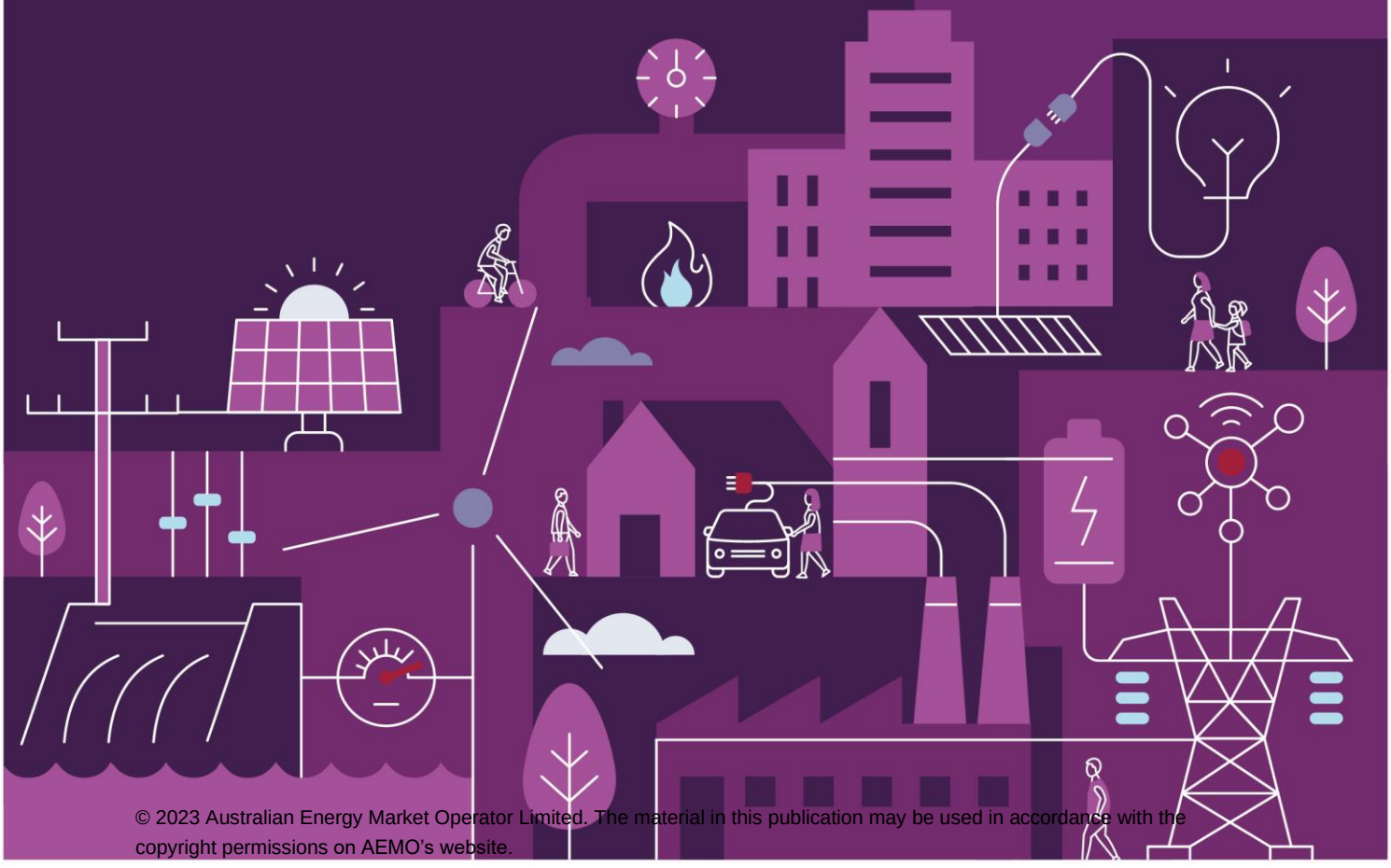
Australian Energy Sector Cyber Security Framework (AESCSF)

Guidance Material for Lo Criticality Organisations

2023 AESCSF Program



Important notice

Purpose

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

This document accompanies other general guidance materials made available to Australian energy organisations in the electricity, gas, and liquid fuels sub-sectors.

Disclaimer

This document or the information in it may be subsequently updated or amended. This document does not constitute legal or organisation-specific advice and should not be relied on as a substitute for obtaining detailed advice about any applicable laws, procedures, or policies. AEMO have made every effort to ensure the quality of the information in this document but cannot guarantee its accuracy or completeness.

This document might contain information which is provided for explanatory purposes and/or provided by third parties. This information is included “as is” and may not be free from errors or omissions. You should verify and check the accuracy, completeness, reliability, and suitability of this information for any intended use you intend to put it to and seek independent expert advice before using it.

Accordingly, to the maximum extent permitted by law, AEMO and its employees and other contributors involved in the preparation of this document:

- Make no representation or warranty, express or implied, as to the currency, accuracy, reliability, or completeness of the information in this document, and;
- Are not liable (whether by reason of negligence or otherwise) for any statements or representations or any omissions from it, or for any use or reliance on the information in it.

