

When you accept card payments in the Amilia SmartRec e-commerce store as well as with a PAX A920 integrated terminal

-This guide is adapted to merchants using Amilia SmartRec-

SAQ D Composite User Guide

PCI v4.0

January 2024 – PCI v3.2.1

SAQ D Composite User Guide

Once your account has been boarded, you will receive log in details to your PCI Account via email.

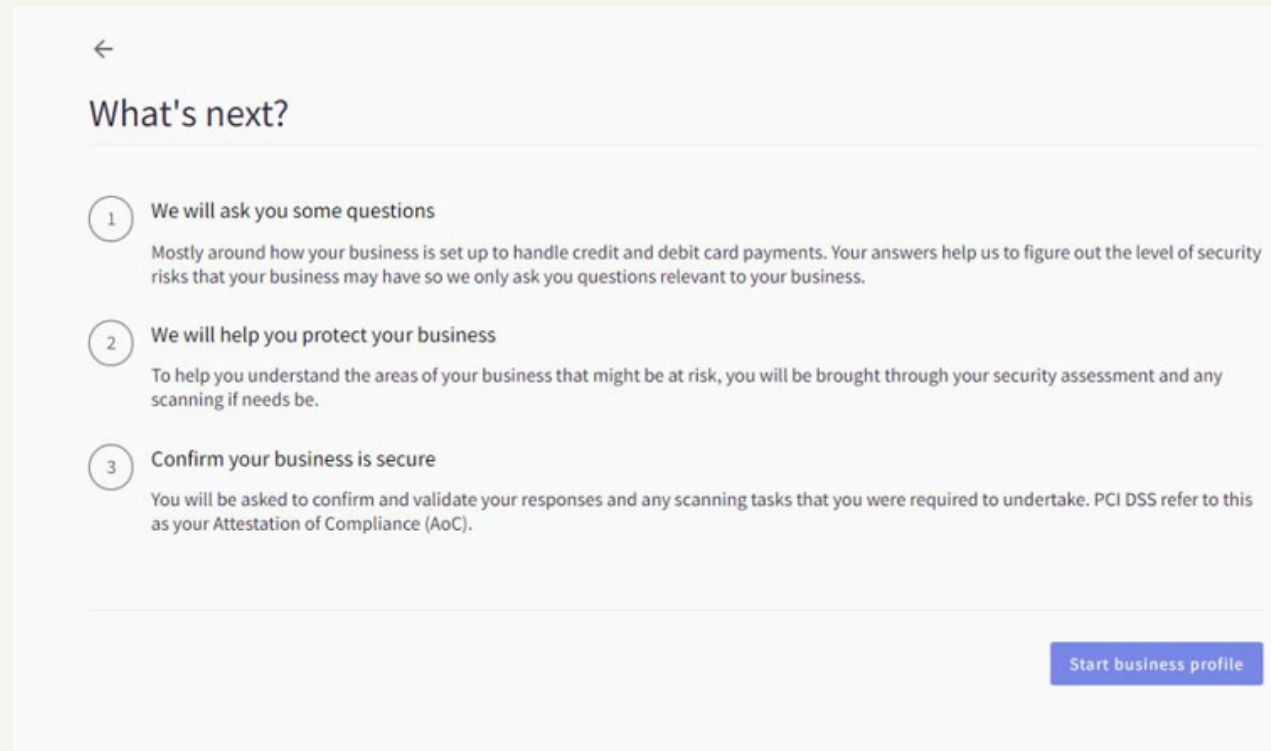
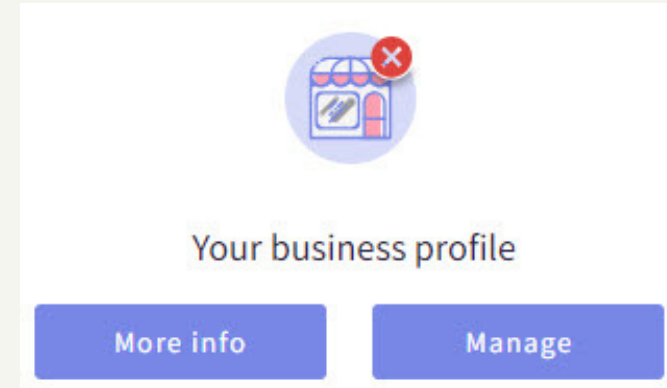
- Your username is your Merchant ID number.
- Please use the link within the email to select a password of your own choosing, ensuring to follow the on-screen instructions.
- Upon your first initial log in, you will need to review your contact information to ensure this is accurate.

