SecureTrust P2PE Instruction Guide

Purpose: These instructions will assist in registering your account for PCI compliance, validating PCI Compliance readiness, and completing the annual PCI questionnaire when using Point-to-Point Encrypted (P2PE) devices.

Disclosure: For use of ID Tech M130s, Wind River Payments is willing to accept PCI Self- Assessment Questionnaire P2PE as a reduced compliance questionnaire. This is despite the ID Tech M130 encrypted keypad not being officially certified by the PCI Council, which is required to reduce PCI scope. This is an option we are extending to customers based on this very secure credit card processing solution. Your business maintains the option to validate PCI compliance to the full extent of the PCI Standard.

Contents

Login and Registration

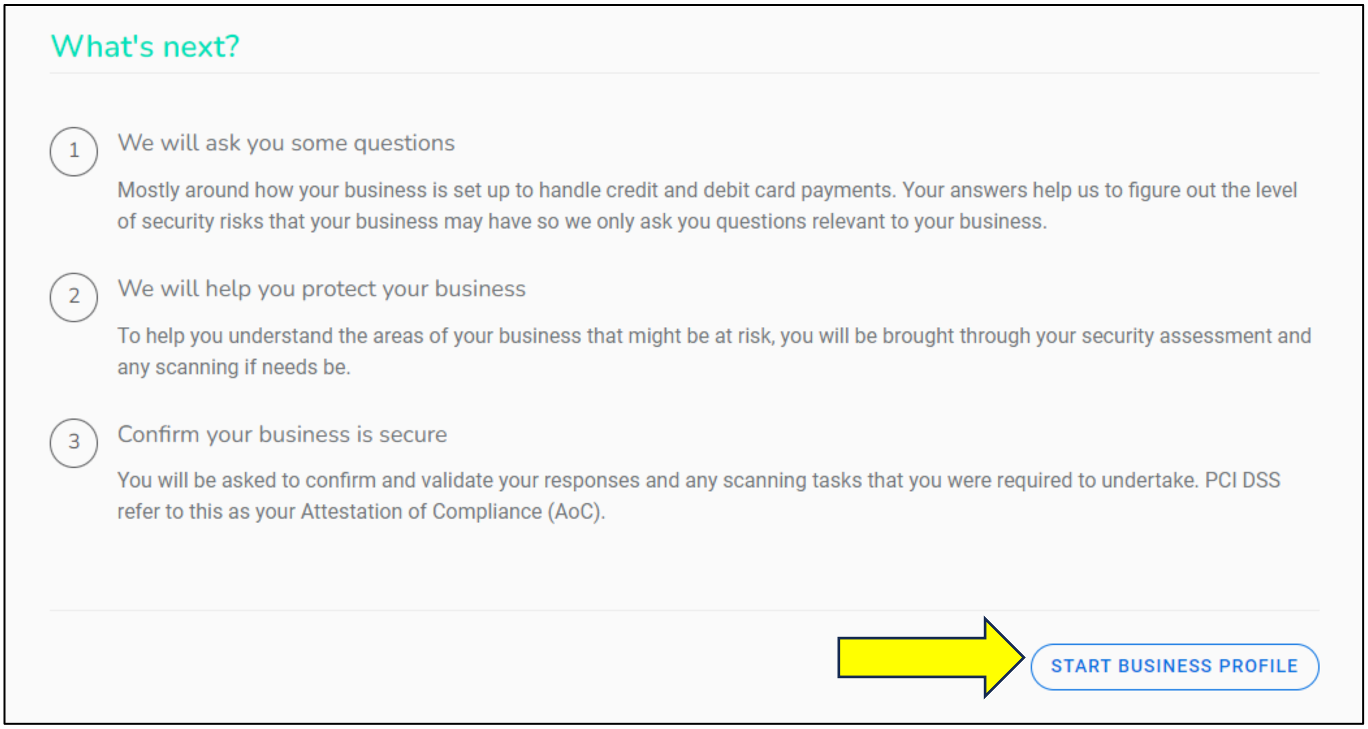
Use the log-in credentials you received in the preregistration email from SecureTrust.

Click the “**Register Now!**” link, and use the information contained in the email to complete registration.

Business Profile:

Once registration is complete, you will begin completing the business profile.

1. Click **Start Business Profile** in the lower right of this screen to begin.



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.

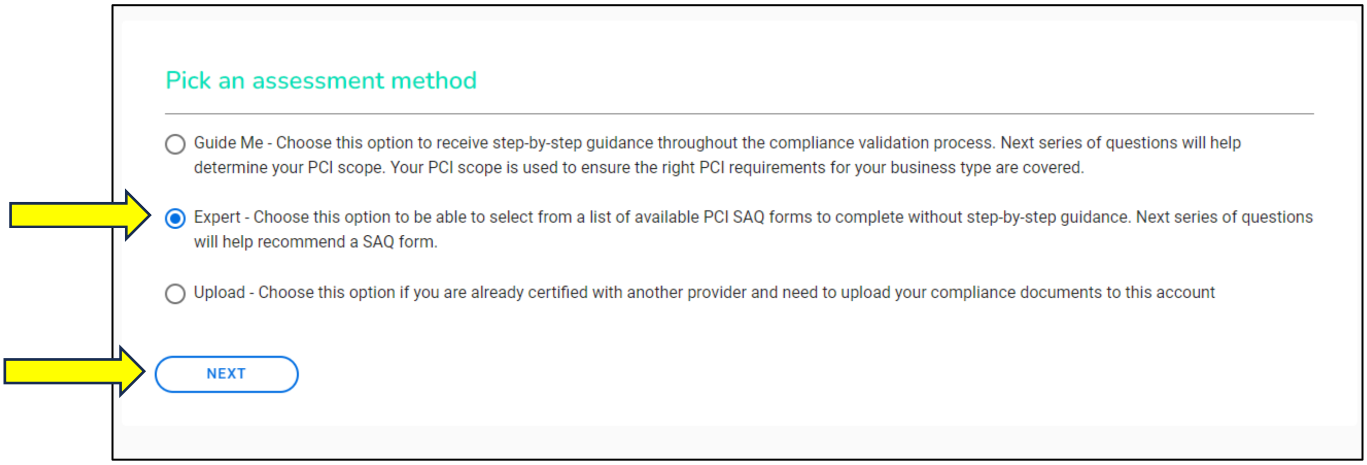
2 We will help you protect your business

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).

2. On the following screen, choose **Expert** for the assessment method, and click **Next**.



Pick an an assessment method

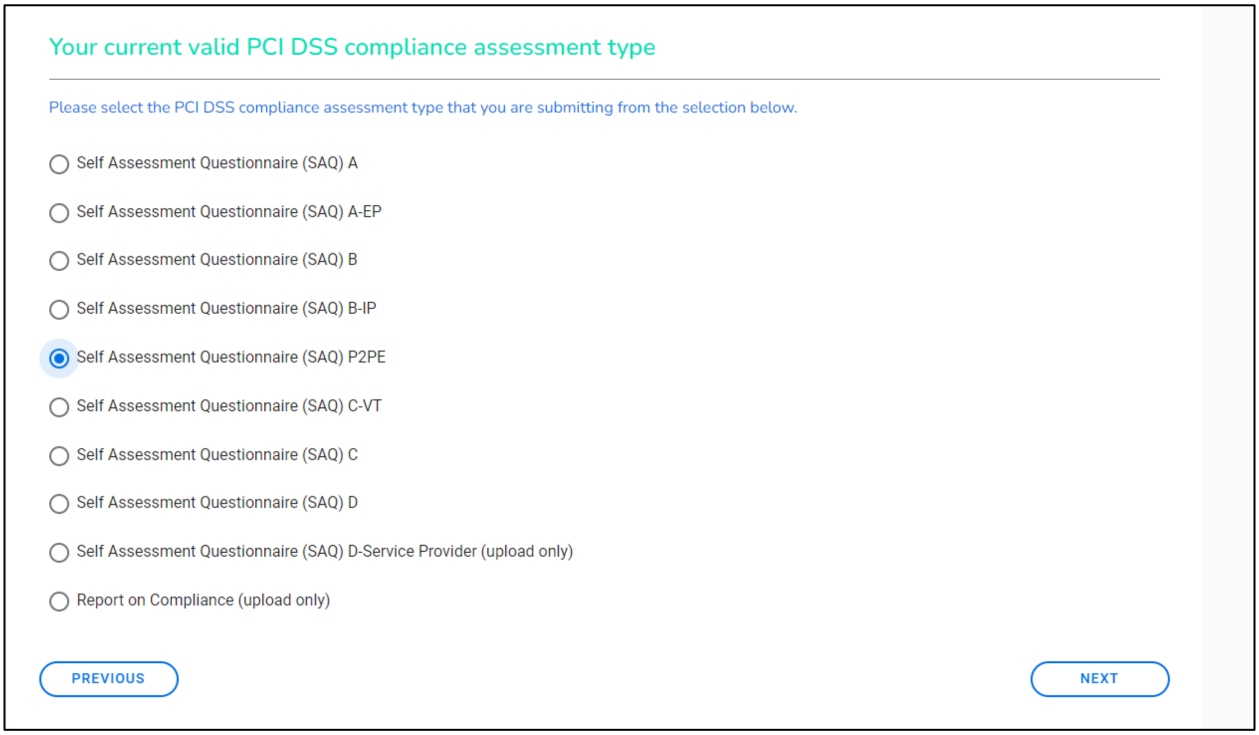
○ Guide Me - Choose this option to receive step-by-step guidance throughout the compliance validation process. Next series of questions will help determine your PCI scope. Your PCI scope is used to ensure the right PCI requirements for your business type are covered.