Conventions used in this document

For clarity when reading this document, key terms are indicated with a capital letter. Each key term has a specific definition that the reader should consider. An example of this is Participants, as defined above.

Key terms are defined centrally in the AESCSF Glossary which is available separately on the AEMO website.

Table of contents

Table of Figures

1. Summary

1.1. Purpose

This document provides guidance for smaller Australian energy organisations to implement foundational capabilities described within the AESCSF. The capabilities included in this guidance have been selected based on it being high-impact and foundational in nature to organisations overall cyber security capability. The guidance in this document is aimed at a foundational level and can be matured over time.

1.2. Audience

The primary audience of this document are cyber security leaders (or individuals who have responsibility for cyber security amongst other duties) of small/less critical organisations in the Australian energy sector. Where possible, guidance is written in 'plain English'. This provides easy to understand content to support awareness and roadmap activities for executive leadership teams and Boards.

1.3. Background

The AESCSF enables participants to assess, prioritise and improve cyber security capability and maturity. Based on feedback from prior AESCSF Assessment Programs, smaller organisations have requested additional guidance to support their implementation of the AESCSF. In response, this document provides guidance material to assist organisations in getting started on their uplift journey.

Please note guidance in this document is not the only way to implement these capabilities, nor is it an exhaustive of all the elements required to obtain 'Security Profile 1' – See Framework Overview document [1].

1.4. AESCSF summary and guidance material mapping

The AESCSF is presented in three formats, each with a different use case. These are the:

- AESCSF 'Full Assessment' Version 1 (v1)
- AESCSF 'Full Assessment' Version 2 (v2)
- AESCSF 'Lite Assessment' Version 2 Lite (v2 Lite)

The full Assessment v1 covers 282 Practices and Anti-Patterns within the Framework, was developed in 2018 and is a recognised compliance tool in assessing organisations cyber maturity to support their Risk Management Plan (RMP) regulatory obligations under the SOCI Act (2018).

The full Assessment v2 is the updated Assessment covering 354 Practices and Anti-Patterns within the Framework incorporating the US Department of Energy's Cybersecurity Capability Maturity Model version 2.1 (June 2022) and was developed in late 2022. v2 is recognised as an 'equivalent tool' under the SOCI Act (2018).

Following the revision of the full Assessment v2 the Lite Assessment was also revised and now consists of 28 multi-select, easy-to-follow questions. The scope of the Lite Assessment is intentionally limited to focus on the maturity guidance from the Australian Cyber Security Centre (ACSC). The guidance contained within this document can be applied irrespective of which Assessment an organisation chooses to complete, and references to both Assessments are provided under each guidance area.

The table below provides an overview of the AESCSF capability areas (known as Domains), and the sections within this document that provide guidance for each of these Domains.

Business Area	AESCSF Domain	Guidance Material Section
Enterprise Wide	Risk Management (RISK)	Section 3.1: Identify and treat cyber security risks
	Cybersecurity Program Management (PROGRAM)	Section 3.2: Cyber security program support
	Workforce Management (WORKFORCE)	Section 3.3: Cyber security in human resource processes
Operating Environments	ARCHITECTURE (AESCSF v2 Only)	Section 3.4: Planning, designing and managing cyber security control environment
	Asset, Change, and Configuration Management (ASSET)	Section 3.5: Documenting and managing asset inventories
	Identity and Access Management (ACCESS)	Section 3.6: Removal of unneeded access and strengthening privileged accounts
	Threat and Vulnerability Management (THREAT)	Section 3.7: Responding to significant cyber security threats and vulnerabilities
	Situational Awareness (SITUATION)	Section 3.8: Defining logging requirements
	Event and Incident Response, Continuity of Operations (RESPONSE)	Section 3.9: Responding to cyber security incidents
	Australian Privacy Management (PRIVACY)	Section 3.10: Defining personal information
External Parties	Supply Chain and External Dependencies Management (THIRD-PARTIES)	Section 3.11: Identifying and addressing third party supplier dependency risk
	Sharing cyber security information (v1 Only)	Section 3.12: Identifying key cyber-related information sharing stakeholders

Table 1: AESCSF summary and guidance material mapping

2. Importance of targeting lower-cost, higher-impact uplift areas

Smaller Australian energy sector participants are often also constrained when it comes to time, and resources to enhance cyber security capability uplift. Therefore, it is important that these organisations focus their efforts on implementing areas of the Framework that will have a higher impact, thus increasing their organisational cyber security capability and maturity, while still being relatively low-cost.

2.1. What are the Priority Practices?

The ACSC has defined a total of 26 Priority Practices within the AESCSF Version 1 and 29 Priority Practices within the AESCSF Version 2. These are the areas of capability and maturity that the ACSC recommends organisations prioritise first as part of any uplift program. This is due to their high-impact on cyber security risk reduction and being the 'must-have' foundational capabilities blocks upon which other AESCSF capabilities are built upon.

