AES CSF
Australian Energy Sector Cyber Security Framework

Australian Government
Department of Industry, Science, Energy and Resources

AEMO
AUSTRALIAN ENERGY MARKET OPERATOR

Australian Energy Sector Cyber Security Framework (AESCSF)

Lite Framework

2022 Program - Minor Refresh

AES | CSF
Australian Energy Sector | Cyber Security Framework

Australian Government
Department of Industry, Science, Energy and Resources

AEMO
AUSTRALIAN ENERGY MARKET OPERATOR

Important Notice

Purpose

This document is made available by The Department of Industry, Science, Energy and Resources (DISER) and The Australian Energy Market Operator (AEMO) to provide information about the 2022 Australian Energy Sector Cyber Security Framework (AESCSF) Program.

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. DISER and 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, DISER, 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.

Table of Contents

1. Overview

The AESCSF Lite framework has been developed to facilitate self-assessment against the AESCSF by lower-criticality market entities, and those with limited time and security resources.

The assessment consists of 29 multi-select easy to follow questions written in plain English. Simply select as many responses that are applicable to your organisation. If none of responses apply, select 'None of the above'.

The length of time required to complete the assessment will vary - if responses to all questions are known, the survey can be filled in around 15-20 minutes. However, some clarification with specialists and outsourced providers may be required in order to answer the questions accurately, in which case the total time to complete the assessment will increase.

PLEASE NOTE

The scope of the Lite assessment is AESCSF Security Profile 1 (the Target State maturity guidance from the Australian Cyber Security Centre (ACSC) for Low criticality entities). Entities with an overall criticality of Medium or High per the AESCSF Criticality Assessment Tool(s) should complete a full AESCSF self-assessment which facilitates comparison of maturity against Security Profiles 1, 2 and 3 (the Target State maturity guidance from the ACSC for Low, Medium and High criticality entities respectively). A full assessment allows organisations to realise the full benefit of year-on-year result comparison and industry benchmarking.

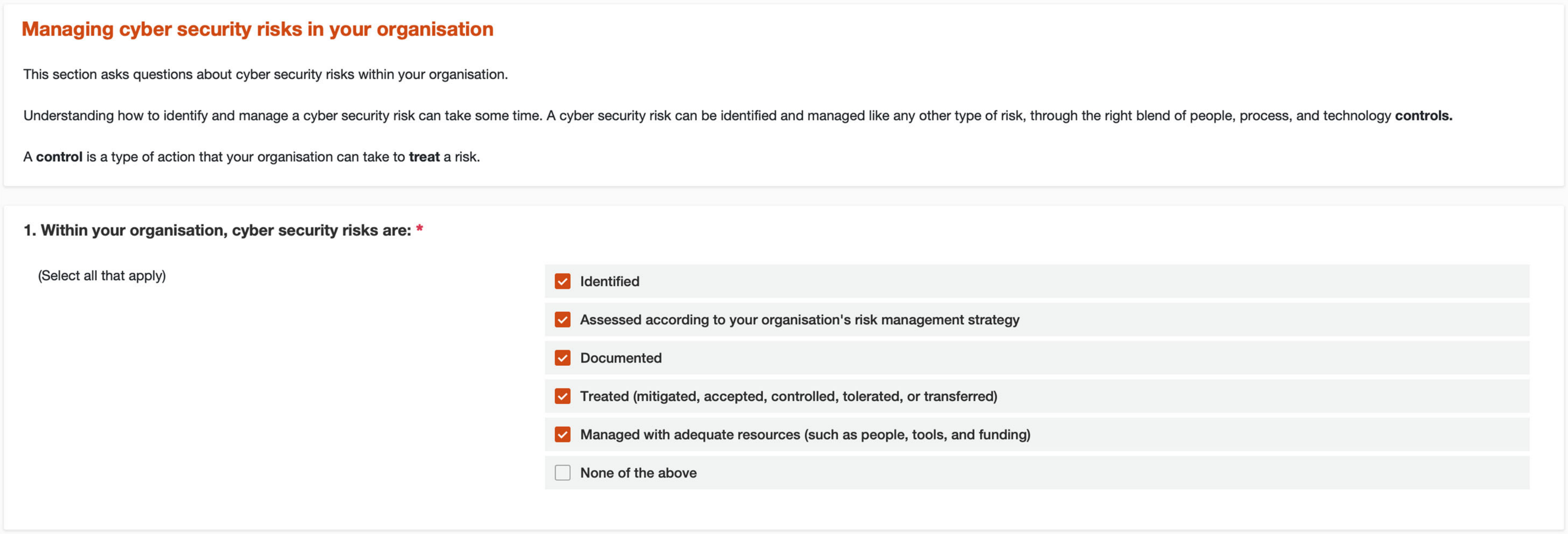
Table 1 indicates which SP an organisation in the electricity sub-sector should achieve based on their criticality (as determined by the E-CAT).

Security Profile (SP)	Participant criticality	Practices and anti-patterns			Total required to achieve SP
		MIL-1	MIL-2	MIL-3	
Security Profile 1 (SP-1)	Low	57	27	4	88
Security Profile 2 (SP-2)	Medium	0	94	18	200 (112+88 from SP-1)
Security Profile 3 (SP-3)	High	0	0	82	282 (82+200 from SP-2)

Table 1: Target State Maturity and Security Profiles

2. Sections of the Lite Framework

2.1. Managing cyber security risks in your organisation



Managing cyber security risks in your organisation

This section asks questions about cyber security risks within your organisation.

Understanding how to identify and manage a cyber security risk can take some time. 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.**

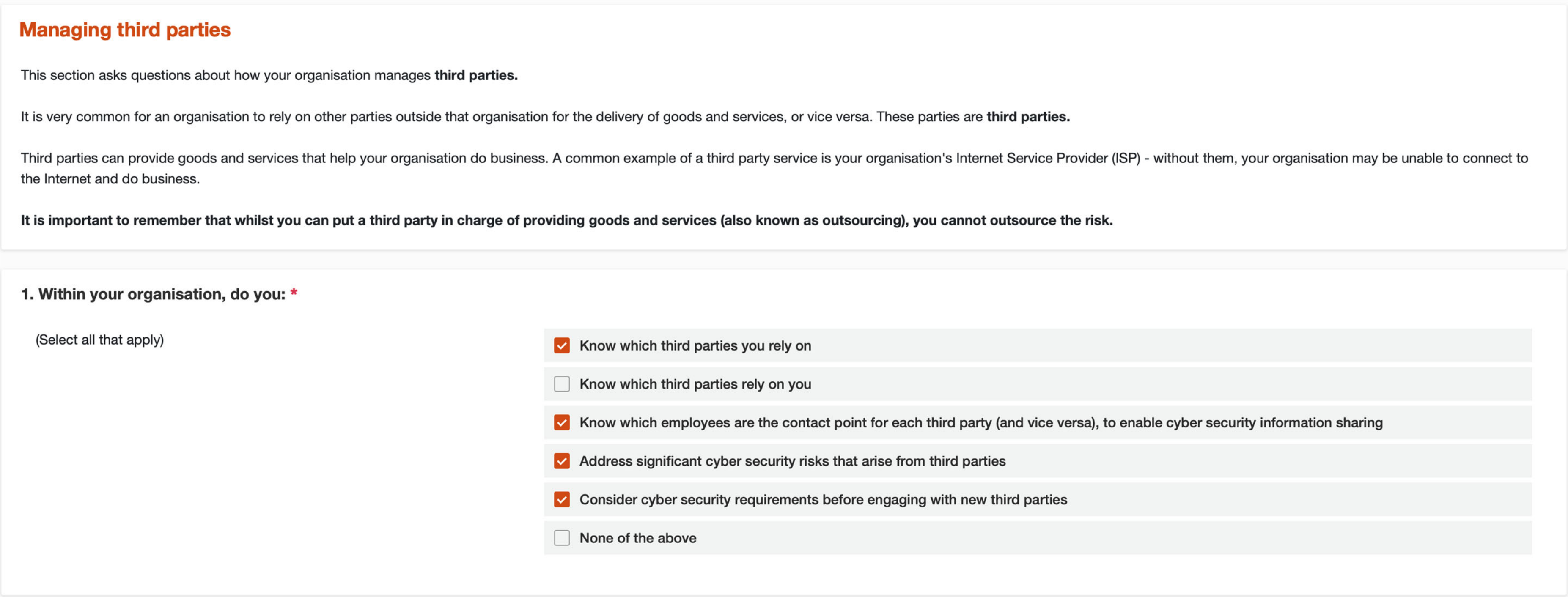
A **control** is a type of action that your organisation can take to **treat** a risk.

1. Within your organisation, cyber security risks are: *

(Select all that apply)

- ☑ Identified
- ☑ Assessed according to your organisation's risk management strategy
- ☑ Documented
- ☑ Treated (mitigated, accepted, controlled, tolerated, or transferred)
- ☑ Managed with adequate resources (such as people, tools, and funding)
- □ None of the above

2.2. Managing third parties



Managing third parties

This section asks questions about how your organisation manages **third parties.**

It is very common for an organisation to rely on other parties outside that organisation for the delivery of goods and services, or vice versa. These parties are **third parties.**

Third parties can provide goods and services that help your organisation do business. A common example of a third party service is your organisation's Internet Service Provider (ISP) - without them, your organisation may be unable to connect to the Internet and do business.

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 the risk.

