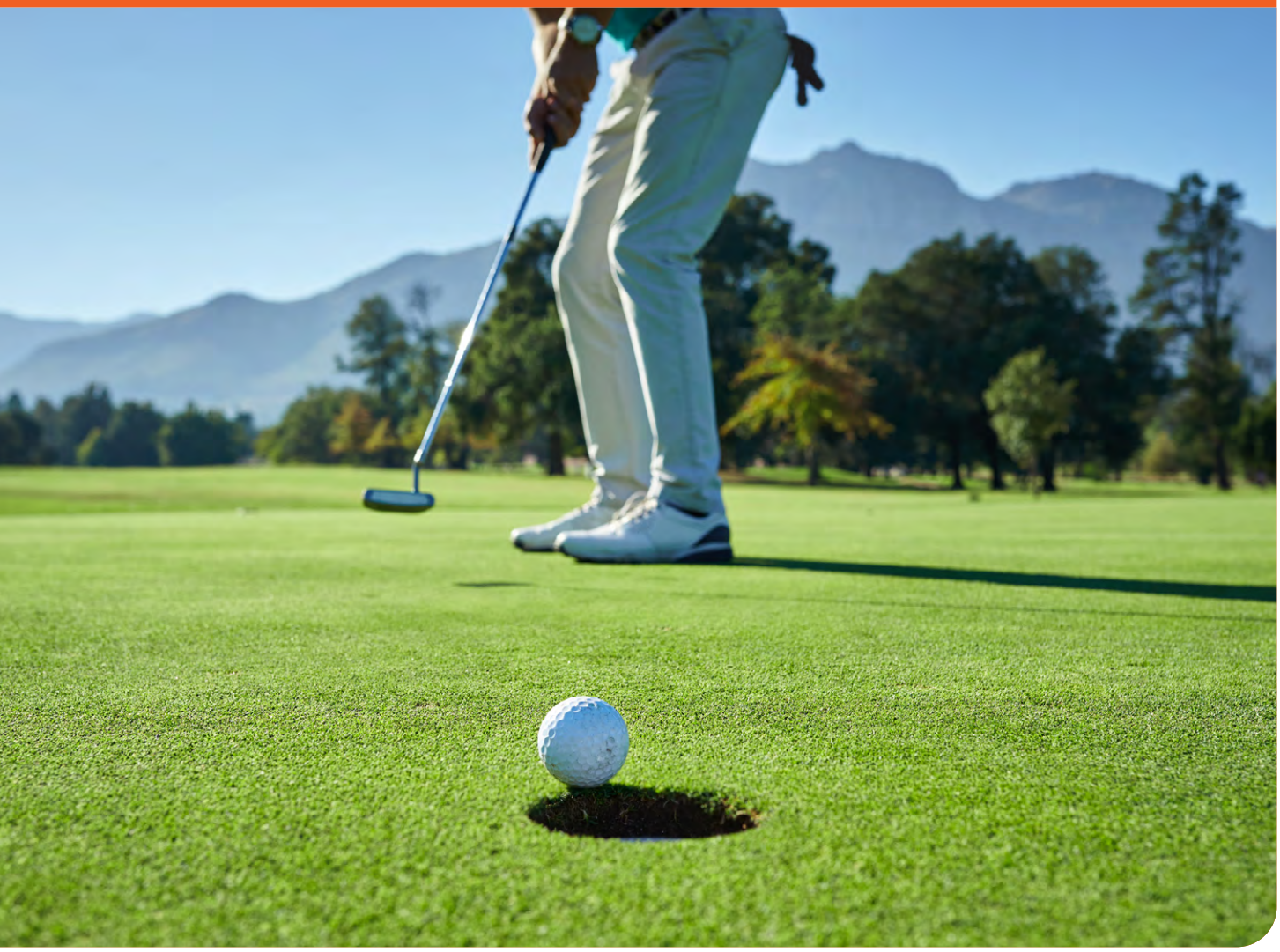
HOWDOIPay
Powered by ClearAccept

Merchant PCI Guide

To help you create your business profile & complete your PCI attestation



HOWDOIPay
Powered by ClearAccept

DISCLAIMER

This document is intended solely as a general guide to assist in the completion of the online forms necessary for your business to complete their annual PCI 'Attestation of Compliance' process, including completing both your Business Profile and your Security Assessment.

While every effort has been made to ensure the accuracy and completeness of the information provided, it is not a substitute for legal, financial, or professional advice. Both your software provider and ClearAccept bear no responsibility for the answers you input.

The user is responsible for ensuring that all information submitted in the form is accurate and compliant with applicable PCI DSS requirements relative to your business and in relation to the software provided to you by your software provider and the associated payment services provided by ClearAccept.

It is recommended to consult with a qualified PCI professional or relevant authority for specific guidance related to your organisation's compliance needs if you are not confident in answering the questions.

HOWDOIPay
Powered by ClearAccept

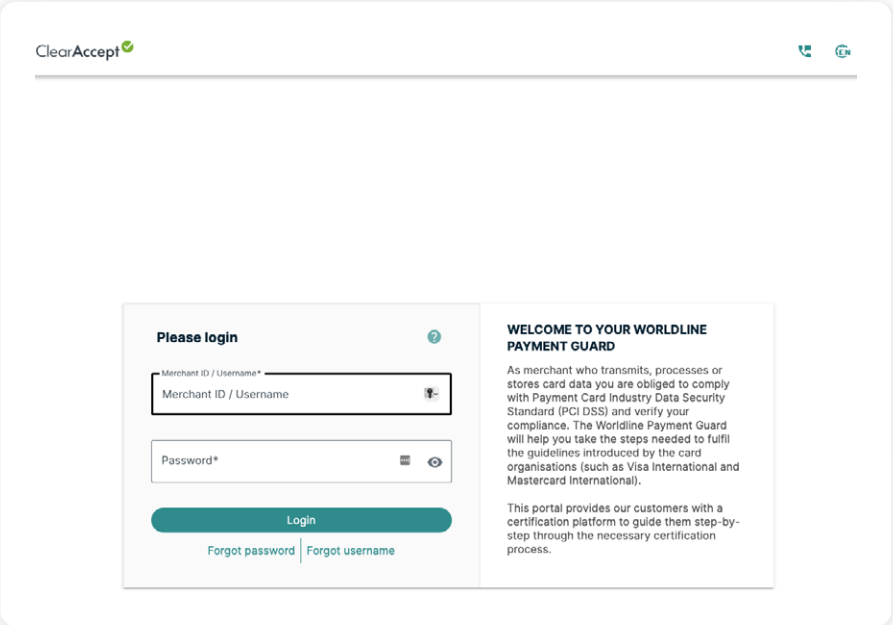
Merchant PCI Guide

To help you create your business profile & complete your PCI attestation

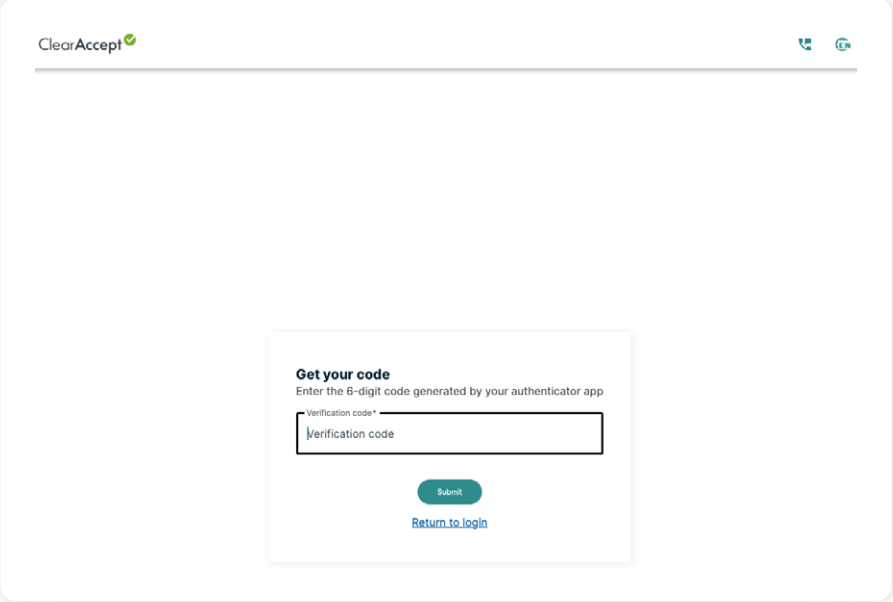
1. Click on the link in your Welcome eMail to go to the ClearAccept Worldline PCI Portal:

   https://clearaccept.worldline-pciportal.com
   Set-up your Password

2. When prompted to login, enter your **Merchant ID** or **Username & Password**



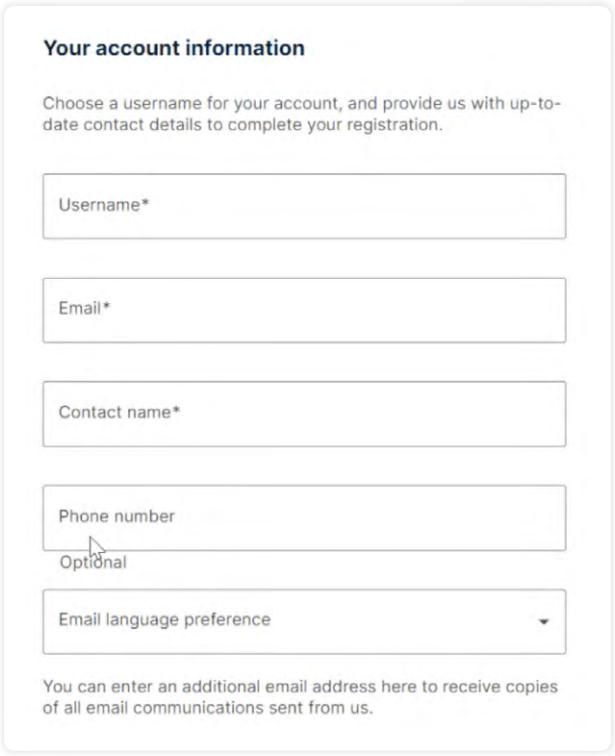
3. Enter your **6-digit verification code** generated by your authentication app (when prompted)



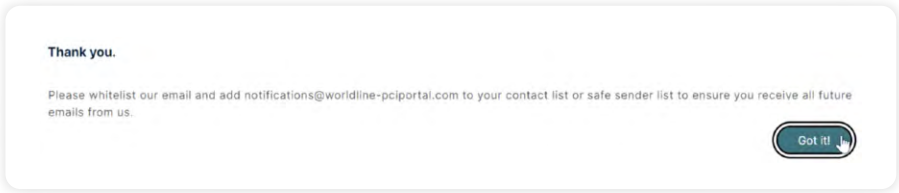
4. Your **account information** will be pre-populated – check and confirm the information.

   By default, the Username is your ClearAccept Merchant ID - you can change this to personalise the Username of your PCI account if you want to.

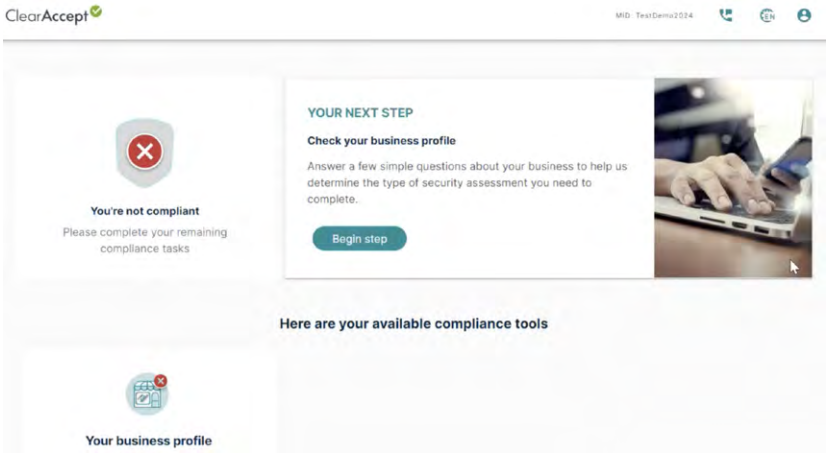
   You can add an additional contact eMail address to your account – this is in addition to the one which was used to send the Welcome eMail to. This is optional.