SAQ D Composite User Guide

- To start, click 'Manage' on your **business profile**.

The profile paints a picture of your business environment & how you accept card payments.

- Follow this (SAQ type D Composite) guide if your organization accepts card payments in the Amilia SmartRec store as well as a PAX A920 integrated terminal .



SAQ D Composite 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

Next

- 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 D Composite 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.

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

- Select '**Guide me**' to complete your compliance using the PCI Portal. (Recommended)
- Select 'Expert' if you don't wish to use the profiling tool to pre-populate some of your PCI requirements. (Not Recommended)
- Select 'Upload' if you've already completed your compliance for the forthcoming year and wish to upload the required documentation.

SAQ D Composite User Guide

* These instructions are for the 'Guide me' option as shown in the previous slide *

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 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 (incl. e-Commerce website/shop, consumer mobile app, etc.) 
- ☐  Mail and/or telephone order card payments 

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

Since you accept card payments in the Amilia SmartRec e-commerce store (through Paysafe's API), as well as Face to Face with a PAX A920 integrated terminal, **please select both the 1st (Face to face) and the 2nd (Online payments) options.**

SAQ D Composite User Guide

Pay by Link

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

☐ Yes ☒ No

Previous

Next

This question is asking if you provide your customers with a secure payment link to process their payment. Since you accept card payments in the Amilia SmartRec e-commerce store (through Paysafe's API) and with a PAX A920 integrated terminal, **please answer this question with 'No'.**

SAQ D Composite User Guide

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

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

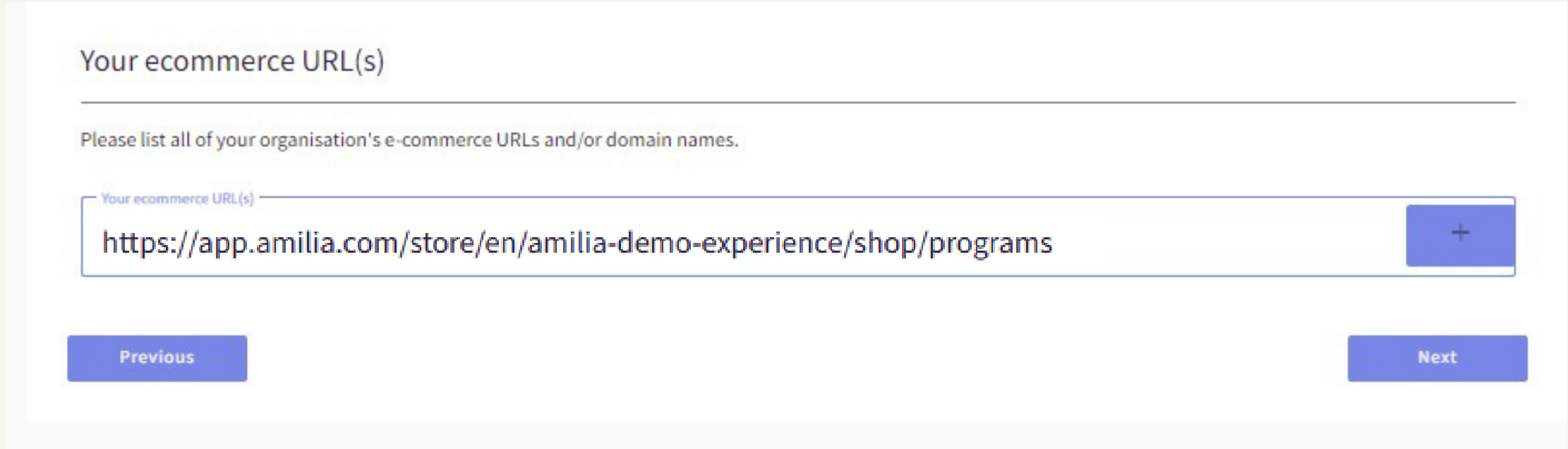
☒ My customers make online payments to my business via a website accessed using a web browser

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

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

- Since you're using the Amilia SmartRec e-commerce store (through Paysafe's API) to accept card payments, **please select the first option.**

SAQ D Composite User Guide



The screenshot shows a web form titled "Your ecommerce URL(s)". Below the title is a horizontal line. Underneath, a text label reads "Please list all of your organisation's e-commerce URLs and/or domain names." Below this is a large text input field. Inside the field, the text "Your ecommerce URL(s)" is at the top left, and the URL "https://app.amilia.com/store/en/amilia-demo-experience/shop/programs" is entered. To the right of the input field is a blue button with a white "+" icon. At the bottom of the form are two blue buttons: "Previous" on the left and "Next" on the right.

