

Merchant PCI Guide

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





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.

Merchant PCI Guide

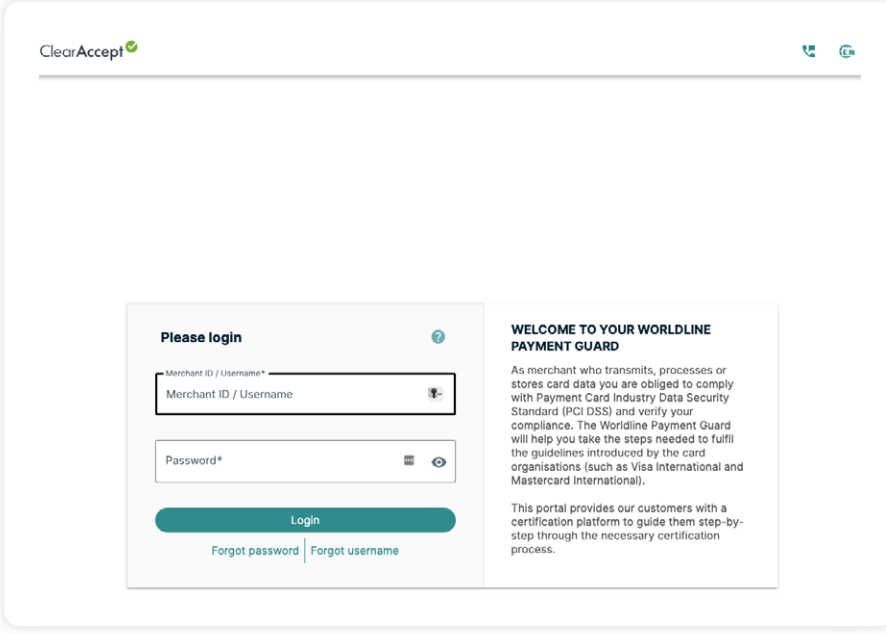
To help you create your business profile & complete your PCI attestation

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

<https://clearaccept.worldline-pciportal.com>

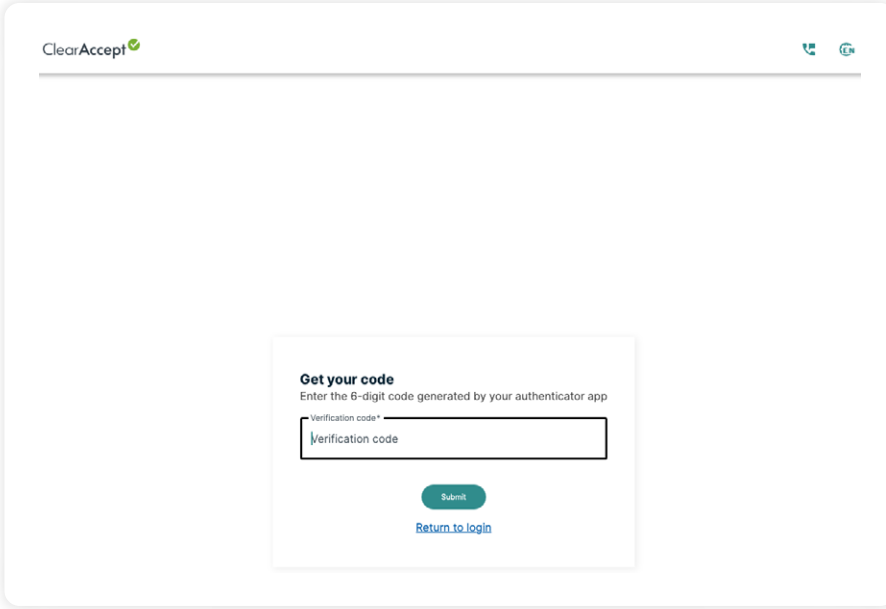
Set-up your Password

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



The screenshot shows the login interface of the ClearAccept Worldline PCI Portal. At the top left is the 'ClearAccept' logo with a green checkmark. At the top right are two small icons: a telephone and a speech bubble. The main content area is divided into two sections. On the left, under the heading 'Please login', there is a form with two input fields: 'Merchant ID / Username*' and 'Password*'. Below these fields is a green 'Login' button. Under the button are two links: 'Forgot password' and 'Forgot username'. On the right, under the heading 'WELCOME TO YOUR WORLDLINE PAYMENT GUARD', there is a paragraph of text explaining the purpose of the portal and a final paragraph stating that the portal provides a certification platform to guide users through the necessary certification process.

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



The screenshot shows the verification code entry interface of the ClearAccept Worldline PCI Portal. At the top left is the 'ClearAccept' logo with a green checkmark. At the top right are two small icons: a telephone and a speech bubble. The main content area is a single section titled 'Get your code' with the instruction 'Enter the 6-digit code generated by your authenticator app'. Below this is a single input field labeled 'Verification code*'. At the bottom of the form is a green 'Submit' button and a blue link 'Return to login'.

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.