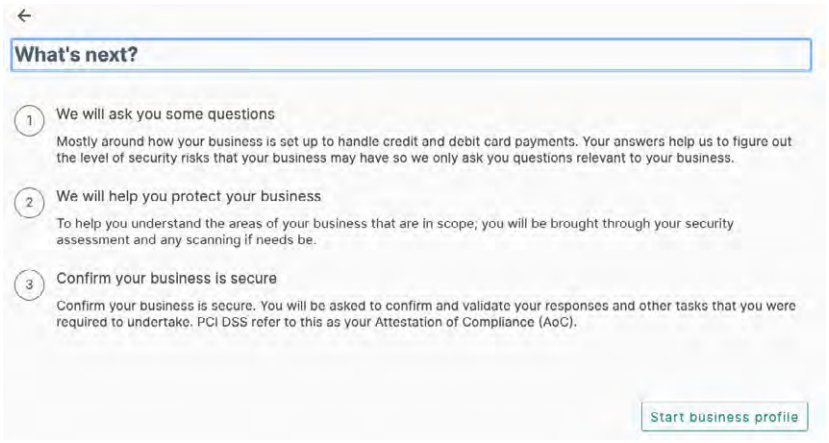
5. Click **'Next'**
   An information dialog is then displayed which recommends you add the eMail address 'notifications@worldline-pciportal.com' to your company eMail server / address book 'whitelist':



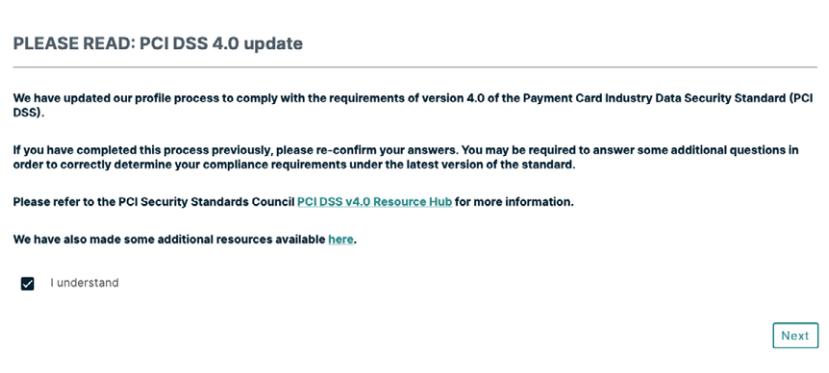
6. Click on '**Begin step'** to create your business profile



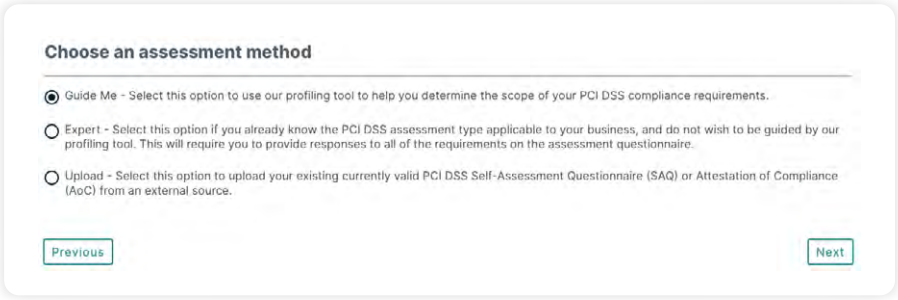
7. Click **'Start business profile'**



5. Click the **'I understand'** checkbox to confirm you understand you are complying with the v4 of the PCI DSS and click **'Next'**



6. Click on the 1st option **'Guide me'** and click **'Next'**

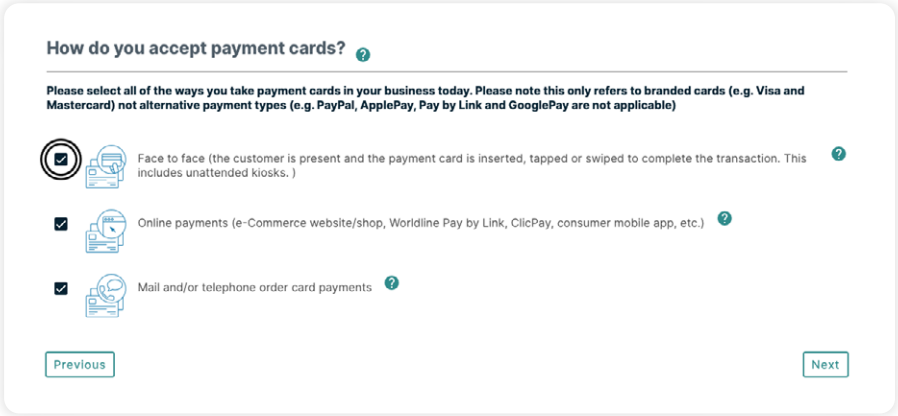


7. Select all the methods that your business take card payments.

   Click on the **'?'** marks for additional info / help text.

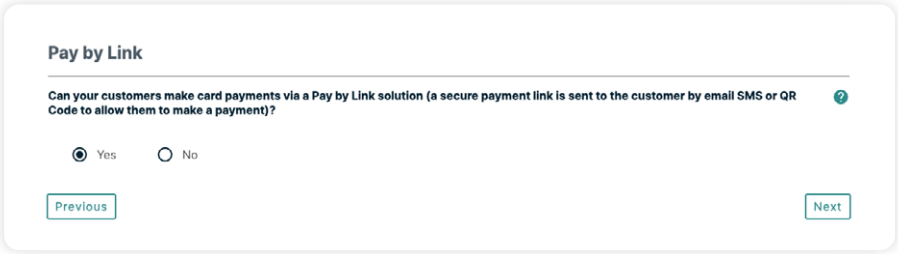
   For this guide, we have selected all 3 of the available methods:

   1. **Face to face:** Point of Sale [POS] payments via a till [POS] & Pin Entry Device [PED]
   2. **Online payments:** e-Commerce [ECOM] via website, Pay-by-Link or mobile app
   3. **Mail and / or Telephone:** MOTO payments

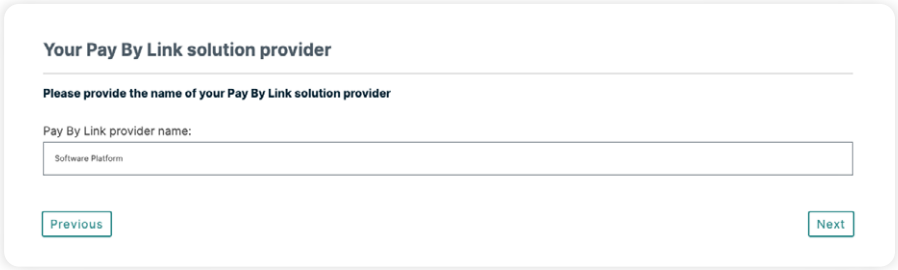


Pay by Link Section

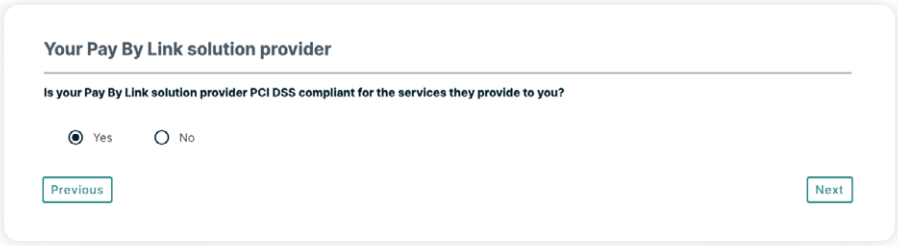
1. Select **'Yes'** for the Pay by Link question and click **'Next'**



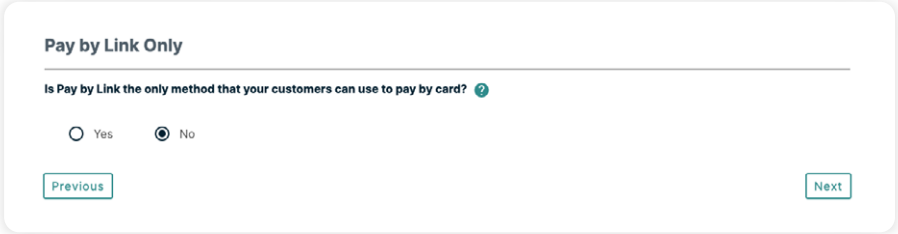
2. Enter **'Software Platform'** for the Pay by Link solution provider and click **'Next'**



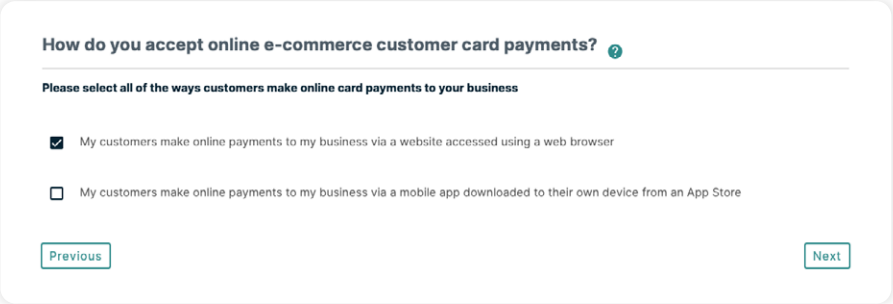
3. Select **'Yes'** for the question is your Pay by Link solution provider PCI DSS compliant and click **'Next'**



4. Select **'No'** for is Pay by Link the only method your customers can pay by card and click **'Next'**

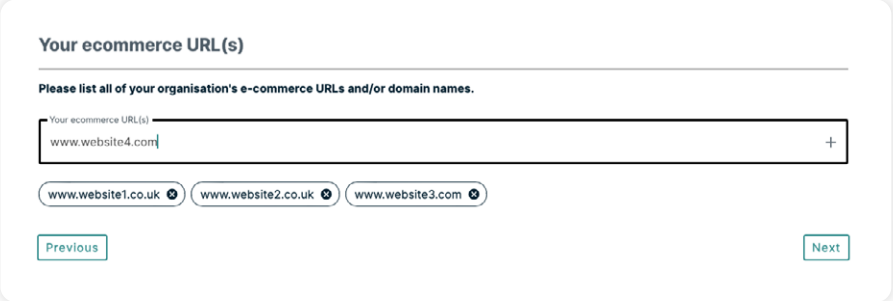


5. Select the 1st option below and click **'Next'**

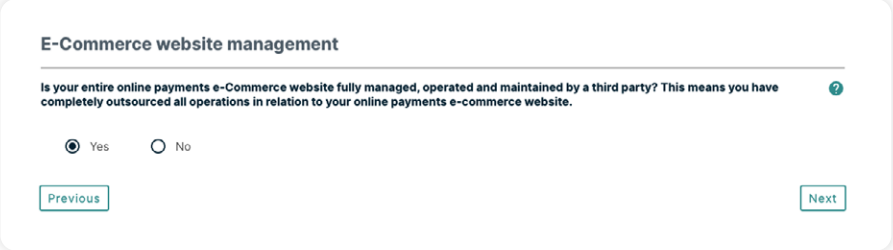


6. Enter your company **website(s)**.

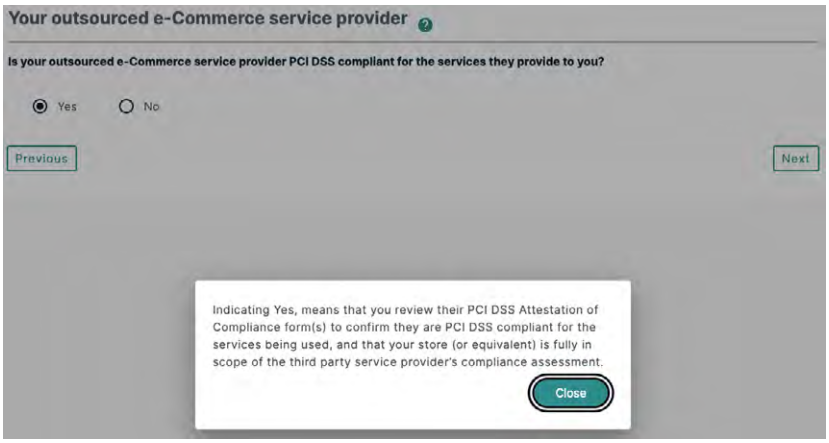
   If your company has more than 1 website, please list them all as per below image and click **'Next'**



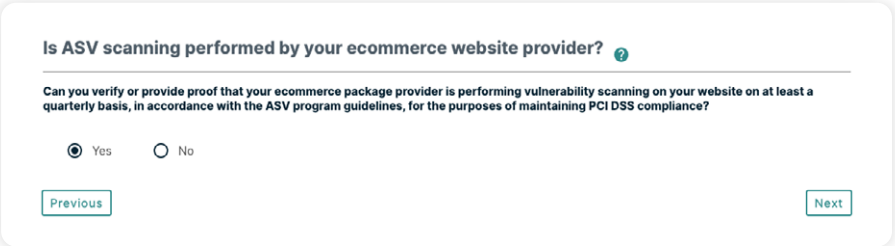
7. Select **'Yes'** for your online e-Commerce website being fully managed by a 3rd party. Click **'Next'**



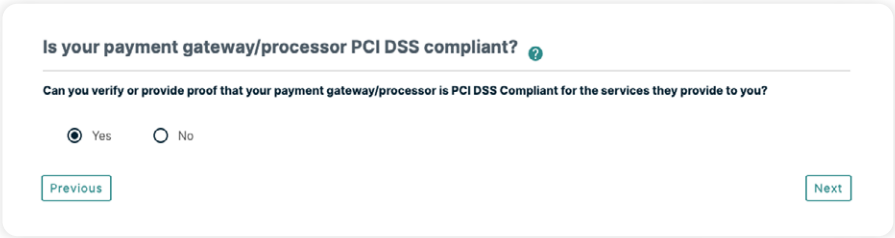
8. Select **'Yes'** for is your e-Commerce service provider PCI DSS compliant. Click **'Next'**



