Australian Energy Sector Cyber Security Framework (AESCSF)

AESCSF Version 2 - Lite Framework

Important Notice

Purpose

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

This document accompanies other general guidance materials made available to Australian energy market Participants 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 business advice and should not be relied on as a substitute for obtaining detailed advice about any applicable laws, procedures, or policies. AEMO has 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.

Please see the AEMO for additional supporting materials.[1]

[1] https://aemo.com.au/initiatives/major-programs/cyber-security/aescsf-framework-and-resources

Table of Contents

1. Overview

The AESCSF Lite Framework has been specifically designed and developed to enable self-assessment against the AESCSF by lower-criticality market entities, and those with limited time and competing priorities in a simple, easy to understand format. If you would like additional background and information to the AESCSF and terms used in the Framework, please refer to the AESCSF Overview [2] document.

The Lite Framework was refreshed in 2023 to reflect the major update in 2022 to develop AESCSF Version 2 (V2). The Lite Framework consists of 28 multi-select questions written in plain English. The questions have been simplified and adapted/tailored from AESCSF V2.

This document outlines each of the 28 Lite Framework questions and their associated responses.

To undertake a self-assessment using the Lite Framework, participate in the annual AESCSF program, or download a copy of the offline toolkit. For each question, simply select all the responses that are applicable to your organisation. If none of the responses apply, select 'None of the above'. A response to all questions is needed to complete a self-assessment and obtain a maturity score.

PLEASE NOTE

Some responses in the Lite Framework describe poor cyber security practices intentionally and should be responded to with a “No” if they do not apply to your organisation. Responding “Yes” to everything will not result in the highest level of maturity.

The length of time required to complete the self-assessment will vary - if responses to all questions are known, the survey can be filled in under an hour. However, some clarification may be required from additional organisational team members and/or outsourced providers may be required to answer the questions.

The intended users of the Lite Framework are smaller, lower criticality organisations. The AESCSF Criticality Assessment Tool (CAT) [2] above for Electricity, Gas, and Liquid Fuels has been created to determine relative criticality for each of the energy sectors. Please participate in the Annual AESCSF program or download the offline toolkit to calculate your organisation’s criticality.

Guidance from the Australian Cyber Security Centre (ACSC) for low criticality organisations is to obtain Security Profile 1 (SP-1) (refer to the AESCSF Overview for further details). The scope of the Lite Framework is only SP-1 and does not include coverage of SP-2 or SP-3. At the conclusion of a Lite Framework self-assessment, organisations will get a score representing their percentage toward obtaining SP-1 maturity.

[2] https://aemo.com.au/en/initiatives/major-programs/cyber-security/aescsf-framework-and-resources

1.1. Key assessment terms

One of the goals of the AESCSF is to enable organisations to perform self-assessments in a consistent and comparable manner across the energy sector. Both the AESCSF Full and AESCSF Lite Framework include some key terms which should be considered when completing a self-assessment (refer to Table 1: Key assessment term definitions). These key assessment terms appear in a **blue font** throughout the Lite Framework.

Key assessment term	Definition
Documented	The activity is documented to the extent that an individual unfamiliar with the activity could understand how the activity occurs or is implemented as expected, **AND** if the practice/activity is intended to generate documentation as an output, this documentation is available and retained for a suitable period.
Adequate resourcing	Adequate resources are available to support the activity taking into consideration the size of your organisation. This includes **ALL** the following aspects: **People** – There are adequate personnel to perform this activity. If dedicated personnel are not assigned to this activity, the personnel performing the work have adequate bandwidth to perform it alongside their other duties. If this activity is outsourced, adequate resources are contracted to perform the work. **Funding** – There is adequate funding to support this activity (where applicable). This may include funding for licensing, third party products or services, and personnel/head count. **Tools** – There are adequate tools available, deployed and operational within your organisation to support this activity. This may include software, hardware, and/or third party products and services.

Table 1: Key assessment term definitions

1.2. Sections covered in the Lite Framework

The Lite Framework consists of 28 questions, grouped into 11 sections. The sections are derived from the Domains in the underlying "Full" version of the AESCSF. Each section includes an introduction to set the context and provide definitions for key terms used in the questions.

