HandPoint/PAX A920 Device

SAQ P2PE User Guide

PCI v4.0

January 2024 – PCI v3.2.1

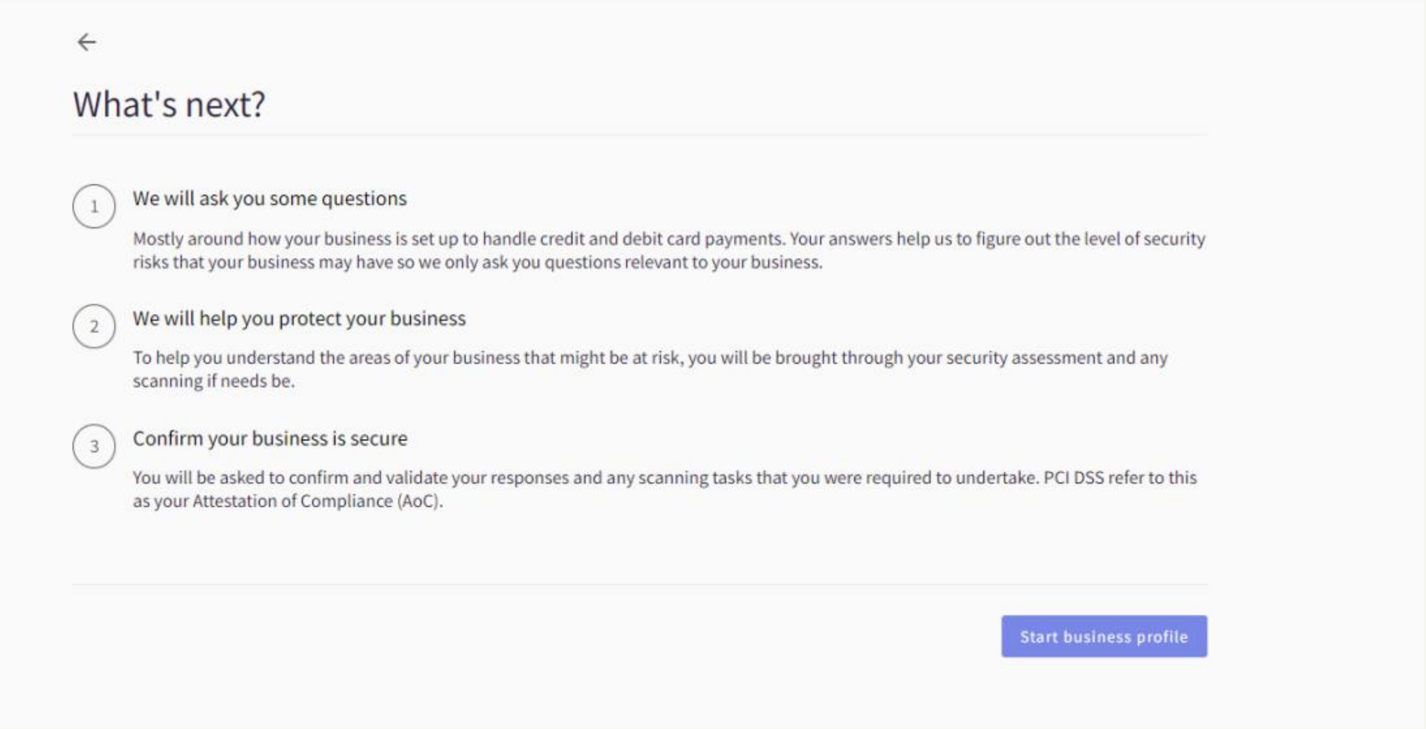
Paysafe

SAQ P2PE User Guide

- Once your account has been boarded, you will receive log in details to your PCI Account via email.
- Your username is your Merchant ID number.
- Please use the link within the email to select a password of your own choosing, ensuring to follow the on-screen instructions.
- Upon your first initial log in, you will need to review your contact information to ensure this is accurate.

SAQ P2PE User Guide

- The first screen you will see relates to the profile section.
- The profile is in place to paint a picture of your business environment and to understand how you are accepting card payments.
- As you are accepting payment using the Paysafe API - please answer the questions as they are listed within this guide.



What's next?

1. We will ask you some questions

   Mostly around how your business is set up to handle credit and debit card payments. Your answers help us to figure out the level of security risks that your business may have so we only ask you questions relevant to your business.

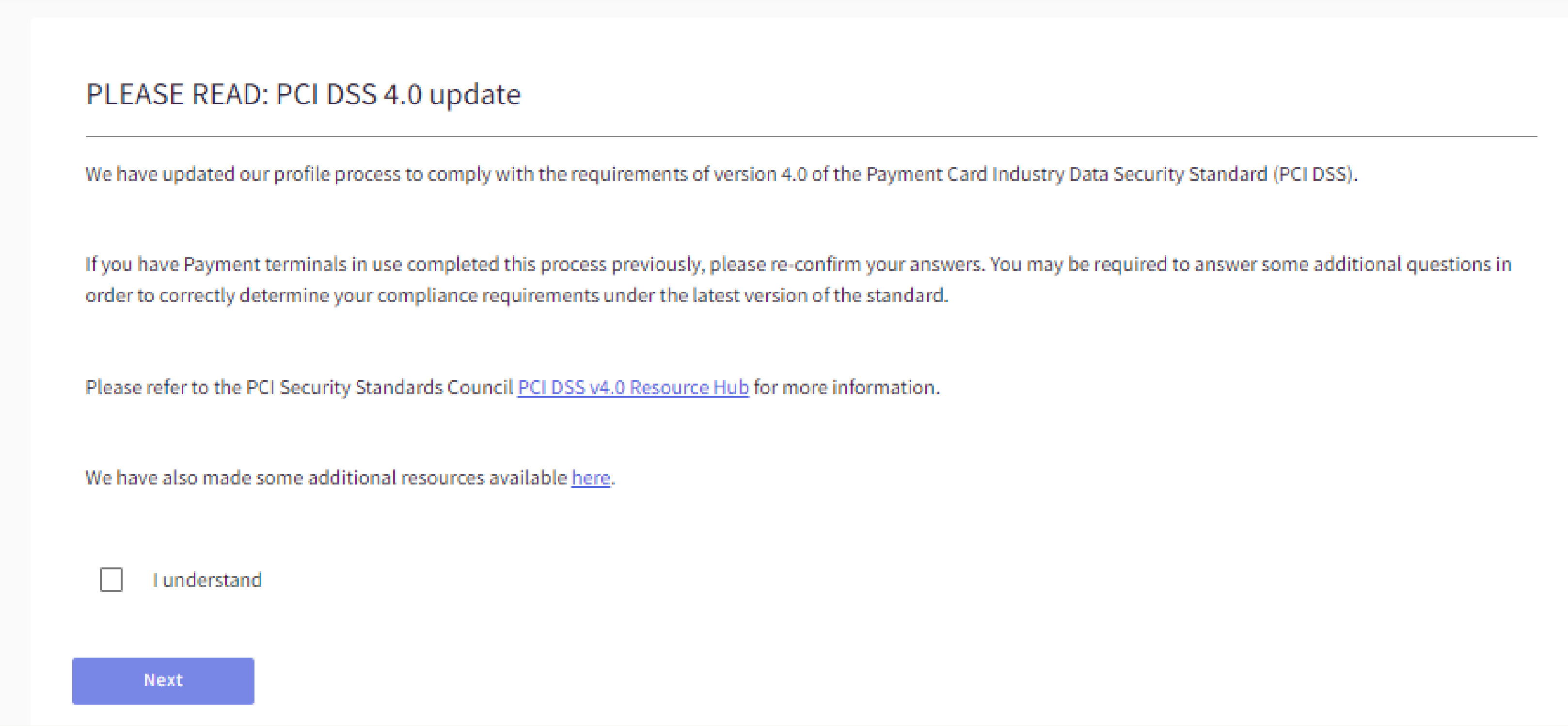
2. We will help you protect your business

   To help you understand the areas of your business that might be at risk, you will be brought through your security assessment and any scanning if needs be.

3. Confirm your business is secure

   You will be asked to confirm and validate your responses and any scanning tasks that you were required to undertake. PCI DSS refer to this as your Attestation of Compliance (AoC).

SAQ P2PE User Guide



PLEASE READ: PCI DSS 4.0 update

We have updated our profile process to comply with the requirements of version 4.0 of the Payment Card Industry Data Security Standard (PCI DSS).

If you have Payment terminals in use completed this process previously, please re-confirm your answers. You may be required to answer some additional questions in order to correctly determine your compliance requirements under the latest version of the standard.

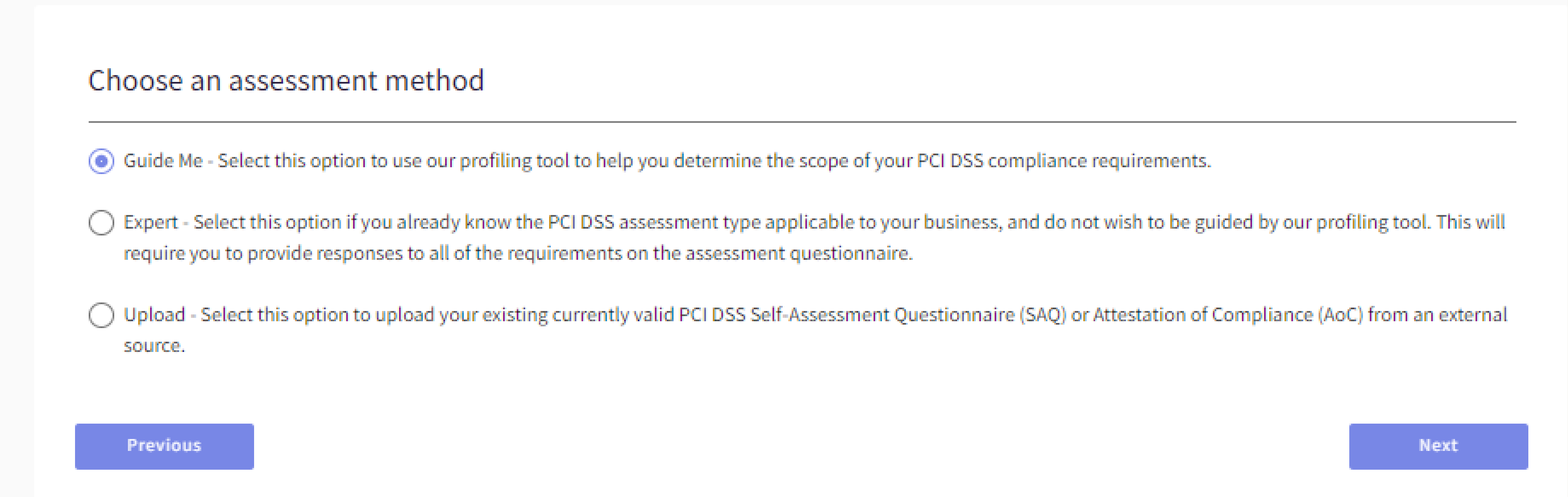
Please refer to the PCI Security Standards Council PCI DSS v4.0 Resource Hub for more information.

We have also made some additional resources available here.

□ I understand

- The PCI standard has now changed from v3.2.1 to v.4.0. The PCI Portal has been upgraded to ensure you are validating against the latest compliance standards.
- Please read the above messaging and select ‘I understand’ to proceed.