● Expert - Choose this option to be able to select from a list of available PCI SAQ forms to complete without step-by-step guidance. Next series of questions will help recommend a SAQ form.

○ Upload - Choose this option if you are already certified with another provider and need to upload your compliance documents to this account

3. This will display a listing of all the Self-Assessment Questionnaires (SAQ). Select **Self-Assessment Questionnaire (SAQ) P2PE**.

4. Click **Next**.



Your current valid PCI DSS compliance assessment type

Please select the PCI DSS compliance assessment type that you are submitting from the selection below.

○ Self Assessment Questionnaire (SAQ) A

○ Self Assessment Questionnaire (SAQ) A-EP

○ Self Assessment Questionnaire (SAQ) B

○ Self Assessment Questionnaire (SAQ) B-IP

● Self Assessment Questionnaire (SAQ) P2PE

○ Self Assessment Questionnaire (SAQ) C-VT

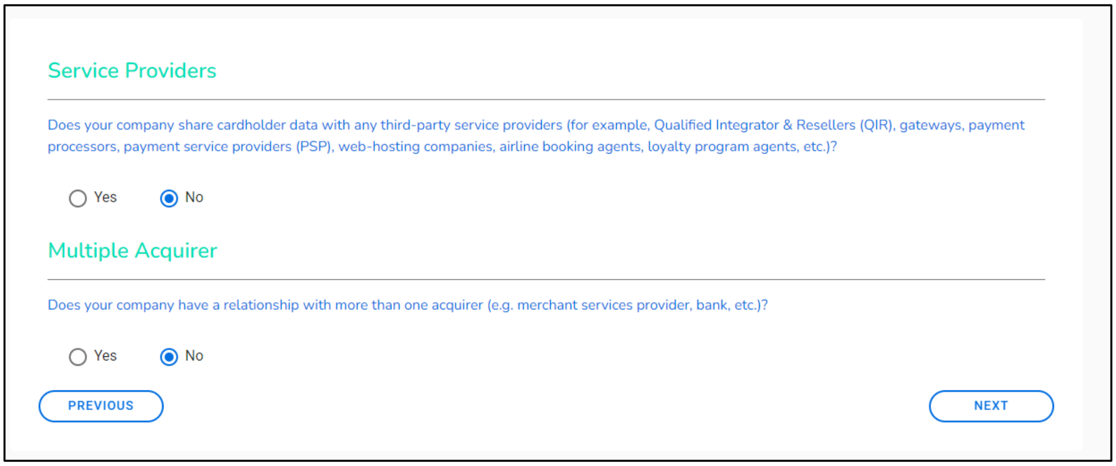
○ Self Assessment Questionnaire (SAQ) C

○ Self Assessment Questionnaire (SAQ) D

○ Self Assessment Questionnaire (SAQ) D-Service Provider (upload only)

○ Report on Compliance (upload only)

5. Answer the following Service Provider and Password Policy questions and click **Next**.



Service Providers

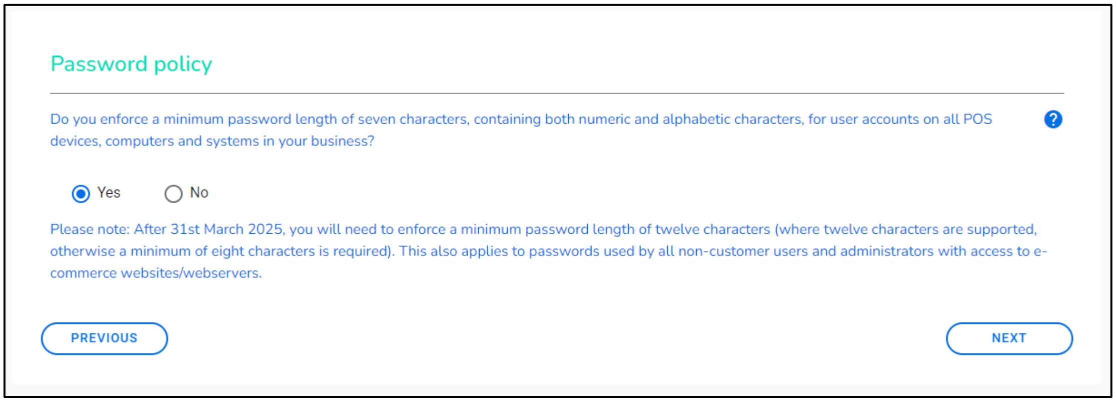
Does your company share cardholder data with any third-party service providers (for example, Qualified Integrator & Resellers (QIR), gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.)?

○ Yes ● No

Multiple Acquirer

Does your company have a relationship with more than one acquirer (e.g. merchant services provider, bank, etc.)?

○ Yes ● No

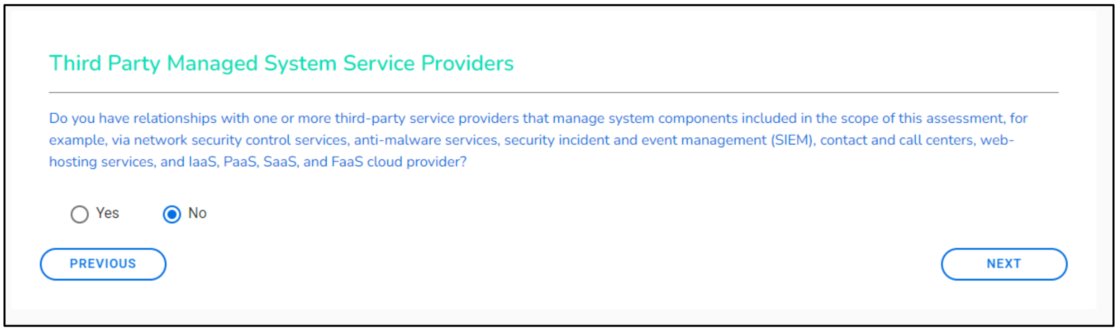


Password policy

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

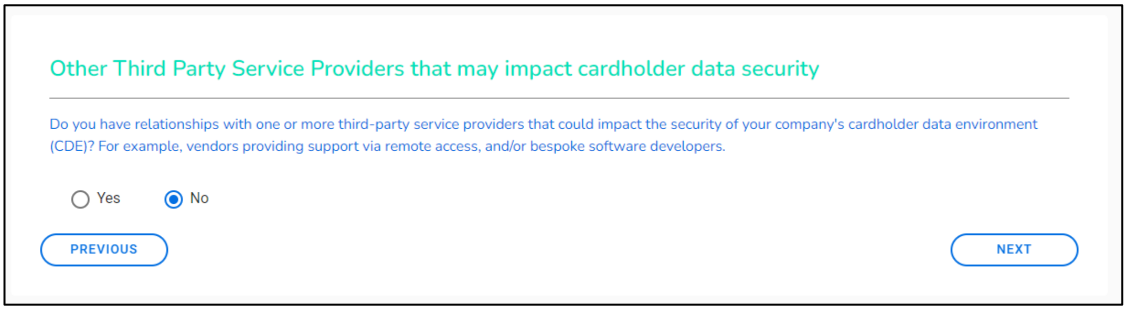
Please note: After 31st March 2025, you will need to enforce a minimum password length of twelve characters (where twelve characters are supported, otherwise a minimum of eight characters is required). This also applies to passwords used by all non-customer users and administrators with access to e-commerce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