Your account information

Choose a username for your account, and provide us with up-to-date contact details to complete your registration.

Optional

You can enter an additional email address here to receive copies of all email communications sent from us.

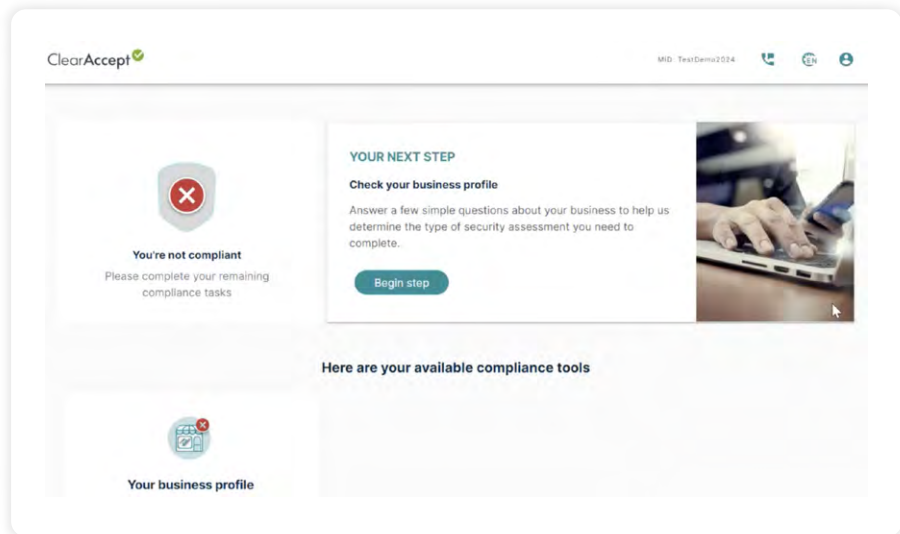
5. Click **'Next'**
- An information dialog is then displayed which recommends you add the eMail address 'notifications@worldline-pciportal.com' to your company eMail server / address book 'whitelist':

Thank you.

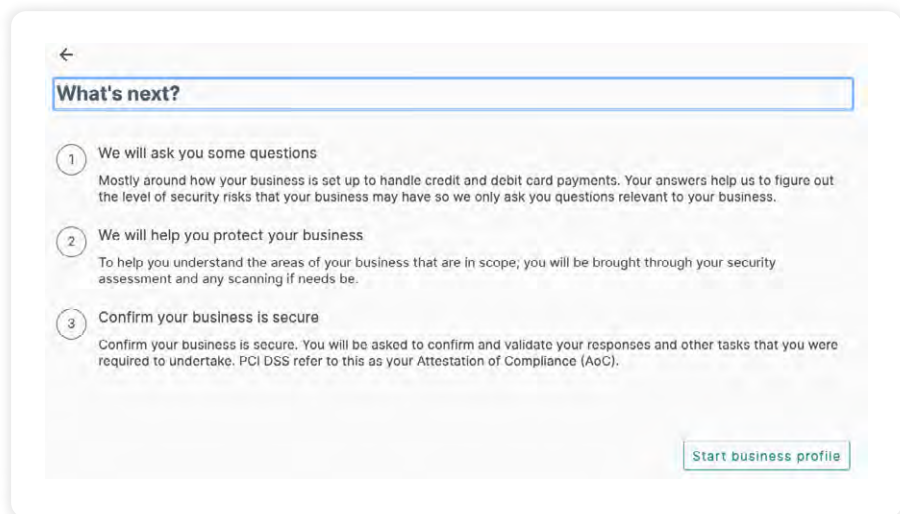
Please whitelist our email and add notifications@worldline-pciportal.com to your contact list or safe sender list to ensure you receive all future emails from us.

Got it!

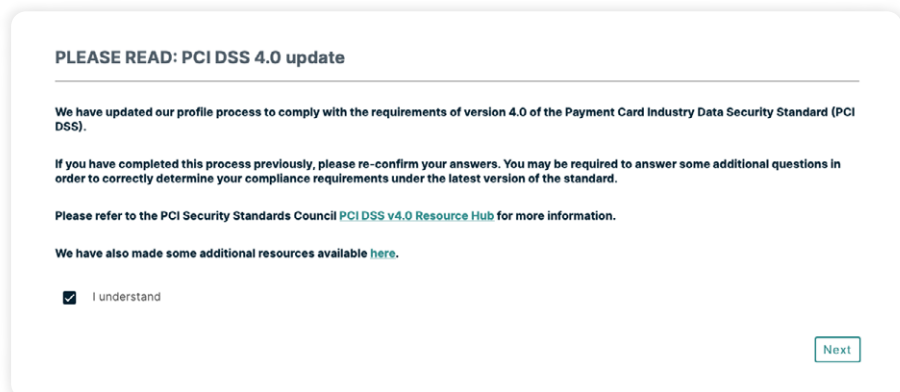
6. Click on **'Begin step'** to create your business profile



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’

Choose an assessment method

☒ **Guide Me** - Select this option to use our profiling tool to help you determine the scope of your PCI DSS compliance requirements.

