covers security monitoring, logging, alerting, threat intelligence, and operational visibility across both IT and OT systems.

WindGrid has **limited monitoring capabilities** across OT assets and **relies on the MSP** for incident detection — but there’s **no clear escalation workflow** or visibility into telemetry from critical systems like SCADA, making it difficult to detect anomalies or confirm system integrity.

Action 1: Deploy centralised logging and SIEM

Implement a SIEM tool or leverage MSP-provided platform. Ingest logs from firewalls, SCADA, endpoint systems, and VPNs.

Action 2: Define detection rules and thresholds

Create use cases (e.g., failed login attempts, changes to SCADA configs) and tune alerts to reduce false positives.

Action 3: Clarify monitoring roles with third parties

Create a RACI matrix for log monitoring, triage, escalation, and resolution across WindGrid and MSP.

Action 4: Conduct proactive threat hunting and analysis

Assign internal staff or external resources to regularly review logs for anomalies or known attack patterns.

Action 5: Run cyber tabletop exercises with OT scenarios

Simulate realistic threats (e.g., SCADA compromise, ransomware) with field teams, leadership, and MSP participation.

Action 6: Establish regular cyber reporting to leadership

Create a monthly/quarterly report showing key cyber KPIs: top threats, incidents, coverage gaps, vendor compliance.

Assessment Outcomes & Next Steps

The next steps for energy sector participants are:

1. Please complete your organisation's assessment – which was made available on **1 May 2025**. The portal will remain open until **6 June 2025** to complete the assessment.

2. The specific closure date of the assessment portal will be **6 June 2025**. Your submission can include your CEO's attestation response letter for full AESCSF assessments if desired.

3. All entities who submit a 2025 Assessment will have access to the AESCSF 2025 Benchmarking Portal. Organisations will be able to compare against deidentified industry benchmarks based on the population of 2025 Assessments submitted.

Support:
For any AESCSF related queries, please email the Program Team via **aescsf@aemo.com.au**