1. Within your organisation, do you: *

(Select all that apply)

☑ Know which third parties you rely on

☐ Know which third parties rely on you

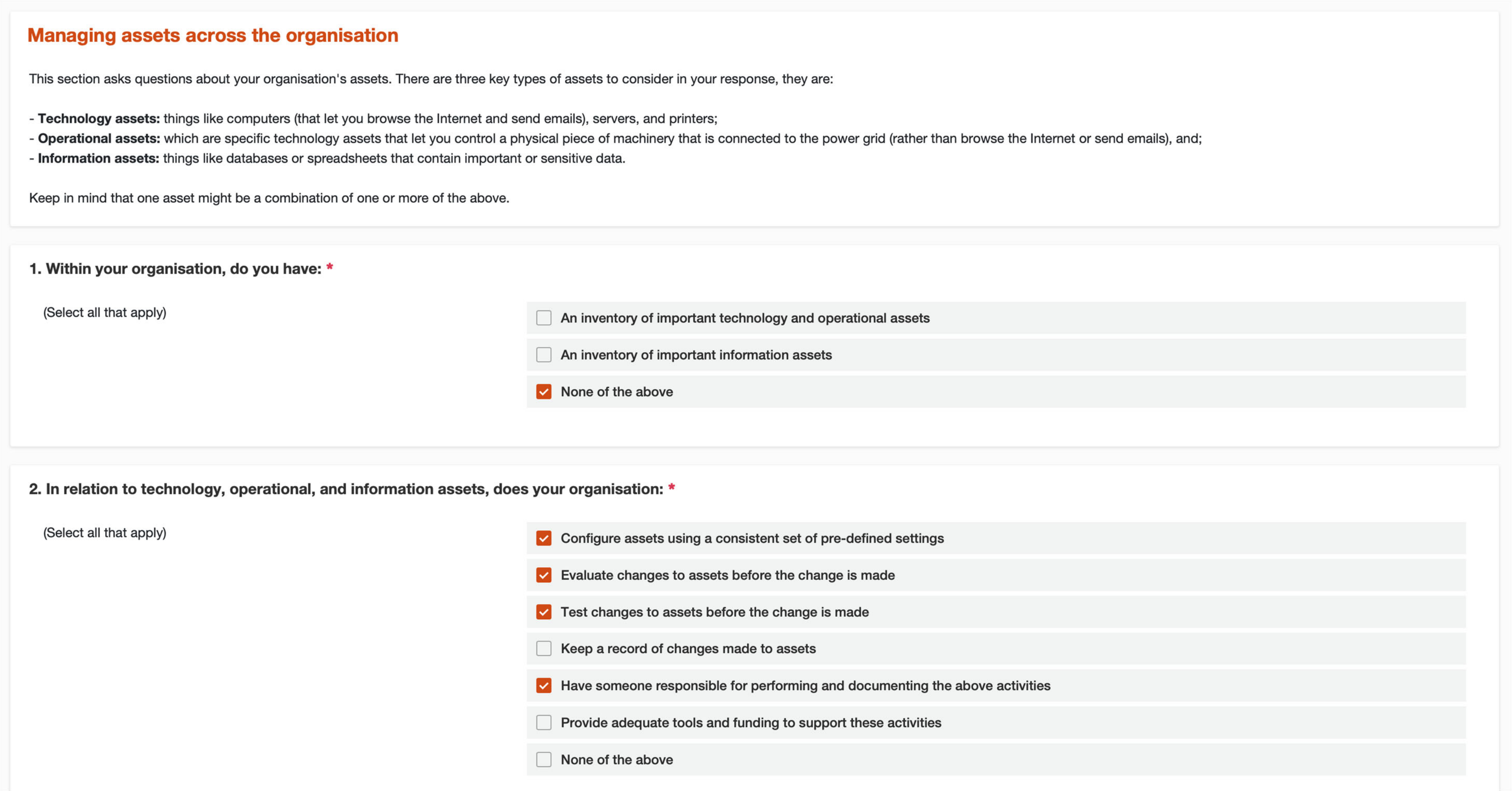
☑ Know which employees are the contact point for each third party (and vice versa), to enable cyber security information sharing

☑ Address significant cyber security risks that arise from third parties

☑ Consider cyber security requirements before engaging with new third parties

☐ None of the above

2.3. Managing assets across the organisation



Managing assets across the organisation

This section asks questions about your organisation's assets. There are three key types of assets to consider in your response, they are:

- **Technology assets:** things like computers (that let you browse the Internet and send emails), servers, and printers;
- **Operational assets:** which are specific technology assets that let you control a physical piece of machinery that is connected to the power grid (rather than browse the Internet or send emails), and;
- **Information assets:** things like databases or spreadsheets that contain important or sensitive data.

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

1. Within your organisation, do you have: *

(Select all that apply)

☐ An inventory of important technology and operational assets

☐ An inventory of important information assets

☑ None of the above

2. In relation to technology, operational, and information assets, does your organisation: *

(Select all that apply)

☑ Configure assets using a consistent set of pre-defined settings

☑ Evaluate changes to assets before the change is made

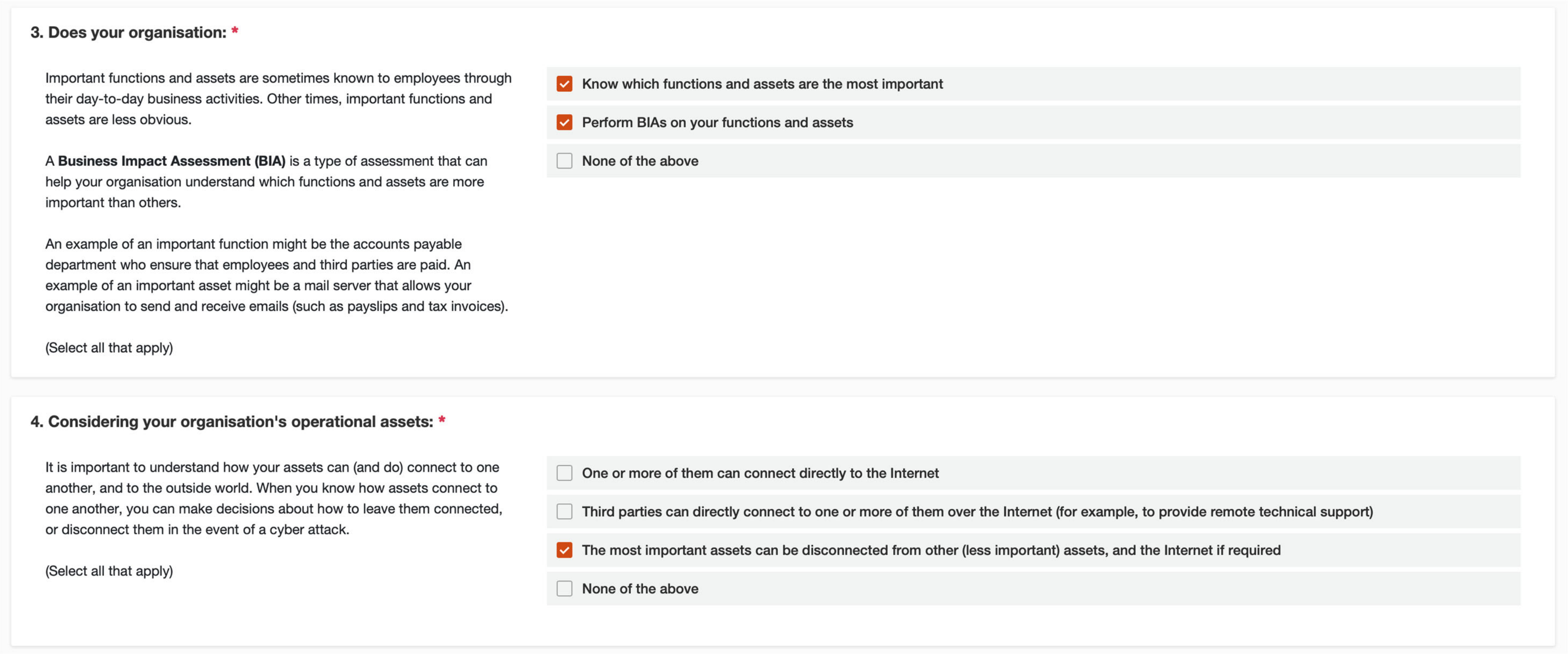
☑ Test changes to assets before the change is made

☐ Keep a record of changes made to assets

☑ Have someone responsible for performing and documenting the above activities

☐ Provide adequate tools and funding to support these activities

☐ None of the above



3. Does your organisation: *

Important functions and assets are sometimes known to employees through their day-to-day business activities. Other times, important functions and assets are less obvious.

A **Business Impact Assessment (BIA)** is a type of assessment that can help your organisation understand which functions and assets are more important than others.

An example of an important function might be the accounts payable department who ensure that employees and third parties are paid. An example of an important asset might be a mail server that allows your organisation to send and receive emails (such as payslips and tax invoices).