☐ **Expert** - Select this option if you already know the PCI DSS assessment type applicable to your business, and do not wish to be guided by our profiling tool. This will require you to provide responses to all of the requirements on the assessment questionnaire.

☐ **Upload** - Select this option to upload your existing currently valid PCI DSS Self-Assessment Questionnaire (SAQ) or Attestation of Compliance (AoC) from an external source.

[Previous](#) [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

How do you accept payment cards?

Please select all of the ways you take payment cards in your business today. Please note this only refers to branded cards (e.g. Visa and Mastercard) not alternative payment types (e.g. PayPal, ApplePay, Pay by Link and GooglePay are not applicable)

☒  Face to face (the customer is present and the payment card is inserted, tapped or swiped to complete the transaction. This includes unattended kiosks.) 

☒  Online payments (e-Commerce website/shop, Worldline Pay by Link, ClicPay, consumer mobile app, etc.) 

☒  Mail and/or telephone order card payments 

[Previous](#) [Next](#)

Pay by Link Section

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

Pay by Link

Can your customers make card payments via a Pay by Link solution (a secure payment link is sent to the customer by email SMS or QR Code to allow them to make a payment)? 

☒ Yes ☐ No

[Previous](#) [Next](#)

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

Your Pay By Link solution provider

Please provide the name of your Pay By Link solution provider

Pay By Link provider name:

Software Platform

[Previous](#) [Next](#)

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

Your Pay By Link solution provider

Is your Pay By Link solution provider PCI DSS compliant for the services they provide to you?

☒ Yes ☐ No

[Previous](#) [Next](#)

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

Pay by Link Only

Is Pay by Link the only method that your customers can use to pay by card? 

☐ Yes ☒ No

[Previous](#) [Next](#)

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

How do you accept online e-commerce customer card payments? 

Please select all of the ways customers make online card payments to your business

☒ My customers make online payments to my business via a website accessed using a web browser

☐ My customers make online payments to my business via a mobile app downloaded to their own device from an App Store

[Previous](#) [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'**

Your ecommerce URL(s)

Please list all of your organisation's e-commerce URLs and/or domain names.

Your ecommerce URL(s) 

[www.website1.co.uk](#)  [www.website2.co.uk](#)  [www.website3.com](#) 

[Previous](#) [Next](#)

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

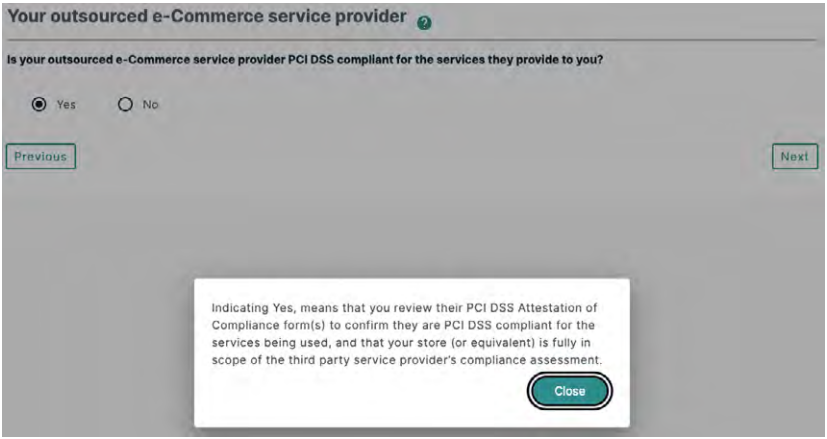
E-Commerce website management

Is your entire online payments e-Commerce website fully managed, operated and maintained by a third party? This means you have completely outsourced all operations in relation to your online payments e-commerce website. 

☒ Yes ☐ No

[Previous](#) [Next](#)

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



Your outsourced e-Commerce service provider 

Is your outsourced e-Commerce service provider PCI DSS compliant for the services they provide to you?

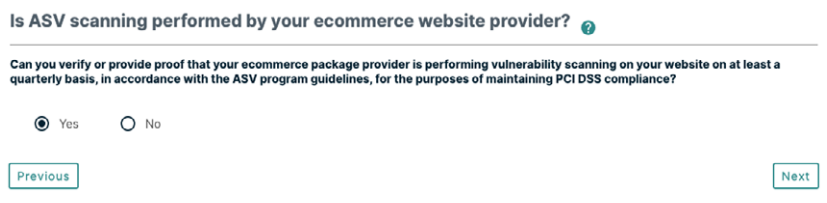
☒ Yes ☐ No

[Previous](#) [Next](#)

Indicating Yes, means that you review their PCI DSS Attestation of Compliance form(s) to confirm they are PCI DSS compliant for the services being used, and that your store (or equivalent) is fully in scope of the third party service provider's compliance assessment.