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

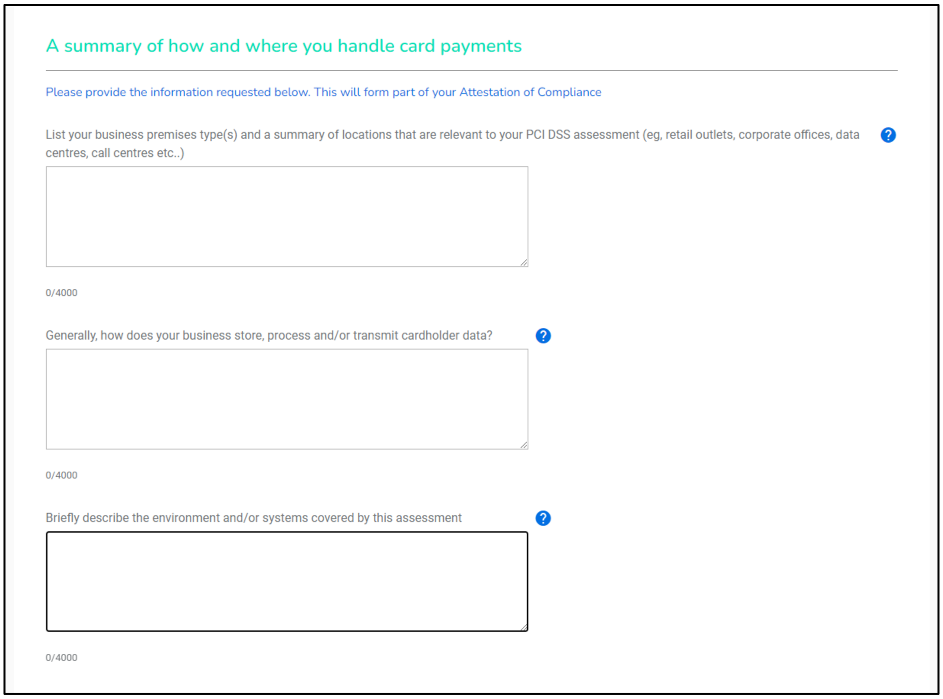


Other Third Party Service Providers that may impact cardholder data security

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

6. On the next screen, answer the free-form questions regarding how your business handles card payments and click **Next** when complete.
    a. All questions must be answered before moving to the next question.



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..) ?

0/4000

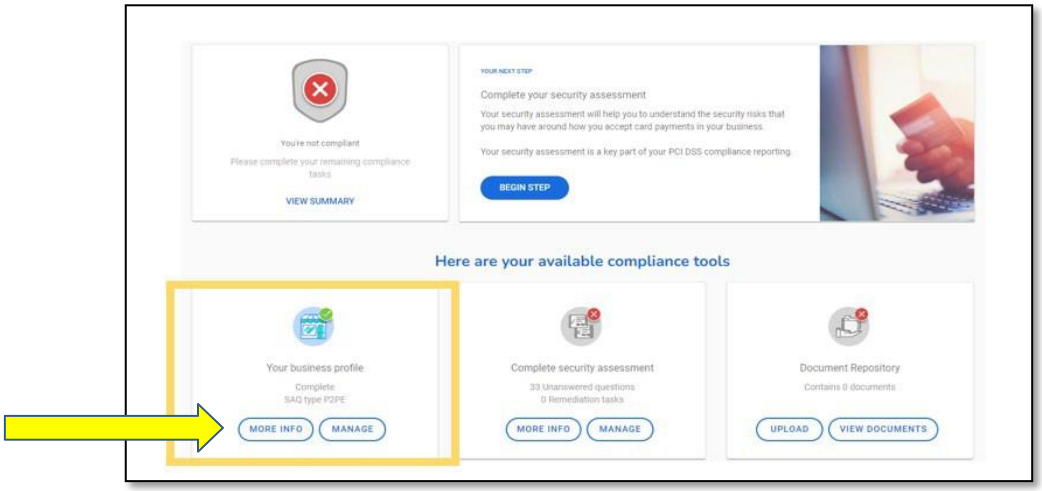
Generally, how does your business store, process and/or transmit cardholder data? ?

0/4000

Briefly describe the environment and/or systems covered by this assessment ?

0/4000

7. After clicking **Next**, the main PCI Dashboard will appear, and **Your Business Profile** should be marked as **Complete**.
    a. If this section does not display as complete, select **Manage** and review the section again for completeness.



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

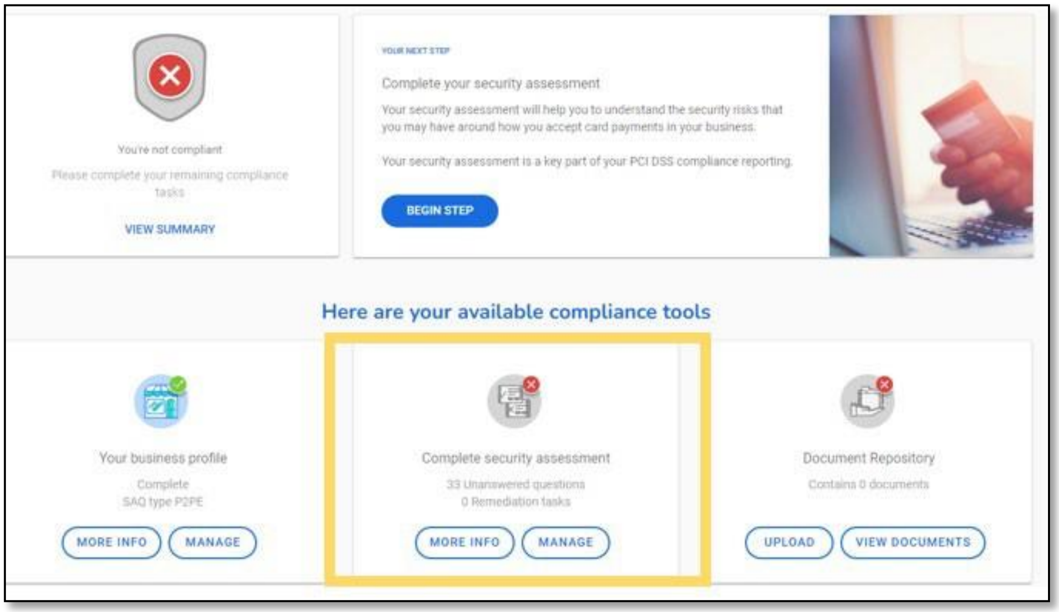
33 Unanswered questions
0 Remediation tasks

Document Repository

Contains 0 documents

Self-Assessment Questionnaire

1. Complete the questionnaire by selecting **Manage** within the **Compete Security Assessment** box.



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

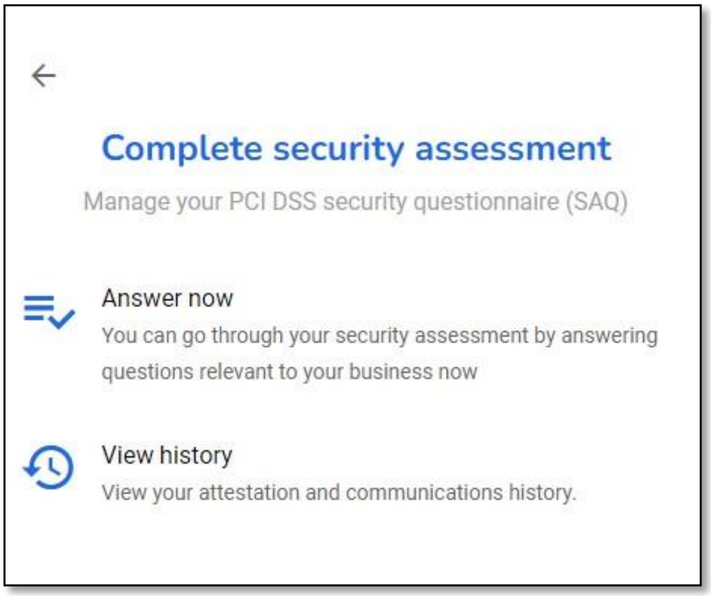
Complete security assessment

33 Unanswered questions
0 Remediation tasks

Document Repository

Contains 0 documents

2. Choose **Answer now** on the next screen to begin.



Complete security assessment

Manage your PCI DSS security questionnaire (SAQ)

Answer now

You can go through your security assessment by answering questions relevant to your business now

View history

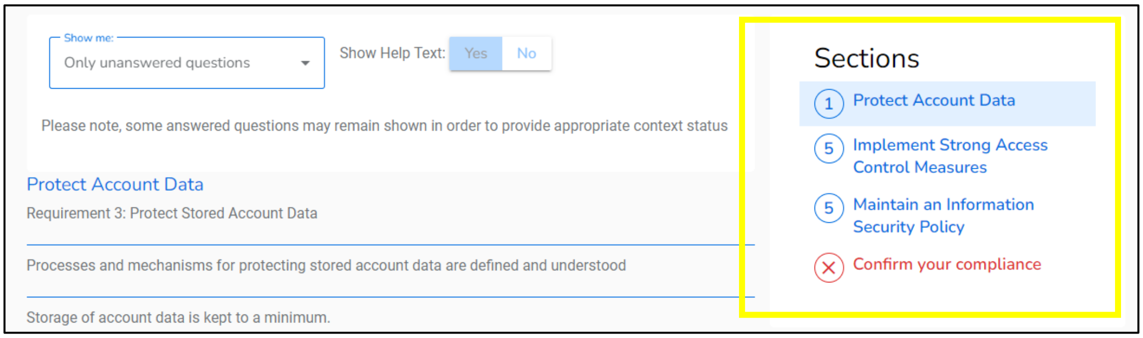
View your attestation and communications history.