9. Select **'Yes'** for is ASV scanning performed by your e-Commerce service provider. Click **'Next'**

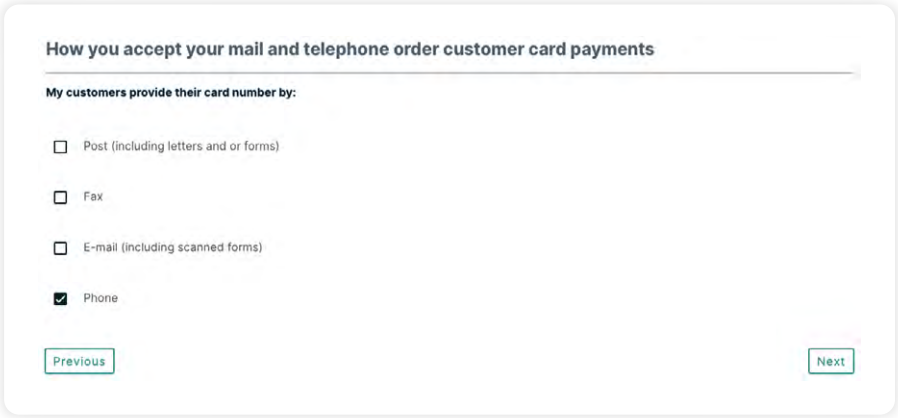


10. Select **'Yes'** for is your payment gateway/processor PCI DSS compliant. Click **'Next'**

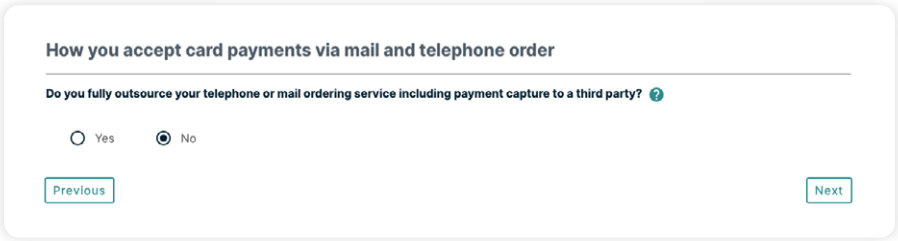


Mail Order / Telephone Order [MOTO] Section

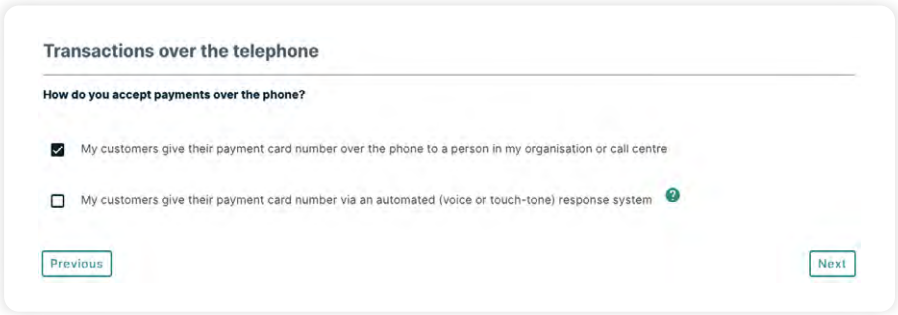
1. Select '**Phone'** to confirm how you accept MOTO card payments. Click **'Next'**



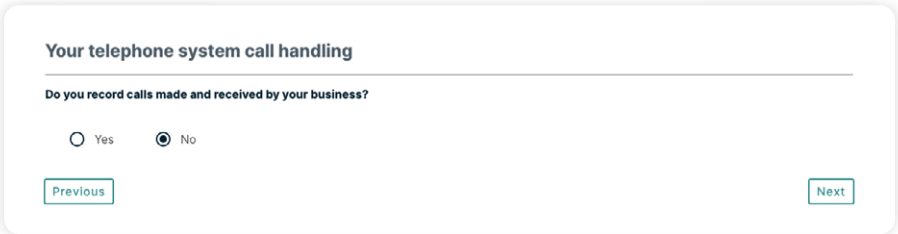
2. Select **'No'** for whether you outsource your MOTO payment capture to a 3rd party. Click **'Next'**



3. Select the 1st option below and click **'Next'**

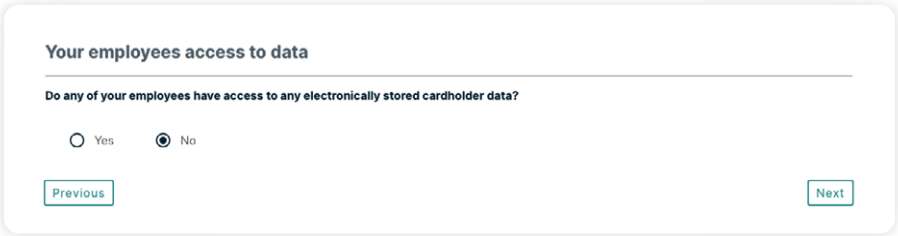


4. Select **'No'** for whether you record calls made and received by your business. Click **'Next'**



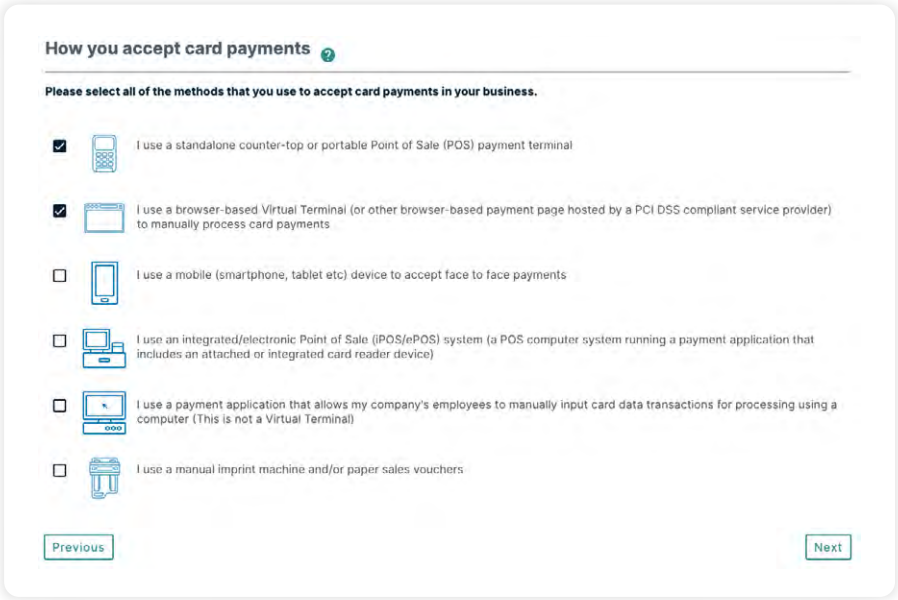
5. Select **'No'** for whether you store cardholder data in your CRM system. Click **'Next'**

6. Select **'No'** for whether your employees have access to stored cardholder data. Click **'Next'**

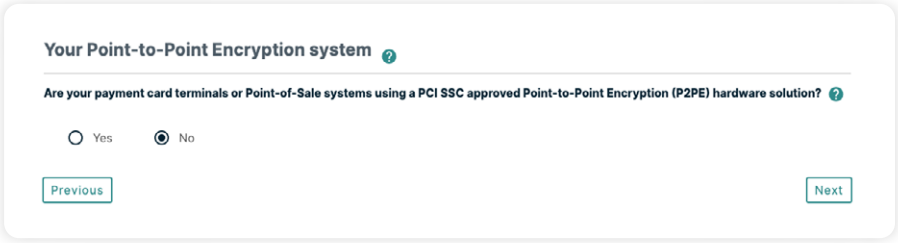


Point of Sale [POS] Section

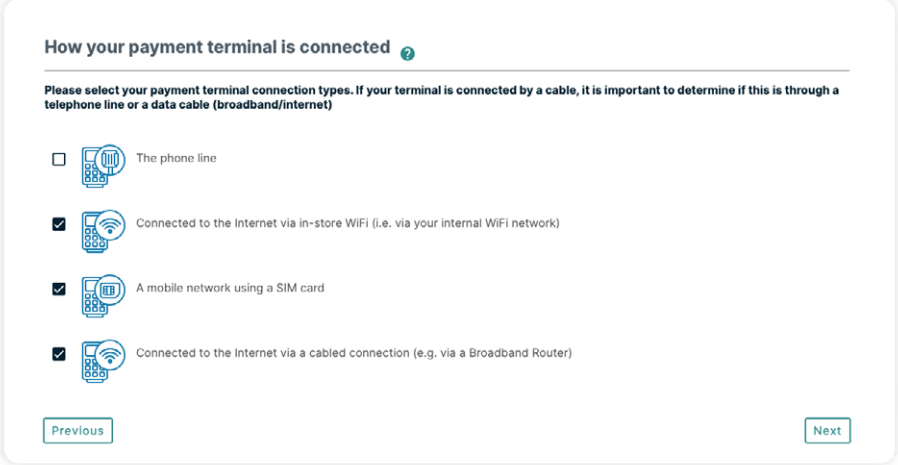
1. Select the top 2 options relating to how you accept card payments. Click **'Next'**



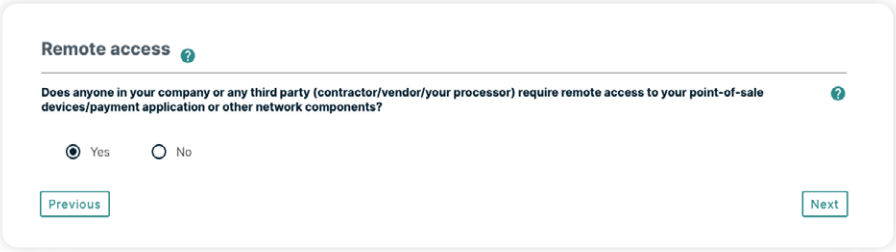
2. Select **'No'** to the P2PE solution question. Click **'Next'**



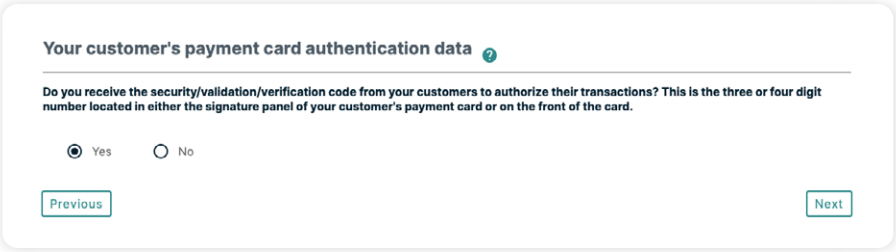
3. Recommended to select options 2, 3 and 4 relating to how your payment terminal(s) are connected. However, if you know the Terminals only use Wi-Fi, or SIM cards, or cabled connection – select what is appropriate. Click **'Next'**



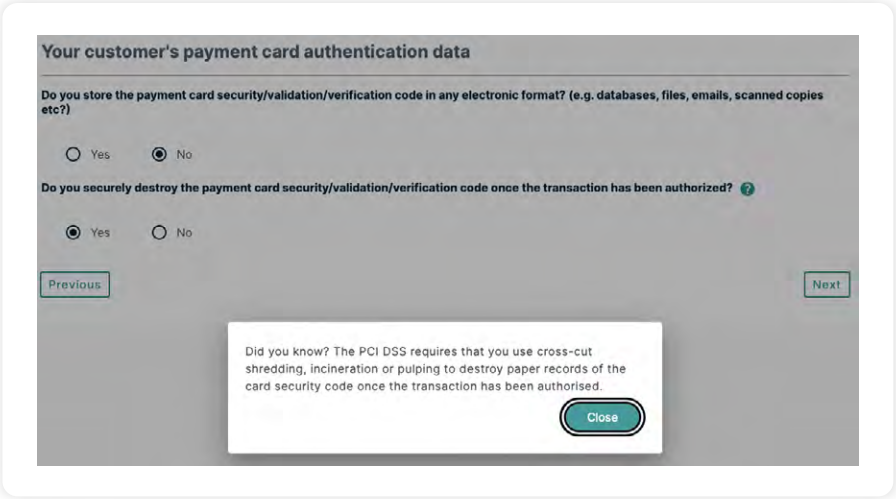
4. Select **'Yes'** to the remote access question. The Point of Sale Terminals are connected to the Ingenico Terminal Estate Management service for the purpose of config and / or Terminal Software updates. Click **'Next'**



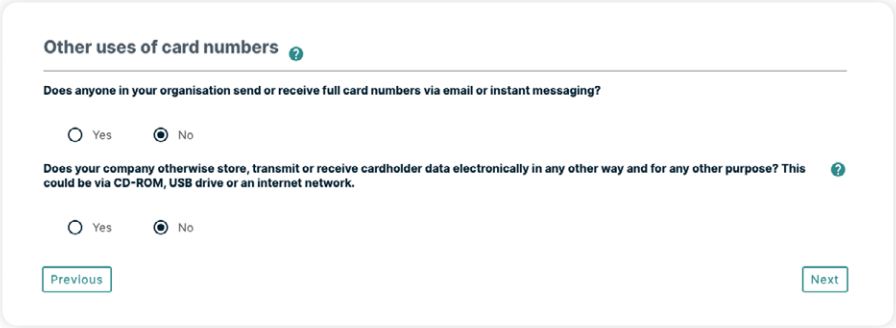
5. Select **'Yes'** to the CVV code question. (This question relates to MOTO payments). Click **'Next'**