SAQ P2PE User Guide



Choose an assessment method

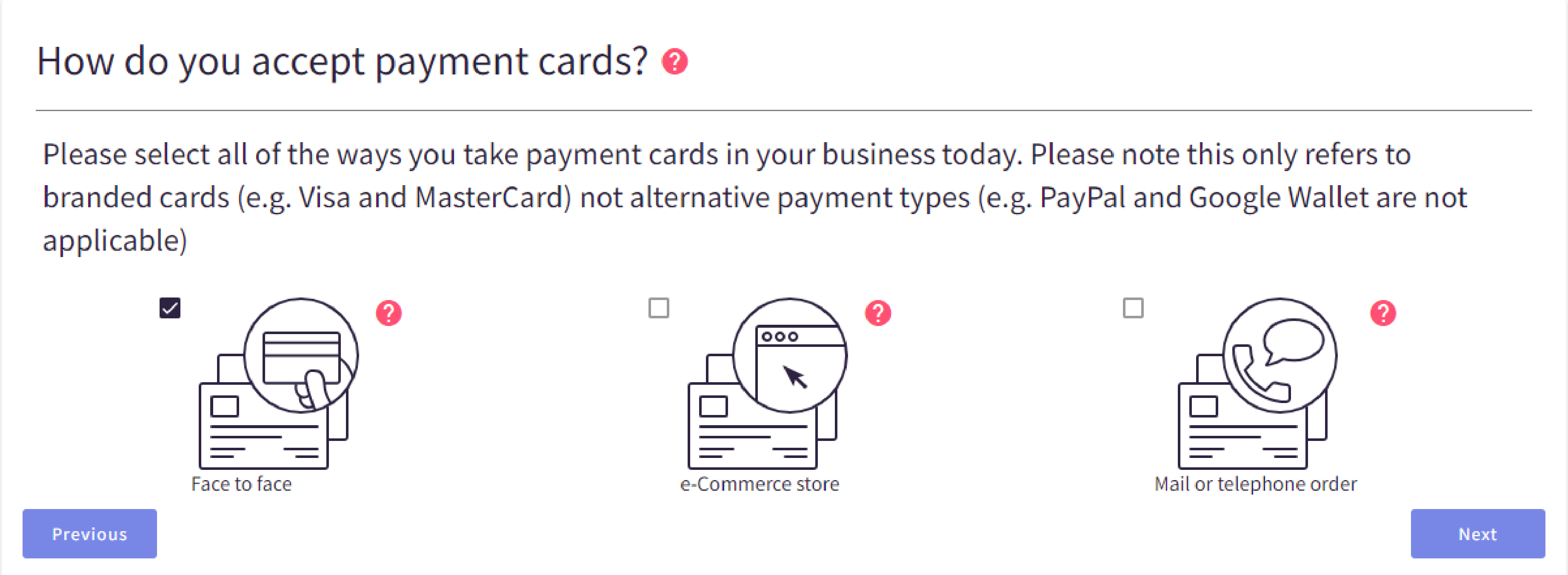
● Guide Me - Select this option to use our profiling tool to help you determine the scope of your PCI DSS compliance requirements.

○ 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.

- Please select one of the three options above in order to complete your compliance.
- Select ‘Guide me’ will allow you to complete your compliance using the PCI Portal.
- Select ‘Expert’ if you do not wish to use the profiling tool which will pre-populate some of your PCI requirements.
- Select ‘Upload’ if you have already completed your compliance for the forthcoming year and wish to upload the required documentation.

SAQ P2PE User Guide



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 and Google Wallet are not applicable)

☑ Face to face

□ e-Commerce store

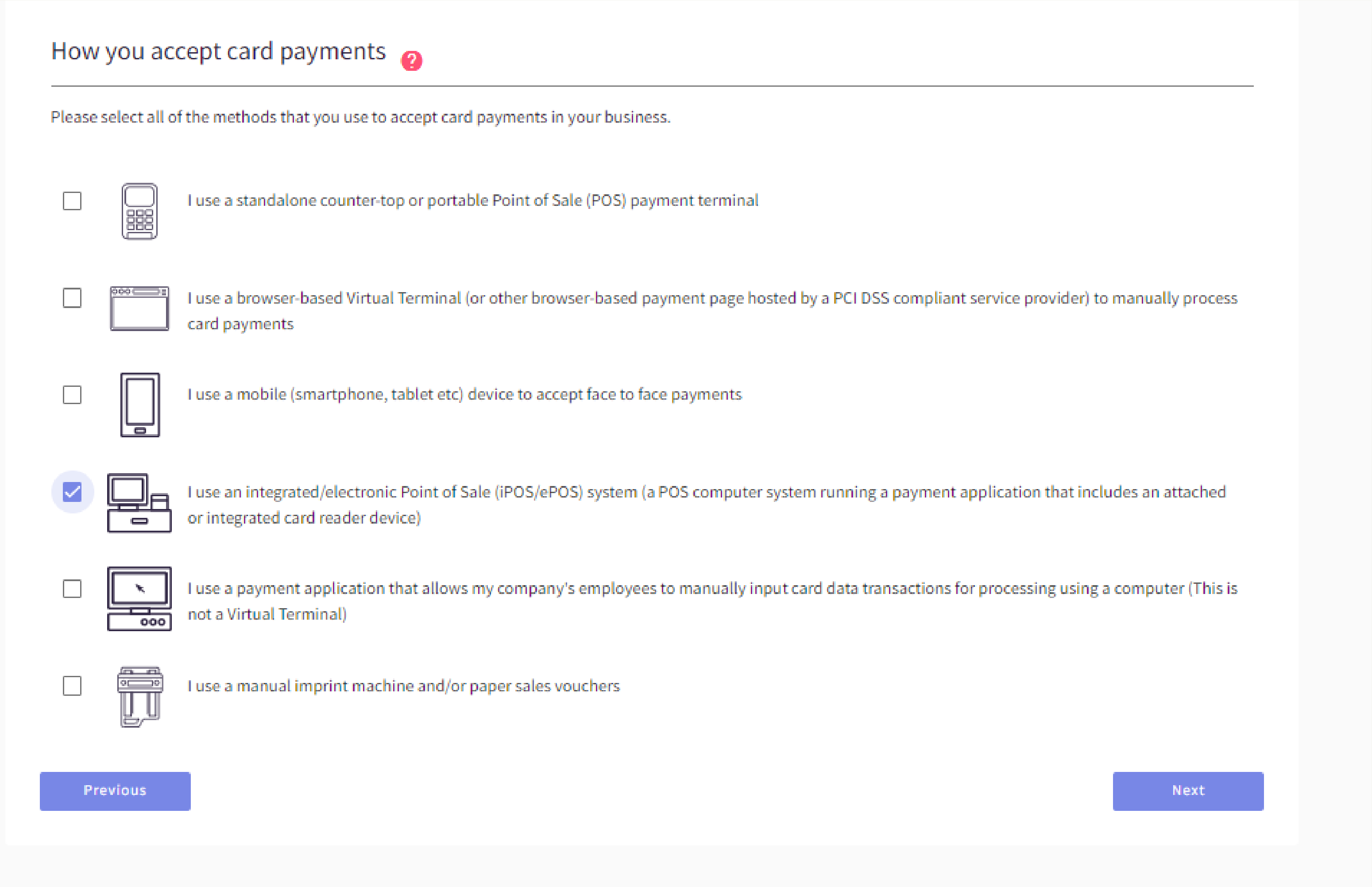
□ Mail or telephone order

- As you are using the HandPoint Terminal for card present transactions - please select that you are accepting card payments face to face.
- If you handle any payments over the phone, please also select this option.

To change footer on all slides > go to Insert > Header Footer > Type detail > click Apply to all

SAQ P2PE User Guide

- As you are using the HandPoint/PAX Terminal – please select the ‘I use an integrated/electronic Point of sale (iPOS/ePOS system’ within the options shown here.



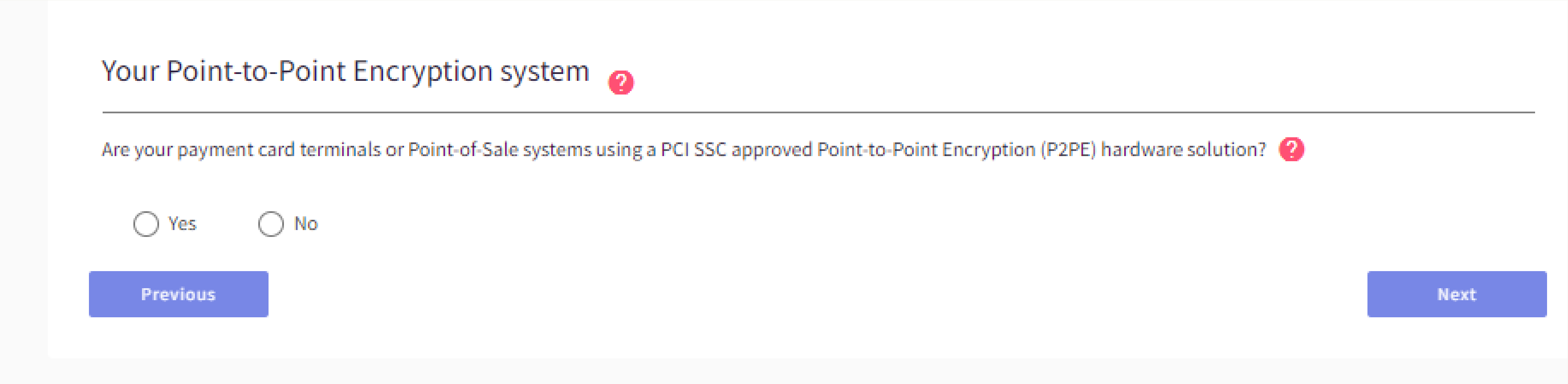
How you accept card payments

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

To change footer on all slides > go to Insert > Header Footer > Type detail > click Apply to all

SAQ P2PE User Guide



Your Point-to-Point Encryption system ?

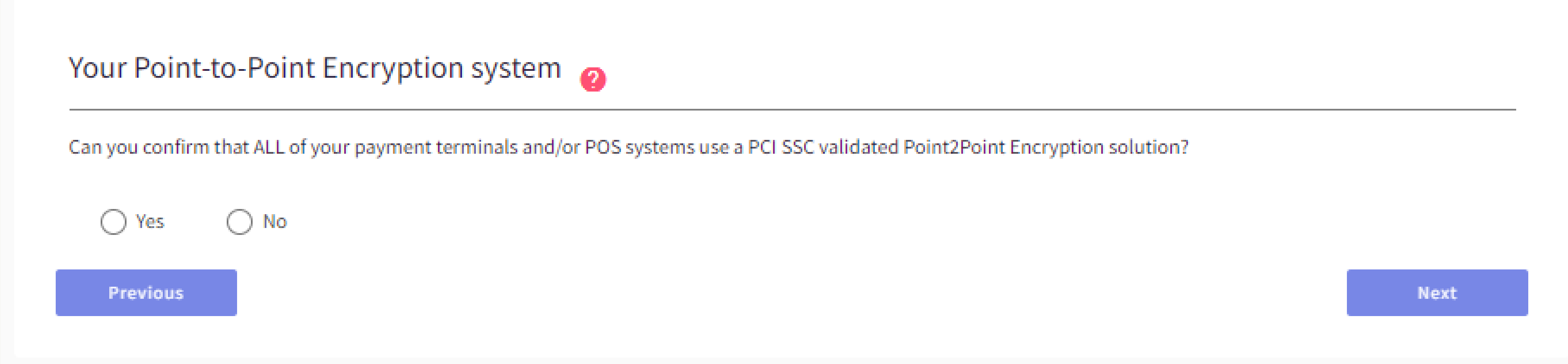
Are your payment card terminals or Point-of-Sale systems using a PCI SSC approved Point-to-Point Encryption (P2PE) hardware solution? ?

○ Yes ○ No

- As you are using the HandPoint/PAX device, we know that this is a Point-to-Point encrypted terminal.
- Due to this, please answer this question as ‘yes’.