- Please enter the URL of your Amilia SmartRec e-commerce store.
- Then select the '+' icon to add it. You can add more than one URL if you have more than one e-commerce store. Select 'Next' when ready to proceed.

SAQ D Composite User Guide

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

- Since you're using your Amilia SmartRec e-commerce store (through Paysafe's API) to accept card payments – **please answer 'Yes' to this question.**

SAQ A User Guide

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

- Amilia SmartRec is Level 1 PCI compliant e-commerce service provider. Please visit trust.amilia.com for a copy of our attestation of compliance in the 'Resources' section.
- **Please answer 'Yes' to this question.**

SAQ D Composite User Guide

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](#)

- Amilia SmartRec is Level 1 PCI compliant e-commerce service provider that performs quarterly external scans of your Amilia SmartRec e-commerce store.
- **Please answer ‘Yes’ to this question.**

SAQ D Composite User Guide

- To select your payment gateway, please type **'Paysafe'** in the field.
- Please choose the 2nd option that appears - **Paysafe Paysafe Group (prev. Netbanx)**

Your payment gateway/processor 

Please select all of your payment gateway/processor(s) below

paysafe

Paysafe Paysafe Group (prev. Netbanx) 

☐ Paysafe Group Plc.

☒ Paysafe Paysafe Group (prev. Netbanx)

☐ PAYSAFE SERVICES (US) CORP.

Previous Next

SAQ D Composite User Guide

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](#)

- Paysafe is a Level 1 Service Provider – **please answer ‘Yes’ to this question.** You can obtain a copy of Paysafe’s attestation of compliance from our trust center at trust.amilia.com in the ‘Resources’ section.

SAQ D Composite User Guide

As you also use the PAX A920 integrated terminal to accept card payments in the Amilia SmartRec store -

- **Please select the 4th option 'I use an integrated Point of Sale (iPOS/ePOS) system that includes an integrated card reader device'.**

Note: In the past, merchants selected the first option (standalone or portable POS terminal). However, this option leads to an SAQ B-IP with a scan (to be avoided). **Do not select the first option. You must select the 4th option.**

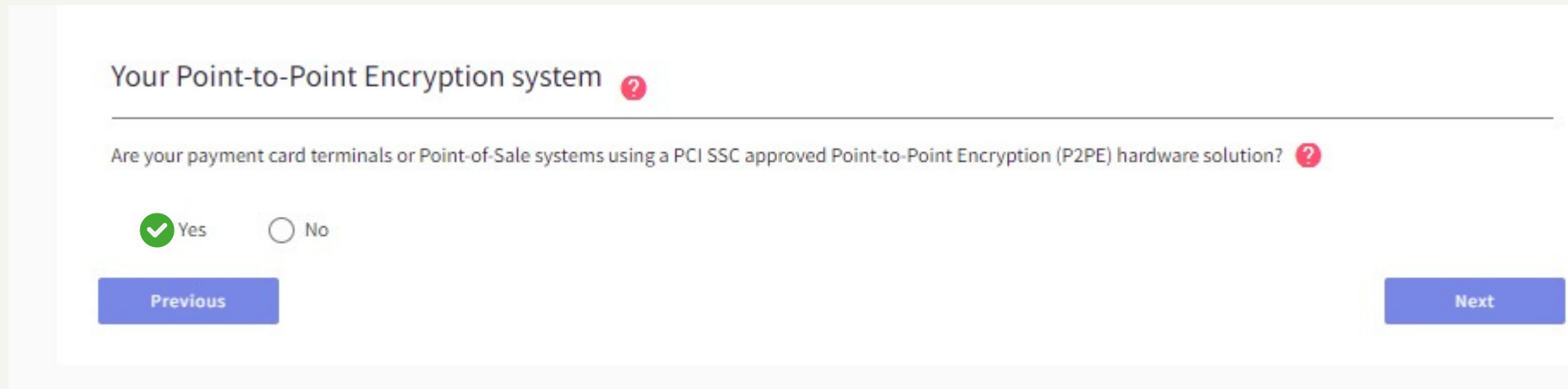
How you accept card payments ?

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

SAQ D Composite 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

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

- The PAX A920 integrated terminal is a Point-to-Point encrypted terminal.
Please answer ‘Yes’ to this question.