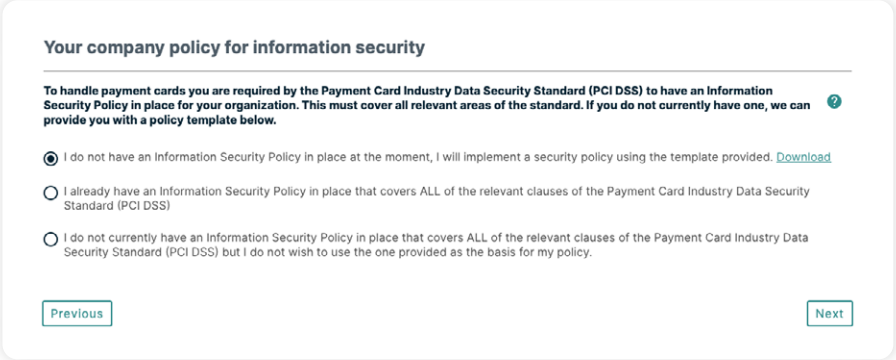
6. Select **'No'** to the 1st storing payment card CVV data question. Select **'Yes'** to the question relating to the secure destruction of CVV data. Click **'Next'**



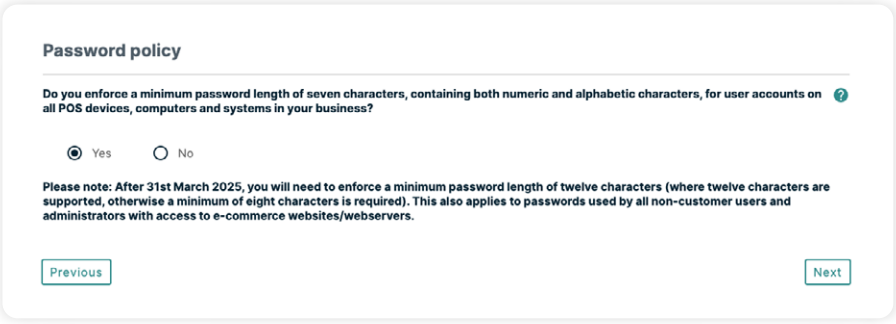
7. Select **'No'** to both of the following questions relating to the use of card numbers. Click **'Next'**



8. Select the 1st option below and click **'Next'**

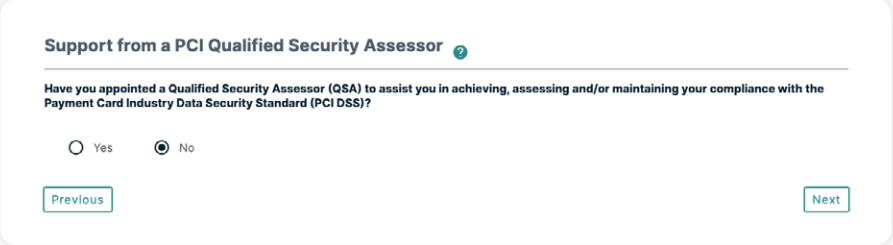


9. Select '**Yes'** to the password policy question. Click **'Next'**



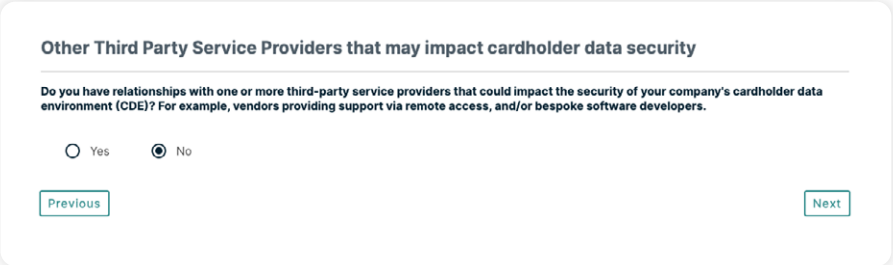
10. Select **'No'** to the Internal Security Assessor [ISA] question. Click **'Next'**

11. Select **'No'** to the Qualified Security Assessor [QSA] question. Click **'Next'**

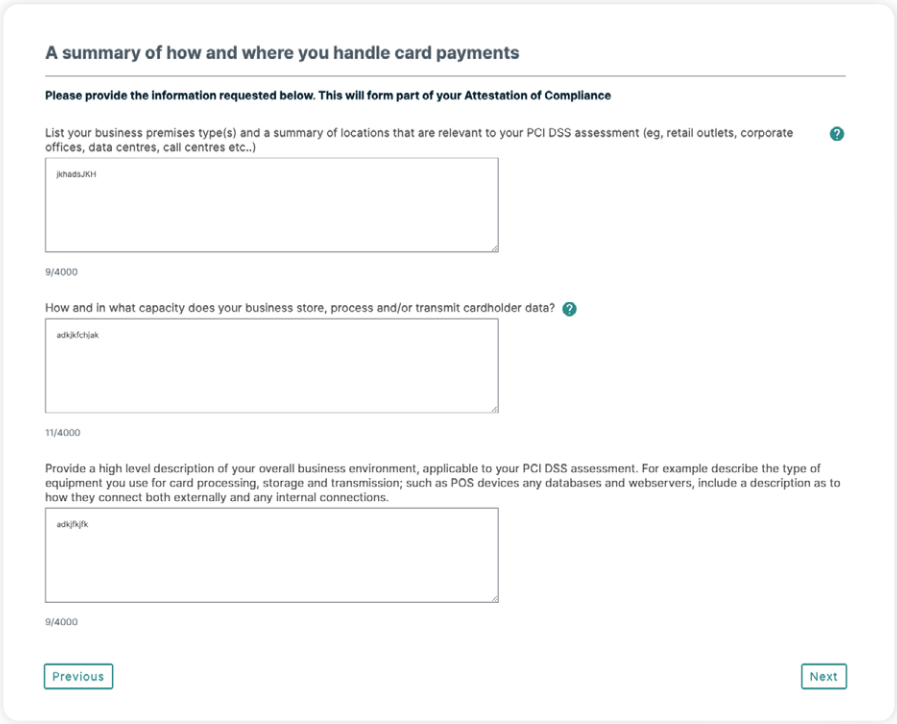


12. Select **'Yes'** to the 3rd Party Managed System Service Provider question. Click **'Next'**

13. Select **'No'** to the Other 3rd Party Service Providers question. Click **'Next'**



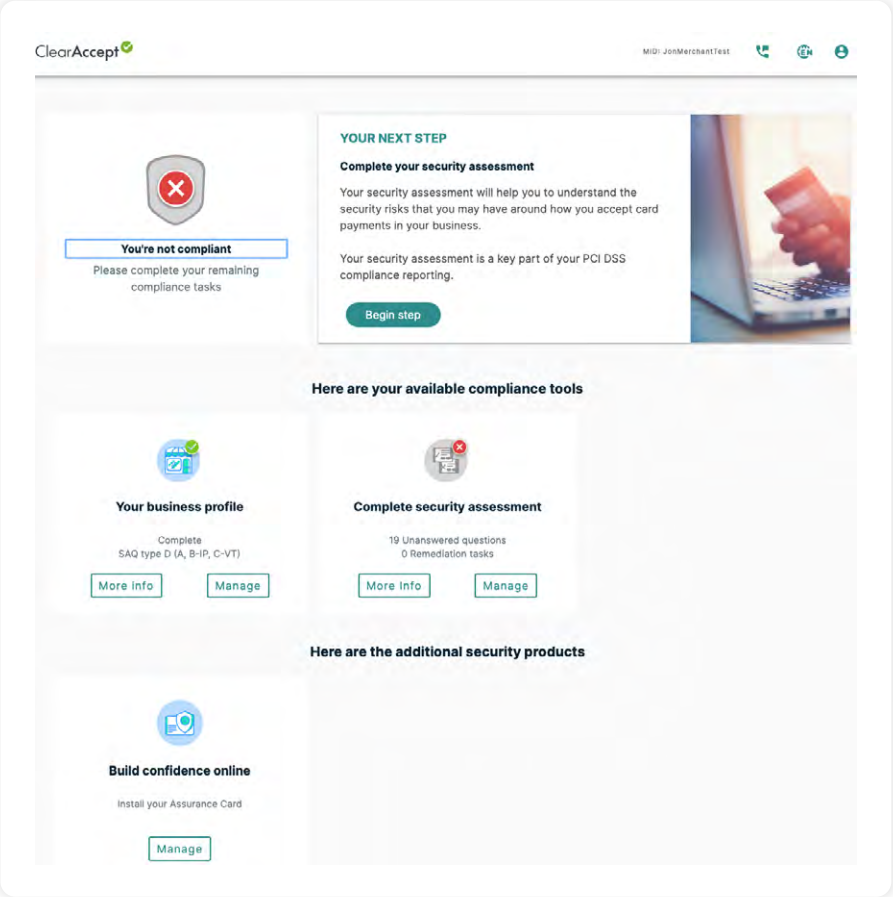
14. Enter text in your own words to complete the below 3 sections relative to your business operation. Click **'Next'**



15. Your business profile is now complete, and you can now move on to complete your PCI attestation / security assessment.

Security Assessment Section

1. Click on **'Begin step'** to complete your security assessment.

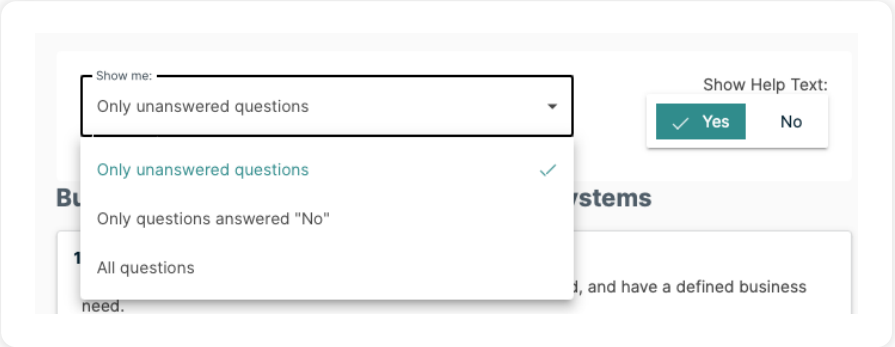


2. **Note:** The number and nature of the remaining 'unanswered' questions now presented to you in the Security Assessment section are specifically related to the selections you made in the business profile section above.

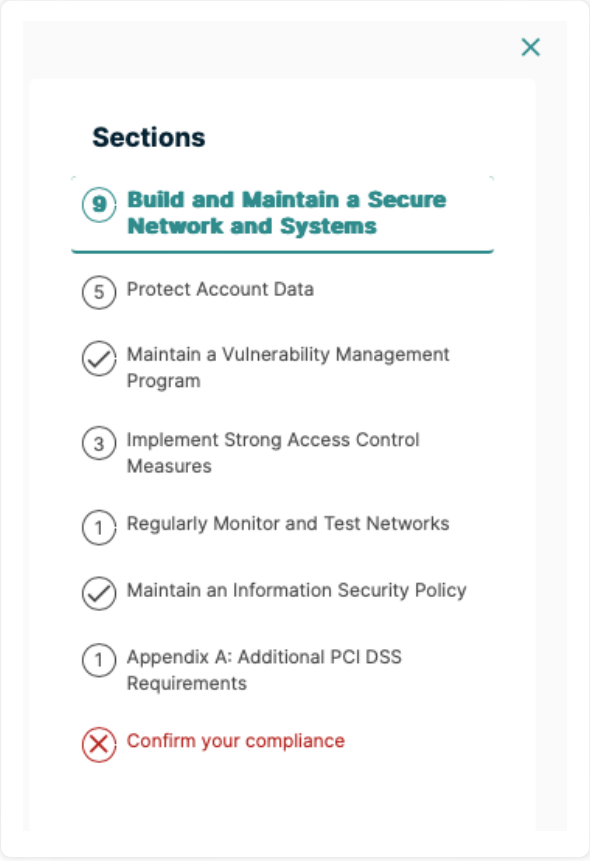
   As such, given the above is a guide and was not written relative to your actual business set-up – the below unanswered questions may not be the same as those now presented to you by the PCI Portal.

3. By default, you are presented with the list of questions left to answer following the selections made when you completed your business profile. You can select **'All questions'** if you want to see those that have already been answered, but for efficiency, it is recommended to show **'Only unanswered questions'**.