To change footer on all slides > go to Insert > Header Footer > Type detail > click Apply to all

SAQ P2PE User Guide



Your Point-to-Point Encryption system

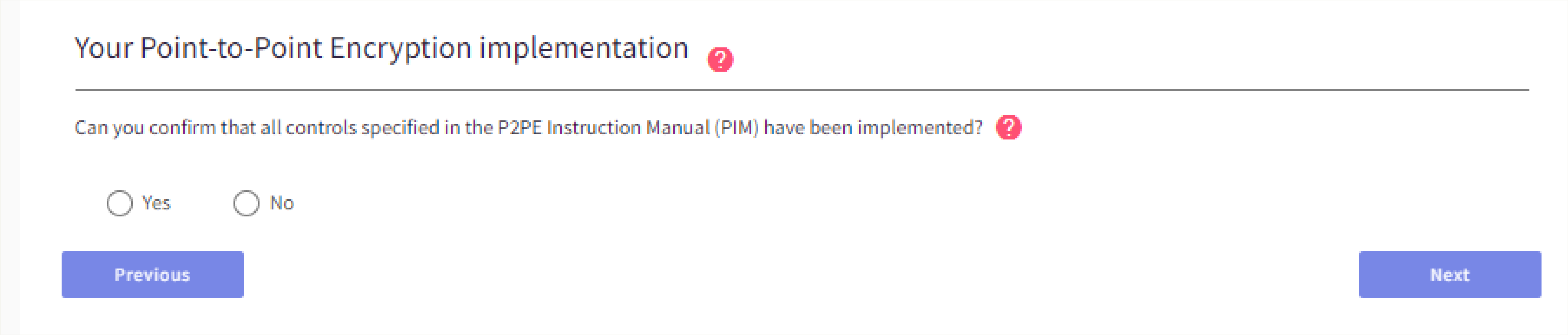
Can you confirm that ALL of your payment terminals and/or POS systems use a PCI SSC validated Point2Point Encryption solution?

○ Yes ○ No

- As you are only using the HandPoint/PAX device, you can answer this question as ‘yes’.

To change footer on all slides > go to Insert > Header Footer > Type detail > click Apply to all

SAQ P2PE User Guide



Your Point-to-Point Encryption implementation

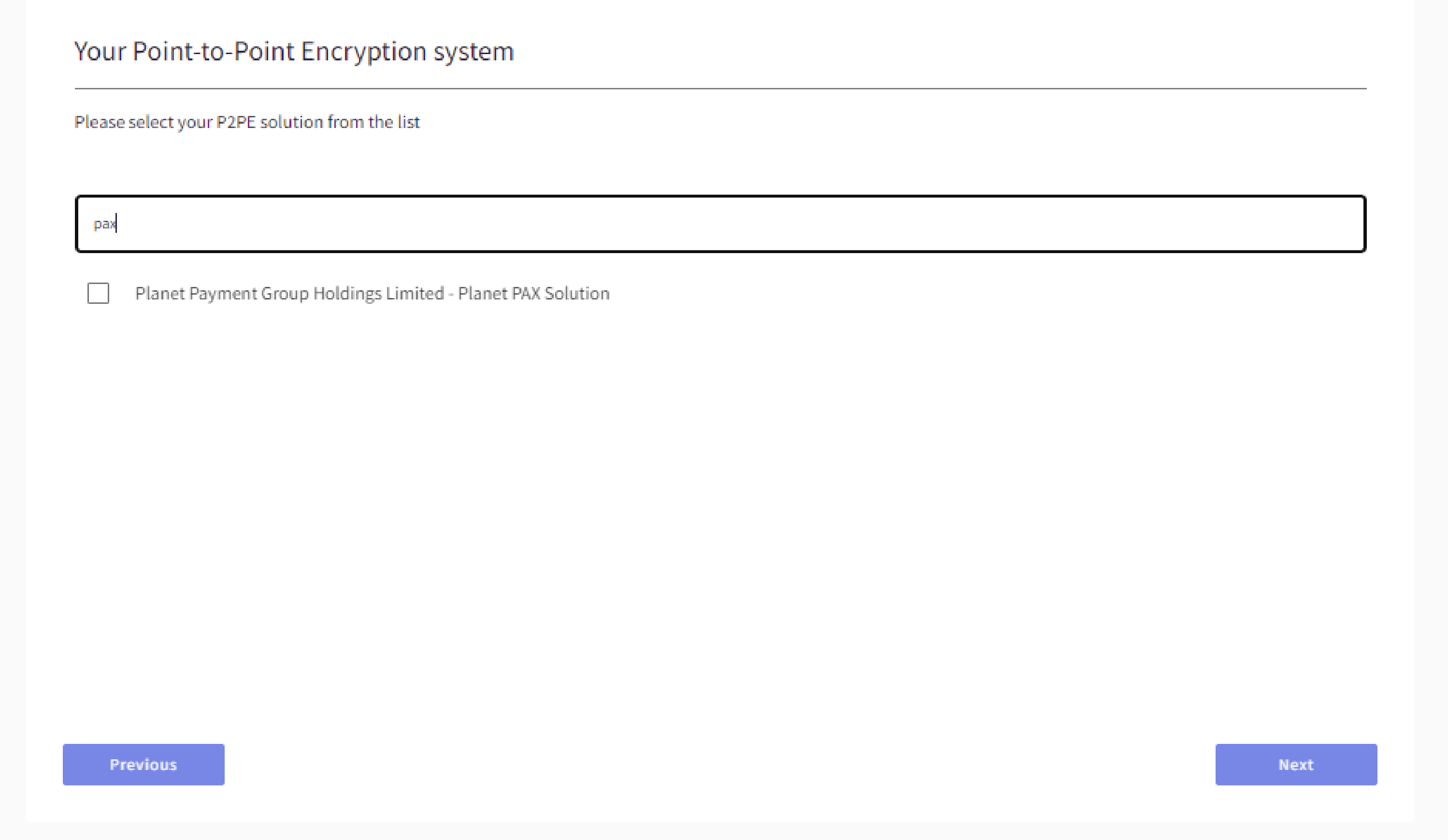
Can you confirm that all controls specified in the P2PE Instruction Manual (PIM) have been implemented?

○ Yes ○ No

- Please answer this question as ‘yes’.

To change footer on all slides > go to Insert > Header Footer > Type detail > click Apply to all

SAQ P2PE User Guide



Your Point-to-Point Encryption system

Please select your P2PE solution from the list

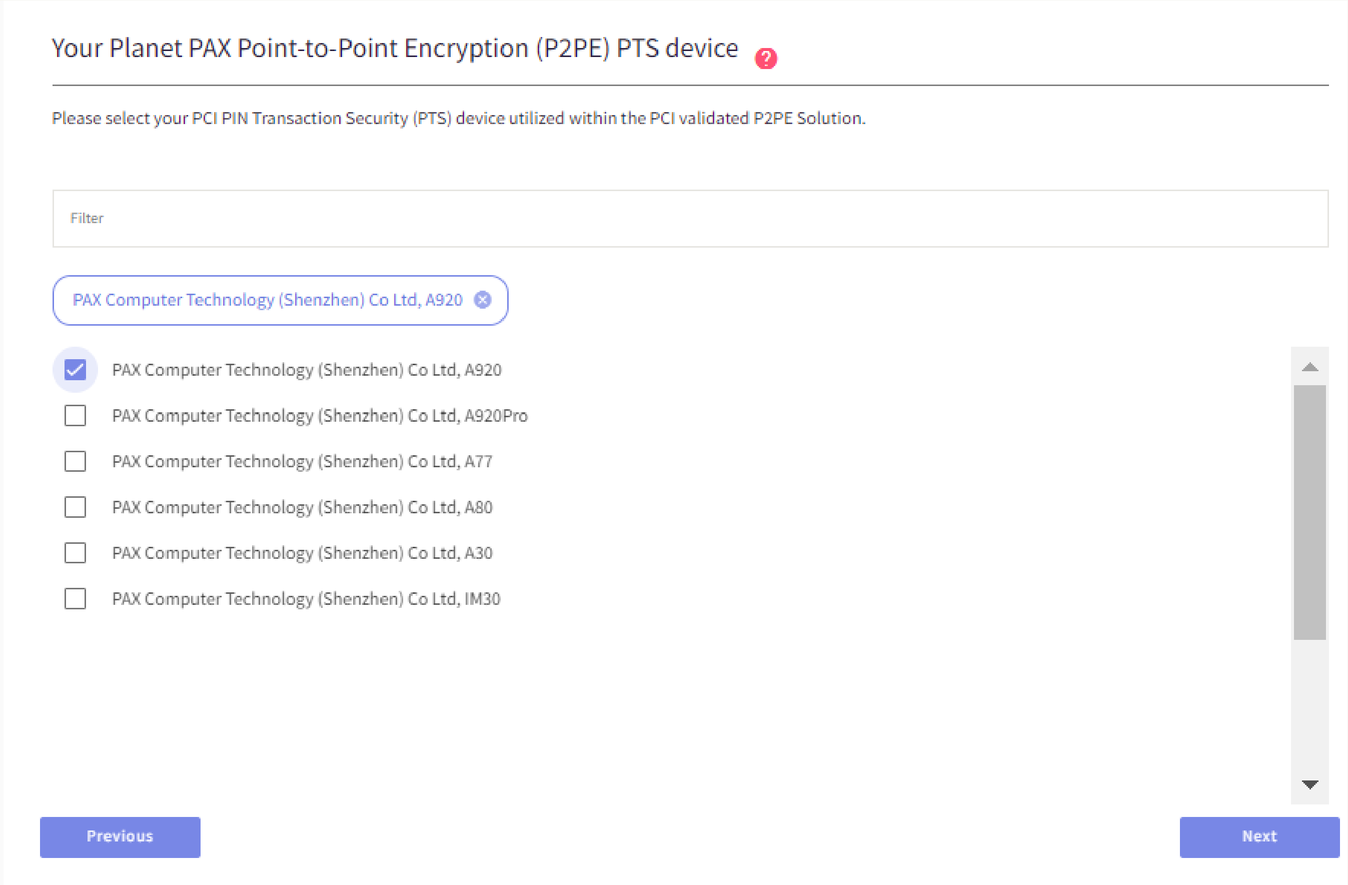
pax

□ Planet Payment Group Holdings Limited - Planet PAX Solution

- You will now be asked to input your Point-to-Point encrypted terminal.
- Please type ‘PAX’ within the search bar and select the option as shown here.

To change footer on all slides > go to Insert > Header Footer > Type detail > click Apply to all

SAQ P2PE User Guide



Your Planet PAX Point-to-Point Encryption (P2PE) PTS device

Please select your PCI PIN Transaction Security (PTS) device utilized within the PCI validated P2PE Solution.

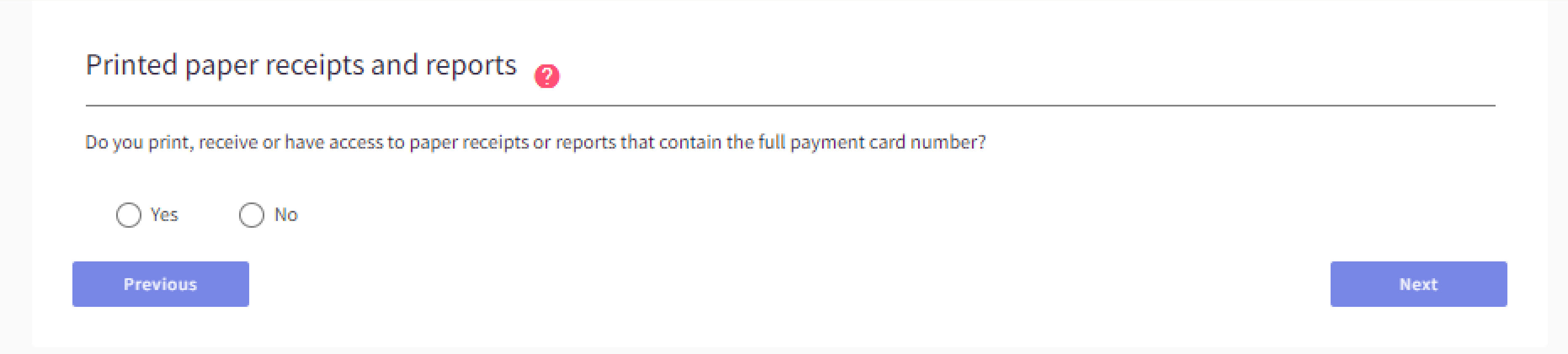
PAX Computer Technology (Shenzhen) Co Ltd, A920

☑ PAX Computer Technology (Shenzhen) Co Ltd, A920
□ PAX Computer Technology (Shenzhen) Co Ltd, A920Pro
□ PAX Computer Technology (Shenzhen) Co Ltd, A77
□ PAX Computer Technology (Shenzhen) Co Ltd, A80
□ PAX Computer Technology (Shenzhen) Co Ltd, A30
□ PAX Computer Technology (Shenzhen) Co Ltd, IM30

- Please select the above make and model of your terminal and then select ‘next’.