3. The questionnaire will have three sections to complete. As each section is complete, a teal check mark will replace the gray circles displayed in the **Sections** box below.

    - The numbers in the box represent how many unanswered questions remain and will update as each question is answered.

4. Navigate through the questions by answering **Yes** to all questions.

    - When a question is answered, it will automatically skip to the next required question to complete.



Show me: Only unanswered questions

Show Help Text: Yes No

Please note, some answered questions may remain shown in order to provide appropriate context status

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.

Sections

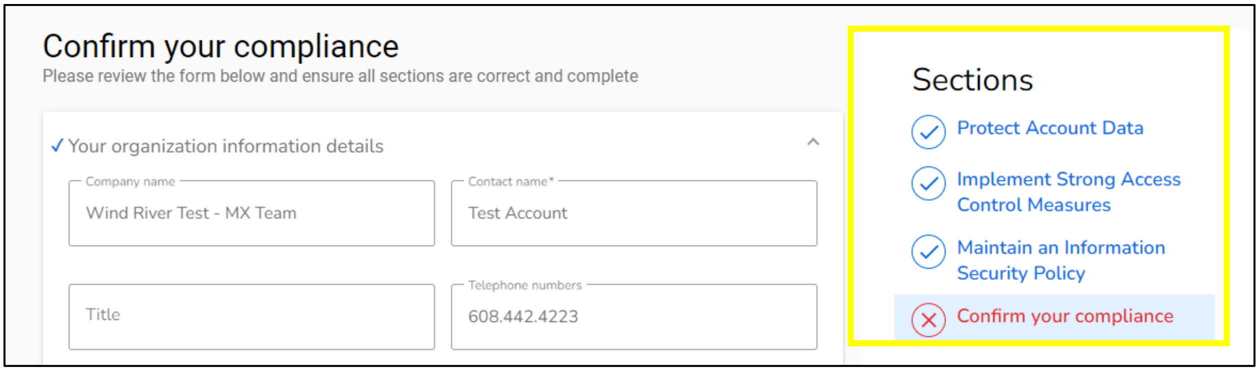
1 Protect Account Data

5 Implement Strong Access Control Measures

5 Maintain an Information Security Policy

✕ Confirm your compliance

5. After completing all three sections, **Confirm your Compliance** by reviewing the information in all of the dropdown sections on this page:
    - ○ Your organization information details
    - ○ Type of business
    - ○ Description of environment
    - ○ Eligibility to complete SAQ P2PE
    - ○ Acknowledge of status and attestation
    - ○ Merchant Executive Officer
    - ○ Attestation
    - ○