(Select all that apply)

- ☑ Know which functions and assets are the most important
- ☑ Perform BIAs on your functions and assets
- □ None of the above

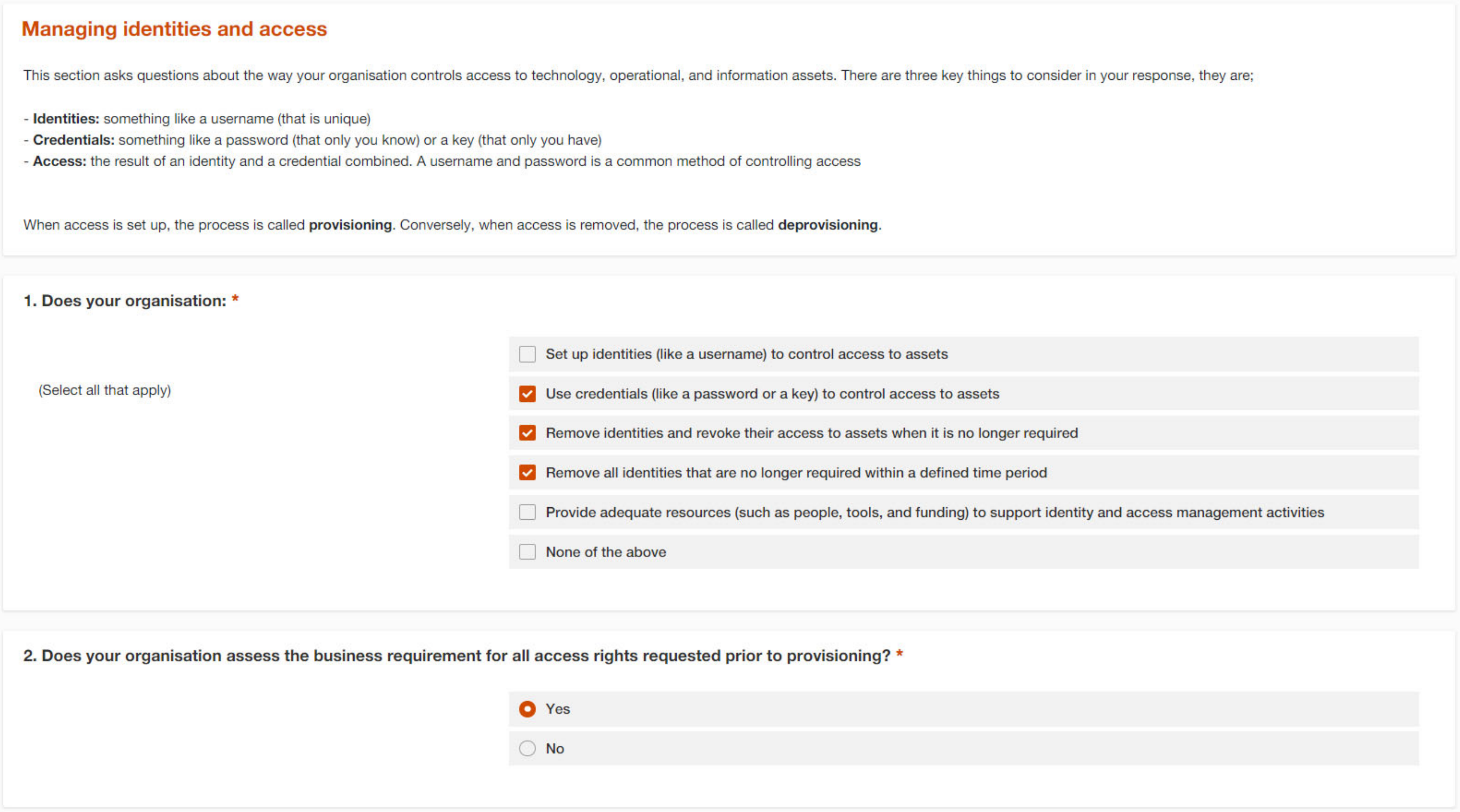
4. Considering your organisation's operational assets: *

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.

(Select all that apply)

- □ One or more of them can connect directly to the Internet
- □ Third parties can directly connect to one or more of them over the Internet (for example, to provide remote technical support)
- ☑ The most important assets can be disconnected from other (less important) assets, and the Internet if required
- □ None of the above

2.4. Managing identities and access



Managing identities and access

This section asks questions about the way your organisation controls access to technology, operational, and information assets. There are three key things to consider in your response, they are;

- **Identities:** something like a username (that is unique)
- **Credentials:** something like a password (that only you know) or a key (that only you have)
- **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**.

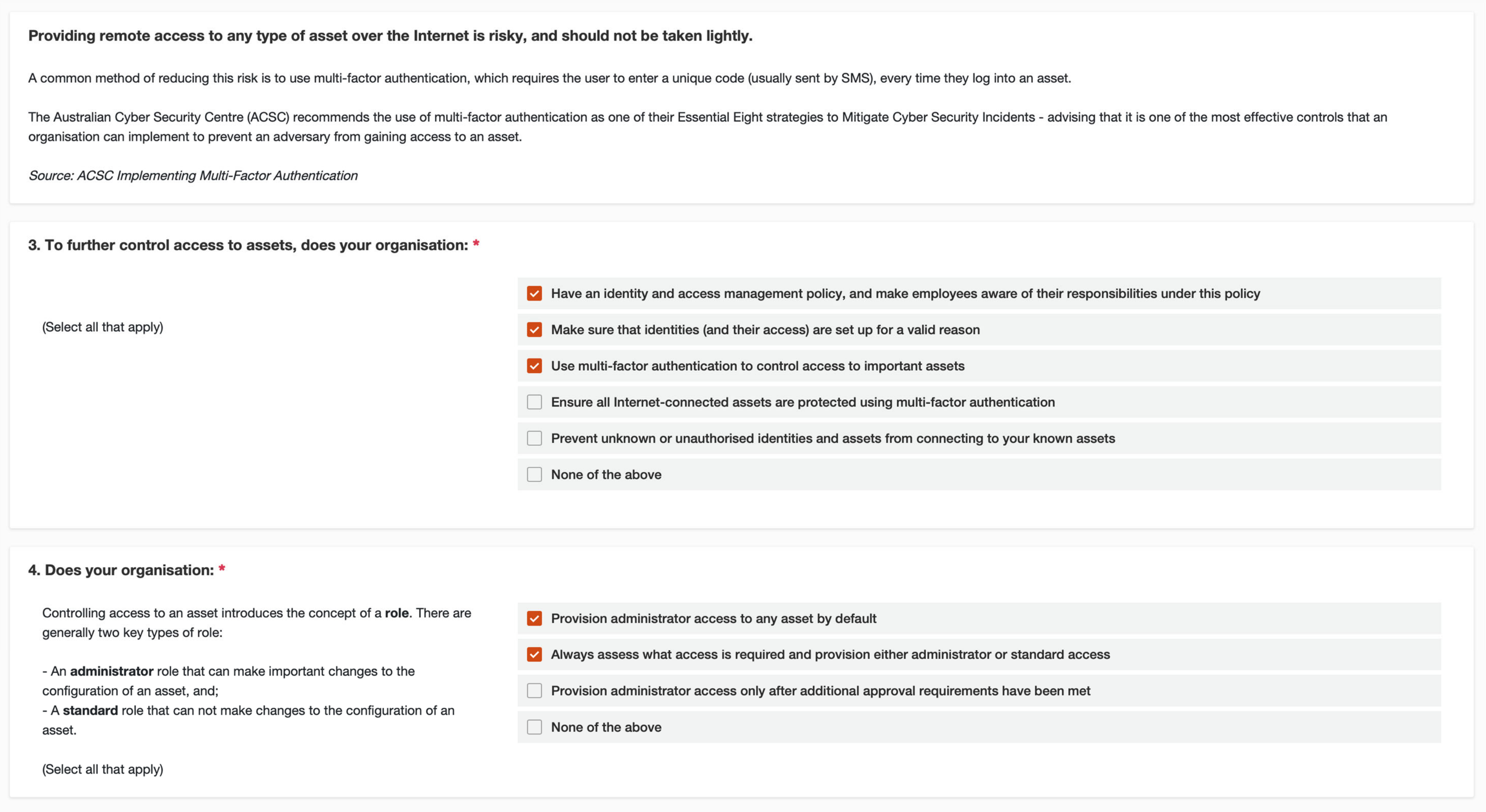
1. Does your organisation: *

(Select all that apply)

☐ Set up identities (like a username) to control access to assets
☑ Use credentials (like a password or a key) to control access to assets
☑ Remove identities and revoke their access to assets when it is no longer required
☑ Remove all identities that are no longer required within a defined time period
☐ Provide adequate resources (such as people, tools, and funding) to support identity and access management activities
☐ None of the above

2. Does your organisation assess the business requirement for all access rights requested prior to provisioning? *

● Yes
○ No



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 the 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 - 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.