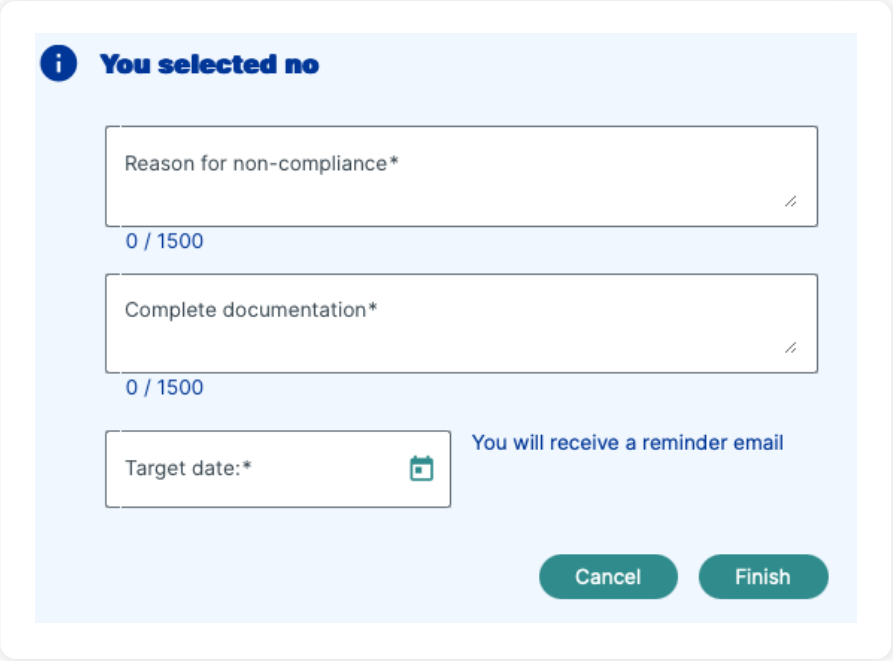
   You can also click on **Show Help Text 'Yes'** to help in understanding of each question.



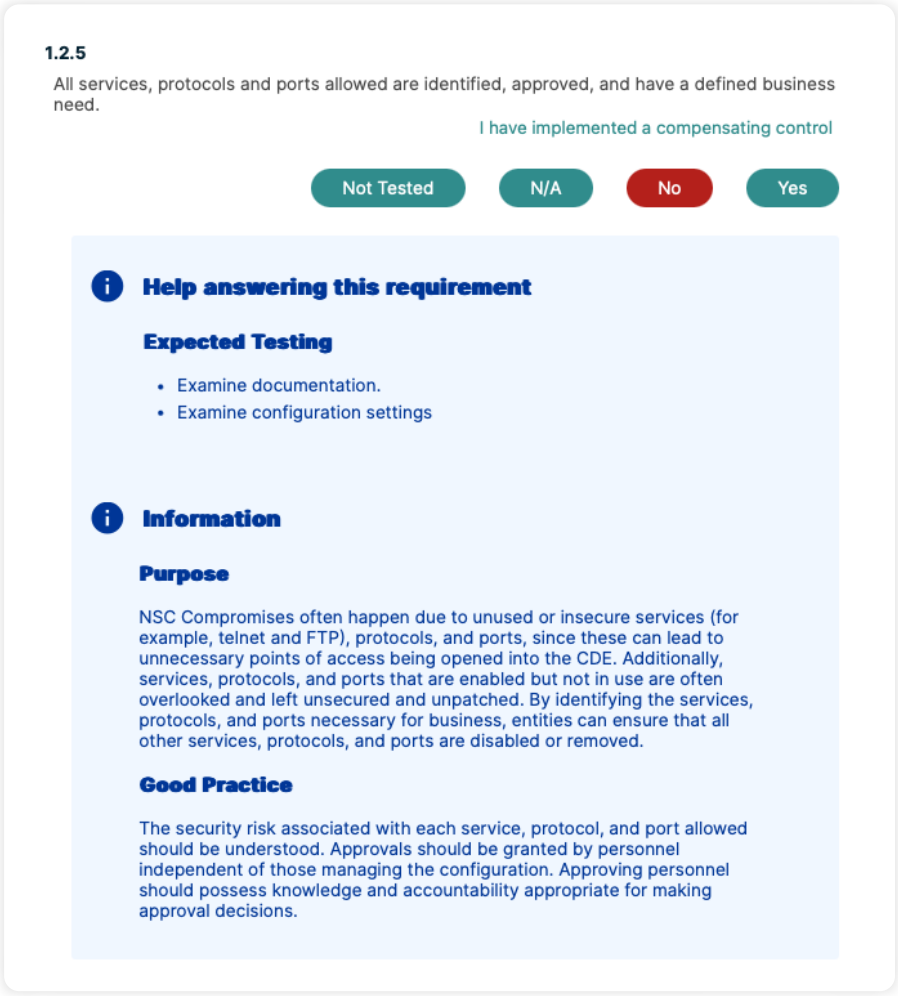
4. There is a panel on the right-hand side which shows you which sections the remaining unanswered questions relate to. The numbers represent the unanswered questions. When you answer a question, the question 'disappears' and the corresponding numbers reflecting the remaining unanswered questions subsequently reduce by 1 each time.



4. For all questions in this section, if you select **'No'** or **'N/A'** then you are required to complete the below fields, explaining in your own words why your business is not currently compliant, relative to the topic of the question, along with any additional documentation + a Target Date for when your business will be compliant.



5. Build and Maintain a Secure Network and Systems



1.2.5: Question Guidance:

If you have an external provider manage your systems and networks, then ask them to provide the response.

If you manage your systems and networks yourself then this question relates to the permissions on the devices that protect your network from attack – Normally a Firewall.

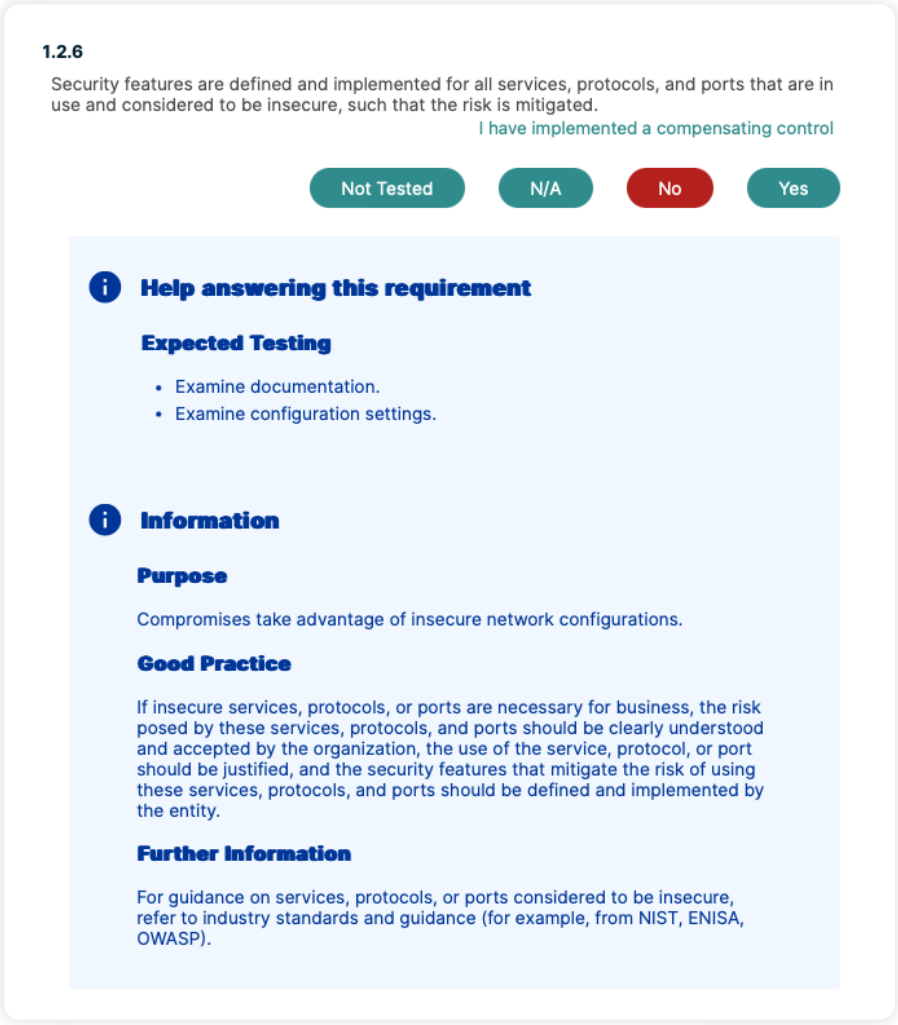
To be compliant you must have set the configuration and rules on this device to only allow connections and services that are required and approved.

You may have an actual firewall device, or it may be part of your Broadband Router:

- If you just installed one of these devices “out of the box” and did not change any settings, then you are unlikely to be compliant.
- If you used a set of recommended settings or a tailored configuration to suit your environment, select **‘Yes’**

If you do not know the answer then check whether you have a separate firewall or just a broadband router, and then check the settings on these devices. This is important as the default settings may make you an easy target for people searching the internet for businesses to hack.

6. Build and Maintain a Secure Network and Systems



1.2.6: Question Guidance:

If you have an external provider manage your systems and networks, then ask them to provide the response.

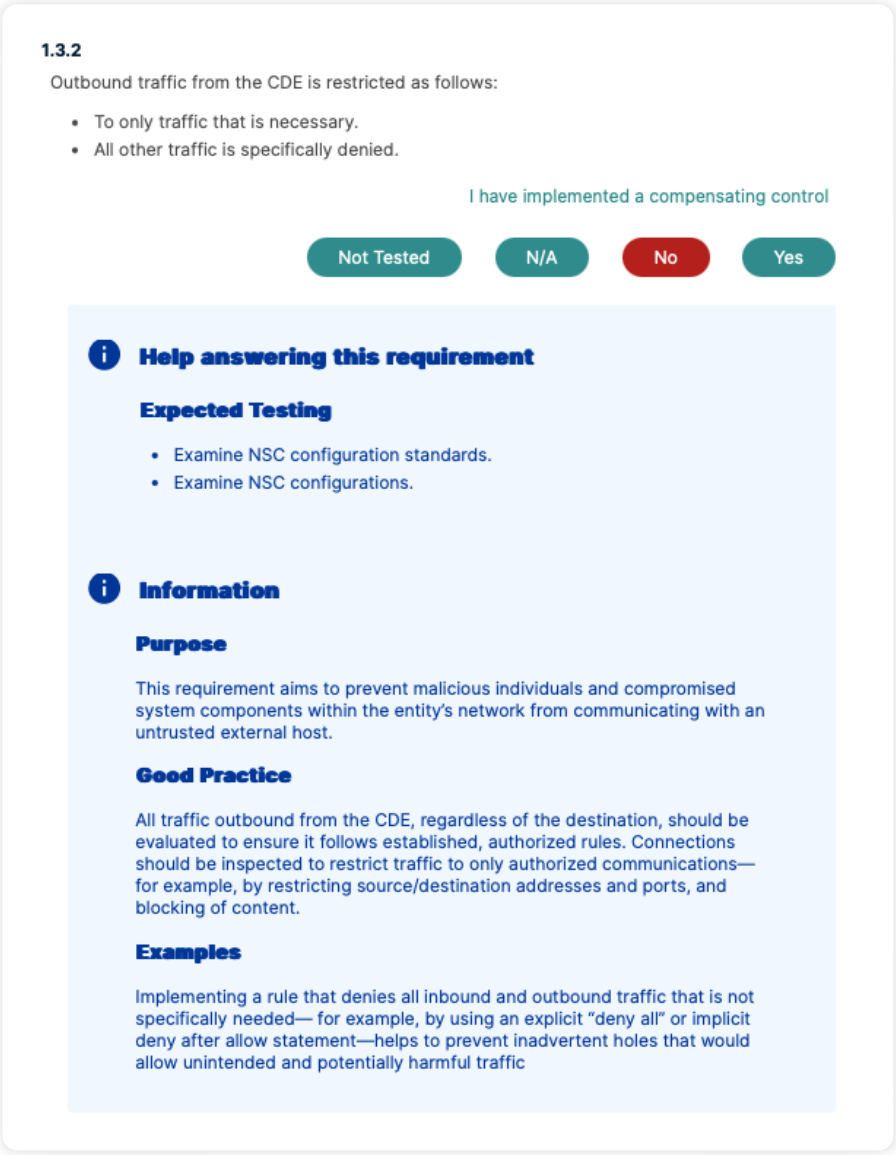
If you manage your systems and networks yourself then this question relates to the way you have configured the devices that protect your network from attack – Normally a Firewall.

To be compliant you must either:

- Not have enabled any insecure services, ports or protocols OR
- Have ensured that any insecure services, ports or protocols have been implemented in a secure manner

Again, if you followed a document to guide your device configurations with the recommended settings or configurations then select **'Yes'**.