Confirm your compliance

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

✓ Your organization information details

Company name: Wind River Test - MX Team

Contact name*: Test Account

Title

Telephone numbers: 608.442.4223

Sections

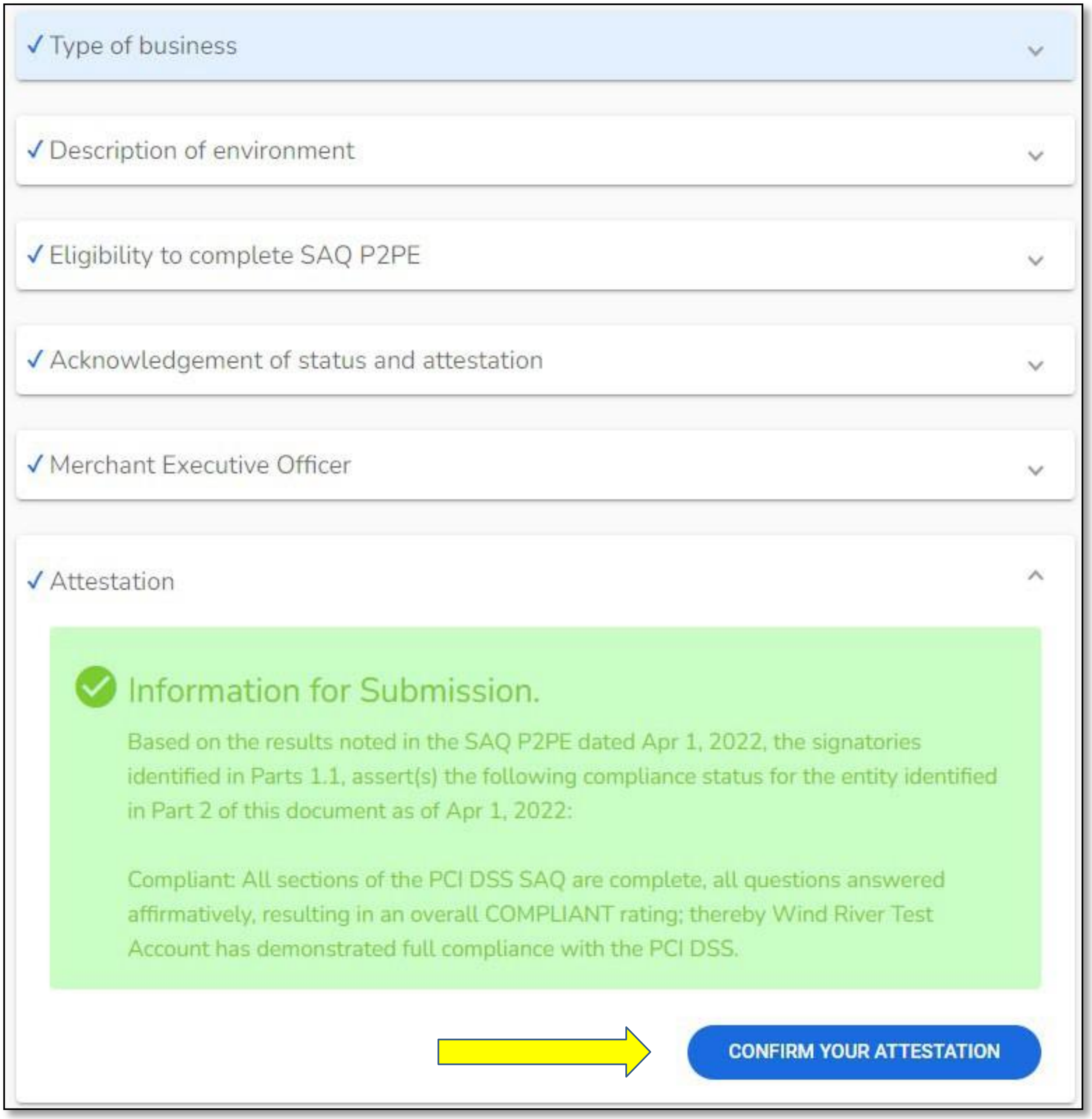
✓ Protect Account Data

✓ Implement Strong Access Control Measures

✓ Maintain an Information Security Policy

✕ Confirm your compliance

6. Select **Confirm Your Attestation** to complete the SAQ.



✓ Type of business

✓ Description of environment

✓ Eligibility to complete SAQ P2PE

✓ Acknowledgement of status and attestation

✓ Merchant Executive Officer

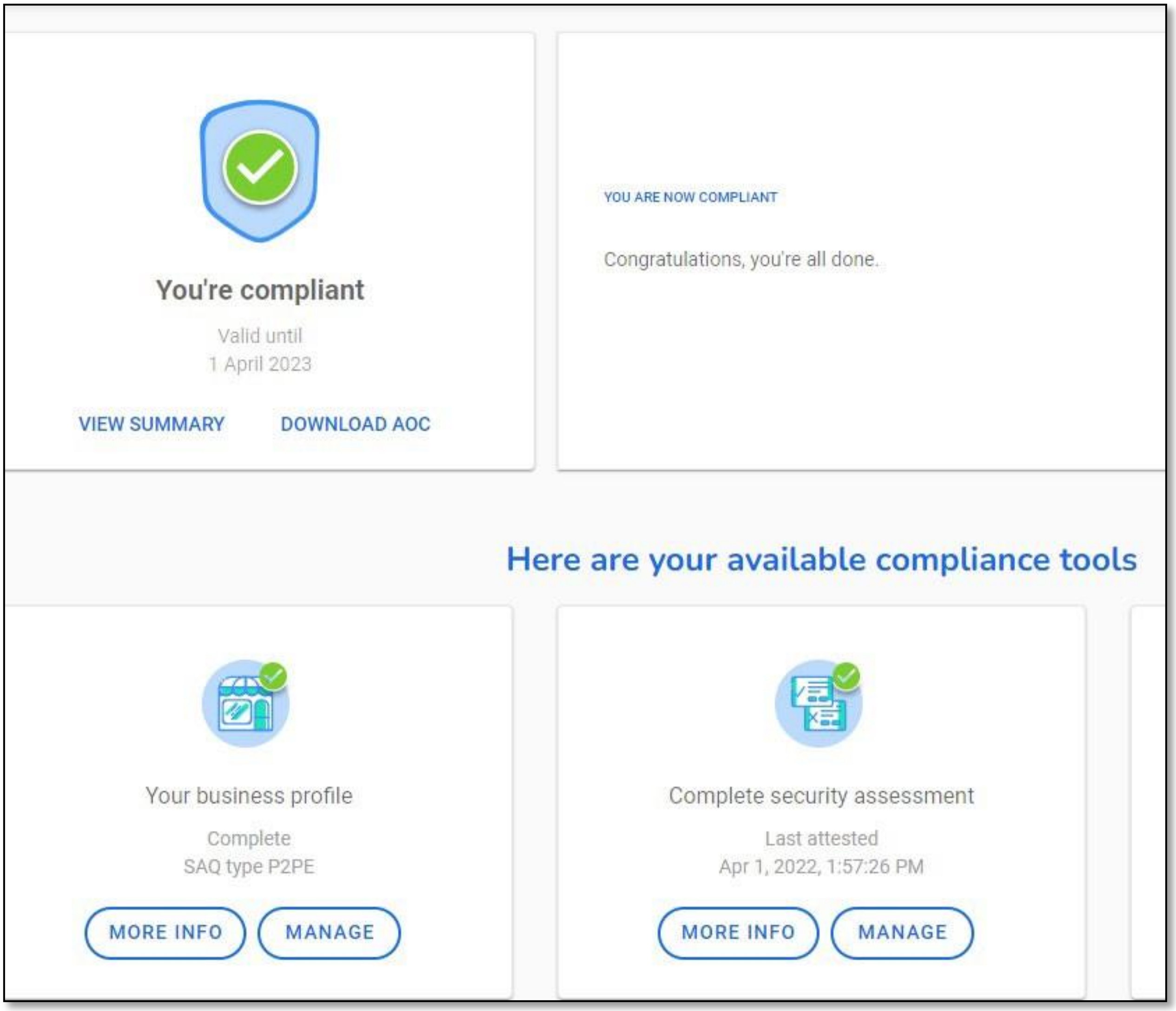
✓ Attestation

Information for Submission.

Based on the results noted in the SAQ P2PE dated Apr 1, 2022, 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 Apr 1, 2022:

Compliant: All sections of the PCI DSS SAQ are complete, all questions answered affirmatively, resulting in an overall COMPLIANT rating; thereby Wind River Test Account has demonstrated full compliance with the PCI DSS.

7. After confirming, it will redirect to the **PCI Dashboard**, where it will display a passing status compliance status.



You're compliant

Valid until
1 April 2023

YOU ARE NOW COMPLIANT

Congratulations, you're all done.

Here are your available compliance tools

Your business profile

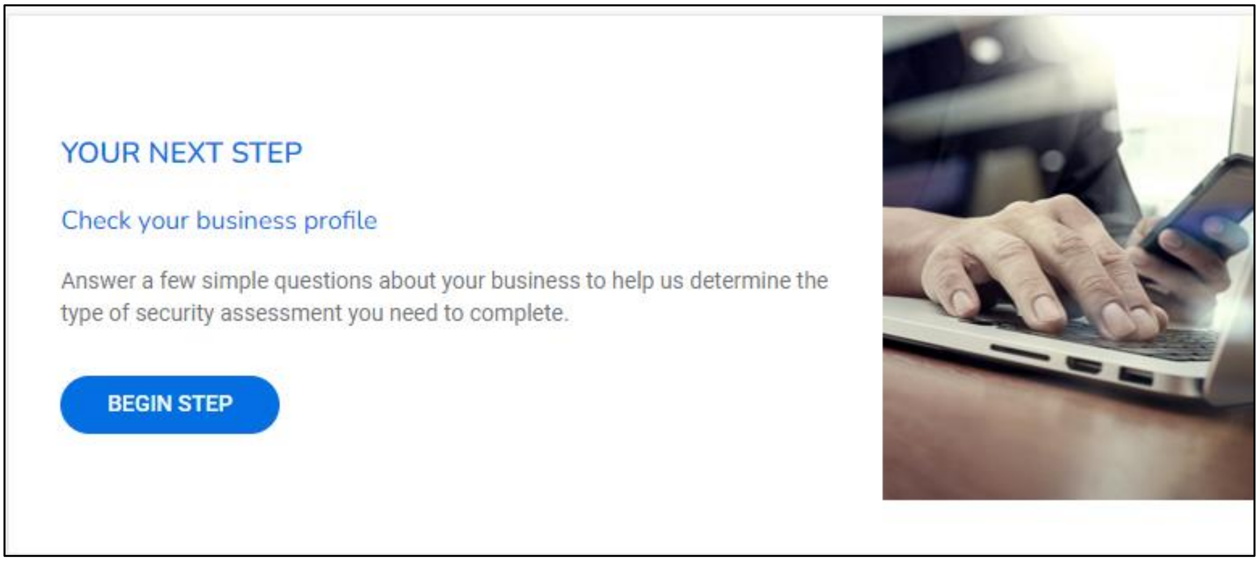
Complete
SAQ type P2PE

Complete security assessment

Last attested
Apr 1, 2022, 1:57:26 PM

Renewal Directions

1. Click **Begin Step.**

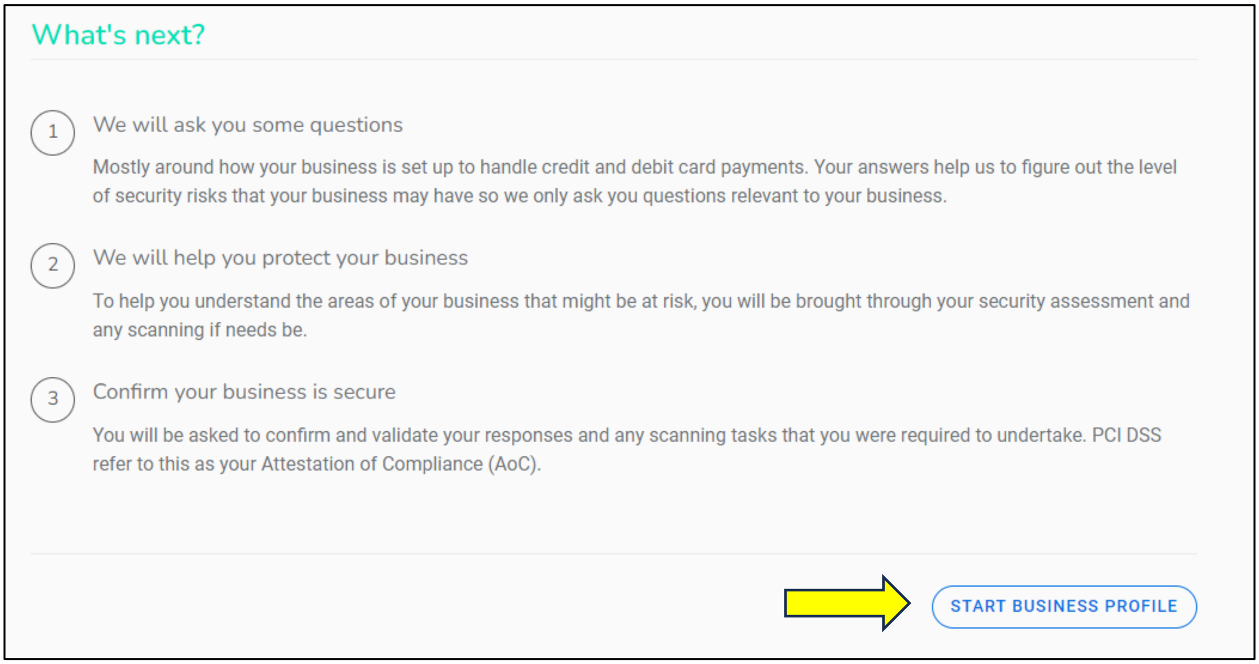


YOUR NEXT STEP

Check your business profile

Answer a few simple questions about your business to help us determine the type of security assessment you need to complete.

2. Click **Start Business Profile.**



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.