Source: ACSC Implementing Multi-Factor Authentication

3. To further control access to assets, does your organisation: *

(Select all that apply)

- ☑ Have an identity and access management policy, and make employees aware of their responsibilities under this policy
- ☑ Make sure that identities (and their access) are set up for a valid reason
- ☑ Use multi-factor authentication to control access to important assets
- □ Ensure all Internet-connected assets are protected using multi-factor authentication
- □ Prevent unknown or unauthorised identities and assets from connecting to your known assets
- □ None of the above

4. Does your organisation: *

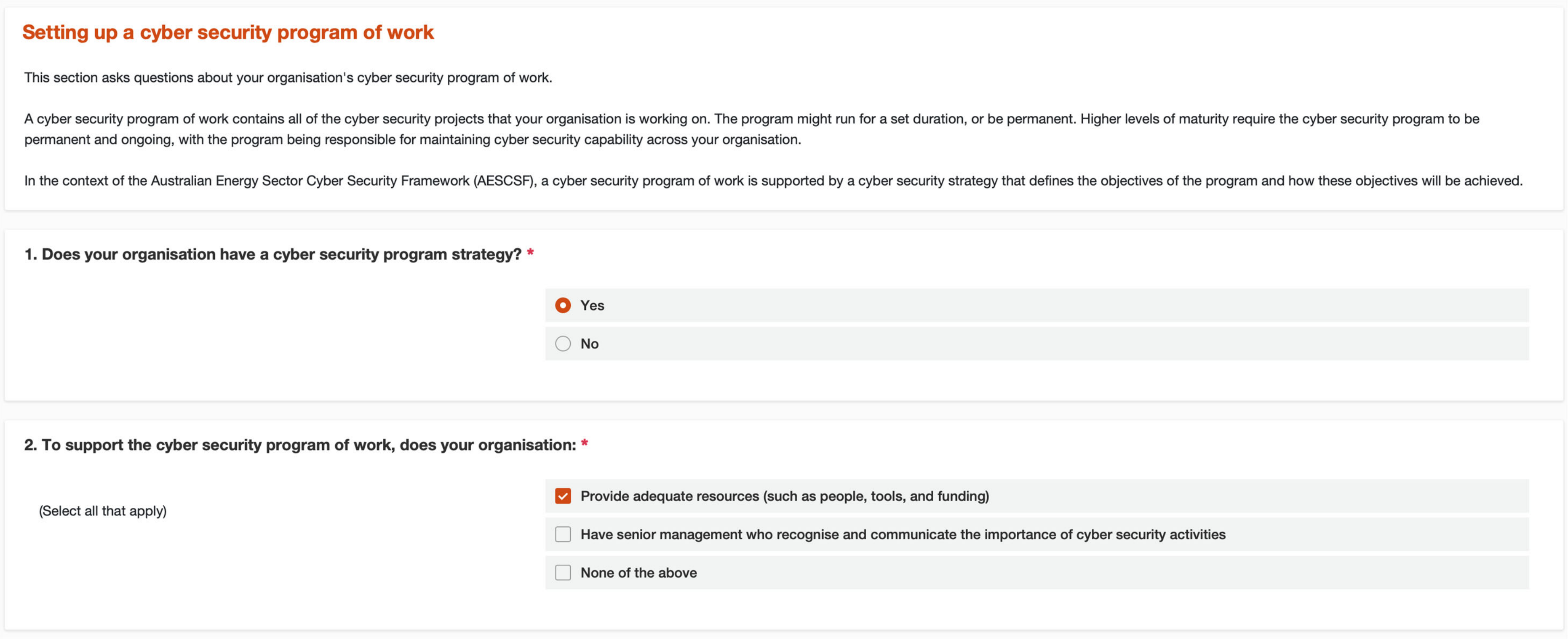
Controlling access to an asset introduces the concept of a **role**. There are generally two key types of role:

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

(Select all that apply)

- ☑ Provision administrator access to any asset by default
- ☑ Always assess what access is required and provision either administrator or standard access
- □ Provision administrator access only after additional approval requirements have been met
- □ None of the above

2.5. Setting up a cyber security program of work



Setting up a cyber security program of work

This section asks questions about your organisation's cyber security program of work.

A cyber security program of work contains all of the cyber security projects that 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.

1. Does your organisation have a cyber security program strategy? *

● Yes

○ No

2. To support the cyber security program of work, does your organisation: *

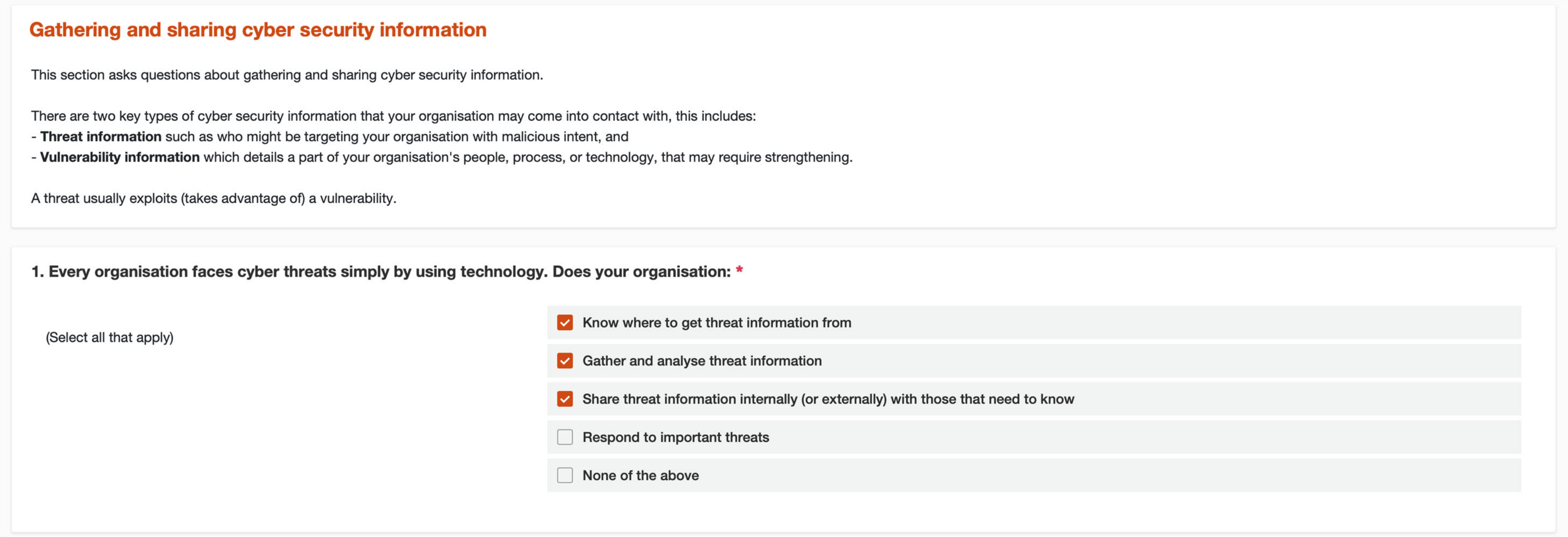
(Select all that apply)

☑ Provide adequate resources (such as people, tools, and funding)

□ Have senior management who recognise and communicate the importance of cyber security activities

□ None of the above

2.6. Gathering and sharing cyber security information



Gathering and sharing cyber security information

This section asks questions about gathering and sharing cyber security information.

There are two key types of cyber security information that your organisation may come into contact with, this includes:
- **Threat information** such as who might be targeting your organisation with malicious intent, and
- **Vulnerability information** which details a part of your organisation's people, process, or technology, that may require strengthening.

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

1. Every organisation faces cyber threats simply by using technology. Does your organisation: *

(Select all that apply)

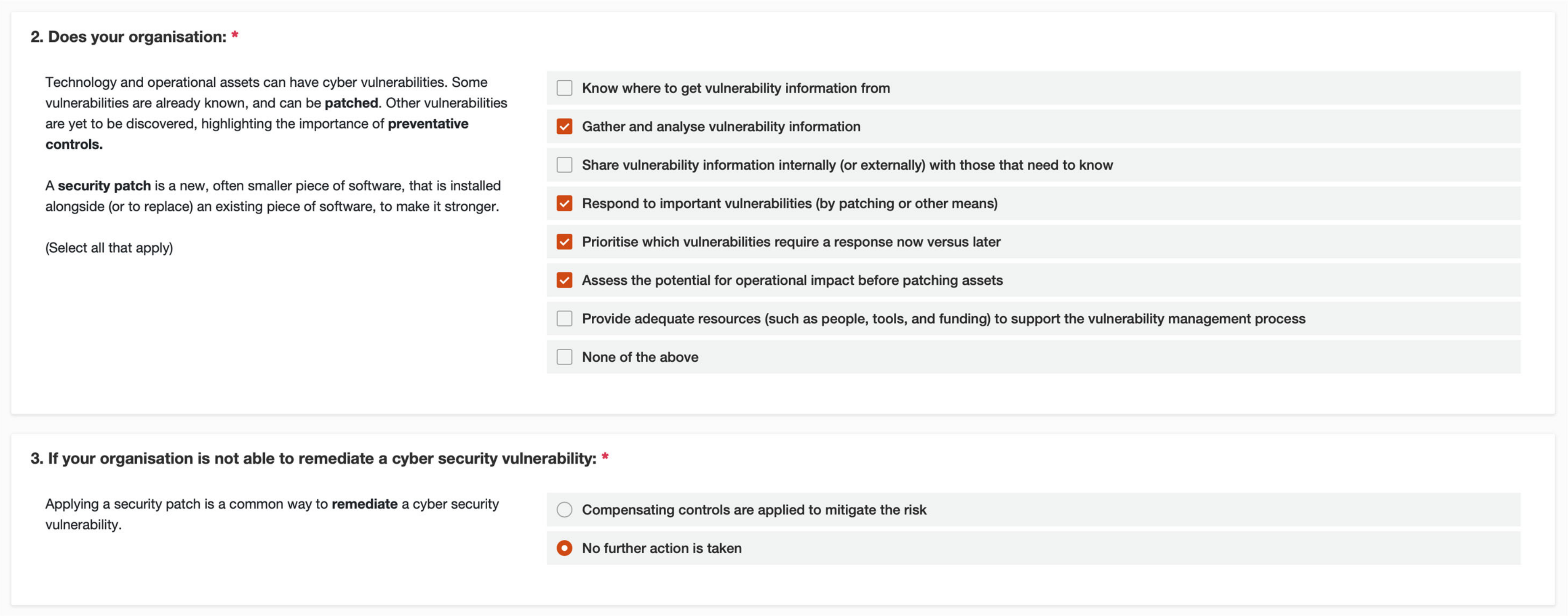
☑ Know where to get threat information from

☑ Gather and analyse threat information

☑ Share threat information internally (or externally) with those that need to know

□ Respond to important threats

□ None of the above



2. Does your organisation: *

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.