The table below shows the mapping between the 20 ACSC-defined Priority Practices and the collating Security Profile 1 (SP-1) practice reference numbers from the AESCSF Overview document [1] and AESCSF Framework Core [2]. All questions in the Lite Framework map back to the 20 ACSC-defined Priority Practices.

AESCSF Domain	Guidance material section	ACSC SP-1 Priority Practices (v1)	ACSC SP-1 Priority Practices (v2)
Risk Management (RISK)	Section 3.1: Identify and treat cyber security risks	RM-2A RM-2B	RISK-2A RISK-3A RISK-4A
Cybersecurity Program Management (PROGRAM)	Section 3.2: Cyber security program support	CPM-2A CPM-2B	PROGRAM-2A
Workforce Management (WORKFORCE)	Section 3.3: Cyber security in human resource processes	WM-2A WM-2B	WORKFORCE-1A WORKFORCE-1B WORKFORCE-1C
ARCHITECTURE	Section 3.4: Planning, designing, and managing cyber security control environment	N/A	ARCHITECTURE-2B ARCHITECTURE-2C ARCHITECTURE-3A
Asset, Change, and Configuration Management	Section 3.5: Documenting and managing asset inventories	ACM-1A ACM-1B	ASSET-1A ASSET-2A ASSET-3A

(ASSET)			ASSET-4D
Identity and Access Management (ACCESS)	Section 3.6: Removal of unneeded access and strengthening privileged accounts	IAM-1F IAM-2F	ACCESS-1B ACCESS-1F ACCESS-2G ACCESS-3H
Threat and Vulnerability Management (THREAT)	Section 3.7: Responding to significant cyber security threats and vulnerabilities	TVM-1C TVM-2G	THREAT-2D THREAT-2H
Situational Awareness (SITUATION)	Section 3.8: Defining logging requirements	SA-1B	SITUATION-1A
Event and Incident Response, Continuity of Operations (RESPONSE)	Section 3.9: Responding to cyber security incidents	IR-3C IR-4A IR-4B	RESPONSE-2G RESPONSE-3C RESPONSE-4E
Australian Privacy Management (PRIVACY)	Section 3.10: Defining personal information	APM-1B	PRIVACY-1B
Supply Chain and External Dependencies Management (THIRD-PARTIES)	Section 3.11: Identifying and addressing third party supplier dependency risk	EDM-1A EDM-2A	THIRD-PARTIES-1A THIRD-PARTIES-1B THIRD-PARTIES-2A THIRD-PARTIES-2B
Information Sharing and Communications	Section 3.12: Sharing cyber security information	ISC-1C	N/A

Table 2: ACSC Priority Practices

Each of the Priority Practices are grouped into one of three Security Profiles. For smaller organisations, the key focus areas follow the Priority Practices listed under Security Profile 1; and subsequently, they form the basis of the guidance outlined below in this document.

2.1.1. The value in iteration

Implementing cyber security capability across the full breadth of an organisation can be a challenging task. For instances where this is the case, instead take an iterative approach to implementing the capability by starting implementation within smaller, higher criticality areas of your organisation. Over time, continue to expand coverage over multiple cycles until the full desired coverage is obtained.

3. Practice implementation guidance

3.1. Identify and treat cyber security risks

3.1.1. Identify cyber security risks

Understanding your organisation's cyber security risks is essential to apply controls to manage these risks. If cyber security risks are not currently identified within your organisation, consider doing the following:

- Create a document/register to capture risk related information. Often for smaller organisations this takes the form of a spreadsheet shared with specific team members.
- Understand what risk information is available from existing organisational processes. This may take the form of:
    - Top-down cyber risk assessments
    - Security control testing and/or audits
    - Vulnerability assessments or penetration testing
    - Project based security architecture or design assessments
- Collate this data into the risk document created above, assigning each identified risk a rating.
- Engage management teams to understand and document known security issues or weaknesses that warrant a risk being raised.

3.1.2. Treat cyber security risks

Risk treatments are needed to reduce the current risk level to an appropriate risk level. If cyber security risks are not currently being treated and controlled within your organisation, consider doing the following:

- Review the risk register and identify the highest rated risks.
- Obtain a copy of your organisation's risk management framework. If none exists, select an industry-regarded risk management framework, for example ISO 31000:2018 [3].
- Using the risk framework as a guide, identify potential risk treatment options for each of the highest rated risks. These treatment options may include:
    - Reduction/Mitigation: Apply new or existing controls to mitigate the risk.
    - Avoidance: If the risk level is too high and the cost of implementing mitigating controls is too costly, avoidance of the risk may be the best treatment.
    - Transfer: Transfer of the risk to an additional party.
    - Acceptance: If the risk is at an acceptable level (i.e. within the organisation's risk appetite), acceptance may be permissible.
- Seek endorsement of proposed risk mitigation activities, document the risk mitigation plan, and target dates in the risk register.