7. Build and Maintain a Secure Network and Systems



1.3.2: Question Guidance:

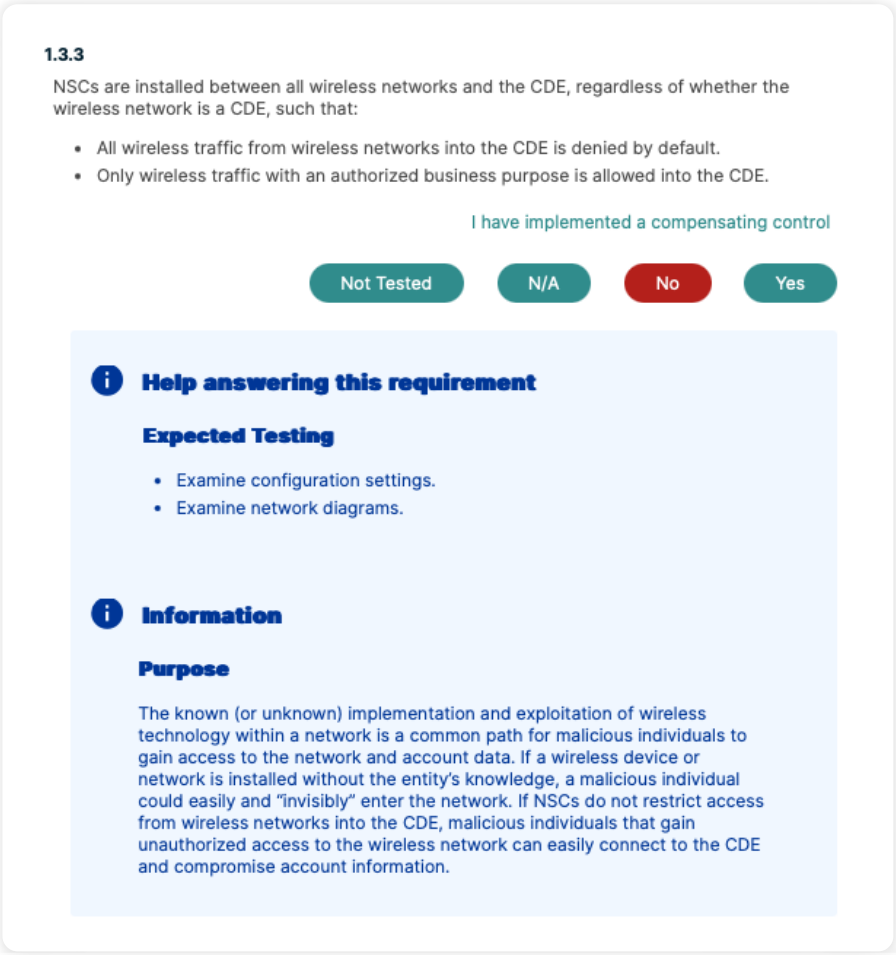
If you have an external provider manage your systems and networks, then ask them to provide the response.

If you manage your systems and networks yourself then this question relates to the way you have configured the devices that protect your network from attack – Normally a Firewall.

Every computer has a unique identifier ("IP address") to differentiate it from other computers and to manage connectivity. This requirement seeks to validate whether your network will not allow your systems to connect to other computers unless you have approved the connection (approved the IP address).

If you have not restricted inbound connections in any way, then you are not compliant. If you have imposed restrictions that meet the requirement below select **'Yes'**.

8. Build and Maintain a Secure Network and Systems



1.3.3: Question Guidance:

If you have an external provider manage your systems and networks, then ask them to provide the response.

If you manage your systems and networks yourself then this question relates to the way you protect your systems from attack by users connected to your wireless networks.

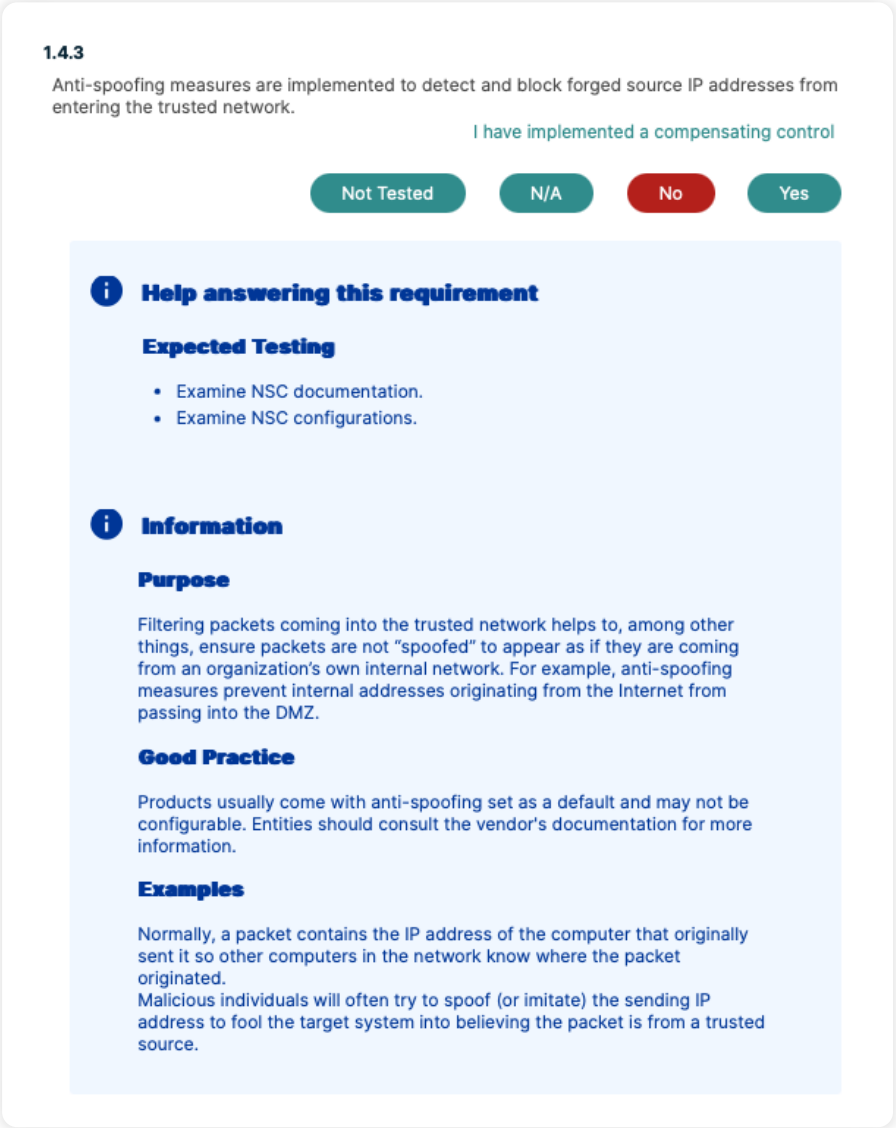
If you do not have wireless, then mark this as '**Yes'**.

If your only wireless networks are on a totally different platform to your business systems, then mark this as **'Yes'**.

If the Wireless network is a "Guest Network" on your internet router and no other wireless networks exist, then mark this as **'Yes'**.

If you have a separate Wi-Fi Router, then this needs to be "separated" from your own systems by either being on a totally network OR you must have a device or system between the Wi-Fi network and your other systems (normally a Firewall). If you have a Firewall or other device protecting your network from attack through the Wi-Fi network, then select **'Yes'**.

9. Build and Maintain a Secure Network and Systems



1.4.3: Question Guidance:

If you have an external provider manage your systems and networks, then ask them to provide the response.

If you manage your systems and networks yourself then this question relates to the way you have configured the devices that protect your network from attack – Normally a Firewall.

If you have a Firewall, then check the specifications: If it supports anti-spoofing then you can mark the requirement as compliant.

Anti spoofing is a way to prevent attackers faking their IP address to trick their way into your systems.

10. Build and Maintain a Secure Network and Systems

1.5.1

Security controls are implemented on any computing devices, including company- and employee-owned devices, that connect to both untrusted networks (including the Internet) and the CDE as follows.

- Specific configuration settings are defined to prevent threats being introduced into the entity's network.
- Security controls are actively running.
- Security controls are not alterable by users of the computing devices unless specifically documented and authorized by management on a case-by-case basis for a limited period.

I have implemented a compensating control

Not Tested | N/A | No | Yes

Help answering this requirement

Expected Testing

- Examine policies and configuration standards.
- Examine device configuration settings.

Applicability Notes

These security controls may be temporarily disabled only if there is legitimate technical need, as authorized by management on a case-by-case basis. If these security controls need to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period during which these security controls are not active. This requirement applies to employee-owned and company-owned computing devices. Systems that cannot be managed by corporate policy introduce weaknesses and provide opportunities that malicious individuals may exploit.

Information

Purpose

Computing devices that are allowed to connect to the Internet from outside the corporate environment—for example, desktops, laptops, tablets, smartphones, and other mobile computing devices used by employees—are more vulnerable to Internet-based threats.
Use of security controls such as host-based controls (for example, personal firewall software or end-point protection solutions), network-based security controls (for example, firewalls, networkbased heuristics inspection, and malware simulation), or hardware, helps to protect devices from Internet-based attacks, which could use the device to gain access to the organization's systems and data when the device reconnects to the network.

Good Practice

The specific configuration settings are determined by the entity and should be consistent with its network security policies and procedures.
Where there is a legitimate need to temporarily disable security controls on a company-owned or employee-owned device that connects to both an untrusted network and the CDE—for example, to support a specific maintenance activity or investigation of a technical problem—the reason for taking such action is understood and approved by an appropriate management representative. Any disabling or altering of these security controls, including on administrators' own devices, is performed by authorized personnel. It is recognized that administrators have privileges that may allow them to disable security controls on their own computers, but there should be alerting mechanisms in place when such controls are disabled and follow up that occurs to ensure processes were followed.

Examples

Practices include forbidding split-tunneling of VPNs for employee-owned or corporate-owned mobile devices and requiring that such devices boot up into a VPN.

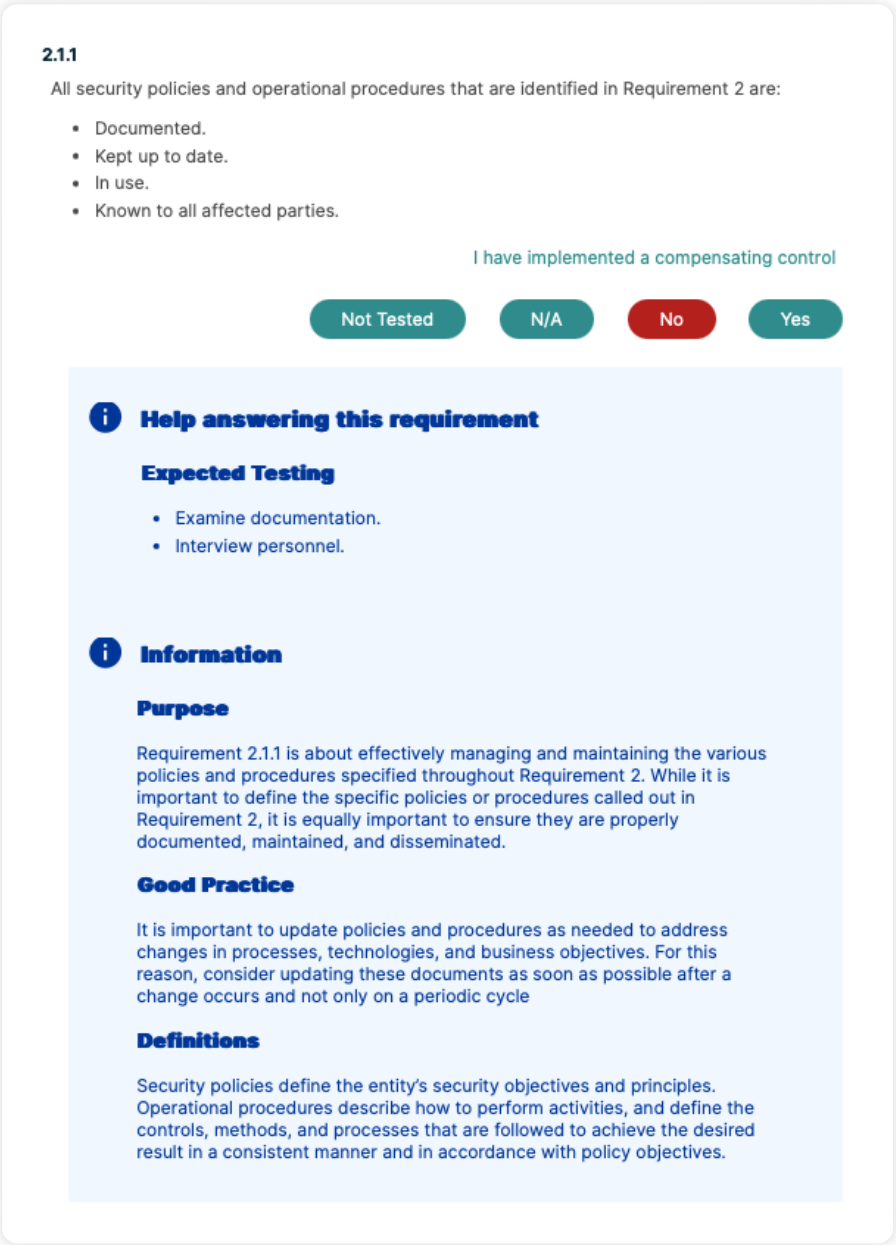
1.5.1: Question Guidance:

If you have an external provider manage your laptops and desktop computers, then ask them to provide the response.

Most Operating Systems come with inbuilt security tools including Firewall software and anti-virus. If your computers have such functionality installed, enabled, and cannot be disabled without express permission and approval then select **'Yes'**.

If you have no computers that can access, process or view any card data you can select **'Yes'**.