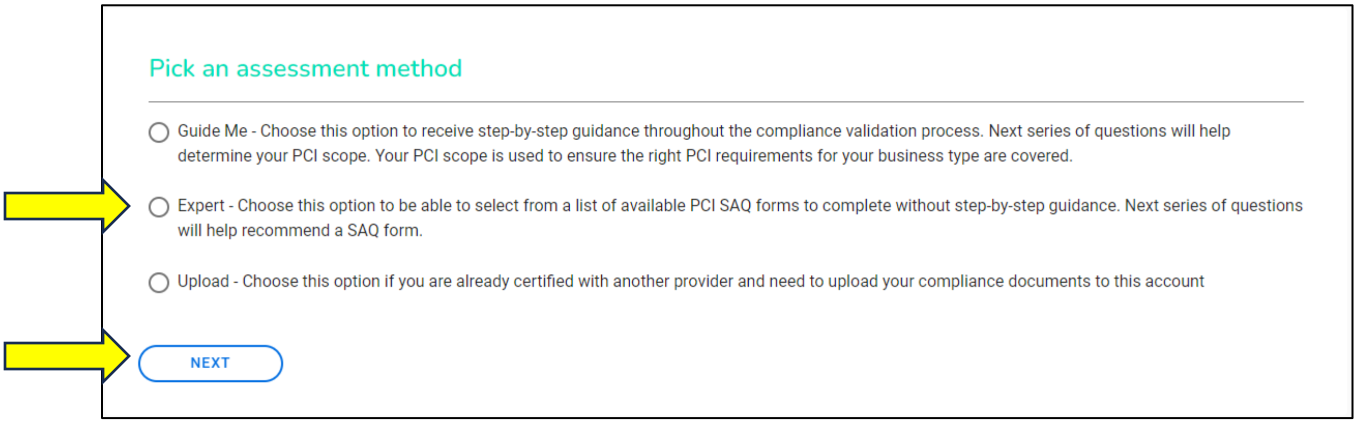
2 We will help you protect your business

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).

3. Click the circle next to **Expert** and then click **Next.**



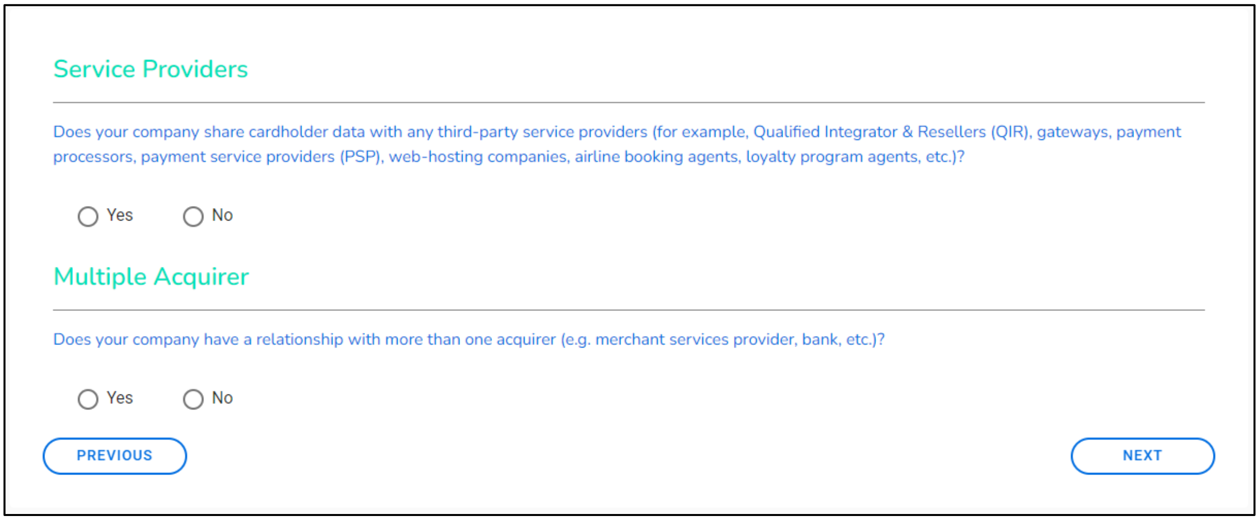
Pick an assessment method

○ Guide Me - Choose this option to receive step-by-step guidance throughout the compliance validation process. Next series of questions will help determine your PCI scope. Your PCI scope is used to ensure the right PCI requirements for your business type are covered.

○ Expert - Choose this option to be able to select from a list of available PCI SAQ forms to complete without step-by-step guidance. Next series of questions will help recommend a SAQ form.

○ Upload - Choose this option if you are already certified with another provider and need to upload your compliance documents to this account

4. Answer the Service Provider and Multiple Provider questions then click **Next.**



Service Providers

Does your company share cardholder data with any third-party service providers (for example, Qualified Integrator & Resellers (QIR), gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.)?

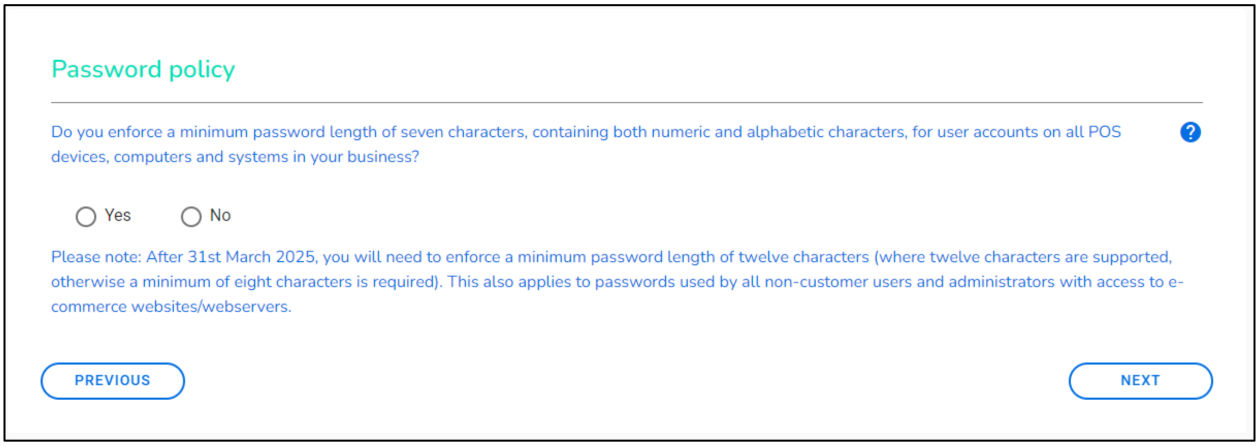
○ Yes ○ No

Multiple Acquirer

Does your company have a relationship with more than one acquirer (e.g. merchant services provider, bank, etc.)?

○ Yes ○ No

5. Answer the Password Policy question then click **Next.**



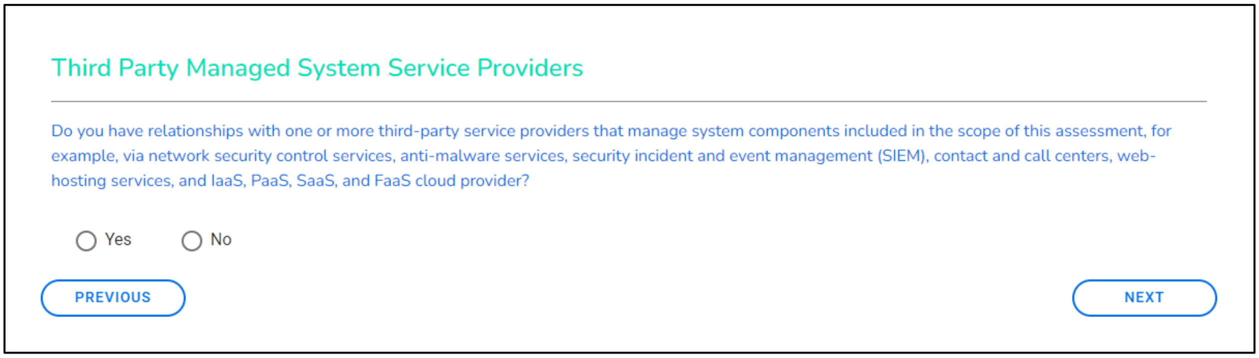
Password policy

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/webservers.