3.2. Cyber security program support

3.2.1. Resource provisioning

A cyber security program is typically the primary mechanism to implement cyber capability uplift activities. A key component of any cyber security program is the provisioning of resources. Establishing a cyber program of work varies between organisations, and can vary significantly in terms of size, investment, and duration. If your organisation does provide sufficient resourcing to a cyber security program, consider the following:

- Identify the scope of uplift being targeted. In the first instance, the scope may be selected to only cover the Priority Practices within SP-1 outlined in this document. Alternatively, it may be to implement any capability gaps within Security Profile 1 as a whole. See section *0*

- *Next steps*, for more details on this.
- Identify which resources type(s) are currently lacking, which may include:
    - People and skills:
        - Employee time
        - Subject matter expertise & knowledge
        - Training
    - Tools:
        - Technology, platforms, software and information assets.
    - Funding
        - Strategic capital expenditure (Capex)
        - Day-to-day operational expenditure (Opex)
- Develop a business case for executive leadership to address current resource gaps which clearly specifies:
    - What resources are being requested
    - Why the increase in resource is required
    - How the additional resources are planned to be used
    - What is the resultant benefit to the organisation from the increase in resourcing

3.2.2. Program sponsorship

The success and impacts of a cyber security program are often related to the level of endorsement and sponsorship of the program from executive management. Having their sponsorship will often result in less roadblocks and push-back being experienced by the program through the course of implementing and maturing cyber capabilities.

The steps taken will vary between organisations, however if a sponsorship for the cyber security program has not been obtained by your organisation, consider the following:

- Identify key leadership sponsorship required.
- Similarly to 3.2, develop a pitch/business case/presentation to:
    - Communicate the importance of cyber security
    - An overview of current cyber capability, and current risk levels
    - High level plans for uplift activities to be implemented through the cyber security program
    - Key asks and next steps in terms of their support, which may include:
        - Resourcing and funding (refer to 3.2)
        - Messaging and communication of support across the team/organisation of the importance of the program
        - Commitment to prioritisation of cyber uplift activities that may compete with other internal processes
        - Support addressing roadblocks and push-back from the organisation if uplift activities impact other internal processes

3.3. Cyber security in human resource processes

3.3.1. Perform personnel vetting for higher risk roles

Some internal staff are granted access to organisational information and assets. Due-diligence should be performed during the hiring process for roles that have access to business-critical assets. If your organisation does not perform vetting on your personnel, consider the following:

- Engage with the HR team to request that vetting be performed for selected roles within the organisation.
- In consultation with HR, understand what vetting checks are available to your organisation. These may include:
    - Consideration of AGSVA clearances
    - Background checks
    - Police checks
    - Drug tests
- Identify the roles that have access to business-critical assets. Request that the HR team include additional checks for those roles or consult with your organisation's cyber security team/contact if clarification is needed for the hiring of any role in the future.

3.4. Cyber-security architecture

3.4.1. Establish and maintain cyber security architecture

Understanding how your organisation's technology environment supports the protection of its IT and OT assets and a plan as to where and how controls should be implemented is fundamental to the effective operation of cyber security controls. Establishing cyber security architecture involves identifying cyber security requirements for your organisations assets and selecting appropriate controls to meet those requirements. Key terms that should be considered in your response include:

- **Control:** an action that you can take to respond to a risk;
- **Network:** an interconnected group of assets; and
- **Asset:** something of value to the organisation. Assets include many things, including technology, information, roles performed by personnel, and facilities.

If your organisation does not currently have a documented cyber security architecture, consider:

- Mapping your environment to understand your network and where your high value assets physically and logically reside.
- Developing documentation that best describes how controls should be selected and implemented to protect those high value assets from cyber threats.
- Ensuring that this set of controls covers all opportunities to implement controls within your technology environment, including across networks, applications, endpoints, infrastructure, and data.
- Implementing network segregation and intrusion detection and/or prevention systems (IDS/IPS).
- Applying additional controls for high value assets or priority assets which support your organisations critical operations.
- Whether your technology environment allows for high value assets or high criticality processes to operate in isolation should parts of your network become untrustworthy during a cyber security attack.

3.5. Documenting and managing asset inventories

3.5.1. Document important technology and operational assets

Understanding your organisation's important information technology (e.g. computers, servers and devices) and operational (e.g. physical machinery which produce or process energy products) assets is a fundamental capability. In this context, 'important' refers to assets which are considered most critical to your organisation. This asset information is used to underpin cyber-related capabilities such as control management, change management, incident response, backup, and disaster recovery. If your organisation does not currently have an inventory containing data on information technology and operational assets, consider the following:

- Create an empty asset inventory if none currently exists. In its most basic form, this may be a spreadsheet, or may be supported by digital platforms designed for managing asset inventories.
- Document what fields/metadata should be documented for each asset (where known). As a start, some key fields to document may include:
    - Asset Identifier
    - Description
    - Site/location
    - Type (Technology or Operational)
    - Make / model / version
    - Vendor
    - Support details
    - Organisation owner
    - Criticality
    - Comments / additional notes.
- Consult technology and operational team representatives within your organisation to understand what information is available and add this to the inventory.
- Perform a technology and operational asset discovery exercise, if appropriate.
- Where feasible, build in trigger points to existing processes such as procurement and change management to update the register when assets are changed within the organisation.