SAQ D Composite 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

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

- Since you're using the PAX A920 integrated terminal, **please answer 'Yes' to this question.**

SAQ D Composite 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

[Previous](#previous) [Next](#next)

- Please answer 'Yes' to this question.

SAQ D Composite 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 ✕

☒ Planet Payment Group Holdings Limited - Planet PAX Solution

Previous Next

- To input your P2PE solution, please type 'PAX' in the search bar and then scroll down.
- **Please select 'Planet Payment Group Holdings Limited - Planet PAX Solution'.**

SAQ D Composite 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.

Filter

☐ PAX Computer Technology (Shenzhen) Co Ltd, A920  **OR**  ☐ 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

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

- Please select the **A920 or A920 Pro** (depending on which one you have). They're the only integrated terminals currently supported in Amilia SmartRec.

SAQ D Composite User Guide

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](#)

- Please answer 'No' to this question.

SAQ D Composite 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

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

- Please answer 'No' to this question.

SAQ D Composite User Guide

- You must never send, receive, transmit or store cardholder data electronically under any circumstances.

This puts your organization and your customers' data at risk of being hacked by malicious individuals who will show you no mercy.

- Please answer 'No' to both questions.**

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

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

SAQ D Composite 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 handle 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.

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

SAQ D Composite 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.

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

- 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 D Composite User Guide

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

- **Please answer ‘No’ to this question.** It’s VERY unlikely you have an Internal Security Assessor for your PCI DSS.

SAQ D Composite User Guide

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](#)

- **Please answer ‘No’ to this question.** It’s VERY unlikely you have a Qualified Security Assessor for your PCI DSS.

SAQ D Composite 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

Previous

Next

- Please answer 'No' to this question.

SAQ D Composite 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

Previous

Next

- **Please answer 'No' to this question.**

SAQ D Composite User Guide

As your organization accepts card payments in the Amilia SmartRec e-commerce store, as well as a PAX A920 integrated terminal, **you may copy and paste this answer in all three fields:** 'Card payments accepted Face to Face with PAX A920 integrated terminal. The integrated terminal connects via (describe how it's connected to the net).

E-commerce setup, Paysafe dot JS system accepting card payments, iFrame in place, Systems are updated throughout the year, No cardholder data is stored, there are X NUMBER of employees who access the Amilia SmartRec back office (Client billing section).'

Paysafe ♦♦

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..)

- E-commerce setup
- Paysafe dot JS system accepting card payments
- iFrame in place
- Systems are updated throughout the year
- No cardholder data is stored
- There are X NUMBER of employees who access the back office

3/4000

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

- E-commerce setup
- Paysafe dot JS system accepting card payments
- iFrame in place
- Systems are updated throughout the year
- No cardholder data is stored
- There are X NUMBER of employees who access the back office

3/4000

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.