To change footer on all slides > go to Insert > Header Footer > Type detail > click Apply to all

SAQ P2PE User Guide



Printed paper receipts and reports

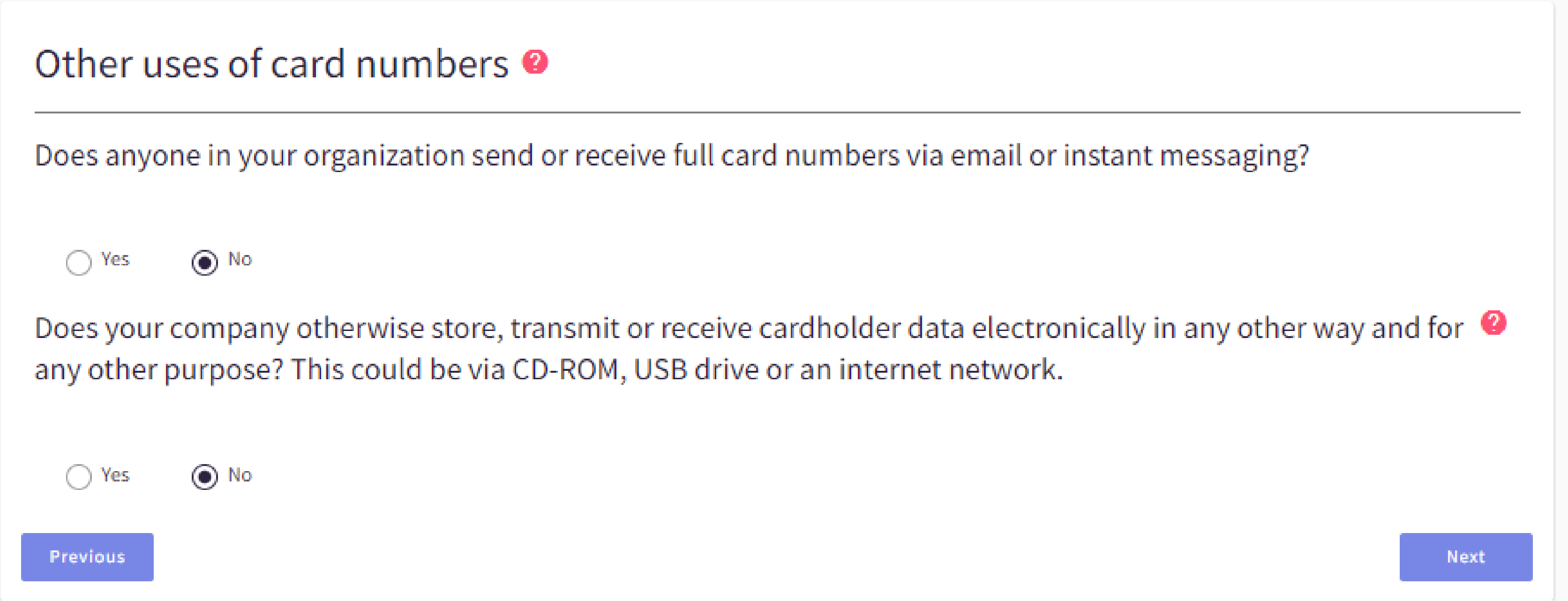
Do you print, receive or have access to paper receipts or reports that contain the full payment card number?

○ Yes ○ No

- If you do not have access to paper receipts or reports that contain the full card details of your customers, please select 'no'

SAQ P2PE User Guide

- In order to become compliant and maintain compliance – you must not send, receive, transmit or store card holder data electronically under any circumstances.
- If you store card holder data electronically, this puts your business and your customers data at risk to be hacked by malicious individuals.
- Both questions shown here must be answered as ‘no’.



Other uses of card numbers ?

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

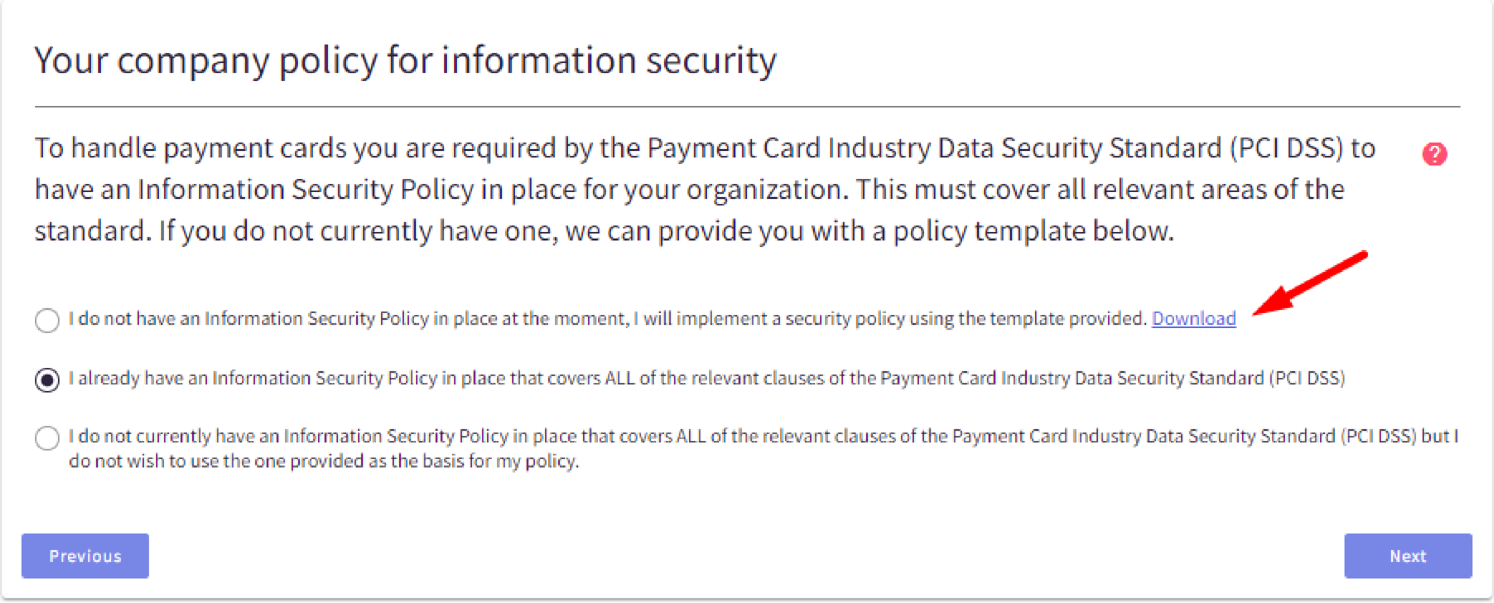
○ Yes ● No

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

SAQ P2PE User Guide

- In order to become and maintain compliance, you must have an Information Security Policy in place within your business.
- You can download this document via the hyperlink as shown.
- You must read, sign and date this document.
- If you have any employees who process card payments, they will also need to do the same.
- This document must be always kept on the business premises and reviewed annually.



Your company policy for information security

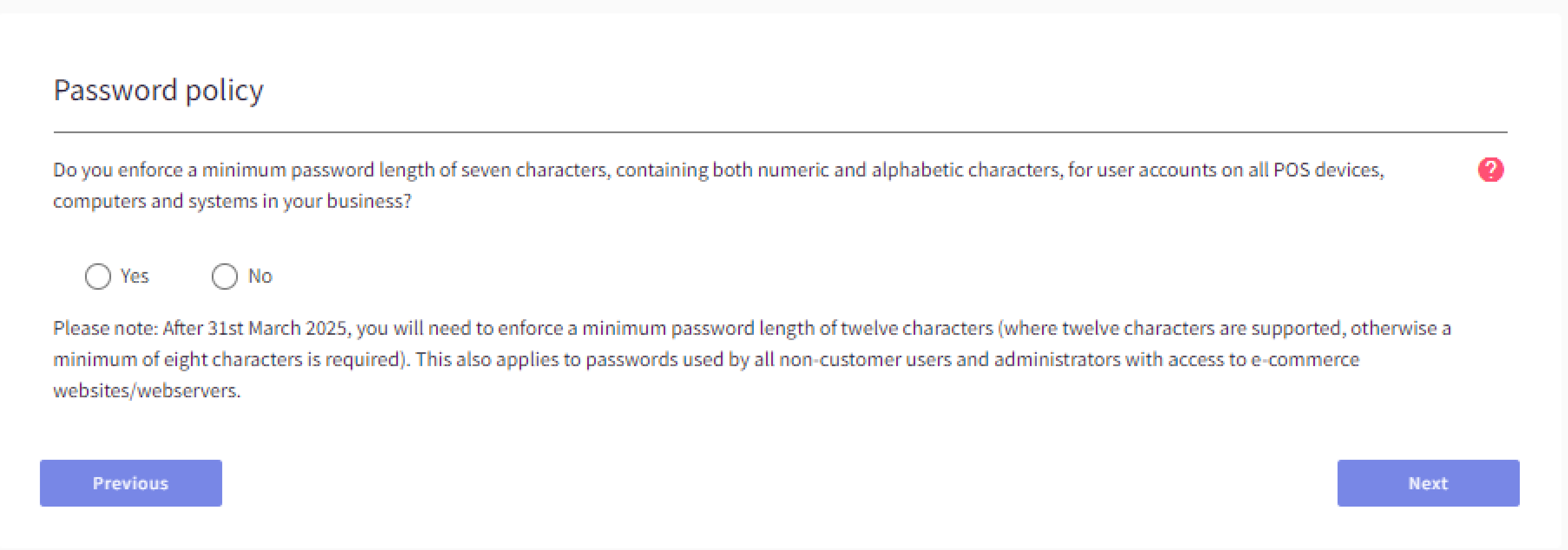
To handle payment cards you are required by the Payment Card Industry Data Security Standard (PCI DSS) to have an Information Security Policy in place for your organization. This must cover all relevant areas of the standard. If you do not currently have one, we can provide you with a policy template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

SAQ P2PE User Guide



Password policy

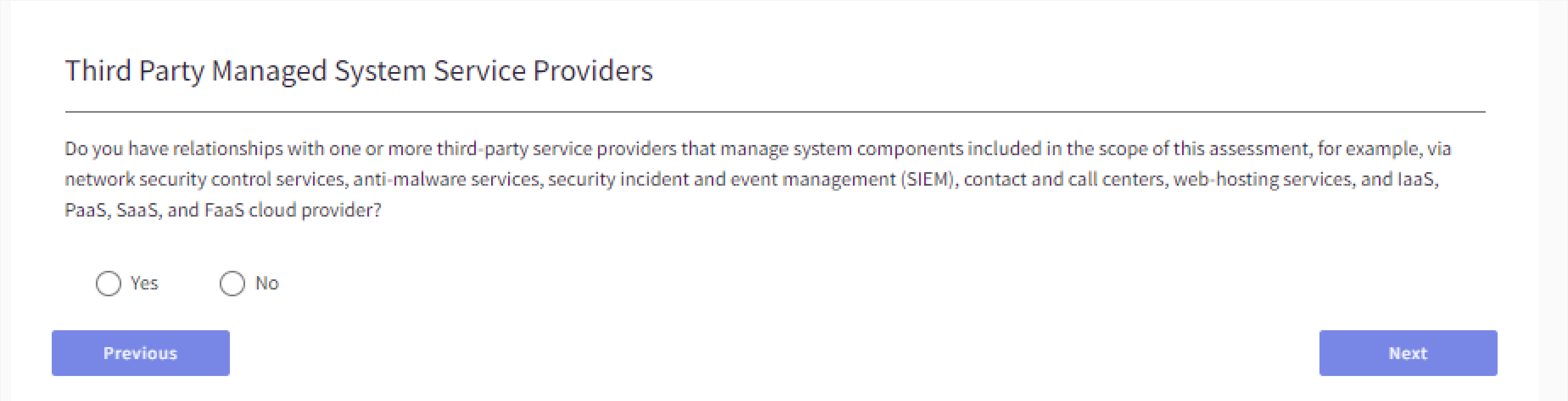
Do you enforce a minimum password length of seven characters, containing both numeric and alphabetic characters, for user accounts on all POS devices, computers and systems in your business?