3.5.2. Document important information assets

Similarly to 3.5.1 above, understanding important information assets is essential. Information assets are the digital repositories where information is contained. These can take the form of applications, systems, databases, or documents. If your organisation does not currently have an inventory containing data on important technology and operational assets, consider the following:

- Create an information asset register in a similar manner to the steps outlined in 3.5.1 above.
- Document what fields/metadata should be documented for each asset (where known). As a start, some key fields to document may include:
    - Asset Identifier
    - Description
    - Type (e.g. Application, system, database, document, etc.)
    - Version
    - Vendor (if applicable)
    - Support details (if applicable)
    - Organisation owner
    - Information classification (e.g. Secret, confidential, internal, public, etc.)
    - Comments / additional notes
- Consult technology and operational team representatives to understand what information is currently available and add this to the inventory.
- Perform an information asset discovery exercise, if appropriate. Some examples of areas to look at include:
    - Customer information
    - Organisational information
    - Financial information
    - Staff/Human Resource (HR) information
    - Configuration and settings information
- Where feasible, build in trigger points to existing processes such as procurement, change management and information management to update the register when information assets are changed within the organisation.

3.6. Removal on unneeded access and strengthening privileged accounts

3.6.1. Deprovisioning identities when no longer required

A user's identity profile is the mechanism through which access to systems, data, and resources are provisioned and allocated. To minimise the potential for abuse of these permissions when the account is not needed, users should have their identity deprovisioned (i.e. disconnected, disabled, or removed) based on an agreed time threshold. If identities are not deprovisioned when no longer required within your organisations, consider the following:

- Understand how user identities are handled within your organisation (e.g. via Active Directory), and what capabilities are available to deprovision accounts (either currently or could reasonably be acquired). Key considerations include the degree of automation, available team capacity, and budget.
- In consultation with HR and Access Management teams (if applicable) define the use cases for when account deprovisioning should take place, and what deprovisioning action should occur (E.g. termination leave of absence, maternity leave, Long Service Leave, etc). Note: If scope for implementation is limited, focus on deprovisioning of terminated staff members as a priority, and/or focusing on specific parts of the organisation.
- Define acceptable and pragmatic timeframes for when the above use cases should be subject to deprovisioning.
- Implement processes and workflows in collaboration with your organisations HR and Access Management teams (if applicable) to complete the deprovisioning activities within the set timeframes defined above.

3.6.2. Strengthening controls for privileged accounts

Administrative, root account, emergency access and shared accounts have a heightened cyber security risk to organisations based on their increased level of access, and therefore should be subject to additional cyber security controls. If additional controls are not applied to privileged accounts within your organisation, consider the following:

- In consultation with access management team members (if applicable), identify the current user access control capabilities for accounts, and identify where new or increased controls could be applied (based on available budget, effort, resourcing) for privileged accounts.
- Controls may include:
    - Prior to obtaining a privileged account:
        - Additional approvals needed.
    - Using a privileged account:
        - Increased complexity of passwords
        - Implementation of Multi-Factor Authentication (MFA)
        - Reducing session duration (e.g. inactivity timeouts)
        - Automatic privileged account expiry, requiring re-application needed to retain the privileged account.
    - Monitoring of privileged accounts:
        - Increased frequency of User Access Reviews (UARs)
        - Increased logging
        - Increased monitoring / frequency of log reviews of privileged accounts
        - Monitoring for specific security events associated with misuse of privileged access.
- Implement the agreed controls, and document these in the suitable policy/standard.

3.7. Responding to significant cyber security threats and vulnerabilities

3.7.1. Responding to significant cyber security threats

The threat environment is constantly evolving, and organisations should act upon significant changes to the threat landscape. If your organisation does not currently respond to significant cyber security threats, consider the following:

- Understand what threat information is being consumed by your organisation, and validate its appropriateness based on available funding, resources, and time.
- Understand the frequency that this information is reviewed and escalated where appropriate.
- Document the process followed to escalate and respond to changes in the threat landscape. This should include:
    - Threat intelligence sources identified above, and the frequency that this is reviewed
    - Where threats should be documented (and create a register for this if none currently exists)
    - What criteria is used to classify a threat as 'significant' in the context of your organisation
    - What action should be taken to respond to these threats, including:
        - Deployment of additional current preventative cyber security controls
        - Deployment of additional current monitoring and responsive cyber security controls (e.g. specific monitoring to identity activity which correlates to the nature of the identified threat)
        - What additional controls could be acquired/procured if deemed appropriate based on the nature of the threat
        - Any notification requirements internally within your organisation
        - Any approvals required to implement the approve responses to cyber threats.
- Implement this process and update it to validate its suitability for the organisation.