[Close](#)

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



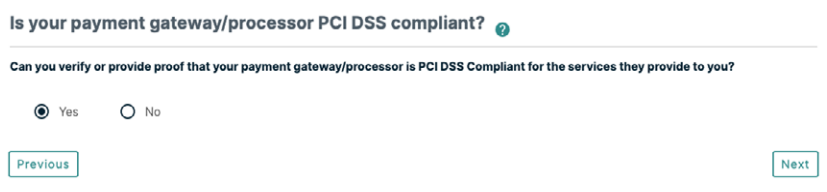
Is ASV scanning performed by your ecommerce website provider? 

Can you verify or provide proof that your ecommerce package provider is performing vulnerability scanning on your website on at least a quarterly basis, in accordance with the ASV program guidelines, for the purposes of maintaining PCI DSS compliance?

☒ Yes ☐ No

[Previous](#) [Next](#)

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



Is your payment gateway/processor PCI DSS compliant? 

Can you verify or provide proof that your payment gateway/processor is PCI DSS Compliant for the services they provide to you?

☒ Yes ☐ No

[Previous](#) [Next](#)

Mail Order / Telephone Order [MOTO] Section

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

How you accept your mail and telephone order customer card payments

My customers provide their card number by:

☐ Post (including letters and or forms)

☐ Fax

☐ E-mail (including scanned forms)

☒ Phone

[Previous](#) [Next](#)

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

How you accept card payments via mail and telephone order

Do you fully outsource your telephone or mail ordering service including payment capture to a third party? 

☐ Yes ☒ No

[Previous](#) [Next](#)

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

Transactions over the telephone

How do you accept payments over the phone?

☒ My customers give their payment card number over the phone to a person in my organisation or call centre

☐ My customers give their payment card number via an automated (voice or touch-tone) response system 

[Previous](#) [Next](#)

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

Your telephone system call handling

Do you record calls made and received by your business?

☐ Yes ☒ No

[Previous](#) [Next](#)

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

Customer Relationship Management (CRM) software setup

Do you store cardholder data in any of your CRM systems?

☐ Yes ☒ No

[Previous](#) [Next](#)

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

Your employees access to data

Do any of your employees have access to any electronically stored cardholder data?

☐ Yes ☒ No

[Previous](#) [Next](#)

Point of Sale [POS] Section

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

How you accept card payments

Please select all of the methods that you use to accept card payments in your business.

- ☒  I use a standalone counter-top or portable Point of Sale (POS) payment terminal
- ☒  I use a browser-based Virtual Terminal (or other browser-based payment page hosted by a PCI DSS compliant service provider) to manually process card payments
- ☐  I use a mobile (smartphone, tablet etc) device to accept face to face payments
- ☐  I use an integrated/electronic Point of Sale (iPOS/ePOS) system (a POS computer system running a payment application that includes an attached or integrated card reader device)
- ☐  I use a payment application that allows my company's employees to manually input card data transactions for processing using a computer (This is not a Virtual Terminal)
- ☐  I use a manual imprint machine and/or paper sales vouchers

[Previous](#)[Next](#)

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

Your Point-to-Point Encryption system

Are your payment card terminals or Point-of-Sale systems using a PCI SSC approved Point-to-Point Encryption (P2PE) hardware solution? 

☐ Yes ☒ No

[Previous](#)[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'

How your payment terminal is connected

Please select your payment terminal connection types. If your terminal is connected by a cable, it is important to determine if this is through a telephone line or a data cable (broadband/internet)

- ☐  The phone line
- ☒  Connected to the Internet via in-store WiFi (i.e. via your internal WiFi network)
- ☒  A mobile network using a SIM card
- ☒  Connected to the Internet via a cabled connection (e.g. via a Broadband Router)

[Previous](#)[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'**

Remote access

Does anyone in your company or any third party (contractor/vendor/your processor) require remote access to your point-of-sale devices/payment application or other network components? 

☒ Yes
 ☐ No

[Previous](#)
[Next](#)

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

Your customer's payment card authentication data

Do you receive the security/validation/verification code from your customers to authorize their transactions? This is the three or four digit number located in either the signature panel of your customer's payment card or on the front of the card.

☒ Yes
 ☐ No

[Previous](#)
[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'**

Your customer's payment card authentication data

Do you store the payment card security/validation/verification code in any electronic format? (e.g. databases, files, emails, scanned copies etc?)

☐ Yes
 ☒ No

Do you securely destroy the payment card security/validation/verification code once the transaction has been authorized? 

☒ Yes
 ☐ No

[Previous](#)
[Next](#)

Did you know? The PCI DSS requires that you use cross-cut shredding, incineration or pulping to destroy paper records of the card security code once the transaction has been authorised.

[Close](#)

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

Other uses of card numbers ?

Does anyone in your organisation send or receive full card numbers via email or instant messaging?

☐ Yes ☒ No

Does your company otherwise store, transmit or receive cardholder data electronically in any other way and for any other purpose? This could be via CD-ROM, USB drive or an internet network. ?