- Managing cyber security risks in your organisation
- Managing third parties
- Managing assets across the organisation
- Establish and maintain cyber security architecture
- Managing identities and access
- Setting up a cyber security program of work
- Managing cyber security threats and vulnerabilities
- Detecting potential cyber security events
- Responding to cyber security incidents
- Creating a cyber secure workforce
- Managing the privacy and confidentiality of personal information

PLEASE NOTE

The ordering of sections in the Lite Framework has been structured to build on and expand key terms used, however you may complete the Lite Framework self-assessment in any order.

2. Lite Framework questions and responses

2.1. Managing cyber security risks in your organisation

Risk management is an important activity to identify and address areas of heightened cyber security risk. A cyber security risk can be identified and managed like any other type of risk, through the right blend of people, process, and technology controls.

1. Within your organisation, are cyber security risks: (Select all that apply)

☑ Identified (at minimum as a once-off activity) [3]

☑ Identified periodically (on an ongoing basis) and upon **documented** triggers [4]

☑ **Documented** in a risk register or similar document

☑ Treated [5]

☑ Treated in a prioritised manner, based on the potential risk impact to the organisation

☑ Managed with **adequate resourcing**

□ None of the above

[3] For example: By conducting risk workshops, risk assessments, control assessments, architecture reviews, vulnerability scanning, penetration testing
[4] For example: Conducting a risk assessment during large system changes or after a cyber incident
[5] For example: Mitigated, accepted, avoided, or transferred

2. To guide cyber security risk management, does your organisation: (Select all that apply)

☑ Have a **documented** methodology or approach to guide how your organisation should identify cyber security risk

☑ Have a **documented** individual or group of people within your organisation who provide governance over cyber security risk management

☑ Have a strategy for managing cyber security risk [6]

☑ **Document** this strategy and align it with your organisation's cyber security program and enterprise architecture

☑ Have **adequate resourcing** to perform cyber security risk management

□ None of the above

[6] For example: A strategy outlining management objectives and activities the organisation will implement to reduce / manage cyber risk. Note that this should be current (i.e., last updated within the past 12-24 months)

2.2. Managing third parties

Organisation often rely on other parties outside the organisation for the delivery of goods and services. These parties are known as third parties. Third parties can provide goods and services that help your organisation do business. A common example of a third party is your organisation's Internet Service Provider (ISP) – without them, your organisation may be unable to connect to the internet and do business. Additionally, some organisations are owned or controlled by an entity outside of Australia, these should also be considered a 'third party'.

It is important to remember that whilst you can put a third party in charge of providing goods and services (also known as outsourcing), you cannot outsource risk.

3. When procuring products and selecting third party services, does your organisation: (Select all that apply)

- ☑ Consider the cyber security capabilities and features of the product or service, and factor this into decision making
- ☑ Consider the security qualifications of third parties and factor this into decision making
- ☑ Apply and **document** additional cyber security controls or requirements for third parties deemed as higher risk
- ☑ Have **adequate resourcing** to identify and manage third party cyber security risk
- □ None of the above

4. To enable prioritised risk management of third parties, does your organisation: (Select all that apply)

- ☑ Identify third parties that support critical business functions [7]
- ☑ Identify which third parties have access to or control your organisation's technology, operational or information assets
- □ None of the above

[7] For example: Control room operations, data management functions

2.3. Managing assets across the organisation

There are three key types of assets to consider in your responses. They are:

- ***Technology assets****: Physical things such as computers (that let you browse the Internet and send emails), servers, mobile phones and printers;*
- ***Operational assets****: A special type of technology assets that let you control a physical piece of equipment that interacts with the energy supply chain; and*
- ***Information assets****: Digital information files, things such as databases or spreadsheets that contain important or sensitive data.*

Keep in mind that an asset might be a combination of one or more of the above.

5. When it comes to documenting information about assets, does your organisation: (Select all that apply)

☑ Have an inventory of important technology and operational assets

☑ Review the asset inventory to ensure that any technology and operational assets likely to be specifically targeted by a threat actor [8] are **documented**

☑ Have an inventory of important information assets

☑ Review the asset inventory to ensure that any information assets likely to be specifically targeted by a threat actor are **documented**

☑ Have **adequate resourcing** to perform asset inventory management

□ None of the above

[8] An entity that is partially or wholly responsible for an incident that impacts – or has the potential to impact – an organisation's security.