○ 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/webservers.

- From March 31st 2025, you will be required to update the password requirements within your business to ensure that it is protected from malicious individuals.
- Anyone who has administrator access to your website will be required to have a password length of twelve characters, rather than eight.
- As this is a future dated requirement, this question will not affect the overall status of your compliance.
- Please answer this question as it applies to your business today.

SAQ P2PE User Guide



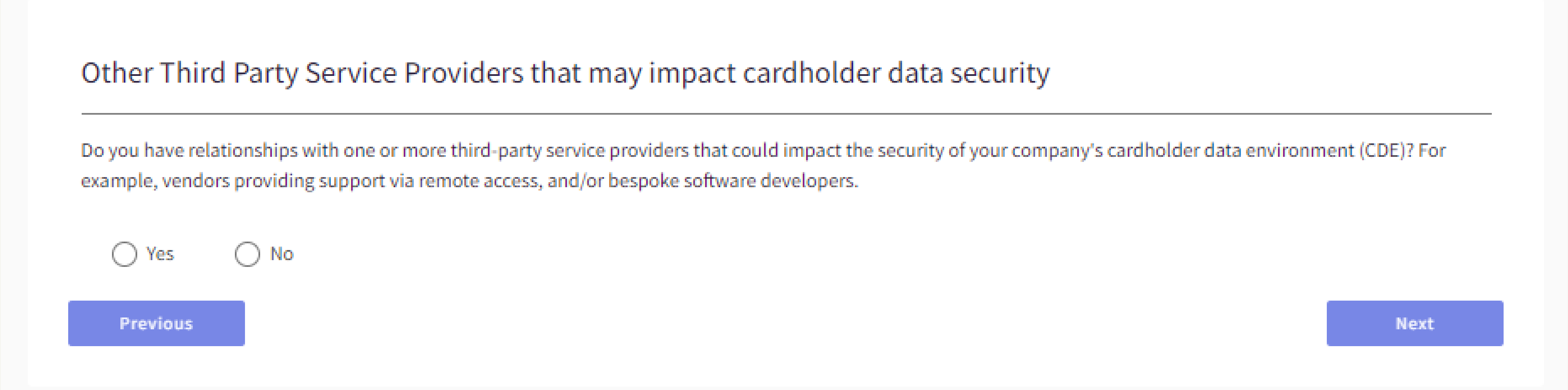
Third Party Managed System Service Providers

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

- If Paysafe is your only service provider, then please answer the above question as ‘no.

SAQ P2PE User Guide



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

- If you do not have any third party vendors that remotely access the systems within your business, please select ‘no’ to the question above.

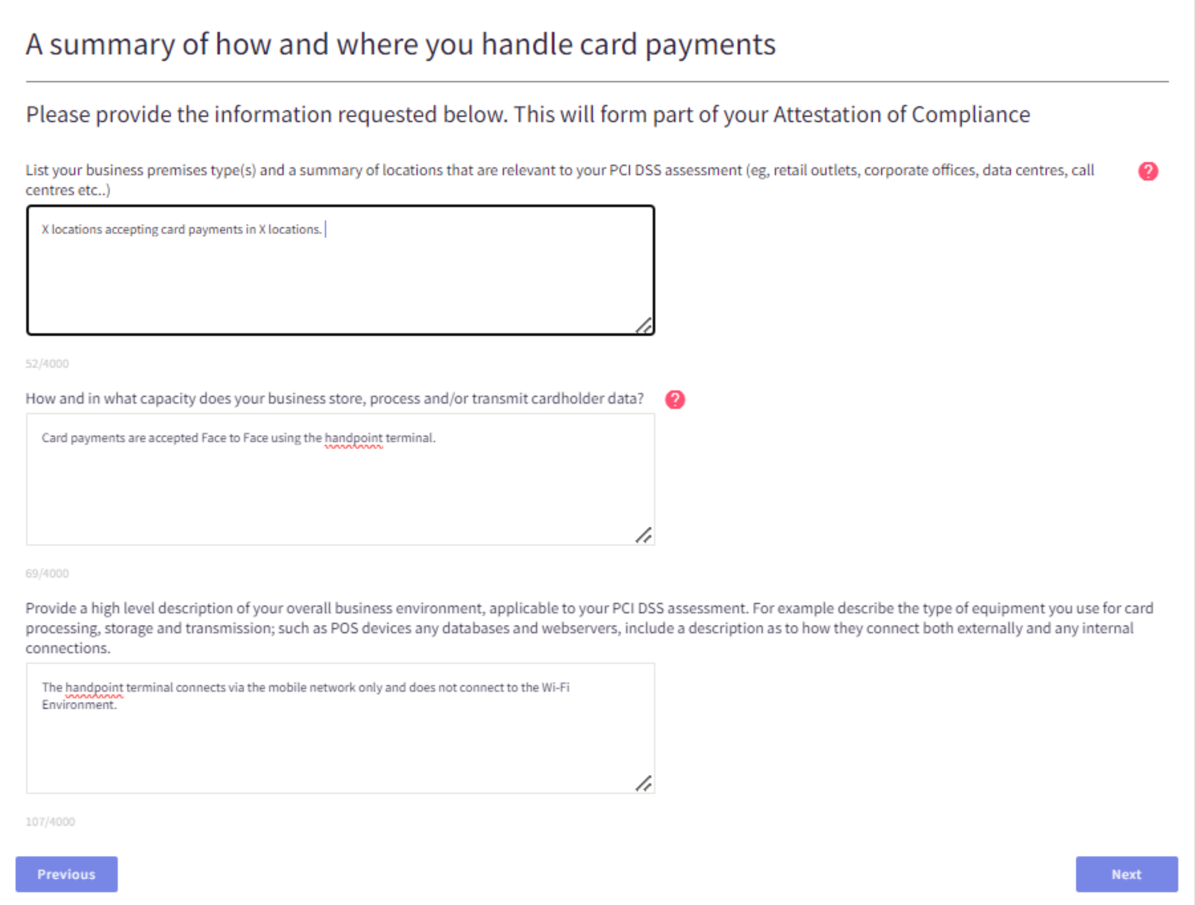
SAQ P2PE User Guide

The last stage of profile will ask you to provide a summary of how and where you handle card payments.

The main points to cover within each box is a summary of the information you have previously answered within this section.

You can include information such as:

- Your payment acceptance method.
- Who owns the solution you are using.
- Confirmation that you maintain the security of your system via relevant security patches.
- How many employee’s process payments on your behalf.



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..) ?

X locations accepting card payments in X locations.

52/4000

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

Card payments are accepted Face to Face using the handpoint terminal.

69/4000

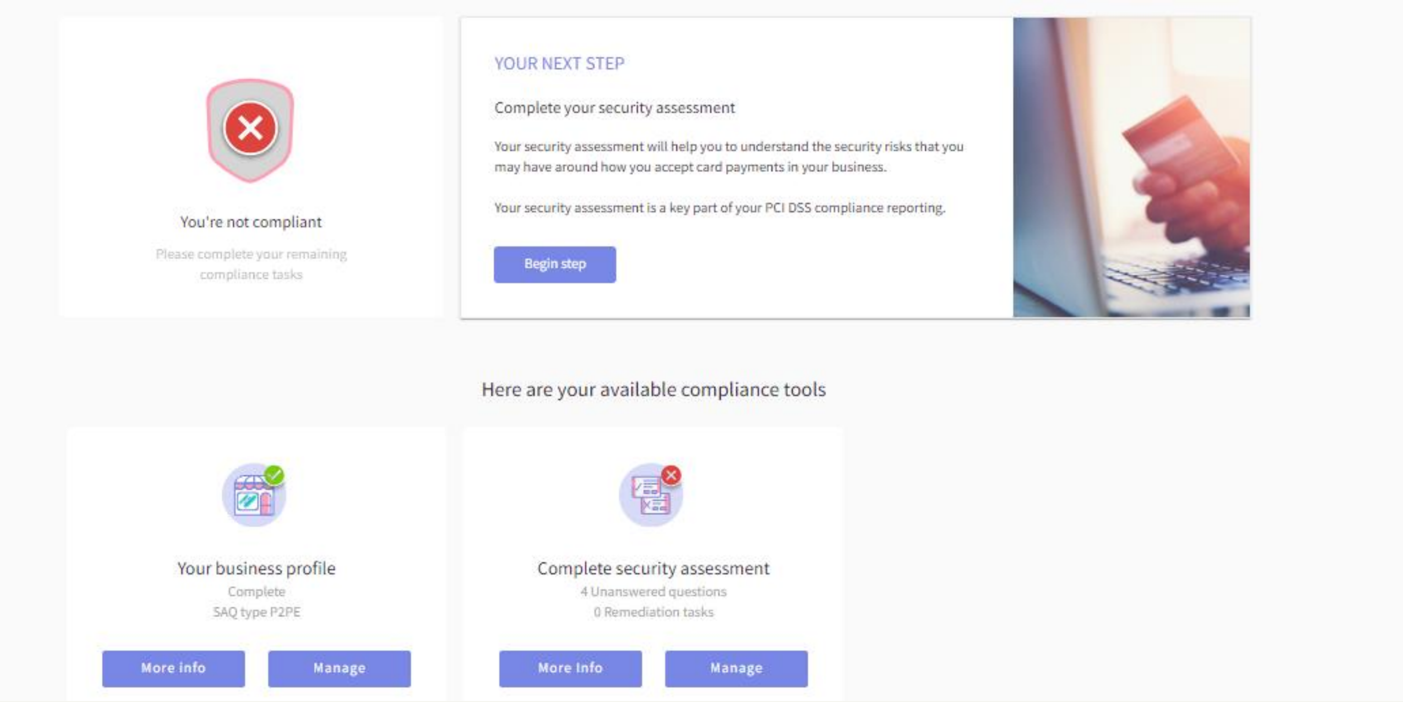
Provide a high level description of your overall business environment, applicable to your PCI DSS assessment. For example describe the type of equipment you use for card processing, storage and transmission; such as POS devices any databases and webservers, include a description as to how they connect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

The handpoint terminal connects via the mobile network only and does not connect to the Wi-Fi Environment.

107/4000

SAQ P2PE User Guide

- Once all steps have been completed as listed within this guide, you will then be met with the following screen.
- You will see that there are just four questions outstanding within the Self Assessment Questionnaire.
- Please select ‘manage’ within the complete security assessment widget in order to proceed.



You're not compliant

Please complete your remaining compliance tasks

YOUR NEXT STEP

Complete your security assessment

Your security assessment will help you to understand the security risks that you may have around how you accept card payments in your business.

Your security assessment is a key part of your PCI DSS compliance reporting.