3.7.2. Addressing and prioritising vulnerabilities

Taking actions towards preventing cyber incidents and events relies on identifying and managing vulnerabilities. Due to some vulnerabilities posing more risk than others, it is beneficial to prioritise and act upon those that are expected to have a larger risk impact to your organisation. If your organisation does not currently address vulnerabilities according to an assigned priority, consider the following:

- Check whether a policy or standard outlines requirements for vulnerability identification, and the scoring of these.
- If this doesn't exist, start by defining a common scoring approach. For example it could be based on National Institute of Standards and Technology NIST's Common Vulnerability Scoring System (CVSS) or could be more detailed and tailored to your organisation using a matrix of Likelihood, Consequence, and Level of access required.
    - Likelihood (Low/Medium/High based on the level of sophistication or skill required to exploit)
    - Impact (Insignificant/Minor/Moderate/Major/Severe based on the impact to the organisation)
    - Level of access needed (External anonymous/Authenticated user/Domain user/Privileged).
- Understand what vulnerability scanning and detection activities are currently performed, and where the outputs from these are located. Note: If no vulnerability scanning is currently being performed, consider starting with scanning of your organisation's internet-facing perimeter.
- Collate the outputs of these activities (either via an automated dashboard if feasible, or via manual collation periodically based on available resources) and identify the highest priority vulnerabilities using the scoring methodology defined above.
- Address those vulnerabilities which have been assessed as high priority by:
    - Continually monitoring at defined period increments, with the timeframe defined by what is practical within your organisation.
    - Log all observations from monitoring and any issues that may be associated with the existence of the vulnerability
    - Put in place mitigating controls that will prevent the vulnerability from becoming a threat.

3.8. Defining logging requirements

3.8.1. Defining logging requirements for important assets

Log data is a valuable resource to enable alerting and early detection of a cyber security incident, and to perform deeper analysis to understand what has occurred in the past. It is important to have logging requirements defined to guide and inform what system and operational data is expected to be retained, in particular for important (most-critical) assets. If your organisation has not defined these requirements, consider the following:

- Refer to an existing or developed asset register to identify what assets exist within your organisation and how they contribute to their respective function (see 3.3.1 above).
- Understand which assets contained in the register are considered important for the operations of your organisation.
- Document the logging requirements (based on available resources) in a policy or standard. This will likely include specification of the following:
    - The types of events that are required to be logged for each type of system/device
    - The information to be captured in event logs
    - Requirements for aggregation of log data
    - Protection of log data from unauthorised access, modification, and deletion
    - Requirements for log file sizes
- When documenting these requirements consider:
    - Known threats, vulnerabilities, and risks related to these important assets
    - Cyber Security requirements – e.g. confidentiality, integrity, availability.

3.8.2. Consider cyber security within termination process

Similarly to 3.10.1 above, some internal staff are granted access to organisational information and assets. It is important that controls are established to protect these assets during the termination process. If your organisation has not incorporated cyber security into the termination process, consider the following:

- In collaboration with HR, update the termination process to include steps which cover:
    - Introduce requirements in the onboarding process to include signing of non-disclosure agreements (if permissible).
    - Requiring terminated employees to return any organisational IT assets that may contain sensitive information – e.g. smartphones, laptops, etc.
    - Deprovision user identities, access and credentials to systems (see 3.6.1 above)
    - Return any physical access assets such as smart cards, ID cards, or physical keys
    - Implement enhanced monitoring for suspicious user behaviour in cases where employment was terminated for disciplinary reasons

3.9. Responding to cyber security incidents

3.9.1. Report and escalate cyber security events and incidents

There are constant digital events that occur within your organisation, ranging from a user logging in, a website being loaded, or an instruction sent to an operational asset. While the majority of these events are routine, there are some that may form part of a cyber security incident, and it is important that these are escalated and reported. If your organisation does not already report the cyber security events and incidents, consider the following:

- Identify reporting channel(s) to be implemented within your organisation. This may include:
  - A dedicated cyber security email inbox
  - A phishing reporting function
  - A form on your organisation's intranet
  - Reporting via your organisations service desk
- Similarly identify and implement report repository capabilities to capture this data. This may include:
  - A dedicated cyber security email inbox (indicated above)
  - A database
  - A dashboard
- Allocate responsibility for monitoring of these reporting channels and repositories to respond to events.
- Conduct user awareness training to inform your organisation's staff about the availability of reporting channels and that they should report events they think may be a cyber security issue.
- Engage technical owners for key systems to define automated alerts to be sent to the report repository when:
  - Particular events or conditions occur (e.g. when a phishing email is detected)
  - After certain thresholds are reached (e.g. more than X successive incorrect login attempts for a domain administrator account).
- Understand your organisations obligations to report cyber security incidents to external bodies, such as the ACSC.