6. For the configuration of assets, does your organisation: (Select all that apply)

- ☑ Have baselines (or pre-defined settings) for different types of assets
- ☑ Use and **document** the process of using baselines to configure assets during deployment and restoration
- ☑ Have **adequate resourcing** to perform asset configuration management
- □ None of the above

7. When changes or updates are needed for assets, does your organisation: (Select all that apply)

- ☑ Evaluate and approve changes prior to the change being deployed [9]
- ☑ Keep a record of the changes made to assets
- ☑ Have requirements **documented** that outline what information is necessary to be recorded for changes
- ☑ Perform and **document** the testing of changes to important assets prior to the change being deployed [10]
- ☑ Implement and **document** the process of implementing changes in a secure manner (to avoid misconfigurations being introduced) [11]
- ☑ Document roll-back details for important assets, and have the ability to roll-back changes if needed [12]
- ☑ Have **adequate resourcing** to perform asset change management
- □ None of the above

[9] For example: Via a change review meeting or panel, such as a Change Advisory Board (CAB)
[10] For example: Using a non-production environment to test the change in
[11] For example: Using secure protocols, verification methods such as digital signatures, or other similar controls
[12] For example: Including the technical steps required to undo the change within change documentation, in the event of an error or unexpected behaviour

2.4. Establish and maintain cyber security architecture

Establishing cyber security architecture involves identifying cyber security requirements for your organisation’s assets and designing appropriate controls to protect them. Key terms that should be considered in your response include:

- ***Control****: an action that you can take to respond to a risk; and*
- ***Network****: an interconnected group of assets.*

8. With regards to protecting your assets using cyber security controls, does your organisation: (Select all that apply)

☑ Have controls implemented to protect your network

☑ Have additional controls implemented and **documented** to protect your network which specifically monitor, analyse, and regulate network traffic for important areas of your network [13]

☑ Have additional controls implemented and **documented** to protect your network which specifically monitor, analyse, and restrict web traffic and emails [14]

☑ Implement and **document** network controls based on asset importance [15]

☑ Implement end-point controls to protect important assets [16]

☑ Implement access controls to protect important assets [17]

☑ Protect important data at rest [18]

[13] For example: Firewalls, allow listing/whitelisting, Intrusion Detection and/or Prevention systems (IDS/IPS)

[14] For example: Link blocking, suspicious email blocking, email authentication techniques, IP address blocking

[15] For example: Applying additional controls for assets associated with higher risk or priority to the organisation’s operations

[16] For example: Secure configuration, deploy security applications, and host monitoring) to protect high importance assets

[17] For example: Locks, swipe card access, Access Control Lists (ACLs)

[18] For example: Using authentication, encryption and/or separation from other assets

- ☑ Have remote or third party access which avoids or bypasses your organisation’s cyber security controls
- ☑ Have **adequate resourcing** to perform the management of cyber security controls
- □ None of the above

It is important to understand how your assets can (and do) connect to one another, and to the outside world. When you know how assets connect to one another, you can make decisions about how to leave them connected or disconnect them in the event of a cyber-attack.

9. Regarding separation of technology and operational environments, does your organisation: (Select all that apply)

- ☑ Have a strategy outlining desired outcomes to guide cyber security architecture
- ☑ Separate your technology assets from your operational assets, either physically or logically
- ☑ Have your operational assets able to operate independently from technology assets in the event of an outage of your technology assets, and have this capability **documented**
- ☑ Have operational assets that have direct Internet access (without going through the technology environment)
- ☑ Have **adequate resourcing** to maintain separation of technology and operational assets
- ☑ Have established policies (or other organisational directives) and governance to guide management of technology and operational asset separation
- ☑ Have a team with adequate skills and knowledge designing and implementing the separation of technology and operational assets
- ☑ Have responsibility, accountability, and authority assigned for architecture of technology and operational asset separation
- □ None of the above

2.5. Managing identities and access

Key terms which should be considered in your response include:

- ***Identities**: something like a username (that is unique);*
- ***Credential**: something like a password (that only you know) or a key (that only you have); and*
- ***Access**: the result of an identity and a credential combined. A username and password is a common method of controlling access.*

*When access is set up, the process is called **provisioning**. Conversely, when access is removed, the process is called **deprovisioning**.*