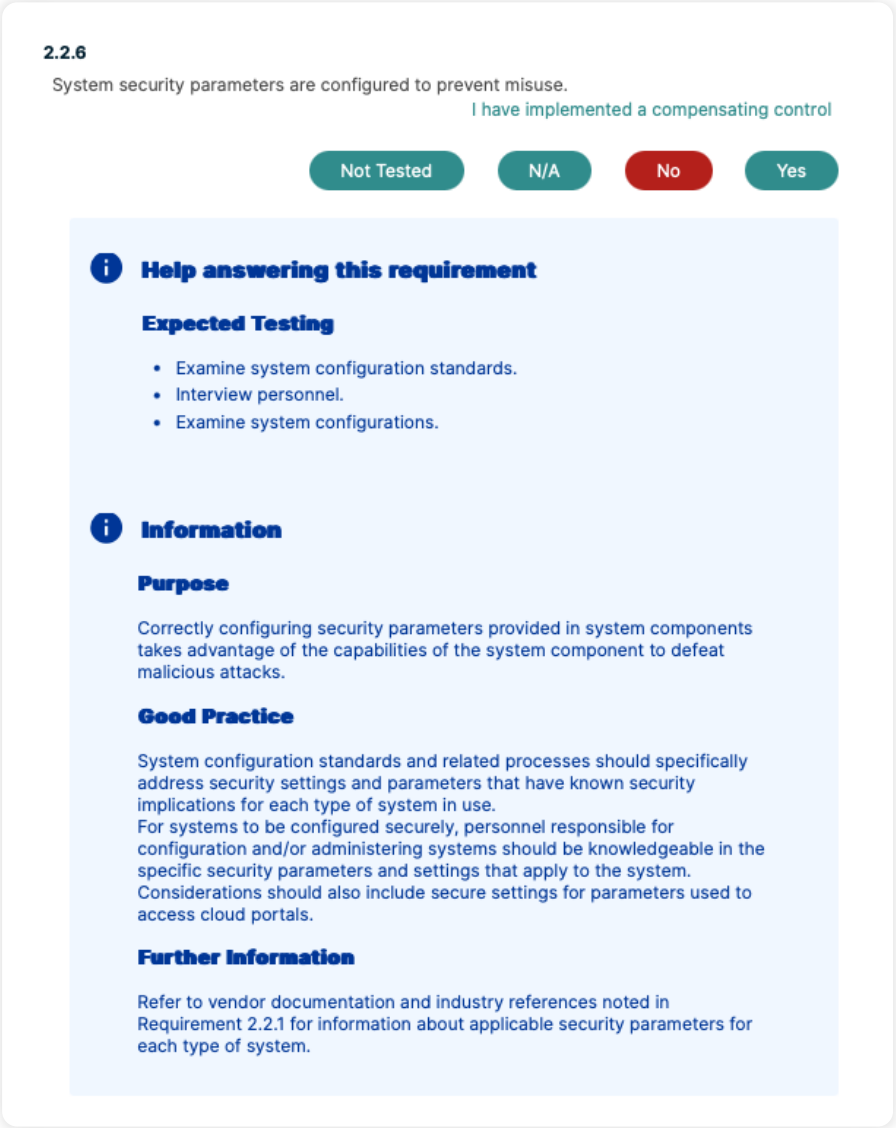
11. Build and Maintain a Secure Network and Systems



2.1.1: Question Guidance:

Select **'Yes'** as implementing a compensating control is a summary requirement covering the rest of the following details. You can only pass the assessment if this question is confirmed with a **'Yes'**.

12. Build and Maintain a Secure Network and Systems



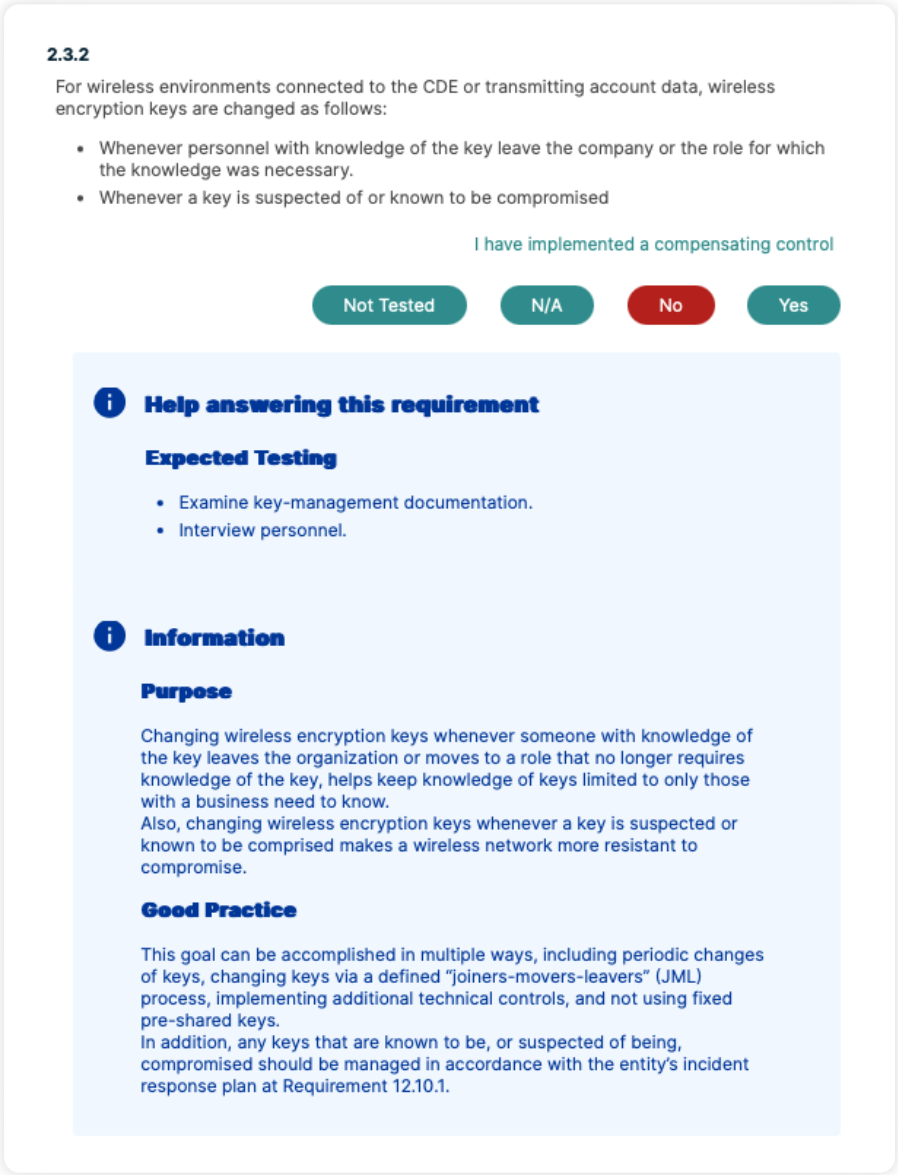
2.2.6: Question Guidance:

If you have an external provider manage your computers, then ask them to provide the response.

A default installation of any operating system such as Windows will need to be able to do everything that could be asked of it, so every possible function is installed. Many of these functions and services are not needed and represent a security risk being present. By using a secure configuration standard, you can reduce the size of the target hackers have to attack as you will have removed the data, they would be able to take advantage of.

You do not have to create your own configuration standards, there are many free sources including the Centre For Internet Security (see Hardened Images here) **CIS Centre for Internet Security**. If you have configured your systems according to a defined configuration standard you can select **'Yes'**.

13. Build and Maintain a Secure Network and Systems



2.3.2: Question Guidance:

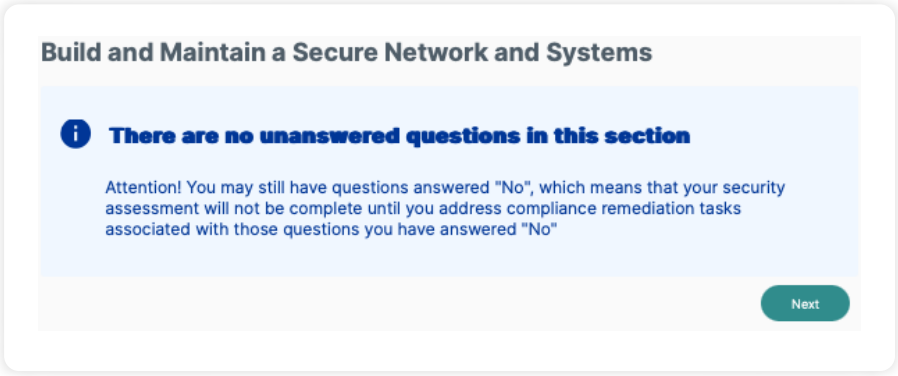
If you have an external provider manage your networks, then ask them to provide the response.

If you do not process card data in any way across wireless networks (none of your computers that take card payments are connected to Wi-Fi) AND any other Wi-Fi that exists but does not take card payments has been configured in line with the earlier requirements then select **'Yes'**.

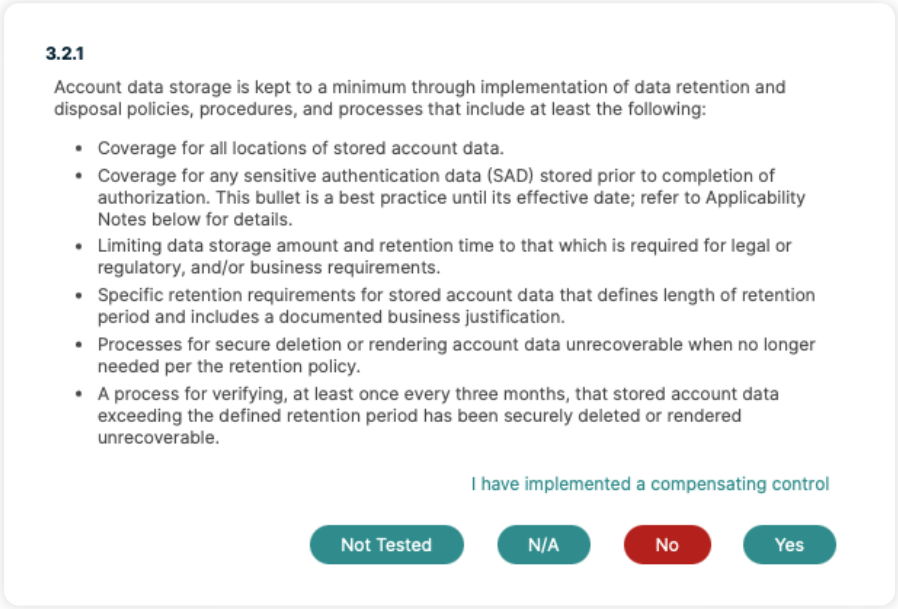
If you have no Wi-Fi whatsoever you can select **'Yes'**

If you have a wireless network that either supports systems that take payment OR is connected to the same network as systems that take payments, then you must meet this requirement.

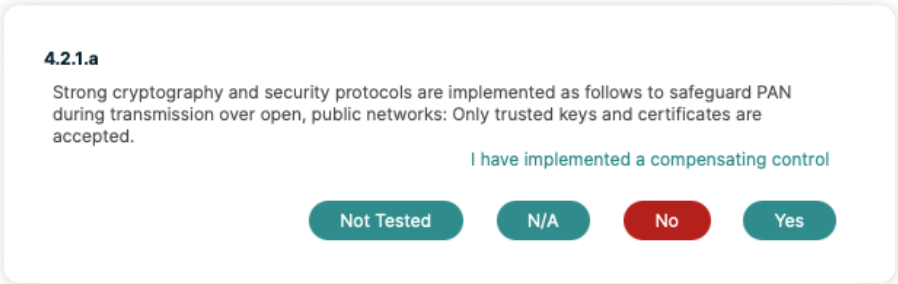
14. Once you reach the end of the section, Click **'Next'**



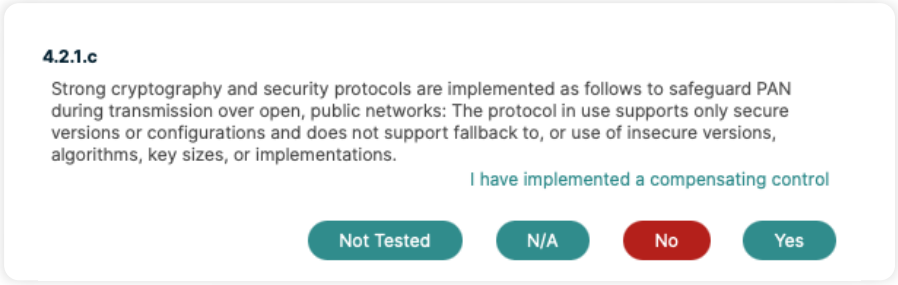
15. **Protect Account Data**



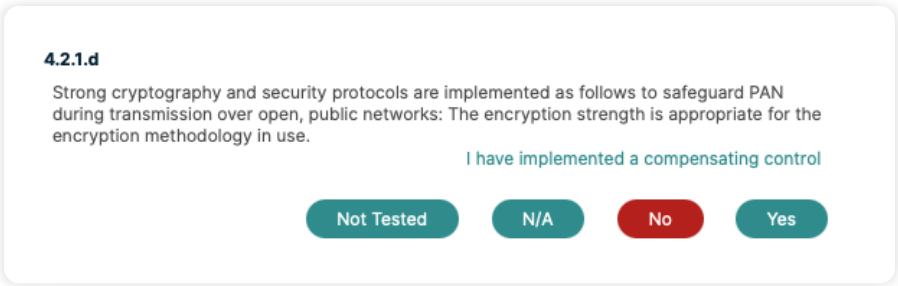
16.