3.9.2. Identify operational activities needed to support business-critical operations.

Not all activities and process are created equal, and there are some activities of critical importance that need to remain operational to support business-critical operations. If your organisation hasn't defined the activities necessary to sustain business-critical operations within your organisation, consider the following:

- Similarly to 3.11.1 below, review your organisation's Business Impact Analysis (BIA) to identify critical business functions and services (typically operations relating to site management and Industrial Control Systems (ICS) management). If a BIA has not recently been completed, identify the core service delivered by your organisation, and the key functions that support it.
- Speak with representatives from these key functions, and understand the operational activities, processes, systems and information necessary to support these functions.
- Document the outputs of this, and store in a location that is easily accessible in the occurrence of an incident.

3.9.3. Identification of steps to restore normal operations

In a worst-case scenario where operational activities, processes, systems or information for business-critical functions are impacted, it is important to identify the sequence of activities needed to restore these critical functions to normal operations. If your organisation has not identified the activities – nor the relevant sequencing – required to return an affected function to its normal state of operations, consider the following:

- Starting with one business-critical function, understand whether the steps taken to restore normal operations have previously been documented, e.g. in a technology disaster recovery plan.
- If not, in collaboration with subject matter experts from the identified internal function, identify and document the sequence that should be followed to restore normal functionality (similar to the process that would be followed in documenting a disaster recovery plan).

3.10. Defining personal information

3.10.1. Defining personal information in line with organisational activities

Most organisations are subject to regulatory responsibilities defined in the Australian *Privacy Act 1988* (the Privacy Act). One of the core pre-requisites to abiding by these responsibilities is having a defined understanding of what 'personal information' means within the context of their organisation. If your organisation does not have an organisation-defined definition of personal information, consider the following:

- Engage your legal team to understand whether your organisation is subject to the Privacy Act.
- If your organisation is subject to the Privacy Act, request that your organisations legal team defines what your organisation considers 'personal information', why this information is collected from individual, and how this information is used and held.

Note: It is each organisation's responsibility to ensure it is compliant with state and federal privacy requirements, and other confidentiality and or related laws that may apply to you. Completion of the AESCSF Privacy domain does not represent your compliance with privacy law, any of the Australian Privacy Principles or any other state or federal legal or regulatory obligations. Please consult with independent legal counsel or contact the Office of the Australian Information Commissioner if you have any questions about your compliance with privacy law.

3.11. Identifying and addressing third party supplier dependency risk

3.11.1. Identification of key IT and OT related supplier dependencies

In our modern interconnected organisational structures, most organisations have dependencies on other suppliers for products and services. Some of these suppliers may be key to your organisation's operations. This might be due to being a sole supplier of a product or service, having detailed knowledge that isn't documented/shared by others, or they provide products or services that are needed for core organisation services. If these key suppliers are not currently identified within your organisation, consider the following:

- Review your organisation's Business Impact Analysis (BIA) to identify critical business functions and services. If a BIA has not recently been completed, identify the core service delivered by your organisation, and the key functions which support it.
- With the support of your organisation's procurement team, identify where third parties support these critical organisational functions and services.
- Document these into a document/repository.
- Note the suppliers where a loss of their services would have a prolonged major impact to service delivery that couldn't be quickly addressed through procuring another supplier.
- Validate the accuracy, completeness and criticality of third-party suppliers identified through consulting management of these organisational departments.

3.11.2. Addressing significant cyber security risks with key suppliers

As covered in 3.11.1 above, some suppliers may be key to critical organisational processes and functions. It is important that risks related to these suppliers are identified, understood, and treated to minimise business impact to your organisation. If significant cyber security risks with key suppliers are not identified and addressed within your organisation, consider the following:

- For the suppliers identified in section 3.11.1 above, understand whether a third-party risk assessment was performed during the point of initial procurement with the supplier.
- If not, undertake a risk assessment of the provider commensurate with available resources and the dependence on the supplier (i.e. this may be a basic or detailed table-top review covering areas such as:
    - the nature of their goods/services provided
    - current certifications
    - reputation
    - availability of suitable alternative suppliers)
- Document this information in a register and document any risks that are identified.
- Review risks identified across your organisation's key suppliers and identify suitable risk treatment options for significant risks (refer to 0 above for more detail on cyber risk treatment).

3.12. Sharing cyber security information

3.12.1. Identifying key cyber-related information sharing stakeholders

Ensuring cyber security is a collaborative effort that takes many stakeholders working together to protect an organisation and the industry. To facilitate this, the sharing of potentially highly confidential information with select stakeholders is needed. It is important that these stakeholders are identified so they can receive timely access to information, while limiting exposure of this sensitive information. If your organisation has not identified these stakeholders, consider the following:

- Information sharing occurs internally and externally. Starting with internal information sharing, identify the key internal stakeholders whose knowledge of current events is important to maintaining continuity of internal operations. This may include:
    - Leadership positions in your cyber/IT team (e.g. CISO, CTO, CIO, Head of technology, Head of security etc).
    - Executive leadership
    - Key organisational/function leads (e.g. site/plant leads, head of technology etc).
- Document these roles and identify when and the nature of information that should be shared (e.g. in a high-severity cyber incident scenario, a daily report should be shared with executive leadership).
- For external information sharing, identify the key legal, regulatory and government bodies that information is shared with. This may include, but not limited to:
    - The Australian Cyber Security Centre (ACSC)
    - Office of the Australian Information Commissioner (OAIC)
    - Australian Energy Market Operator (AEMO)
    - Department of Climate Change, Energy, the Environment and Water (DCCEEW)
    - Department of Home Affairs (DHA).
- Identify what circumstances it is appropriate (or required) to share information to the above external parties, what types of information is shared, and what approval or authorisation is needed prior to sharing it externally.