*Providing remote access to any type of asset over the internet is risky and should not be taken lightly. A common method of reducing this risk is to use **multi-factor authentication**, which requires a user to enter a unique code (usually sent by SMS) every time they log into an asset. The Australian Cyber Security Centre (ACSC) recommends the use of multi-factor authentication as one of their Essential Eight strategies to mitigate cyber security incidents* [19] *– advising that it is one of the most effective controls that an organisation can implement to prevent an adversary from gaining access to an asset.*

Finally, controlling access to an asset introduces the concept of a role. There are generally two key role types:

- *An **administrator** role that can make important changes to the configuration of an asset; and*
- *A **standard** role that cannot make changes to the configuration of an asset.*

10. To facilitate access to assets, does your organisation: (Select all that apply)

☑ Set up identities (like a username) to control access to assets [20]

☑ Deprovision identities when they are no longer required

☑ Deprovision identities within a **documented** time period [21]

[19] https://www.cyber.gov.au/acsc/view-all-content/essential-eight

[20] For example: Identities may be for persons, devices, systems and processes

[21] For example: By 5:00pm on the day of employment termination

- ☑ Issue credentials to control access to assets
- ☑ Implement and **document** password requirements (strength and re-use) [22]
- ☑ Implement and **document** stronger authentication controls for high-risk access (multi-factor authentication) [23]
- ☑ Have asset(s) that are accessible from the Internet using only a username and password (not requiring a multi-factor authentication)
- ☑ Limit the usage of administrator access to only activities that require it and have this **documented** [24]
- ☑ Have **adequate resourcing** to perform identity and credential management
- ☐ None of the above

*Access to assets takes two forms, **logical access** which requires the use of a computer or other electronic device, and **physical access** which requires physically being present at the same location as the asset.*

11. To control logical access to assets, does your organisation: (Select all that apply)

- ☑ Implement logical access controls to limit which identities can access an asset [25]
- ☑ Deprovision logical access when no longer required (due to employment termination or role change)
- ☑ Maintain and **document** requirements for logical access [26]

[22] For example: Requiring special characters, numbers, and minimum password length
[23] For example: Requiring multi-factor authentication or single-use credentials for privileged accounts or remote access
[24] For example: Prohibiting usage of these accounts for day-to-day work activities
[25] For example: Which identities are granted access to systems and applications, and whether an identity has the ability to view or edit information
[26] For example: Restrictions on which type of identities are allowed to access an asset, or whether remote access is allowed

☑ Perform additional scrutiny and monitoring of logical access which is deemed to be higher-risk based on your **documented** requirements [27]

☑ Have **adequate resourcing** to perform logical access management

□ None of the above

12. To control physical access to assets, does your organisation: (Select all that apply)

☑ Implement physical access controls to restrict unauthorised access to an asset [28]

☑ Deprovision physical access when longer required (return of keys and swipe cards)

☑ Maintain logs of physical access [29]

☑ Maintain and **document** requirements for physical access [30]

☑ Include the principle of 'least privilege' (where only the minimum access should be provisioned in line with personnel's duties) in your organisation's **documented** requirements for physical access.

☑ Perform additional scrutiny and monitoring of physical access which is deemed to be higher risk based on your **documented** requirements [31]

☑ Have **adequate resourcing** to perform physical access management

□ None of the above

13. Does your organisation: (Select all that apply)

[27] For example: Privileged accounts, service accounts, remote access, administrative accounts, emergency (or break-glass) accounts, etc

[28] For example: Fences, locks, and swipe-card enabled doors

[29] For example: Guestbooks for visitors and logs of swipe card access

[30] For example: Defining requirements for visitors, what type of team members can be given physical access to specific areas

[31] For example: Server rooms, access to networking equipment, and access to data centres

☑ Make sure that identities (and their associated access) are provisioned for valid business reasons prior to creating or updating them

☑ Provision administrator access to one or more assets by default (instead of provisioning standard access by default)

☑ Have assets which can be accessed anonymously (without having to provide your identity or credentials)

☐ None of the above

2.6. Setting up a cyber security program of work

*A **cyber security program** of work contains all cyber security projects your organisation is working on. The program might run for a set duration or be permanent. Higher levels of maturity require the cyber security program to be permanent and ongoing, with the program being responsible for maintaining cyber security capability across your organisation.*

*In the context of the Australian Energy Sector Cyber Security Framework (AESCSF), a cyber security program of work is supported by **a cyber security strategy** that defines the objectives of the program and how these objectives will be achieved.*