(Select all that apply)

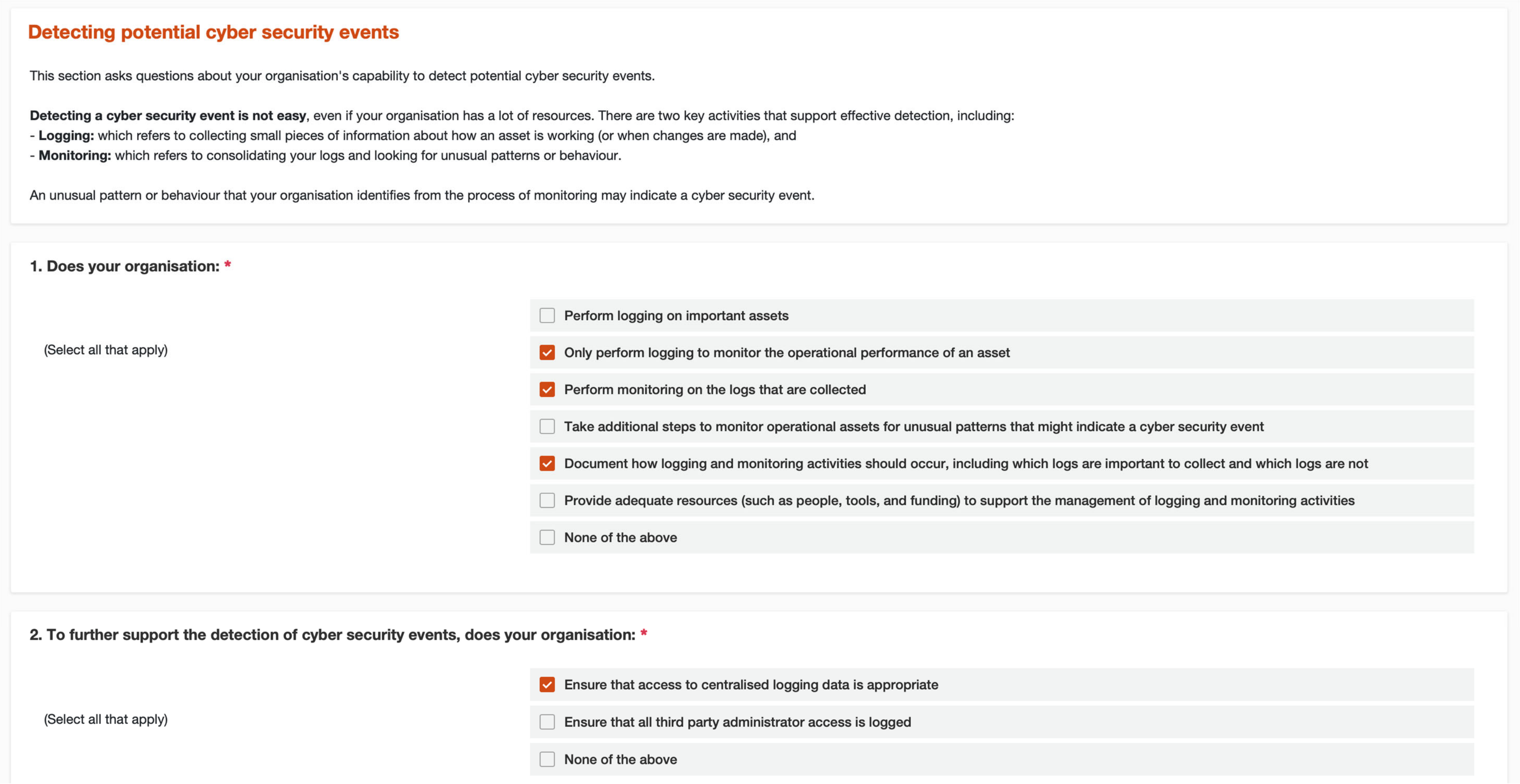
- □ Know where to get vulnerability information from
- ☑ Gather and analyse vulnerability information
- □ Share vulnerability information internally (or externally) with those that need to know
- ☑ Respond to important vulnerabilities (by patching or other means)
- ☑ Prioritise which vulnerabilities require a response now versus later
- ☑ Assess the potential for operational impact before patching assets
- □ Provide adequate resources (such as people, tools, and funding) to support the vulnerability management process
- □ None of the above

3. If your organisation is not able to remediate a cyber security vulnerability: *

Applying a security patch is a common way to **remediate** a cyber security vulnerability.

- ○ Compensating controls are applied to mitigate the risk
- ● No further action is taken

2.7. Detecting potential cyber security events



Detecting potential cyber security events

This section asks questions about your organisation's capability to detect potential cyber security events.

Detecting a cyber security event is not easy, even if 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 changes are made), 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.

1. Does your organisation: *

(Select all that apply)

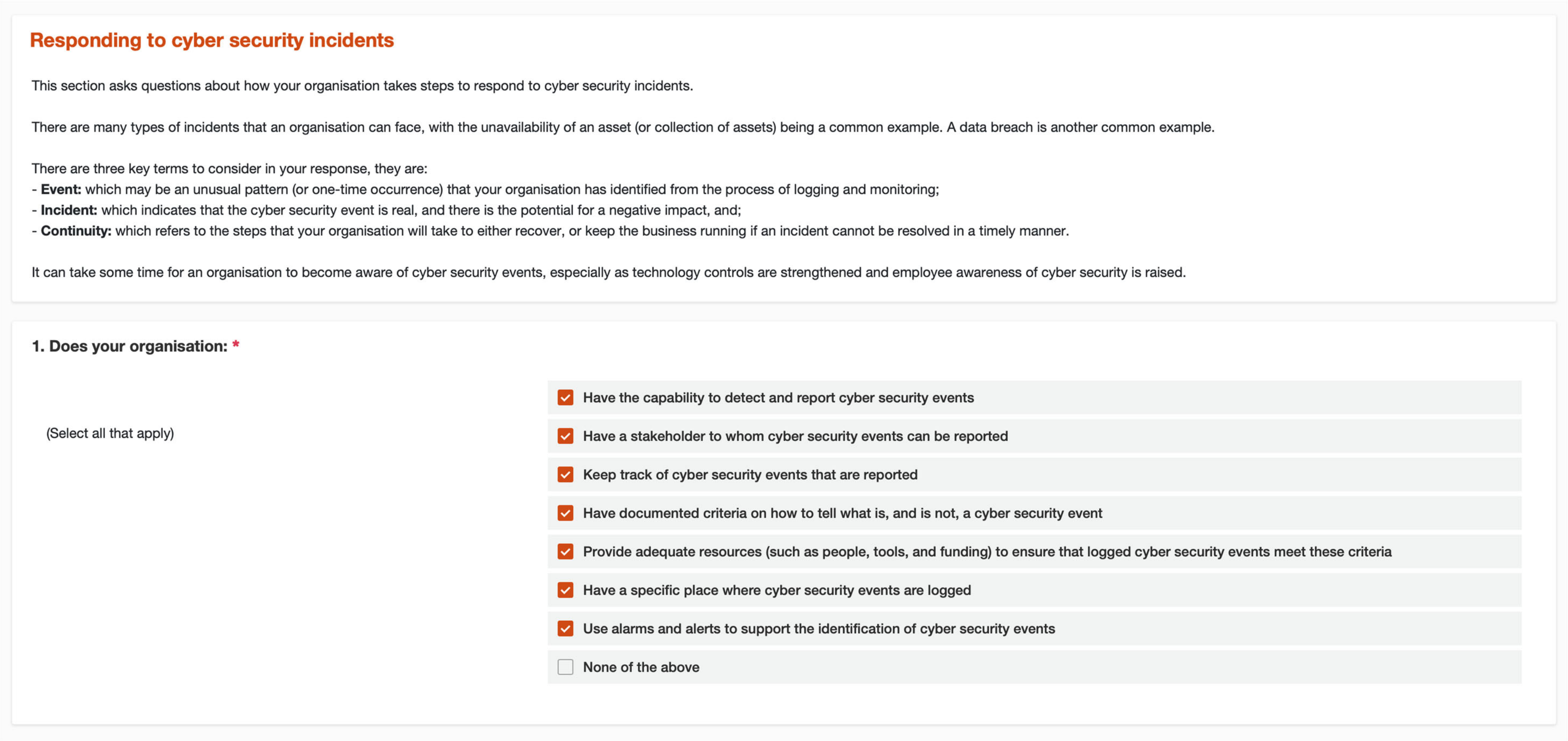
- □ Perform logging on important assets
- ☑ Only perform logging to monitor the operational performance of an asset
- ☑ Perform monitoring on the logs that are collected
- □ Take additional steps to monitor operational assets for unusual patterns that might indicate a cyber security event
- ☑ Document how logging and monitoring activities should occur, including which logs are important to collect and which logs are not
- □ Provide adequate resources (such as people, tools, and funding) to support the management of logging and monitoring activities
- □ None of the above

2. To further support the detection of cyber security events, does your organisation: *

(Select all that apply)

- ☑ Ensure that access to centralised logging data is appropriate
- □ Ensure that all third party administrator access is logged
- □ None of the above

2.8. Responding to cyber security incidents



Responding to cyber security incidents

This section asks questions about how your organisation takes steps to respond 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;
- **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.