6. Answer the Third Party Managed System Service Providers question then click **Next**.

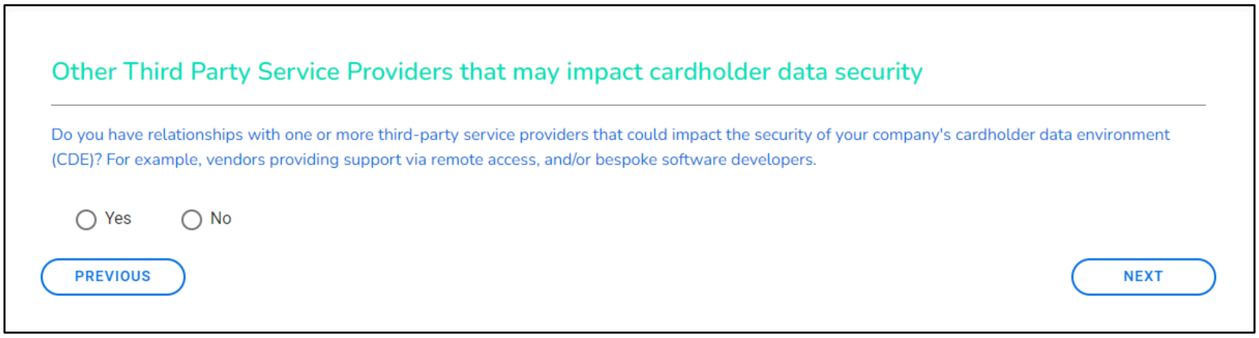


Third Party Managed System Service Providers

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

7. Answer the Other Third-Party Service Providers question then click **Next.**

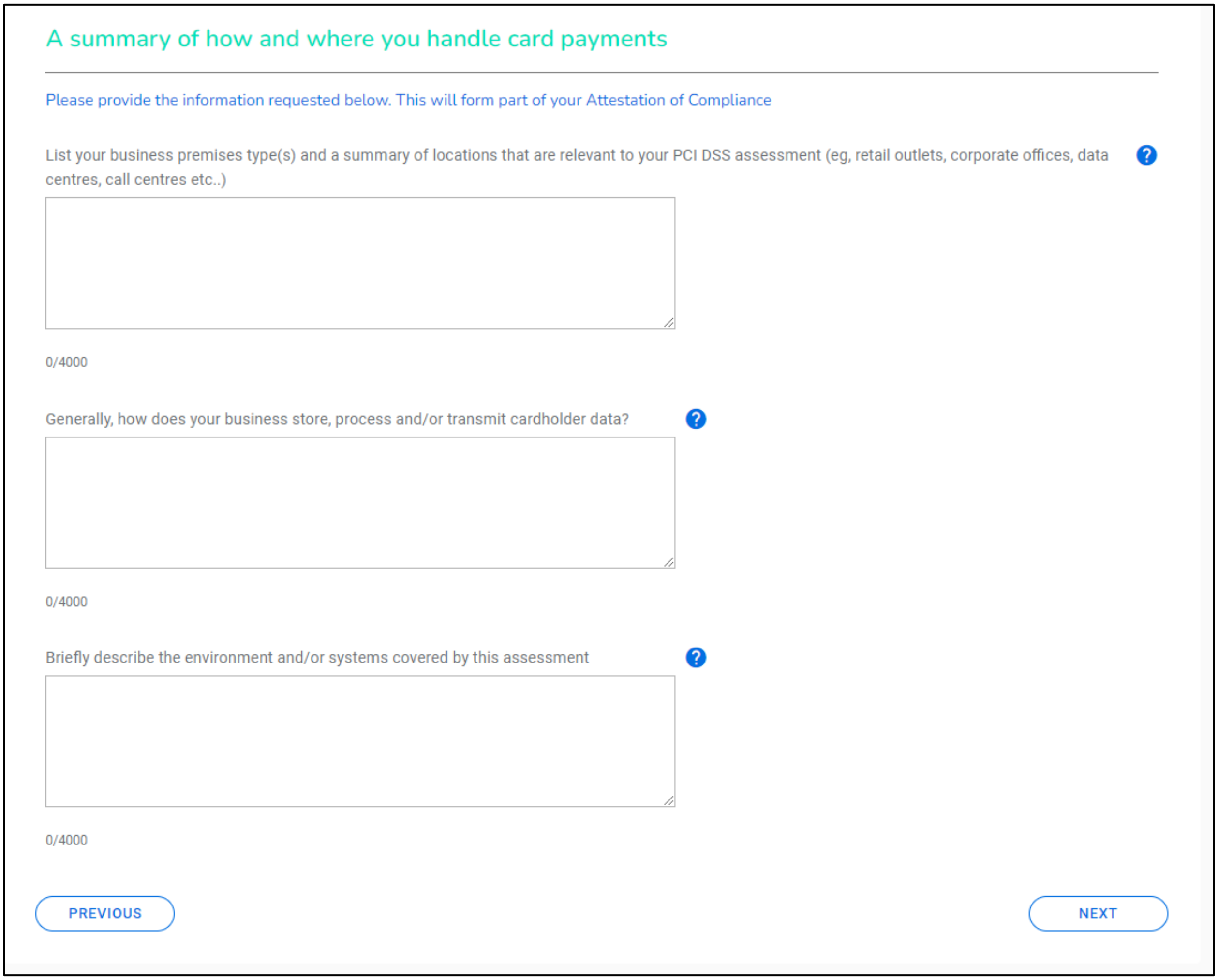


Other Third Party Service Providers that may impact cardholder data security

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

8. Fill out the summary information then 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..)

0/4000

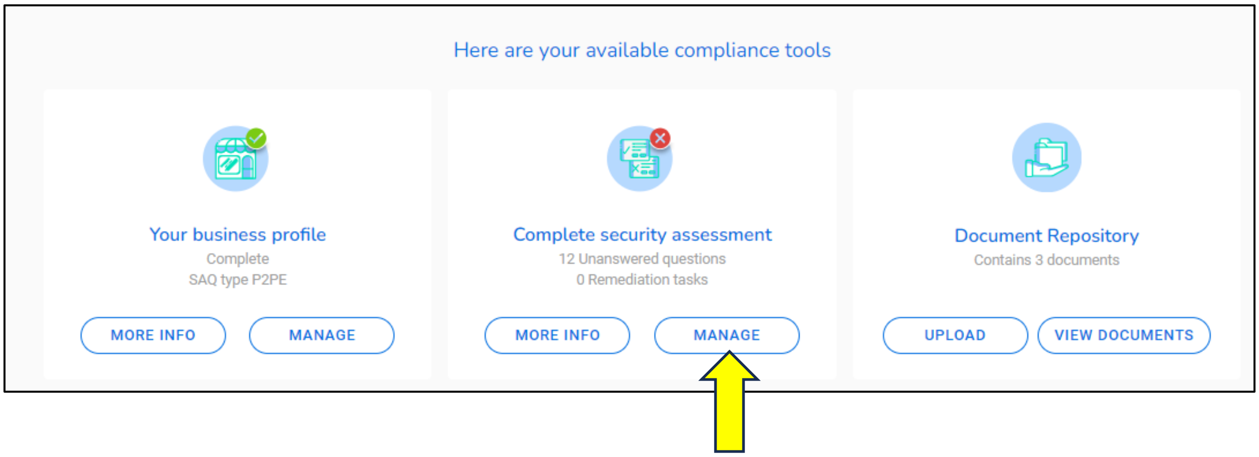
Generally, how does your business store, process and/or transmit cardholder data?

0/4000

Briefly describe the environment and/or systems covered by this assessment

0/4000

9. Click **Manage** in the **Complete Security Assessment** box (the number of questions may vary).



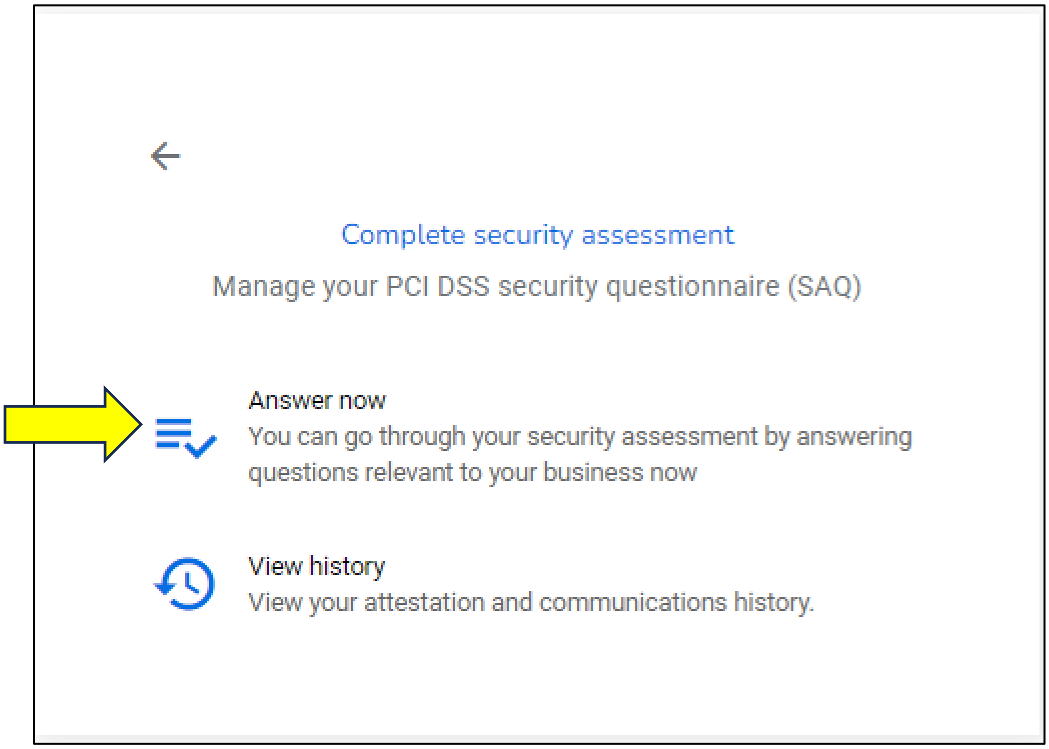
Here are your available compliance tools