14. Does your organisation have a cyber security strategy?

● Yes

○ No

15. To support the cyber security program of work, does your organisation: (Select all that apply)

☑ Have senior management who recognise and communicate the importance of the cyber security program

☑ Identify, integrate, and **document** any applicable regulatory or compliance requirements into your organisation’s cyber security program [32]

[32] For example: SOCI and PCI-DSS

☑ Have **adequate resourcing** to support your organisation’s cyber security program

☐ None of the above

2.7. Managing cyber security threats and vulnerabilities

While these two are sometimes confused, these two areas are different and should be defined as the following for your response:

- ***Threat**: An entity who is partially or wholly responsible for an incident that impacts (or has the potential to impact) an organisations cyber security; and*
- ***Vulnerability**: a weakness in a part of your organisation’s people, process, or technology that may require strengthening, which may be how a threat actor attacks your organisation.*

A threat usually exploits (or takes advantage of) a vulnerability.

16. In preparation for cyber security threats targeting you, does your organisation: (Select all that apply)

☑ Identify internal and external cyber security threat information sources

☑ Gather and analyse threat information from these sources

☑ Use threat information to identify threat outcomes of concern to your organisation

☑ Apply controls to protect against applicable threats [33]

☑ Share threat information internally to relevant positions and teams and externally to other similar organisations based on **documented** requirements or guidelines defined by your organisation

[33] For example: Implementation of additional controls or threat monitoring

☑ Have **adequate resourcing** to perform threat management activities

☐ None of the above

Technology and operational assets can have cyber vulnerabilities. Some vulnerabilities are already known and can be ***patched.*** *Other vulnerabilities are yet to be discovered, highlighting the importance of* ***preventative controls****. A* ***security patch*** *is a new, often smaller piece of software that is installed alongside (or to replace) an existing piece of software to make it stronger. Applying a security patch is a common way to* ***remediate*** *a cyber security vulnerability.*

17. To manage vulnerabilities, does your organisation: (Select all that apply)

☑ Identify cyber security vulnerability information sources [34]

☑ Gather and analyse vulnerability information from these sources

☑ Perform vulnerability assessments (or scans)

☑ Mitigate vulnerabilities that are present through patching or other controls

☑ Perform testing of patches before rollout to identify issues and **document** this testing [35]

☑ Have **adequate resourcing** to perform vulnerability management activities

☐ None of the above

[34] For example: Vendor feeds, security researchers, responsible bug disclosure
[35] For example: Using a non-production environment

18. For instances where your organisation is not able to remediate a cyber security vulnerability:

● Compensating controls are applied to mitigate the risk

○ No further action is taken

2.8. Detecting potential cyber security events

Detecting a cyber security event is not always straightforward, even when your organisation has a lot of resources. There are two key activities that support effective detection, including:

- ***Logging**: which refers to collecting small pieces of information about how an asset is working (or when something changes); and*
- ***Monitoring**: which refers to consolidating your logs and looking for unusual patterns or behaviour.*

An unusual pattern or behaviour that your organisation identifies from the process of monitoring may indicate a cyber security event and may be escalated into an incident.

19. To enable cyber security event detection, does your organisation: (Select all that apply)

☑ Perform event logging on important assets

☑ **Document** how logging activities should occur, including which logs are important to collect

☑ Log all third-party privileged access based on **documented** requirements

☑ Ensure that access to centralised logging data is restricted to only those that require it

☑ Perform monitoring (or periodic reviews) of log data that is collected

☑ Maintain alarms and alerts for when cyber security events occur, or thresholds are met based on **documented** requirements

☑ Perform periodic reviews of alarms and alerts that are triggered

☑ Have **documented** methods established to communicate and report the status of cyber security logging and monitoring

☑ Have **adequate resourcing** to perform logging and monitoring activities

□ None of the above

2.9. Responding to cyber security incidents

There are many types of incidents that an organisation can face, with the unavailability of an asset (or collection of assets) being a common example. A data breach is another common example.

There are three key terms to consider in your response, they are:

- ***Event**: which may be an unusual pattern (or one-time occurrence) that your organisation has identified from the process of logging and monitoring. Not all events are deemed cyber security incidents, and as such these events should be analysed to identify the events that should be escalated into an incident;*
- ***Incident**: which indicates that the cyber security event is real, and there is the potential for a negative impact; and*
- ***Continuity**: which refers to the steps that your organisation will take, to either recover or keep the business running, if an incident cannot be resolved in a timely manner.*

It can take some time for an organisation to become aware of cyber security events, especially as technology controls are strengthened and employee awareness of cyber security is raised.