☐ Yes ☒ No

[Previous](#) [Next](#)

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

Your company policy for information security

To handle payment cards you are required by the Payment Card Industry Data Security Standard (PCI DSS) to have an Information Security Policy in place for your organization. This must cover all relevant areas of the standard. If you do not currently have one, we can provide you with a policy template below. ?

☒ I do not have an Information Security Policy in place at the moment, I will implement a security policy using the template provided. [Download](#)

☐ I already have an Information Security Policy in place that covers ALL of the relevant clauses of the Payment Card Industry Data Security Standard (PCI DSS)

☐ I do not currently have an Information Security Policy in place that covers ALL of the relevant clauses of the Payment Card Industry Data Security Standard (PCI DSS) but I do not wish to use the one provided as the basis for my policy.

[Previous](#) [Next](#)

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

Password policy

Do you enforce a minimum password length of seven characters, containing both numeric and alphabetic characters, for user accounts on all POS devices, computers and systems in your business? ?

☒ Yes ☐ No

Please note: After 31st March 2025, you will need to enforce a minimum password length of twelve characters (where twelve characters are supported, otherwise a minimum of eight characters is required). This also applies to passwords used by all non-customer users and administrators with access to e-commerce websites/web servers.

[Previous](#) [Next](#)

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

Do you use an Internal Security Assessor for your PCI DSS?

Are you validating your compliance through an Internal Security Assessor (ISA) who is certified by the Payment Card Industry Security Standards Council (PCI SSC)? ?

☐ Yes ☒ No

[Previous](#) [Next](#)

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

Support from a PCI Qualified Security Assessor 

Have you appointed a Qualified Security Assessor (QSA) to assist you in achieving, assessing and/or maintaining your compliance with the Payment Card Industry Data Security Standard (PCI DSS)?

☐ Yes ☒ No

[Previous](#) [Next](#)

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

Third Party Managed System Service Providers

Do you have relationships with one or more third-party service providers that manage system components included in the scope of this assessment, for example, via network security control services, anti-malware services, security incident and event management (SIEM), contact and call centers, web-hosting services, and IaaS, PaaS, SaaS, and FaaS cloud provider?

☒ Yes ☐ No

[Previous](#) [Next](#)

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

Other Third Party Service Providers that may impact cardholder data security

Do you have relationships with one or more third-party service providers that could impact the security of your company's cardholder data environment (CDE)? For example, vendors providing support via remote access, and/or bespoke software developers.

☐ Yes ☒ No

[Previous](#) [Next](#)

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

A summary of how and where you handle card payments

Please provide the information requested below. This will form part of your Attestation of Compliance

List your business premises type(s) and a summary of locations that are relevant to your PCI DSS assessment (eg, retail outlets, corporate offices, data centres, call centres etc...) 

jkhadsJKH

9/4000

How and in what capacity does your business store, process and/or transmit cardholder data? 

adklfchjak

11/4000

Provide a high level description of your overall business environment, applicable to your PCI DSS assessment. For example describe the type of equipment you use for card processing, storage and transmission; such as POS devices any databases and web servers, include a description as to how they connect both externally and any internal connections.