Here are your available compliance tools

Your business profile

Complete

SAQ type P2PE

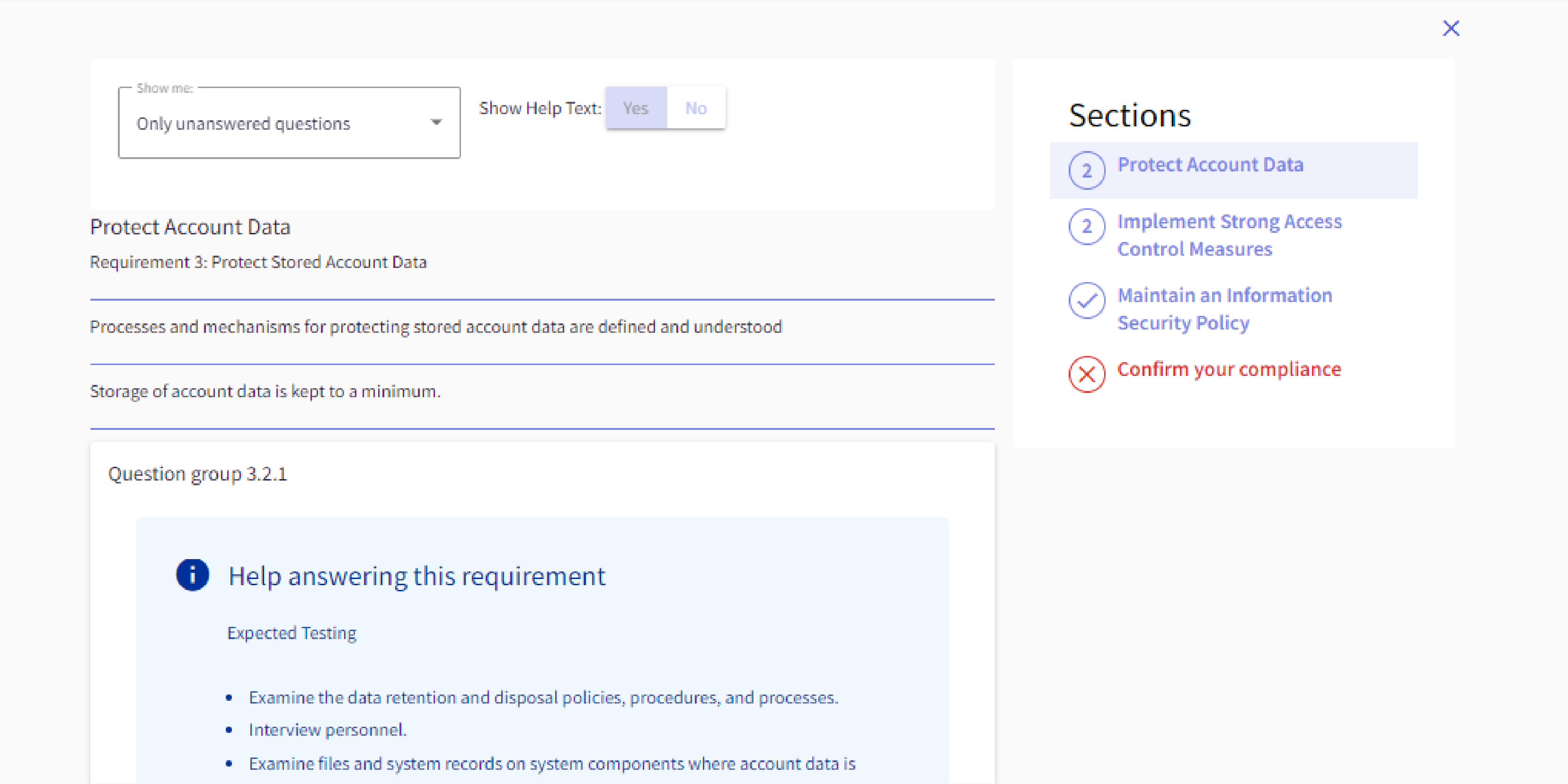
Complete security assessment

4 Unanswered questions

0 Remediation tasks

SAQ P2PE User Guide

- Once you have selected 'manage' and then 'answet now', you will be met with this screen.
- You will see that there are two questions within the Protect Account Data 'section', alongside, two questions within the Implement Strong Access Control Measures.



Show me: Only unanswered questions

Show Help Text: Yes No

Protect Account Data

Requirement 3: Protect Stored Account Data

Processes and mechanisms for protecting stored account data are defined and understood

Storage of account data is kept to a minimum.

Question group 3.2.1

Help answering this requirement

Expected Testing

- Examine the data retention and disposal policies, procedures, and processes.
- Interview personnel.
- Examine files and system records on system components where account data is

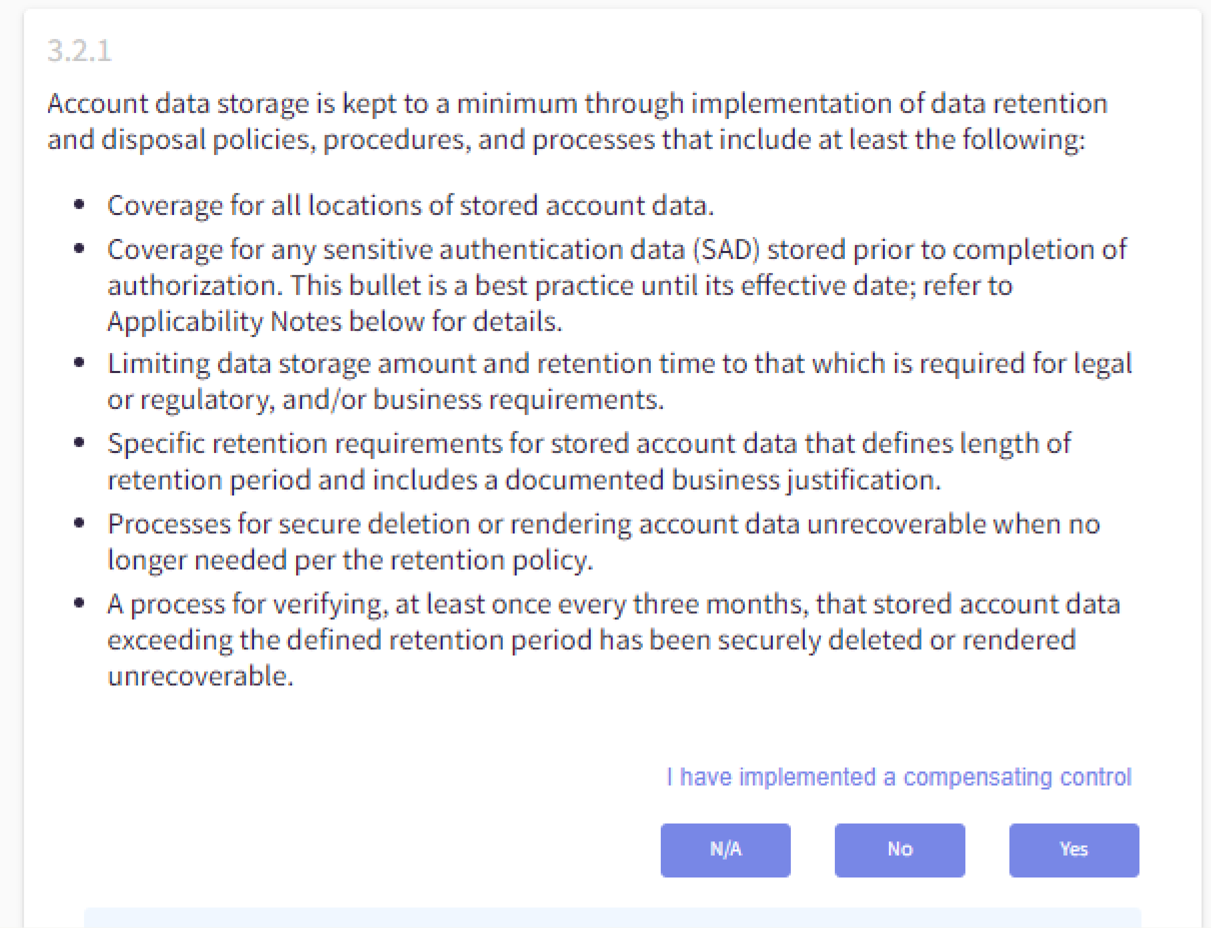
Sections

- 2 Protect Account Data
- 2 Implement Strong Access Control Measures
- ✓ Maintain an Information Security Policy
- ✕ Confirm your compliance

SAQ P2PE User Guide

- This question is asking you to confirm if you have a data retention policy in place that covers all locations of your businesses that may store sensitive information.

- If you do not store any sensitive card holder information anywhere within the business, please answer this question as ‘N/A’ and input this as the reasoning.



3.2.1

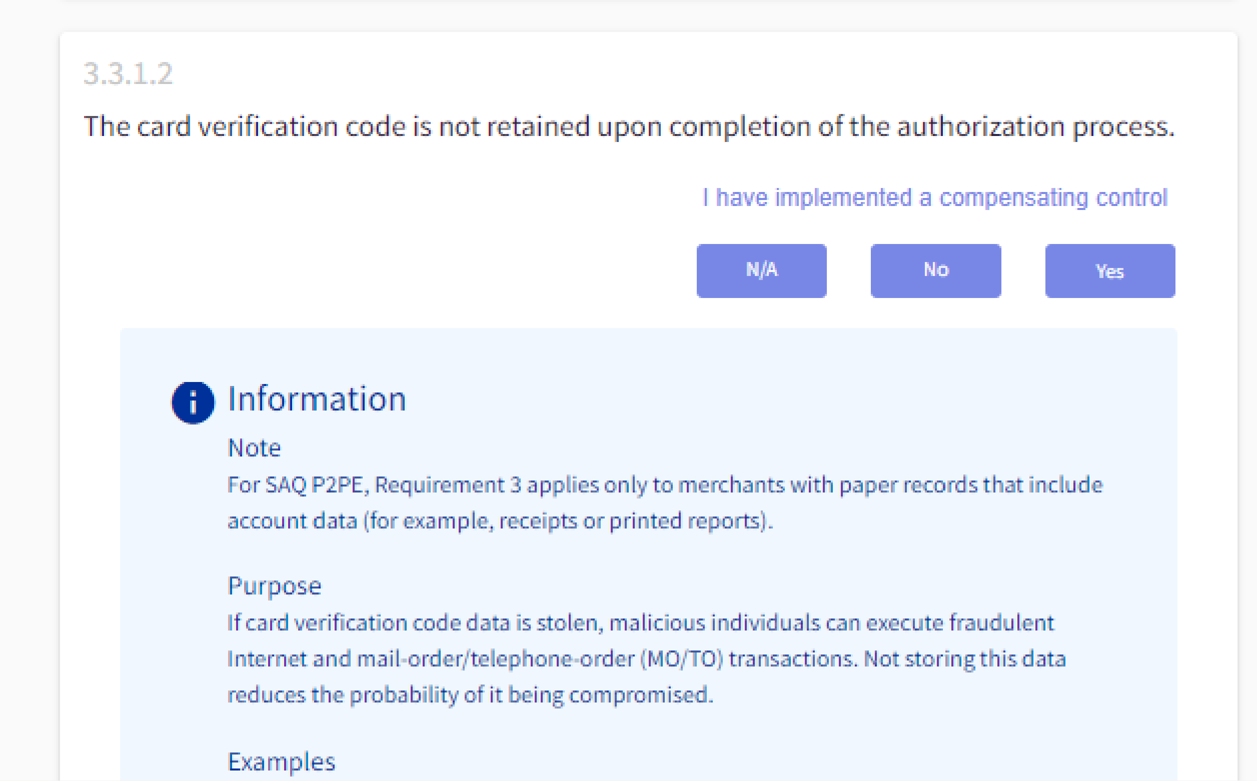
Account data storage is kept to a minimum through implementation of data retention and disposal policies, procedures, and processes that include at least the following:

- 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.

SAQ P2PE User Guide

- This question is asking you to confirm that you do not store the CVV/CVV2 code once the transaction has been processed.