1. Does your organisation: *

(Select all that apply)

☑ Have the capability to detect and report cyber security events

☑ Have a stakeholder to whom cyber security events can be reported

☑ Keep track of cyber security events that are reported

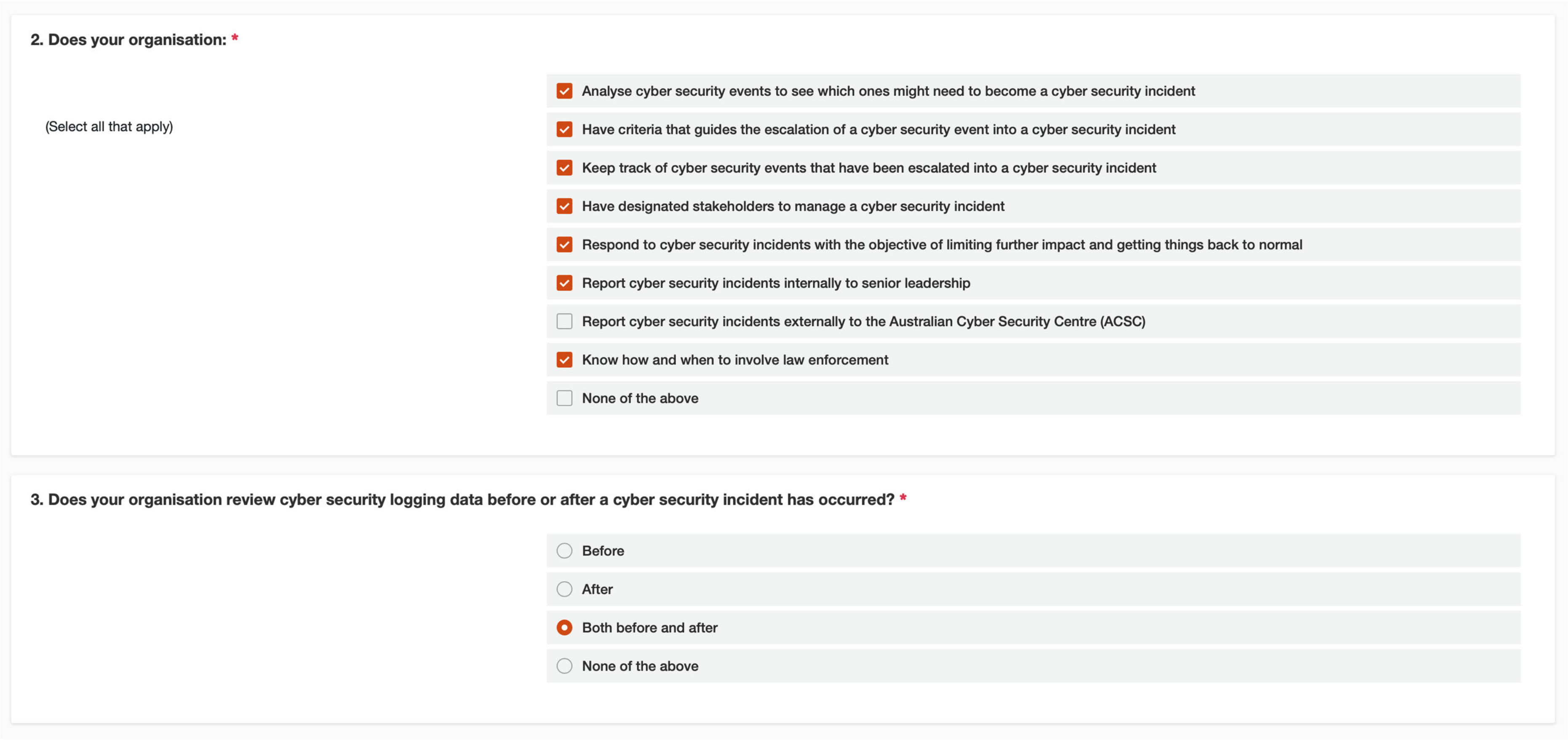
☑ Have documented criteria on how to tell what is, and is not, a cyber security event

☑ Provide adequate resources (such as people, tools, and funding) to ensure that logged cyber security events meet these criteria

☑ Have a specific place where cyber security events are logged

☑ Use alarms and alerts to support the identification of cyber security events

□ None of the above



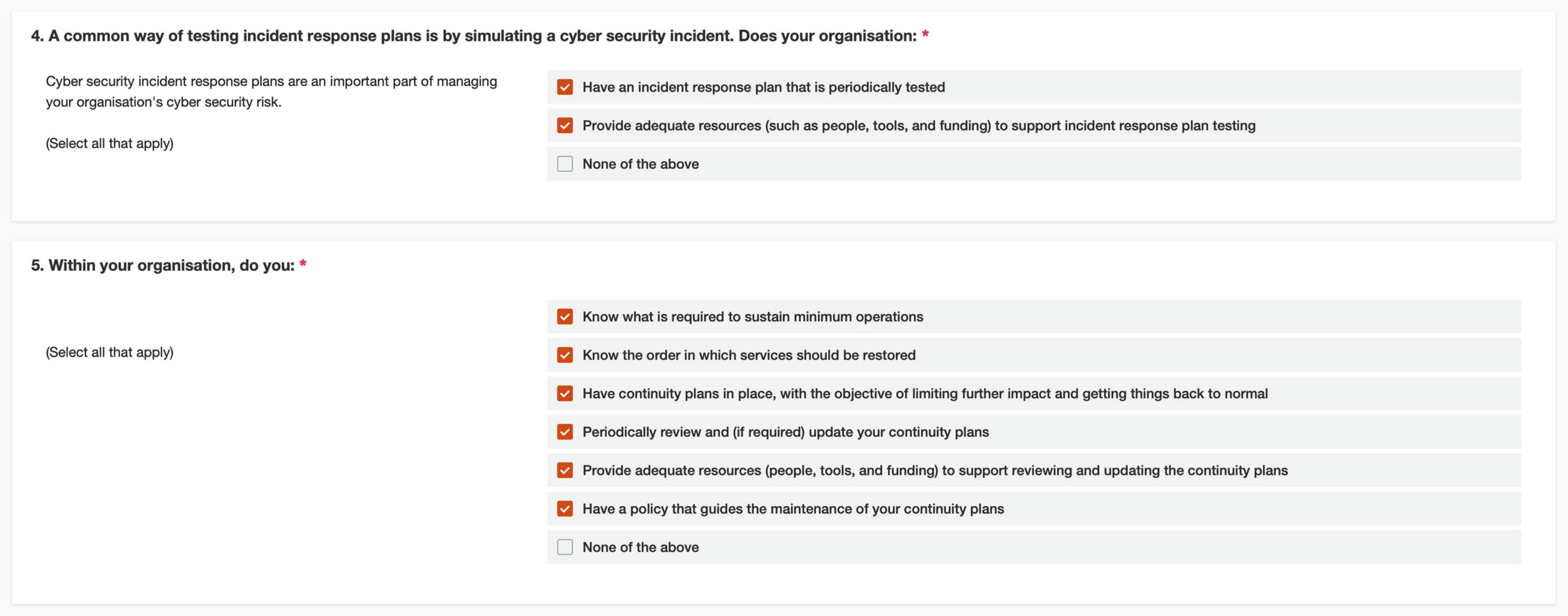
2. Does your organisation: *

(Select all that apply)

- ☑ Analyse cyber security events to see which ones might need to become a cyber security incident
- ☑ Have criteria that guides the escalation of a cyber security event into a cyber security incident
- ☑ Keep track of cyber security events that have been escalated into a cyber security incident
- ☑ Have designated stakeholders to manage a cyber security incident
- ☑ Respond to cyber security incidents with the objective of limiting further impact and getting things back to normal
- ☑ Report cyber security incidents internally to senior leadership
- ☐ Report cyber security incidents externally to the Australian Cyber Security Centre (ACSC)
- ☑ Know how and when to involve law enforcement
- ☐ None of the above

3. Does your organisation review cyber security logging data before or after a cyber security incident has occurred? *

- ○ Before
- ○ After
- ● Both before and after
- ○ None of the above



4. A common way of testing incident response plans is by simulating a cyber security incident. Does your organisation: *

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

(Select all that apply)

☑ Have an incident response plan that is periodically tested

☑ Provide adequate resources (such as people, tools, and funding) to support incident response plan testing

☐ None of the above

5. Within your organisation, do you: *

(Select all that apply)

☑ Know what is required to sustain minimum operations

☑ Know the order in which services should be restored

☑ Have continuity plans in place, with the objective of limiting further impact and getting things back to normal