Your business profile
Complete
SAQ type P2PE

Complete security assessment
12 Unanswered questions
0 Remediation tasks

Document Repository
Contains 3 documents

10. Click **Answer Now.**



Complete security assessment

Manage your PCI DSS security questionnaire (SAQ)

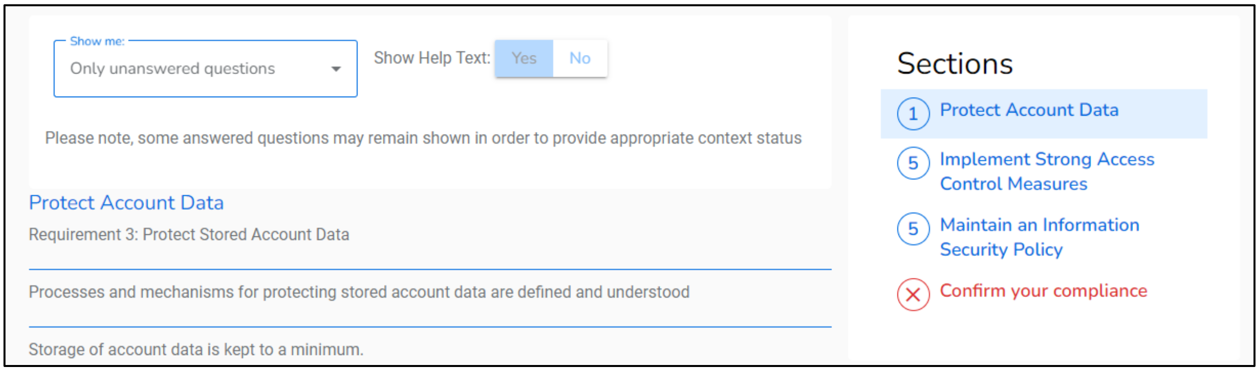
Answer now

You can go through your security assessment by answering questions relevant to your business now

View history

View your attestation and communications history.

11. Answer **Yes** to all the unanswered questions (the number of questions may vary).



Show me: Only unanswered questions

Show Help Text: Yes No

Please note, some answered questions may remain shown in order to provide appropriate context status

Protect Account Data

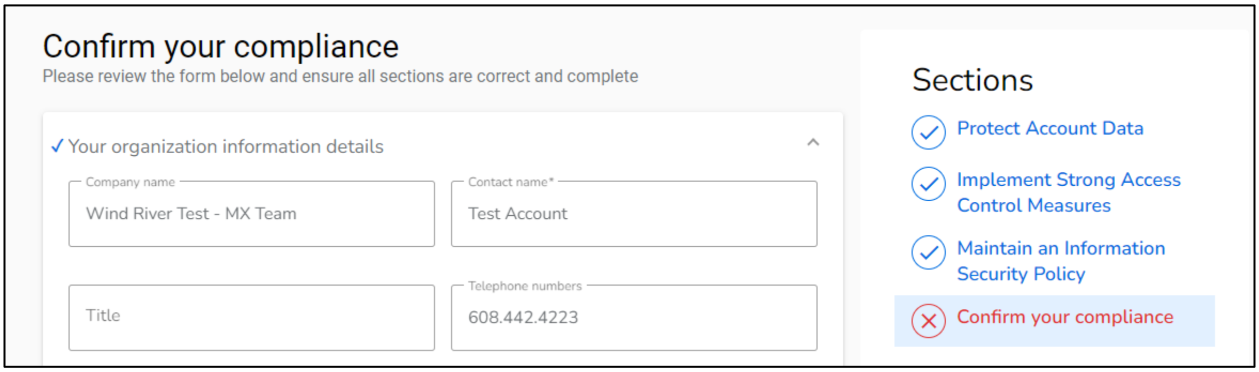
Requirement 3: Protect Stored Account Data

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

Storage of account data is kept to a minimum.

Sections
1 Protect Account Data
5 Implement Strong Access Control Measures
5 Maintain an Information Security Policy
Confirm your compliance

12. Click **Confirm Your Compliance** (if not already in that section).



Confirm your compliance

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

✓ Your organization information details

Company name: Wind River Test - MX Team

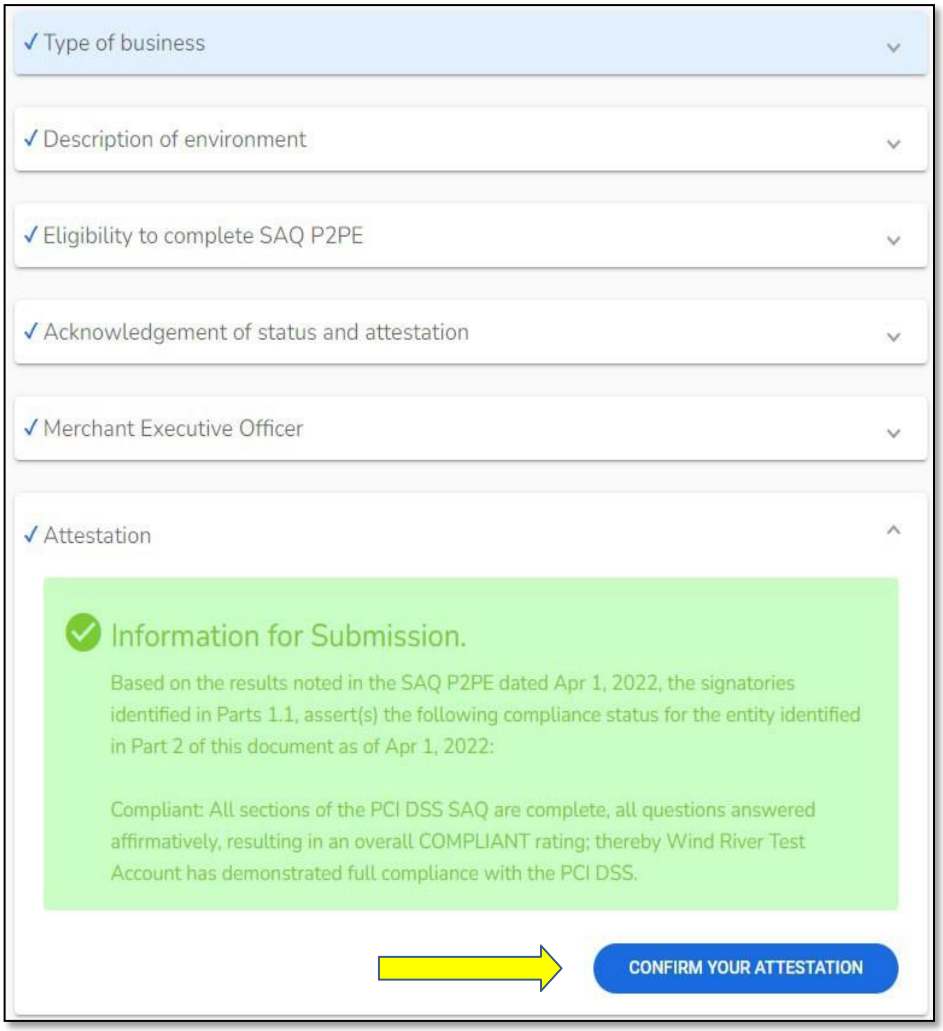
Contact name*: Test Account

Title

Telephone numbers: 608.442.4223

Sections
Protect Account Data
Implement Strong Access Control Measures
Maintain an Information Security Policy
Confirm your compliance

13. Click **Confirm Your Attestation**.



✓ Type of business

✓ Description of environment

✓ Eligibility to complete SAQ P2PE

✓ Acknowledgement of status and attestation

✓ Merchant Executive Officer

✓ Attestation

Information for Submission.

Based on the results noted in the SAQ P2PE dated Apr 1, 2022, 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 Apr 1, 2022:

Compliant: All sections of the PCI DSS SAQ are complete, all questions answered affirmatively, resulting in an overall COMPLIANT rating; thereby Wind River Test Account has demonstrated full compliance with the PCI DSS.