20. To raise a cyber security incident, does your organisation: (Select all that apply)

☑ Have a designated person or role to whom cyber security events are reported [36]

☑ Have **documented** criteria on how to tell what is and is not a cyber security event

[36] For example: This may be your security manager, a designated security email account, the service desk, or a Managed Service Provider (MSP)

- ☑ **Document** cyber security events that meet the defined criteria of an incident
- ☑ Have documented criteria to guide when an event should be raised as a cyber security incident
- ☑ Analyse cyber security events to determine whether they should be raised as incidents
- ☑ Have a specific place where cyber security events and incidents are **documented** and tracked through to resolution
- ☑ Notify internal and external stakeholders of incidents based on **documented** reporting requirements
- ☑ Have **adequate resourcing** to perform cyber security event analysis and raising of incidents
- ☐ None of the above

Cyber security incident response plans are an important part of managing your organisation's cyber security risk.

21. For situations when a cyber security incident has been raised, does your organisation: (Select all that apply)

- ☑ Have a **documented** plan and use it for responding to cyber security incidents
- ☑ Have designated personnel to respond to a cyber security incident, including having assigned roles and responsibilities
- ☑ Respond to cyber security incidents with the objective of limiting impact and restoring normal operations
- ☑ Include within the response plan **documented** guidance for communications with both internal and external stakeholders
- ☑ Identify which authorities should be contacted during a cyber security incident and how to contact them
- ☑ Report cyber security incidents to the Australian Cyber Security Centre (ACSC)

☑ Conduct periodic cyber security incident response exercises to rehearse the plan based on a **documented** frequency, and perform testing after pre-determined triggers [37]

☑ **Document** lessons learned after executing the response plan, and include corrective actions to address identified improvements

☑ Have **adequate resourcing** to perform cyber security incident response

□ None of the above

22. With regards to maintaining continuity of business operations, does your organisation: (Select all that apply)

☑ Have continuity plans in place to sustain and restore business operations if a cyber security incident occurs

☑ Identify which critical business functions are required to sustain minimum operations [38]

☑ Continuity plans are **documented** and include which assets and services support these critical business functions

☑ Continuity plans for important technology, operational, and information assets are **documented** and includes relevant details covering backups, replacement, and any requirements for spare assets.

☑ Periodically review and update continuity plans

☑ Have **adequate resourcing** to perform business continuity management

☑ Have established policies (or other organisational directives) and governance to guide management of continuity plans

☑ Have a team with adequate skills and knowledge managing continuity planning

☑ Have responsibility, accountability, and authority assigned for management of continuity plans

□ None of the above

[37] For example: Large system changes or external events
[38] For example: Through performing a Business Impact Analysis (BIA)

23. To support recovery from a cyber security incident, does your organisation: (Select all that apply)

☑ Perform backups and test the ability to restore operations from backup

☑ Implement and **document** cyber security controls protecting backup data that are equivalent or more rigorous than the controls protecting the source data

☑ Implement and **document** data backup separation from source data, either via logical or physical means

☑ Identify what assets require having spares available in the event of an asset failure

☑ Have spares available for assets based on **documented** requirements

☑ Have **adequate resourcing** to perform backup management and handling of spare assets

□ None of the above

2.10. Creating a cyber secure workforce

Cyber security is everyone's responsibility, and some employees have additional responsibilities compared with others. There are four key activities that support a cyber secure workforce, including:

- ***Assigning responsibilities**: so that employees know what they can do to prevent cyber security events;*
- ***Vetting employees**: so that the organisation knows the background of their employees;*
- ***Training employees**: so that they have the skills required to stay cyber secure in their role; and*
- ***Raising awareness**: so that employees know cyber security is a priority.*

24. Does your organisation perform the following across the employee lifecycle: (Select all that apply)

☑ Personnel vetting as part of hiring a new team member [39]

☑ Make employees aware of expectations for acceptable use and their cyber security obligations during employment in a **documented** manner

☑ Conduct cyber security awareness activities or training during employment [40]

☑ Have an employee termination process which includes cyber security considerations [41]

☑ Have **adequate resourcing** to manage cyber security across the employee lifecycle

□ None of the above

[39] For example: Background and/or police checks
[40] For example: eLearn modules, phishing simulations, and watching videos
[41] For example: Return of assets including laptops and building pass, and disabling of access

25. Regarding assigning cyber security responsibilities, does your organisation: (Select all that apply)

☑ Identify the roles and responsibilities needed to achieve your organisation's cyber security objectives, covering both cyber and non-cyber security roles.