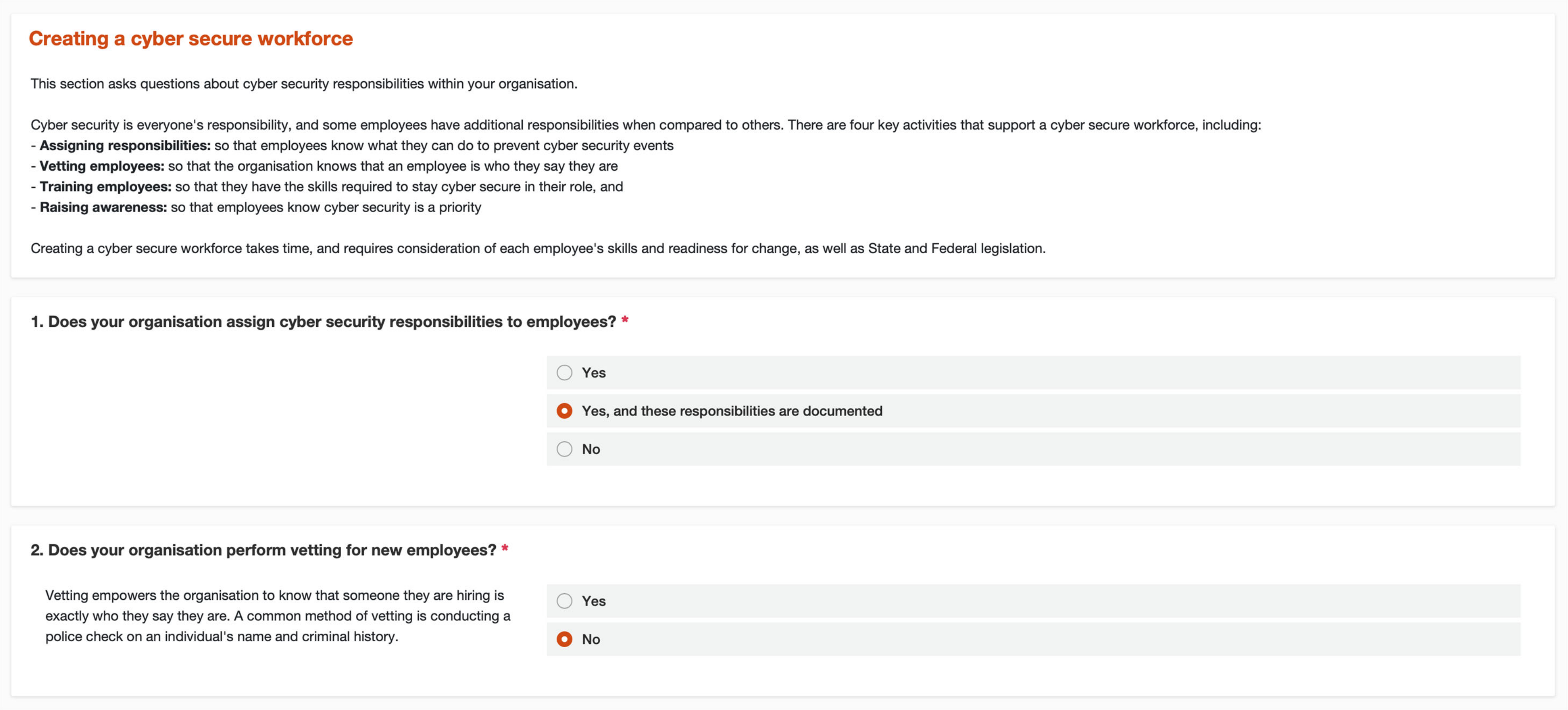
☑ Periodically review and (if required) update your continuity plans

☑ Provide adequate resources (people, tools, and funding) to support reviewing and updating the continuity plans

☑ Have a policy that guides the maintenance of your continuity plans

☐ None of the above

2.9. Creating a cyber secure workforce



Creating a cyber secure workforce

This section asks questions about cyber security responsibilities within your organisation.

Cyber security is everyone's responsibility, and some employees have additional responsibilities when compared to 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 that an employee is who they say they are
- **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

Creating a cyber secure workforce takes time, and requires consideration of each employee's skills and readiness for change, as well as State and Federal legislation.

1. Does your organisation assign cyber security responsibilities to employees? *

○ Yes

● Yes, and these responsibilities are documented

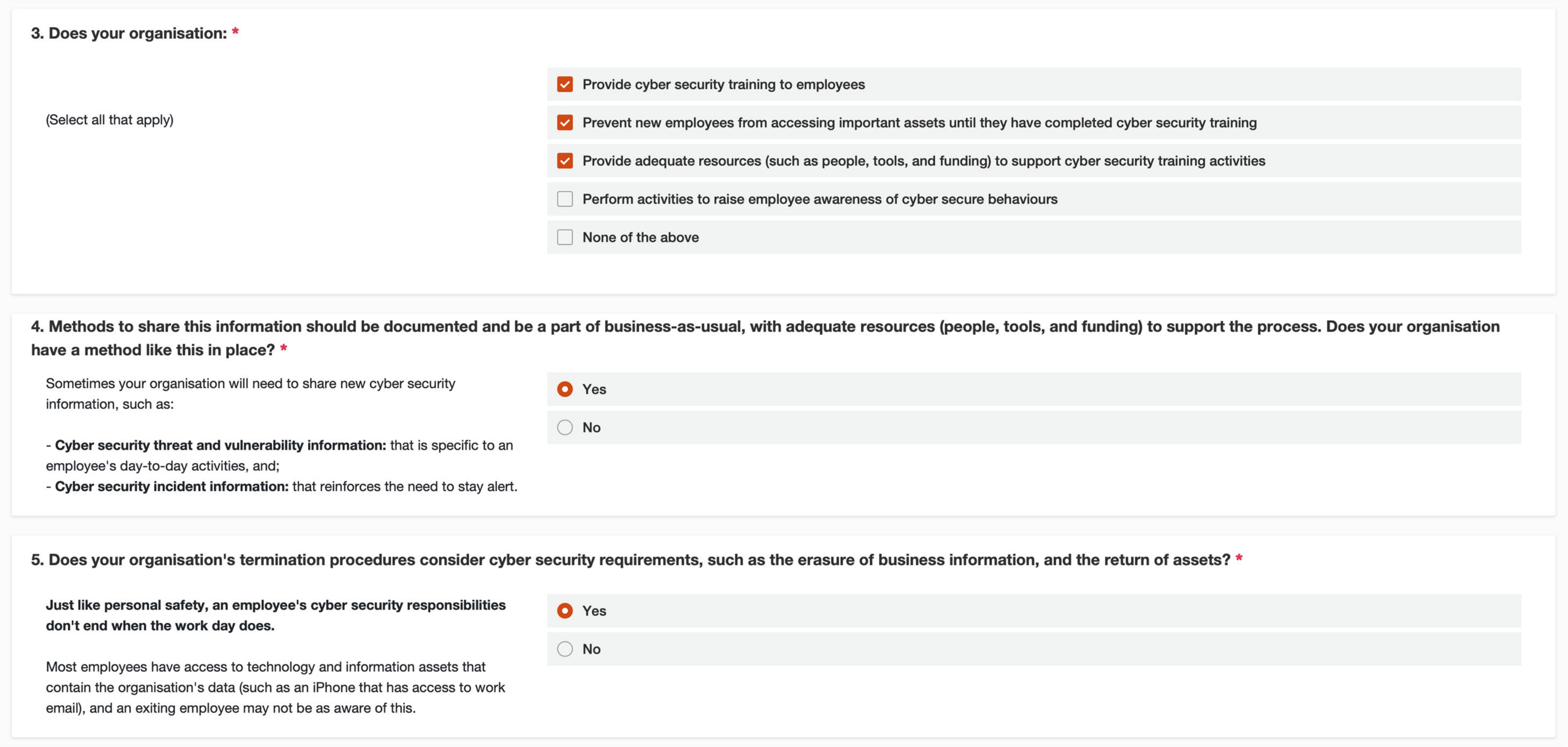
○ No

2. Does your organisation perform vetting for new employees? *

Vetting empowers the organisation to know that someone they are hiring is exactly who they say they are. A common method of vetting is conducting a police check on an individual's name and criminal history.

○ Yes

● No



3. Does your organisation: *

(Select all that apply)

- ☑ Provide cyber security training to employees
- ☑ Prevent new employees from accessing important assets until they have completed cyber security training
- ☑ Provide adequate resources (such as people, tools, and funding) to support cyber security training activities
- □ Perform activities to raise employee awareness of cyber secure behaviours
- □ None of the above

4. Methods to share this information should be documented and be a part of business-as-usual, with adequate resources (people, tools, and funding) to support the process. Does your organisation have a method like this in place? *

Sometimes your organisation will need to share new cyber security information, such as:

- **Cyber security threat and vulnerability information:** that is specific to an employee's day-to-day activities, and;
- **Cyber security incident information:** that reinforces the need to stay alert.