adklfjfk

9/4000

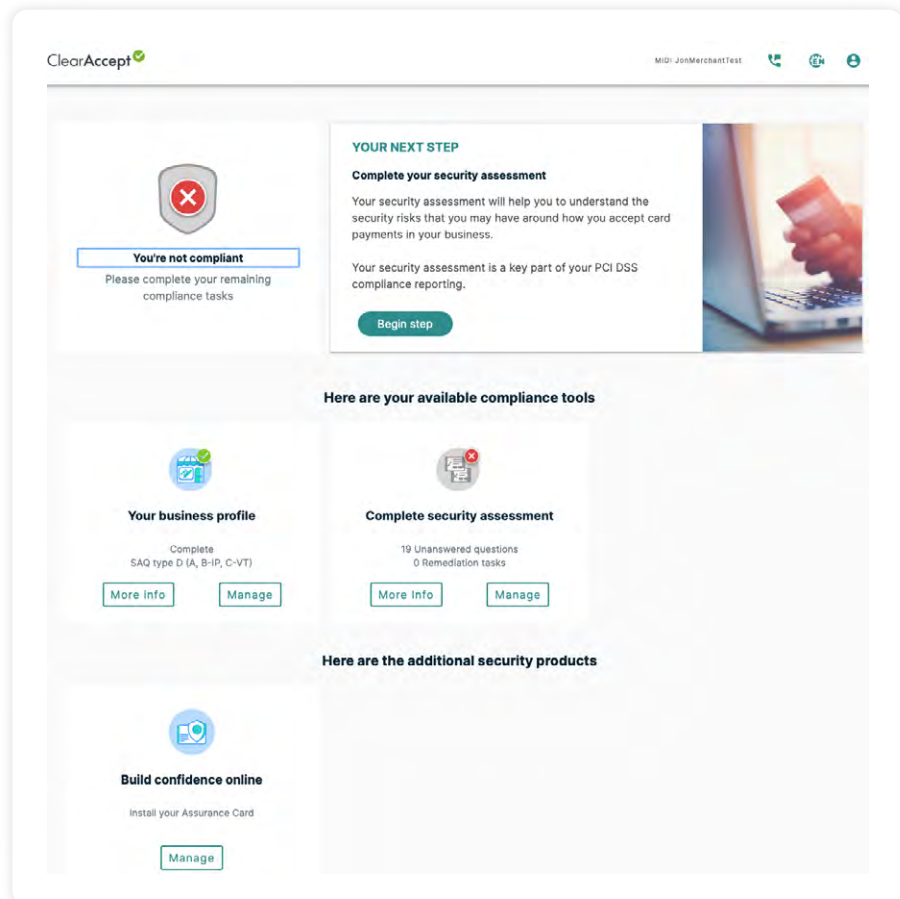
Previous

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.

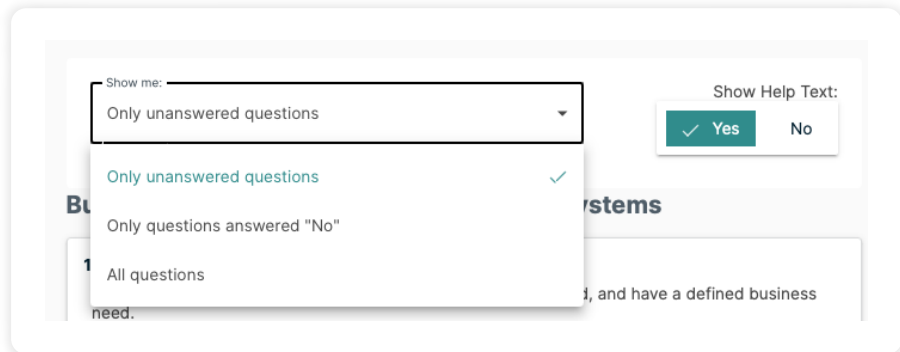


2. **Note:** The number and nature of the remaining 'unanswered' questions now presented to you in the Security Assessment section are specifically related to the selections you made in the business profile section above.

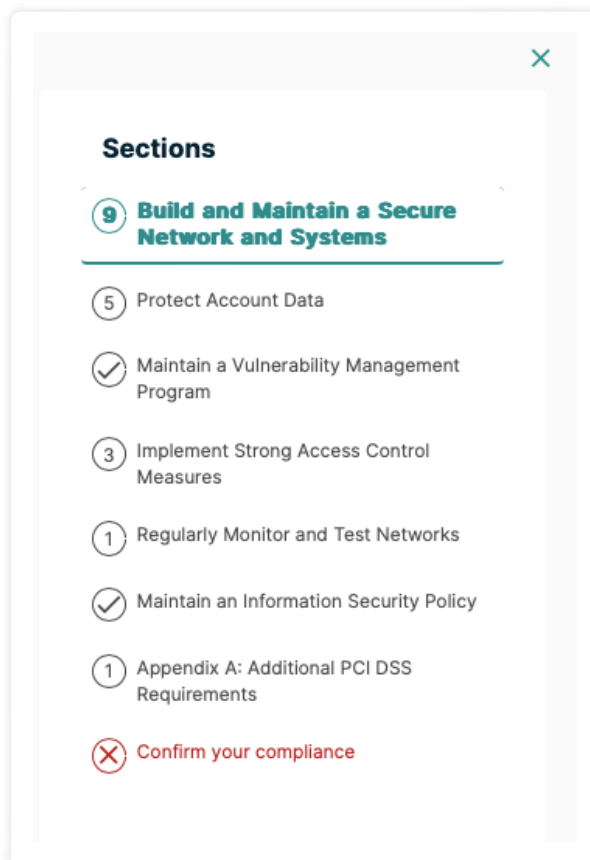
As such, given the above is a guide and was not written relative to your actual business set-up – the below unanswered questions may not be the same as those now presented to you by the PCI Portal.

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.

 **You selected no**

Reason for non-compliance*

0 / 1500

Complete documentation*

0 / 1500

Target date:*



You will receive a reminder email

Cancel

Finish

5. Build and Maintain a Secure Network and Systems

1.2.5

All services, protocols and ports allowed are identified, approved, and have a defined business need.

I have implemented a compensating control

Not Tested

N/A

No

Yes

Help answering this requirement

Expected Testing

- Examine documentation.
- Examine configuration settings

Information

Purpose

NSC Compromises often happen due to unused or insecure services (for example, telnet and FTP), protocols, and ports, since these can lead to unnecessary points of access being opened into the CDE. Additionally, services, protocols, and ports that are enabled but not in use are often overlooked and left unsecured and unpatched. By identifying the services, protocols, and ports necessary for business, entities can ensure that all other services, protocols, and ports are disabled or removed.

Good Practice

The security risk associated with each service, protocol, and port allowed should be understood. Approvals should be granted by personnel independent of those managing the configuration. Approving personnel should possess knowledge and accountability appropriate for making approval decisions.

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

Security features are defined and implemented for all services, protocols, and ports that are in use and considered to be insecure, such that the risk is mitigated.