- If you do not store this code, then please answer this question as ‘yes’,



3.3.1.2

The card verification code is not retained upon completion of the authorization process.

Information

Note

For SAQ P2PE, Requirement 3 applies only to merchants with paper records that include account data (for example, receipts or printed reports).

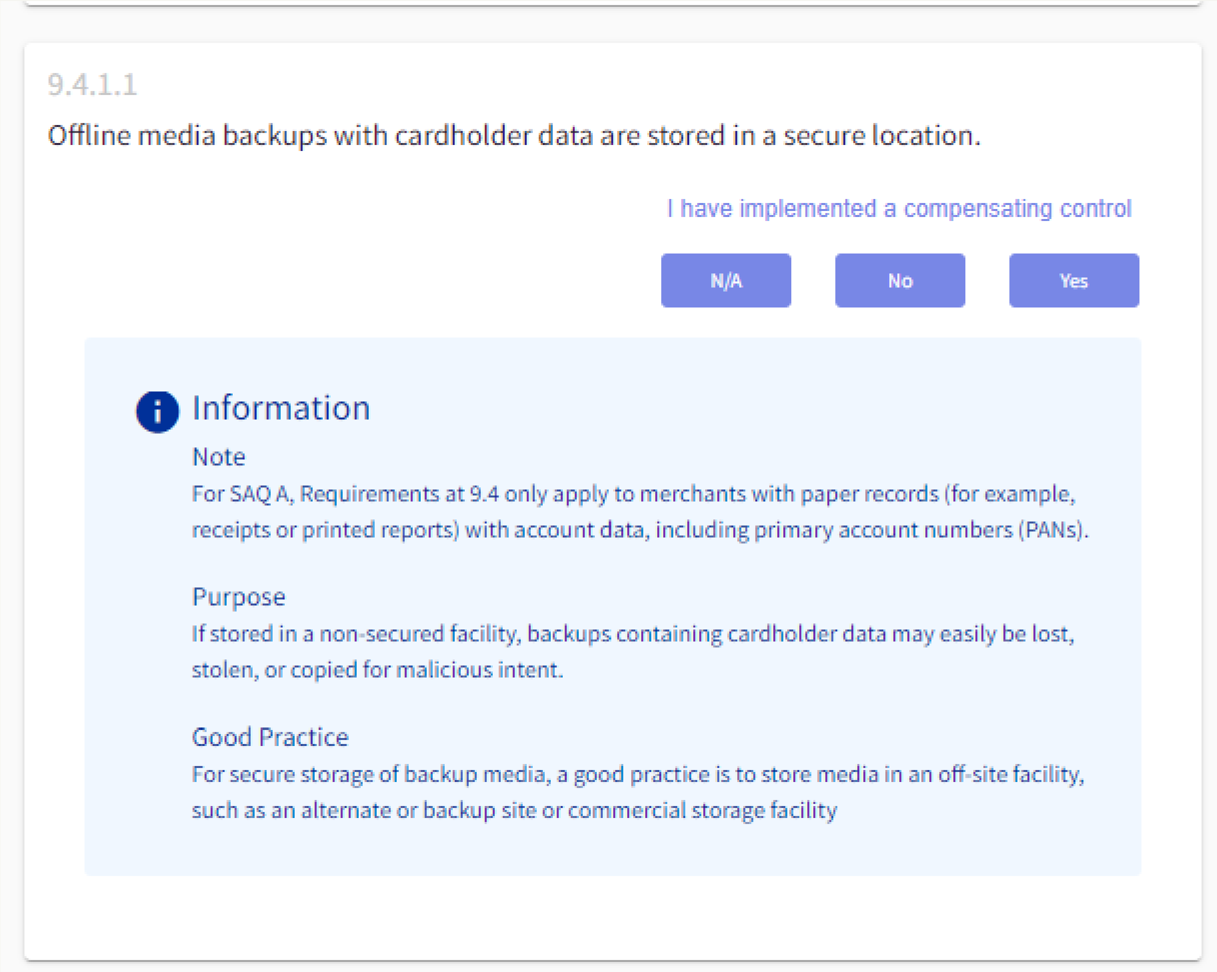
Purpose

If card verification code data is stolen, malicious individuals can execute fraudulent Internet and mail-order/telephone-order (MO/TO) transactions. Not storing this data reduces the probability of it being compromised.

Examples

SAQ P2PE User Guide

- If you are not storing any card holder data within any systems, you can answer this question as 'N/A' and input this as the reasoning.



9.4.1.1

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

Information

Note

For SAQ A, Requirements at 9.4 only apply to merchants with paper records (for example, receipts or printed reports) with account data, including primary account numbers (PANs).

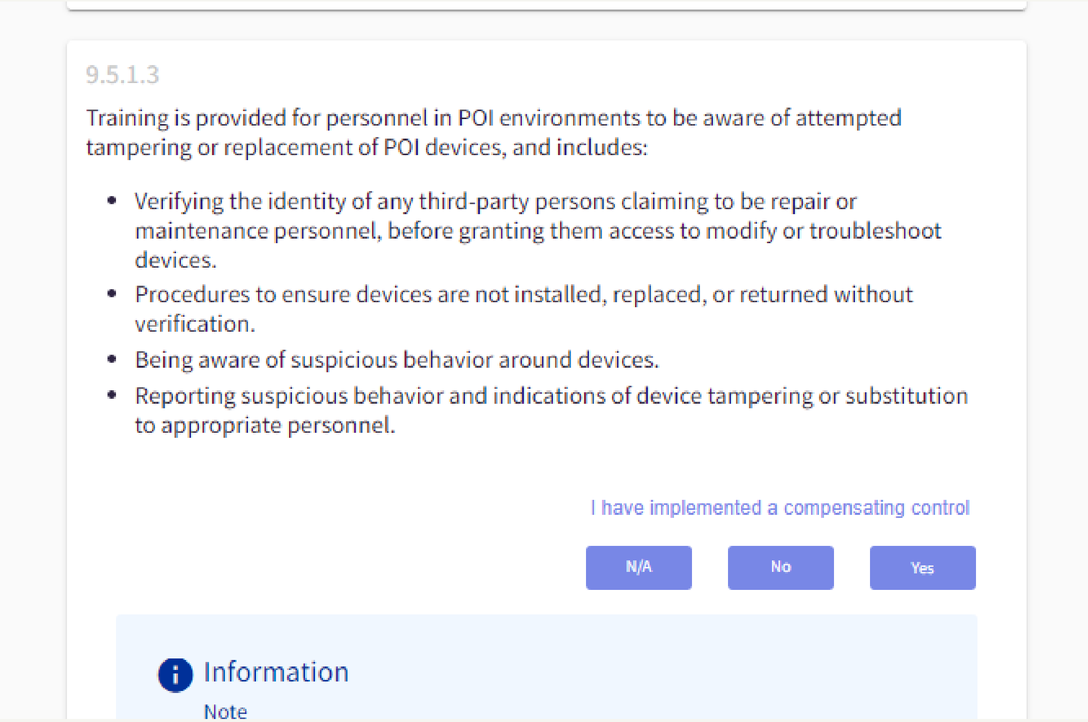
Purpose

If stored in a non-secured facility, backups containing cardholder data may easily be lost, stolen, or copied for malicious intent.

Good Practice

For secure storage of backup media, a good practice is to store media in an off-site facility, such as an alternate or backup site or commercial storage facility

SAQ P2PE User Guide



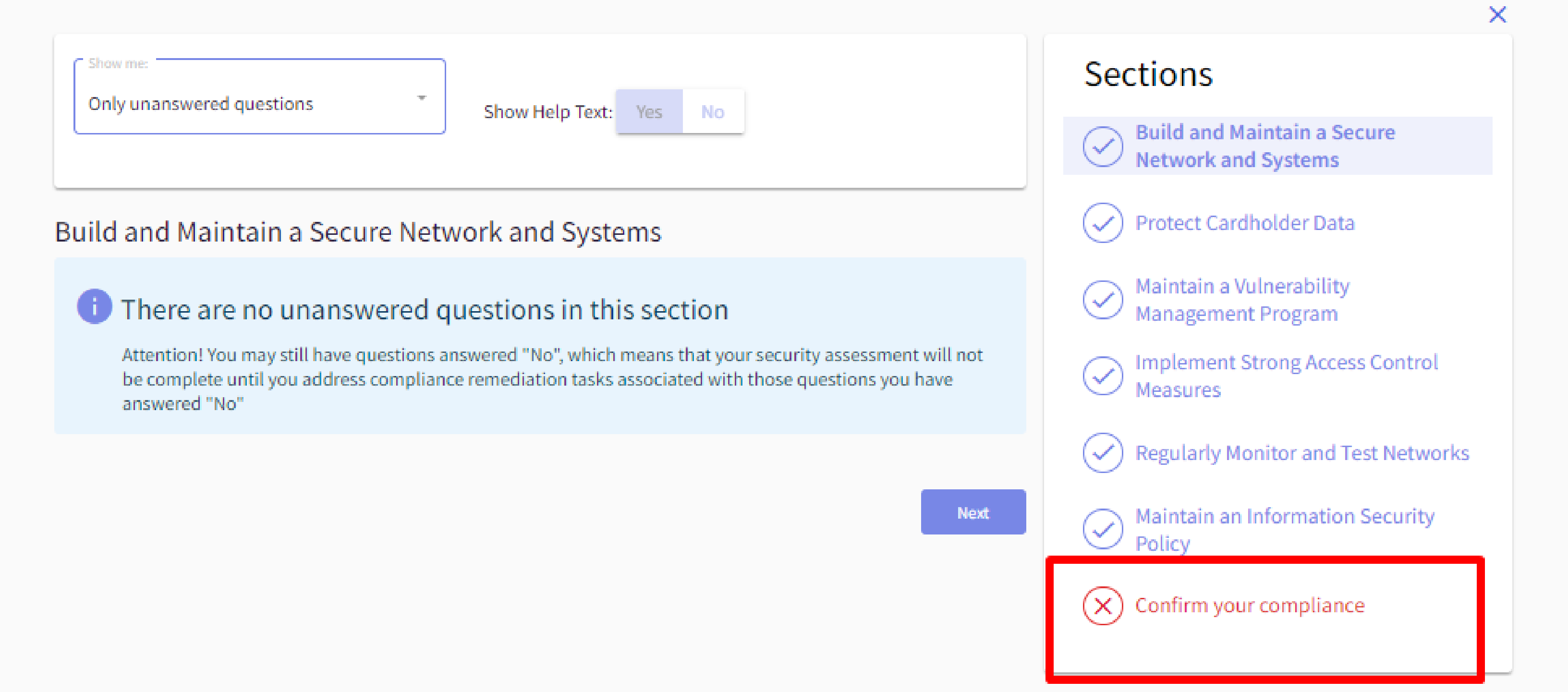
9.5.1.3

Training is provided for personnel in POI environments to be aware of attempted tampering or replacement of POI devices, and includes:

- Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, before granting them access to modify or troubleshoot devices.
- Procedures to ensure devices are not installed, replaced, or returned without verification.
- Being aware of suspicious behavior around devices.
- Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel.

- This question is asking you to confirm that your staff have adequate knowledge to review your card terminal to confirm it has not been tampered with.
- If your staff regularly check the card terminal to ensure it has not been swapped out with another device and check to see if all components have not been tampered with, please answer this question as ‘yes’.