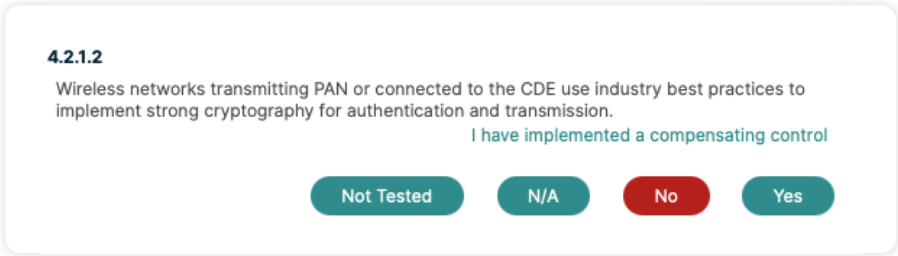
17.



18.



19.



4.2.1.2: Question Guidance:

If you have an external provider manage your networks, then ask them to provide the response.

If you do not process card data in any way across wireless networks (none of your computers that take card payments are connected to Wi-Fi) AND any other Wi-Fi that exists but does not take card payments has been configured in line with the earlier requirements then select **'Yes'**.

If you have no Wi-Fi whatsoever you can select **'Yes'**

If you have a wireless network that either supports systems that take payment OR is connected to the same network as systems that take payments, then you must meet this requirement.

This is only applicable if you host any of the software services in your own environment – making the wireless network 'in scope'. Given your software provider hosts the services your business uses; the expectation is you would select **'N/A'** to this question.

20. Implementing Strong Access Control Measures

8.1.1

All security policies and operational procedures that are identified in Requirement 8 are:

- Documented.
- Kept up to date.
- In use.
- Known to all affected parties.

I have implemented a compensating control

Not Tested | N/A | No | Yes

21.

8.2.4

Addition, deletion, and modification of user IDs, authentication factors, and other identifier objects are managed as follows:

- Authorized with the appropriate approval.
- Implemented with only the privileges specified on the documented approval.

I have implemented a compensating control

Not Tested | N/A | No | Yes

22.

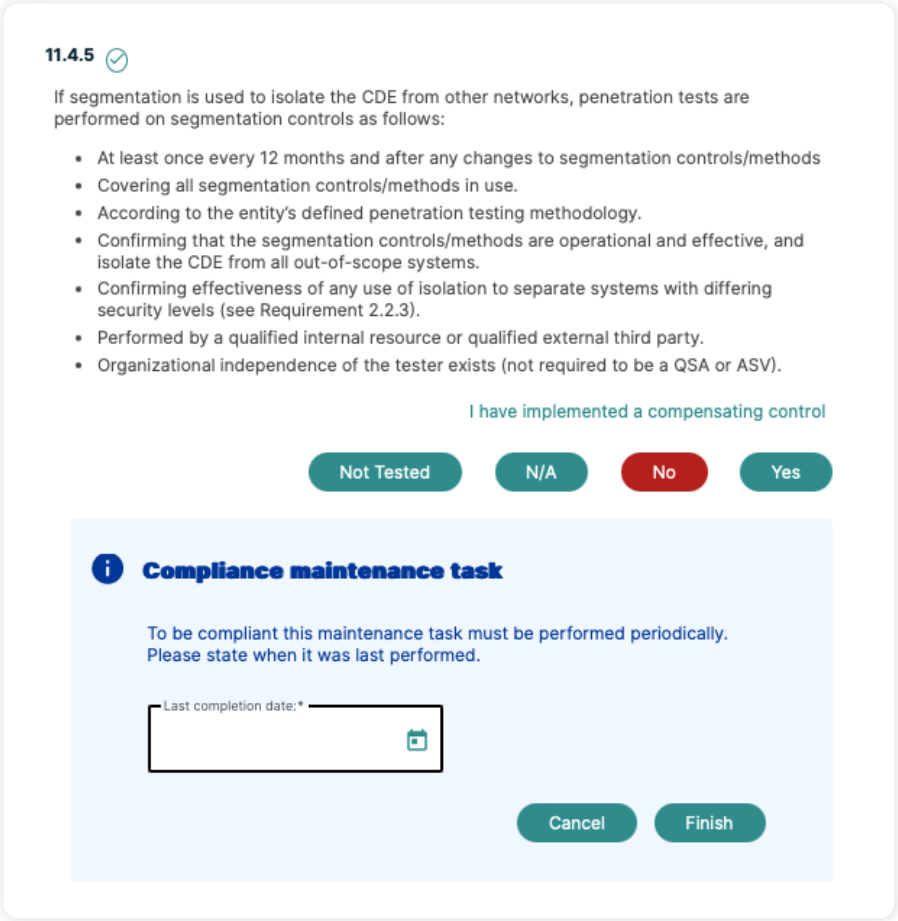
9.4.1.1

Offline media backups with cardholder data are stored in a secure location.

I have implemented a compensating control

Not Tested | N/A | No | Yes

23. Regularly Monitor and Test Networks



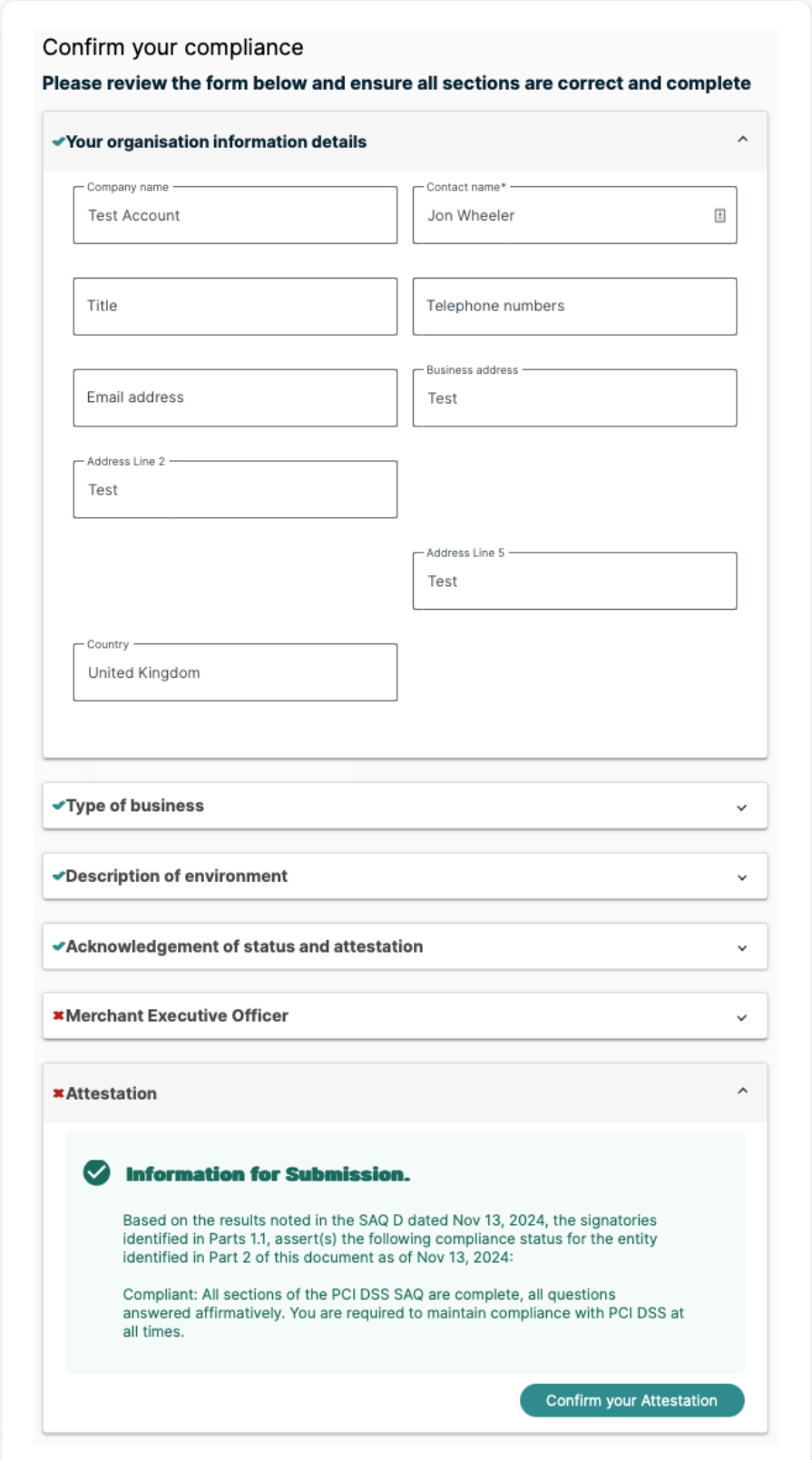
11.4.5: Question Guidance:

If you are presented with this question – it applies to your software provider and as such, select **'N/A'** to this question.

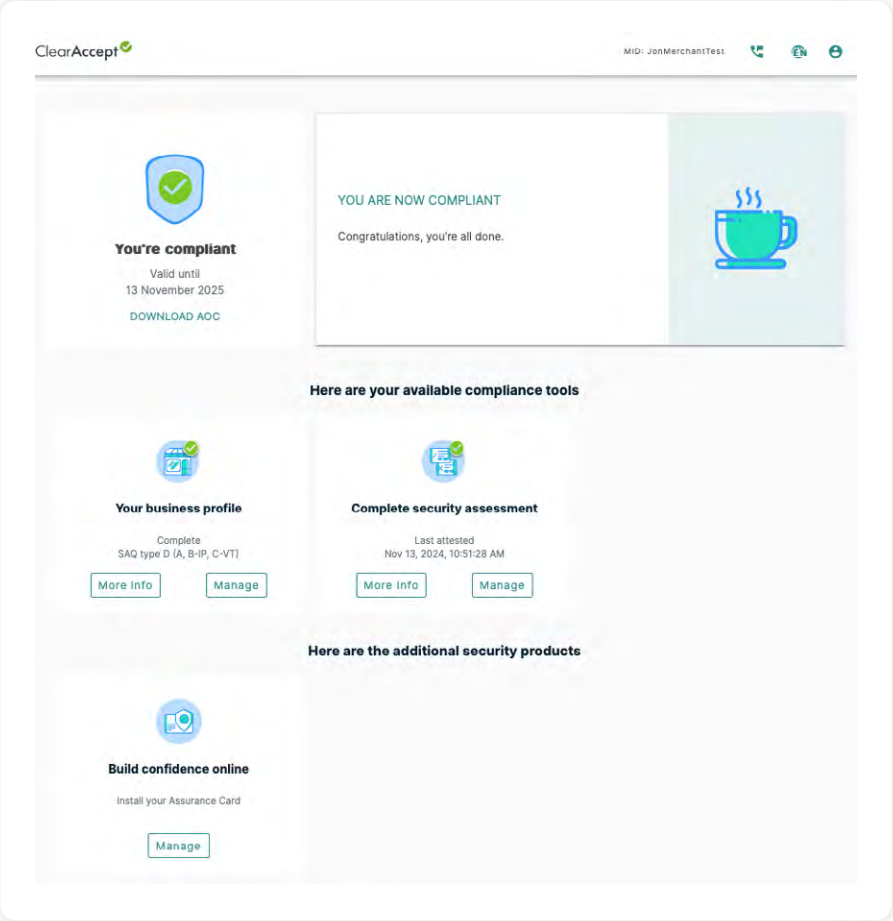
Confirm you Compliance

This form will be pre-populated. Check the details, amend if necessary. Once complete:

Click **'Confirm you Attestation'**.



Compliance Confirmation



eMail Compliance Confirmation

You will receive an eMail from Worldline Payment Guard **notifications@worldline-pciportal.com** confirming your business is now compliant and the Attestation of Compliance is valid from 1 year.

You will be sent reminders to complete your Attestation of Compliance on an annual basis moving forward.

ClearAccept

Thank you for completing your compliance with the PCI DSS

Merchant ID: JonMerchantTest

Dear Ms./Dear Mr. Jon Wheeler,

Our records show you have just validated your compliance with the Payment Card Industry Data Security Standard (PCI DSS).

Your Attestation of Compliance is valid for one year, after which it must be renewed on an annual basis. This involves updating your details and reporting on your compliance, similar to what you have just done, depending on changes to your business.

Thank you for helping to keep your customer's payment card data secure.

Please remember that the security of cardholder data is a continuous process and should be normal practice in your business. If you are required to conduct tasks such as scanning to maintain your compliance with the PCI DSS, please ensure you do so throughout the year.

If you need any assistance, the PCI Support Team will be happy to help by phone +443339961811 or e-mail support@worldline-pciportal.com.

Kind regards,
Your PCI Support

Your contact
PCI Support
support@worldline-pciportal.com
+443339961811
www.clearaccept.com