- ● Yes
- ○ No

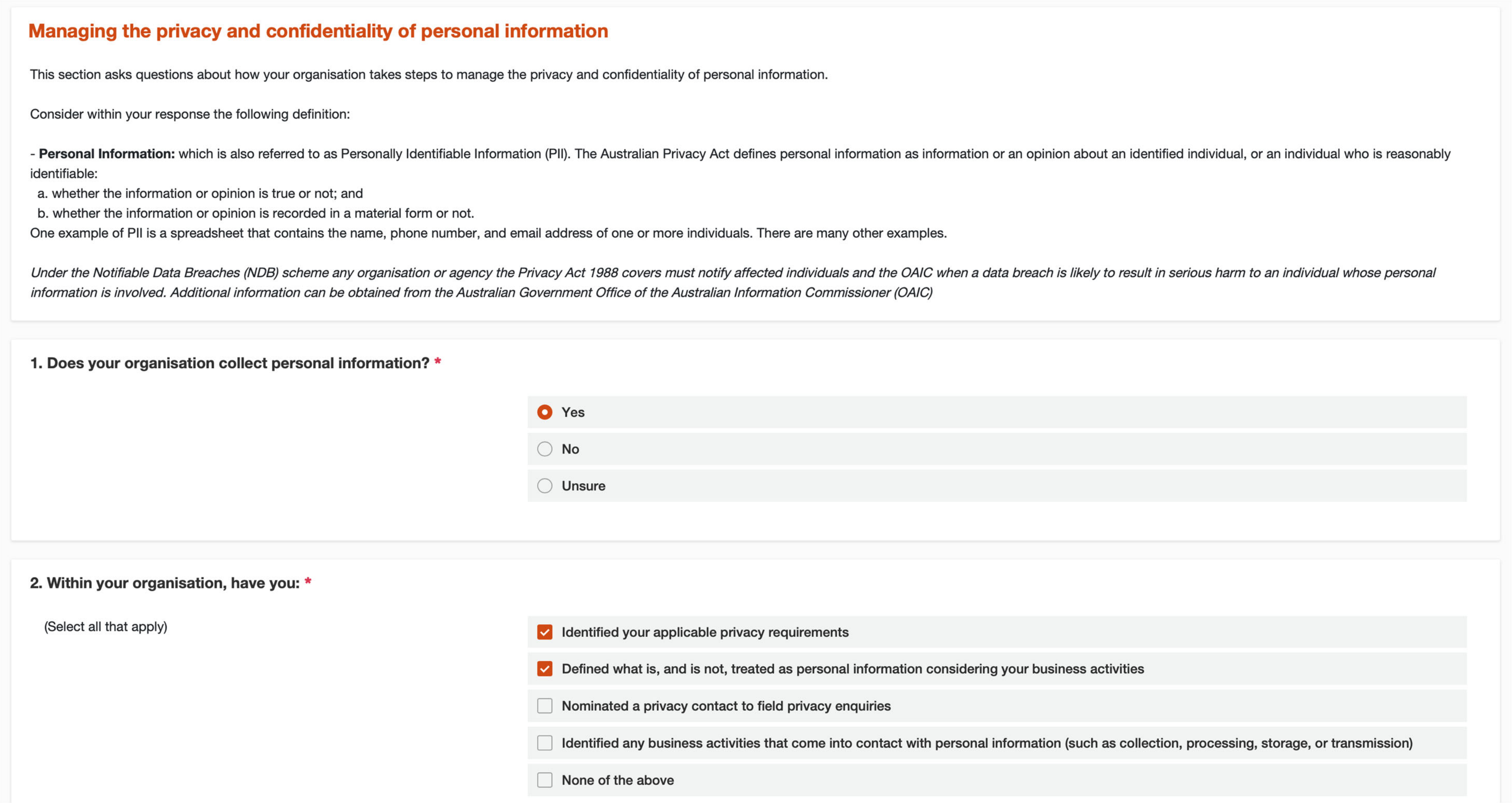
5. Does your organisation's termination procedures consider cyber security requirements, such as the erasure of business information, and the return of assets? *

Just like personal safety, an employee's cyber security responsibilities don't end when the work day does.

Most employees have access to technology and information assets that contain the organisation's data (such as an iPhone that has access to work email), and an exiting employee may not be as aware of this.

- ● Yes
- ○ No

2.10. Managing the privacy and confidentiality of personal information



Managing the privacy and confidentiality of personal information

This section asks questions about how your organisation takes steps to manage the privacy and confidentiality of personal information.

Consider within your response the following definition:

- **Personal Information:** which is also referred to as Personally Identifiable Information (PII). The Australian Privacy Act defines personal information as information or an opinion about an identified individual, or an 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 Breaches (NDB) scheme any organisation or agency the Privacy Act 1988 covers must notify affected individuals and the 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 Office of the Australian Information Commissioner (OAIC)

1. Does your organisation collect personal information? *

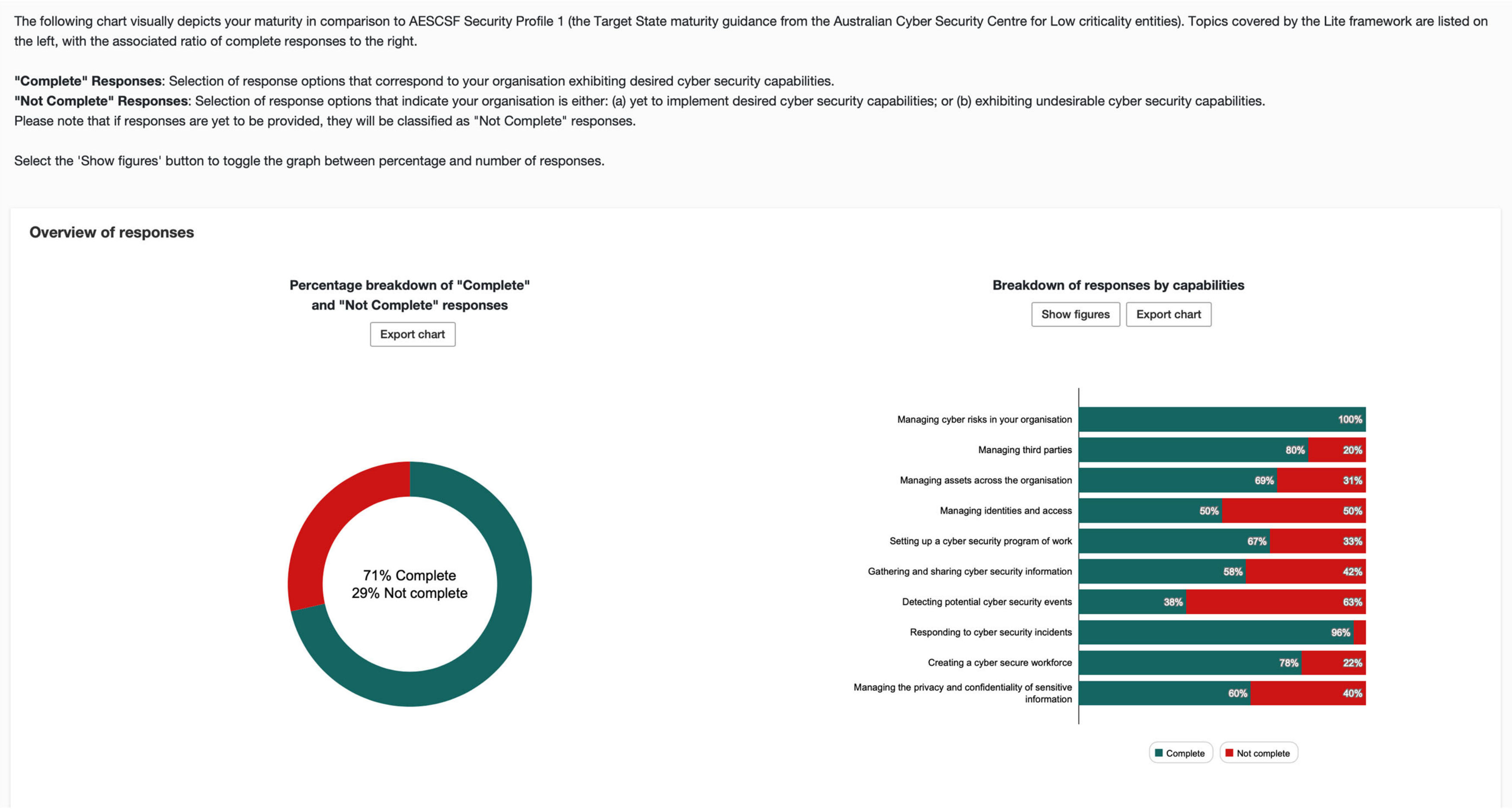
● Yes
○ No
○ Unsure

2. Within your organisation, have you: *

(Select all that apply)

☑ Identified your applicable privacy requirements
☑ Defined what is, and is not, treated as personal information considering your business activities
□ Nominated a privacy contact to field privacy enquiries
□ Identified any business activities that come into contact with personal information (such as collection, processing, storage, or transmission)
□ None of the above

2.11. Summary of results



The following chart visually depicts your maturity in comparison to AESCSF Security Profile 1 (the Target State maturity guidance from the Australian Cyber Security Centre for Low criticality entities). Topics covered by the Lite framework are listed on the left, with the associated ratio of complete responses to the right.

"Complete" Responses: Selection of response options that correspond to your organisation exhibiting desired cyber security capabilities.
"Not Complete" Responses: Selection of response options that indicate your organisation is either: (a) yet to implement desired cyber security capabilities; or (b) exhibiting undesirable cyber security capabilities.
Please note that if responses are yet to be provided, they will be classified as "Not Complete" responses.

Select the 'Show figures' button to toggle the graph between percentage and number of responses.

Overview of responses

Percentage breakdown of "Complete" and "Not Complete" responses
Export chart
71% Complete
29% Not complete
Breakdown of responses by capabilities
Show figures
Export chart
Managing cyber risks in your organisation
100%
Managing third parties
80%
20%
Managing assets across the organisation
69%
31%
Managing identities and access
50%
50%
Setting up a cyber security program of work
67%
33%
Gathering and sharing cyber security information
58%
42%
Detecting potential cyber security events
38%
63%
Responding to cyber security incidents
96%
Creating a cyber secure workforce
78%
22%
Managing the privacy and confidentiality of sensitive information
60%
40%
🟩 Complete
🟥 Not complete

Note that this summary of results is illustrative only.