I have implemented a compensating control

Not Tested

N/A

No

Yes

Help answering this requirement

Expected Testing

- Examine documentation.
- Examine configuration settings.

Information

Purpose

Compromises take advantage of insecure network configurations.

Good Practice

If insecure services, protocols, or ports are necessary for business, the risk posed by these services, protocols, and ports should be clearly understood and accepted by the organization, the use of the service, protocol, or port should be justified, and the security features that mitigate the risk of using these services, protocols, and ports should be defined and implemented by the entity.

Further Information

For guidance on services, protocols, or ports considered to be insecure, refer to industry standards and guidance (for example, from NIST, ENISA, OWASP).

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

Outbound traffic from the CDE is restricted as follows:

- To only traffic that is necessary.
- All other traffic is specifically denied.

I have implemented a compensating control

Not Tested

N/A

No

Yes

Help answering this requirement

Expected Testing

- Examine NSC configuration standards.
- Examine NSC configurations.

Information

Purpose

This requirement aims to prevent malicious individuals and compromised system components within the entity's network from communicating with an untrusted external host.

Good Practice

All traffic outbound from the CDE, regardless of the destination, should be evaluated to ensure it follows established, authorized rules. Connections should be inspected to restrict traffic to only authorized communications—for example, by restricting source/destination addresses and ports, and blocking of content.

Examples

Implementing a rule that denies all inbound and outbound traffic that is not specifically needed—for example, by using an explicit “deny all” or implicit deny after allow statement—helps to prevent inadvertent holes that would allow unintended and potentially harmful traffic

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

NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that:

- All wireless traffic from wireless networks into the CDE is denied by default.
- Only wireless traffic with an authorized business purpose is allowed into the CDE.

I have implemented a compensating control

Not Tested

N/A

No

Yes

Help answering this requirement

Expected Testing

- Examine configuration settings.
- Examine network diagrams.

Information

Purpose

The known (or unknown) implementation and exploitation of wireless technology within a network is a common path for malicious individuals to gain access to the network and account data. If a wireless device or network is installed without the entity's knowledge, a malicious individual could easily and "invisibly" enter the network. If NSCs do not restrict access from wireless networks into the CDE, malicious individuals that gain unauthorized access to the wireless network can easily connect to the CDE and compromise account information.

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

Anti-spoofing measures are implemented to detect and block forged source IP addresses from entering the trusted network.

I have implemented a compensating control

Not Tested

N/A

No

Yes

Help answering this requirement

Expected Testing

- Examine NSC documentation.
- Examine NSC configurations.

Information

Purpose

Filtering packets coming into the trusted network helps to, among other things, ensure packets are not "spoofed" to appear as if they are coming from an organization's own internal network. For example, anti-spoofing measures prevent internal addresses originating from the Internet from passing into the DMZ.

Good Practice

Products usually come with anti-spoofing set as a default and may not be configurable. Entities should consult the vendor's documentation for more information.

Examples

Normally, a packet contains the IP address of the computer that originally sent it so other computers in the network know where the packet originated. Malicious individuals will often try to spoof (or imitate) the sending IP address to fool the target system into believing the packet is from a trusted source.

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, network-based 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

All security policies and operational procedures that are identified in Requirement 2 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

Help answering this requirement

Expected Testing

- Examine documentation.
- Interview personnel.

Information

Purpose

Requirement 2.1.1 is about effectively managing and maintaining the various policies and procedures specified throughout Requirement 2. While it is important to define the specific policies or procedures called out in Requirement 2, it is equally important to ensure they are properly documented, maintained, and disseminated.

Good Practice

It is important to update policies and procedures as needed to address changes in processes, technologies, and business objectives. For this reason, consider updating these documents as soon as possible after a change occurs and not only on a periodic cycle

Definitions

Security policies define the entity's security objectives and principles. Operational procedures describe how to perform activities, and define the controls, methods, and processes that are followed to achieve the desired result in a consistent manner and in accordance with policy objectives.

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

System security parameters are configured to prevent misuse.

I have implemented a compensating control

Not Tested

N/A

No

Yes

Help answering this requirement

Expected Testing

- Examine system configuration standards.
- Interview personnel.
- Examine system configurations.

Information

Purpose

Correctly configuring security parameters provided in system components takes advantage of the capabilities of the system component to defeat malicious attacks.

Good Practice

System configuration standards and related processes should specifically address security settings and parameters that have known security implications for each type of system in use. For systems to be configured securely, personnel responsible for configuration and/or administering systems should be knowledgeable in the specific security parameters and settings that apply to the system. Considerations should also include secure settings for parameters used to access cloud portals.

Further Information

Refer to vendor documentation and industry references noted in Requirement 2.2.1 for information about applicable security parameters for each type of system.

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

For wireless environments connected to the CDE or transmitting account data, wireless encryption keys are changed as follows:

- Whenever personnel with knowledge of the key leave the company or the role for which the knowledge was necessary.
- Whenever a key is suspected of or known to be compromised

I have implemented a compensating control

Not Tested

N/A

No

Yes

Help answering this requirement

Expected Testing

- Examine key-management documentation.
- Interview personnel.