☑ Assign identified cyber security responsibilities to ensure accountability

☑ **Document** the assignment of cyber security responsibilities

☑ Have **adequate resourcing** to support the management of cyber security responsibilities

☐ None of the above

26. To upskill and train employees, does your organisation: (Select all that apply)

☑ Have training available to employees with assigned cyber security responsibilities in line with their duties

☑ Identify core cyber security skill requirements for employees and gaps against these

☑ Require cyber security training be completed prior to being granted access to important assets and have this **documented**

☑ Have **adequate resourcing** to support management of cyber security training

☐ None of the above

2.11. Managing the privacy and confidentiality of personal information

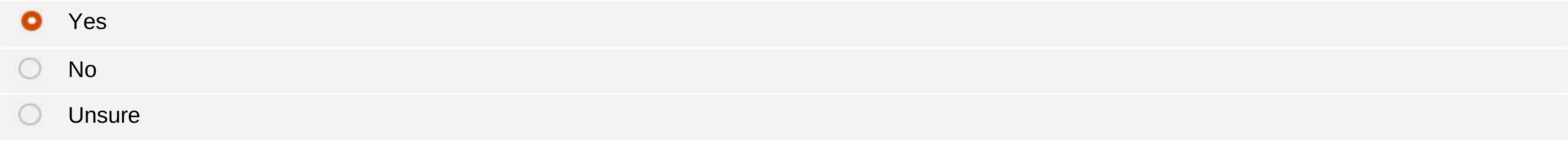
Australia's Privacy Act 1988 (Privacy Act) defines ***personal information*** *(which is also referred to as Personally Identifiable Information (PII)) as information or an opinion about an identified individual, or individual who is reasonably identifiable:*

a. whether the information or opinion is true or not; and
b. whether the information or opinion is recorded in a material form or not.

One example of PII is a spreadsheet that contains the name, phone number, and email address of one or more individuals. There are many other examples.

Under the Notifiable Data Breach (NDB) scheme any organisation or agency that the Privacy Act covers must notify affected individuals and the Office of the Australian Information Commissioner (OAIC) when a data breach is likely to result in serious harm to an individual whose personal information is involved. Additional information can be obtained from the Australian Government OAIC.

27. Does your organisation collect personal information: (Select all that apply)



● Yes

○ No

○ Unsure

28. Has your organisation: (Select all that apply)

☑ Identified privacy requirements applicable to your organisation

☑ Defined what is, and is not, treated as personal information considering your business activities

☑ Nominated a privacy contact to respond to privacy enquiries

☑ Identified and **documented** any business activities that come into contact with personal information [42]

☑ Have **adequate resourcing** to support management of personal information and privacy

□ None of the above

[42] For example: Collection, processing, storage, or transmission

2.12. Summary of self-assessment results

After completing a Lite Framework self-assessment using either the AESCSF program platform, or the offline toolkit, you will receive a score as a percentage which represents your organisation’s progress towards completing Security Profile 1 (SP-1). [43] In addition to this, progress indicators will also be displayed for each section, allowing your organisation to identify areas of relative strength and opportunity.

The ACSC has identified 29 ‘priority practices’ – this is guidance provided by the ACSC on the capabilities that organisations should focus on implementing first to build their cyber security. The AESCSF program platform or the offline toolkit will indicate if your organisation has any of these priority areas still to implement, and what these capabilities are.

Additional guidance material for organisations starting their cyber security maturity journey is available in the AESCSF guidance material for low criticality organisations [44], and from the ACSC website. [45]

[43] the Target State maturity guidance from the Australian Cyber Security Centre for Low criticality entities
[44] https://aemo.com.au/en/initiatives/major-programs/cyber-security/aescsf-framework-and-resources
[45] https://www.cyber.gov.au/acsc/small-and-medium-businesses/acsc-small-business-guide