SAQ P2PE User Guide



Show me:
Only unanswered questions

Show Help Text: Yes No

Build and Maintain a Secure Network and Systems

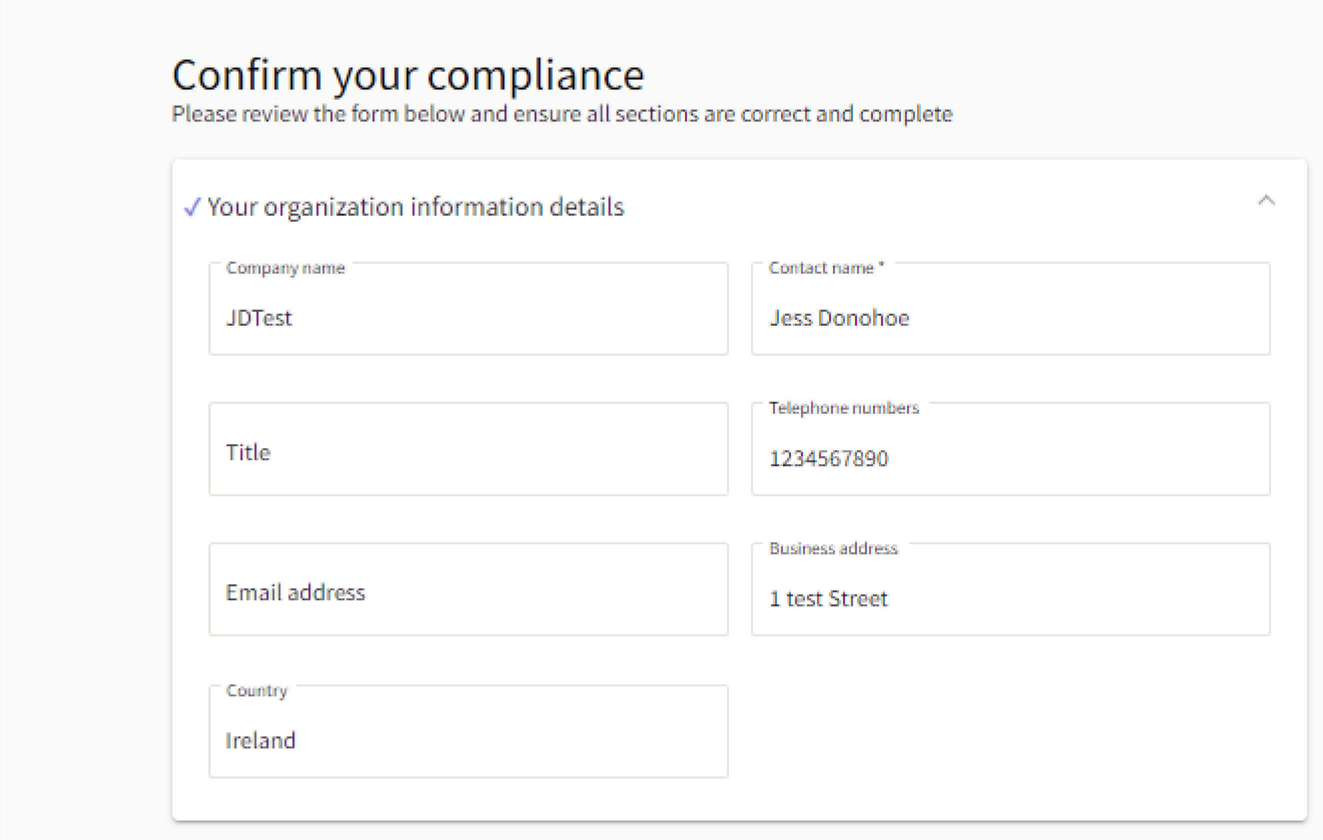
There are no unanswered questions in this section

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
Sections
Build and Maintain a Secure Network and Systems
Protect Cardholder Data
Maintain a Vulnerability Management Program
Implement Strong Access Control Measures
Regularly Monitor and Test Networks
Maintain an Information Security Policy
Confirm your compliance

- Once all questions are answered within this section – you can then confirm your compliance and complete one final item before becoming validated for the forthcoming year.
- Please select the ‘confirm your compliance’ section as highlighted in the red box above.

SAQ P2PE User Guide



Confirm your compliance

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

✓ Your organization information details

Company name: JDTest

Contact name *: Jess Donohoe

Title

Telephone numbers: 1234567890

Email address

Business address: 1 test Street

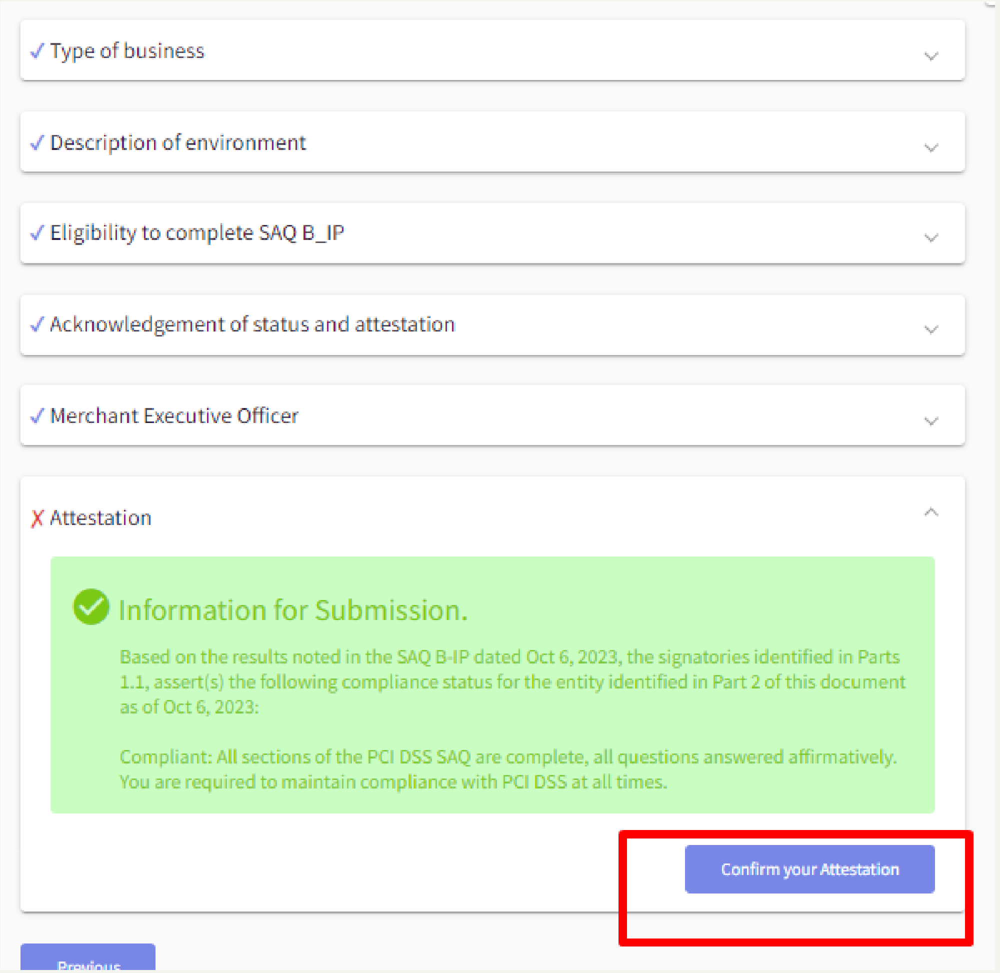
Country: Ireland

- You will need to review the contact information as this will be added to the e-signature of your attestation of compliance documentation.

- Please ensure to fill in all details.

SAQ P2PE User Guide

- Once you have updated the contact information, please scroll down and click the button as shown.



✓ Type of business

✓ Description of environment

✓ Eligibility to complete SAQ B_IP

✓ Acknowledgement of status and attestation

✓ Merchant Executive Officer

✗ Attestation

Information for Submission.

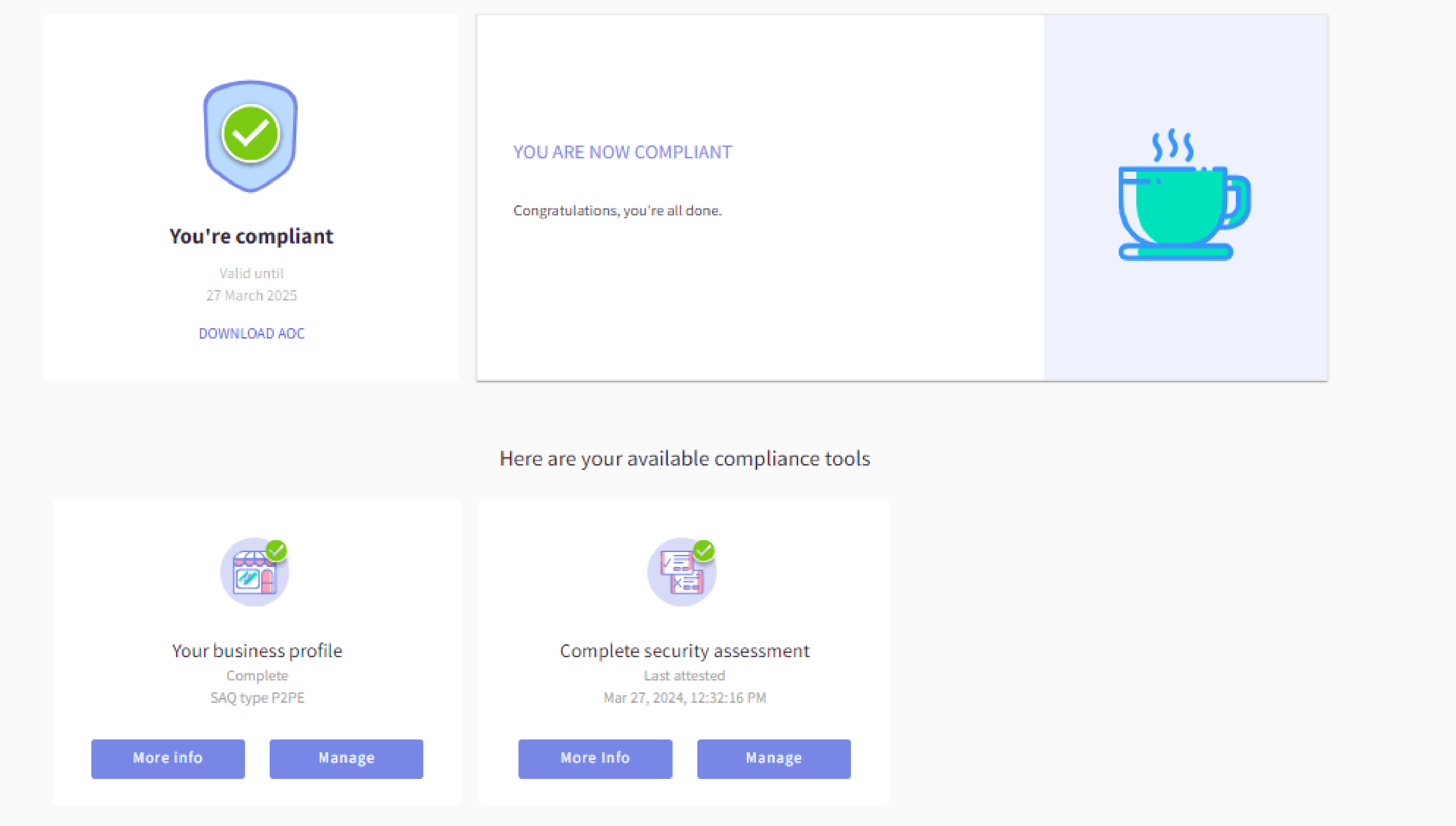
Based on the results noted in the SAQ B-IP dated Oct 6, 2023, the signatories identified in Parts 1.1, assert(s) the following compliance status for the entity identified in Part 2 of this document as of Oct 6, 2023:

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.

SAQ P2PE User Guide

Once all stages are completed – you will then be redirected to this screen to advise that you are now compliant for the forthcoming year.

If there is anything outstanding throughout the year, the PCI portal will email you to advise that action is required.



You're compliant

Valid until
27 March 2025

DOWNLOAD AOC

YOU ARE NOW COMPLIANT

Congratulations, you're all done.

Here are your available compliance tools

Your business profile
Complete
SAQ type P2PE

Complete security assessment
Last attested
Mar 27, 2024, 12:32:16 PM