Information

Purpose

Changing wireless encryption keys whenever someone with knowledge of the key leaves the organization or moves to a role that no longer requires knowledge of the key, helps keep knowledge of keys limited to only those with a business need to know. Also, changing wireless encryption keys whenever a key is suspected or known to be comprised makes a wireless network more resistant to compromise.

Good Practice

This goal can be accomplished in multiple ways, including periodic changes of keys, changing keys via a defined "joiners-movers-leavers" (JML) process, implementing additional technical controls, and not using fixed pre-shared keys. In addition, any keys that are known to be, or suspected of being, compromised should be managed in accordance with the entity's incident response plan at Requirement 12.10.1.

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'

Build and Maintain a Secure Network and Systems

i There are no unanswered questions in this section

Attention! You may still have questions answered "No", which means that your security assessment will not be complete until you address compliance remediation tasks associated with those questions you have answered "No"

Next

15. Protect Account Data

3.2.1

Account data storage is kept to a minimum through implementation of data retention and disposal policies, procedures, and processes that include at least the following:

- Coverage for all locations of stored account data.
- Coverage for any sensitive authentication data (SAD) stored prior to completion of authorization. This bullet is a best practice until its effective date; refer to Applicability Notes below for details.
- Limiting data storage amount and retention time to that which is required for legal or regulatory, and/or business requirements.
- Specific retention requirements for stored account data that defines length of retention period and includes a documented business justification.
- Processes for secure deletion or rendering account data unrecoverable when no longer needed per the retention policy.
- A process for verifying, at least once every three months, that stored account data exceeding the defined retention period has been securely deleted or rendered unrecoverable.

I have implemented a compensating control

Not Tested

N/A

No

Yes

16.

4.2.1.a

Strong cryptography and security protocols are implemented as follows to safeguard PAN during transmission over open, public networks: Only trusted keys and certificates are accepted.

I have implemented a compensating control

Not Tested

N/A

No

Yes

17.

4.2.1.c

Strong cryptography and security protocols are implemented as follows to safeguard PAN during transmission over open, public networks: The protocol in use supports only secure versions or configurations and does not support fallback to, or use of insecure versions, algorithms, key sizes, or implementations.

I have implemented a compensating control

Not Tested

N/A

No

Yes

18.

4.2.1.d

Strong cryptography and security protocols are implemented as follows to safeguard PAN during transmission over open, public networks: The encryption strength is appropriate for the encryption methodology in use.

I have implemented a compensating control

Not Tested

N/A

No

Yes

19.

4.2.1.2

Wireless networks transmitting PAN or connected to the CDE use industry best practices to implement strong cryptography for authentication and transmission.

I have implemented a compensating control

Not Tested

N/A

No

Yes

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

If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows:

- At least once every 12 months and after any changes to segmentation controls/methods
- Covering all segmentation controls/methods in use.
- According to the entity's defined penetration testing methodology.
- Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems.
- Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3).
- Performed by a qualified internal resource or qualified external third party.
- Organizational independence of the tester exists (not required to be a QSA or ASV).

I have implemented a compensating control

Not Tested

N/A

No

Yes

Compliance maintenance task

To be compliant this maintenance task must be performed periodically.
Please state when it was last performed.

Last completion date:*



Cancel

Finish

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'**.

Confirm your compliance

Please review the form below and ensure all sections are correct and complete

✔Your organisation information details

Company name

Test Account

Contact name*

Jon Wheeler

Title

Telephone numbers

Email address

Business address

Test

Address Line 2

Test

Address Line 5

Test

Country

United Kingdom

✔Type of business

✔Description of environment

✔Acknowledgement of status and attestation

✖Merchant Executive Officer

✖Attestation

✔ Information for Submission.

Based on the results noted in the SAQ D dated Nov 13, 2024, the signatories identified in Parts 1.1, assert(s) the following compliance status for the entity identified in Part 2 of this document as of Nov 13, 2024:

Compliant: All sections of the PCI DSS SAQ are complete, all questions answered affirmatively. You are required to maintain compliance with PCI DSS at all times.

Confirm your Attestation

Compliance Confirmation

ClearAccept

MID: JonMerchantTest





You're compliant

Valid until
13 November 2025

DOWNLOAD AOC

YOU ARE NOW COMPLIANT

Congratulations, you're all done.



Here are your available compliance tools



Your business profile

Complete
SAQ type D (A, B-IP, C-VT)

More Info

Manage



Complete security assessment

Last attested
Nov 13, 2024, 10:51:28 AM

More Info

Manage

Here are the additional security products



Build confidence online

Install your Assurance Card

Manage

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.



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

This message has been automatically generated. Please do not reply to this e-mail. The content of this e-mail is intended only for the confidential use of the person addressed.

If you are not the intended recipient, please notify the sender and delete this e-mail immediately.