4. Next steps

The guidance within section *3. Practice implementation guidance* are the recommended first steps for organisations to implement as part of their cyber security capability uplift journey. Once this foundational capability is implemented, the focus can then turn towards acquiring 'Security Profile 1 (SP-1)' of the AESCSF [1] to further improve your organisations cyber security capabilities.

4.1. Attaining Security Profile 1

Security Profile 1 (SP-1) is a grouping of 88 (v1) and 123 (v2) practices from the AESCSF which was defined by the ACSC in consultation with industry and government. All organisations within the Australian energy sector should aspire to reach or surpass this maturity threshold, especially larger, higher criticality organisations which should be targeting SP-2 and SP-3 maturity. For more detail on Security Profiles, refer to the AESCSF Framework Core [2].

As high-level guidance for organisations, consider:

- Reviewing the outcomes from your organisations most recent Lite or Full AESCSF Assessment to identify capability gaps which are required to attain SP-1.
  Note: If a Lite Assessment was completed, the scope of this is SP-1 practices so any gaps are those that are needed to obtain SP-1. If a Full Assessment was completed, export the results to CSV, and filter practices marked as 'Not Complete' and those tagged with 'SP-1'.
- Identify the scope of the cyber security uplift program. This may be all of the gaps to attain SP-1, or may only be a selection of them, with the rest to be addressed at a later time.
- Group these practices into logical focus areas, identify any dependencies, and overlay your organisation's priorities and risk landscape to target the most important uplift areas as early as possible.
- Use the 'Informative References' defined for each practice in the Full Framework [1] as examples and guidance for implementing each practice.
- Identify the resourcing and funding needed to support the program (see section **Error! Reference source not found.**).
- Commence the cyber security program.

4.1.1. Other considerations

- Continue to perform an annual AESCSF Assessment to monitor progress against the program and validate that the intended benefits are being achieved.
- Cyber security capabilities require ongoing support to sustain them, so verify that your organisation can continue to support existing capabilities before introducing new capability via the uplift program.
- Re-establish prospective timelines and priorities where necessary.
- Uplifting maturity is challenging and takes considerable time, effort, and resources. The uplift program should consider the reasonable time to mature, relative to the organisation.

5. References and bibliography

5.1. Useful resources and additional reading

AEMO have published and periodically update a diverse range of resources which can be used to assist your organisations uplift journey, in addition to works published by the Australian government.

Title of Document	Document Source
AESCSF Resources Webpage	AEMO Website
ACSC Small Business Cyber Security Guide V6	Cyber.gov.au Website
ACSC Small Business Survey Report 04/11/2022	Cyber.gov.au Website

Table 3: Useful resources and additional reading

6. References

1	Australian Energy Market Operator (AEMO), “AESCSF Overview,” 2023. [Online]. Available: https://aemo.com.au/en/initiatives/major-programs/cyber-security/aescsf-framework-and-resources.
2	Australian Energy Market Operator (AEMO), “AESCSF Framework Core,” 2023. [Online]. Available: https://aemo.com.au/en/initiatives/major-programs/cyber-security/aescsf-framework-and-resources.
3	ISO, “ISO 31000:2018 Risk management — Guidelines,” 02 2018. [Online]. Available: https://www.iso.org/standard/65694.html#:~:text=ISO%2031000%3A2018%20provides%20guidelines,not%20industry%20or%20sector%20specific..
4	ACSC, “ACSC Small Business Survey Report,” 20 06 220. [Online]. Available: https://www.cyber.gov.au/sites/default/files/2020-07/ACSC Small Business Survey Report.pdf.
5	ACSC, “ACSC Small Business Cyber Security Guide V6,” 10 2022. [Online]. Available: https://www.cyber.gov.au/acsc/view-all-content/publications/small-business-cyber-security-guide.
6	Australian Energy Market Operator (AEMO), “AESCSF Education Workshop Pack,” 2022. [Online]. Available: https://aemo.com.au/en/initiatives/major-programs/cyber-security/aescsf-framework-and-resources.
7	Australian Energy Market Operator (AEMO), “AESCSF Glossary,” 2022. [Online]. Available: https://aemo.com.au/en/initiatives/major-programs/cyber-security/aescsf-framework-and-resources.
8	Australian Energy Market Operator (AEMO), “AESCSF Lite Framework,” 2022. [Online]. Available: https://aemo.com.au/en/initiatives/major-programs/cyber-security/aescsf-framework-and-resources.