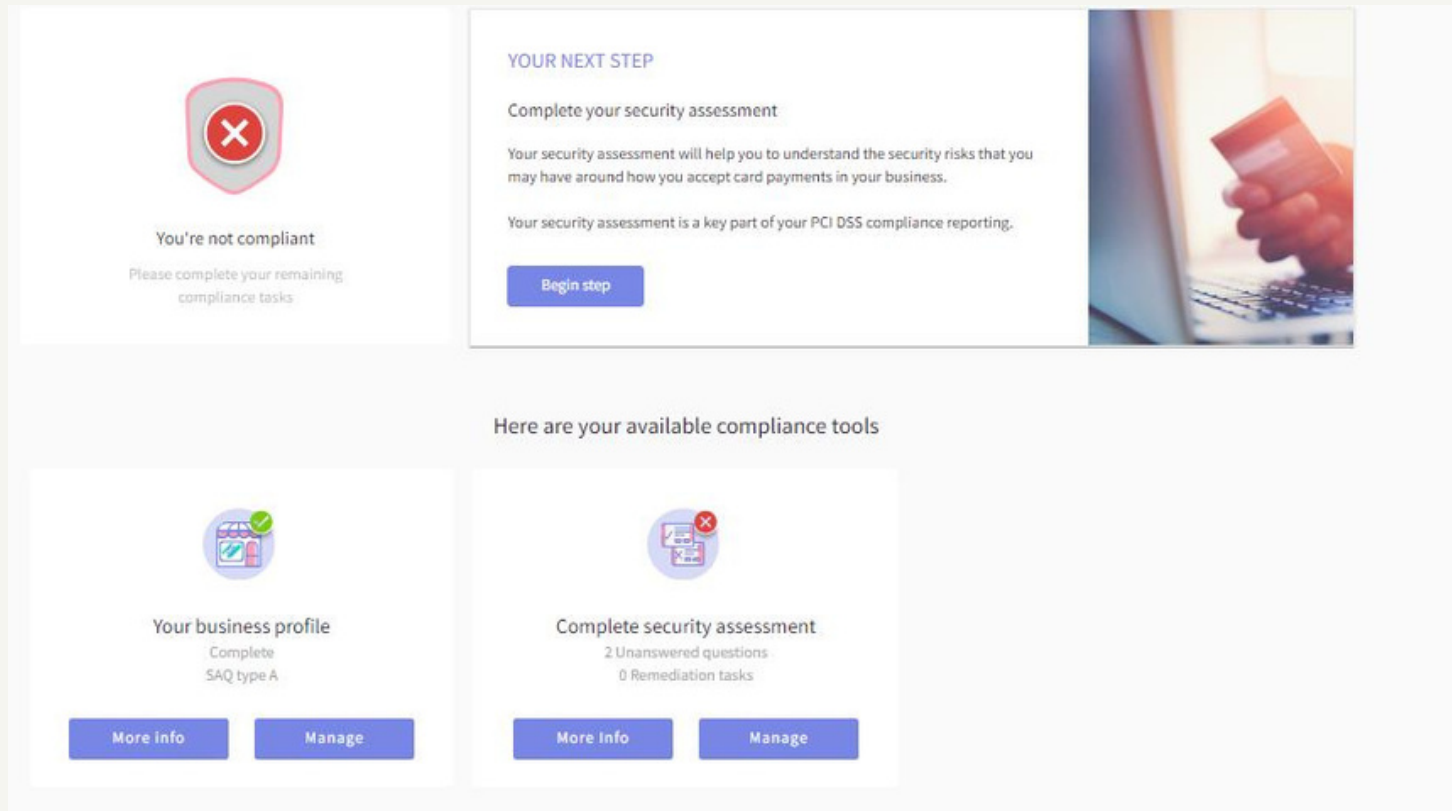
- E-commerce setup
- Paysafe dot JS system accepting card payments
- iFrame in place
- Systems are updated throughout the year
- No cardholder data is stored
- There are X NUMBER of employees who access the back office

3/4000

Previous

Next

SAQ D Composite User Guide



- Once all steps have been completed in the business profile, you will see there are a handful of questions outstanding in the security assessment.
- Click '**Manage**' to begin the security assessment.

SAQ D Composite User Guide

The screenshot displays the SAQ D Composite User Guide interface. At the top, there are two filters: 'Show me:' with a dropdown menu set to 'Only unanswered questions', and 'Show Help Text:' with 'Yes' and 'No' buttons. Below these filters, the main content area is titled 'Protect Account Data' and 'Requirement 3: Protect Stored Account Data'. It contains two text boxes: 'Processes and mechanisms for protecting stored account data are defined and understood' and 'Storage of account data is kept to a minimum.' Below these is a section titled 'Question group 3.2.1' with a blue bar containing an information icon and the text 'Help answering this requirement'. On the right side, there is a 'Sections' panel with a list of items: 'Build and Maintain a Secure Network and Systems' (checked), '1 Protect Account Data' (selected with a blue background), 'Maintain a Vulnerability Management Program' (checked), '3 Implement Strong Access Control Measures' (checked), 'Maintain an Information Security Policy' (checked), and 'Confirm your compliance' (marked with a red X).

- In the 'Sections' area shown above, you may have some questions related to 'protecting account data' and 'implementing strong access control measures'.

SAQ D Composite 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.

- **Please answer 'N/A' to this question and write 'My organization uses the Amilia SmartRec e-commerce store and PAX A920 integrated terminal to handle card payments. We don't store or transmit cardholder information.' as the reason.**

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

N/A

No

Yes

SAQ D Composite User Guide

- This question is asking you to confirm that you do not store the CVV/CVV2 code once the transaction has been processed.
- Please answer 'N/A' to this question and write 'The PAX A920 integrated terminal does not store cardholder data, and neither does the Amilia SmartRec e-commerce store' as the answer.

3.3.1.2

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

I have implemented a compensating control

i 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 A User Guide

If you answered 'No' to enforcing a password policy in your business profile, you will see this question in your security assessment.

- **Please answer 'Yes' to this question or 'N/A'.** If you answer 'No', you will fail the security assessment.

8.3.6

If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they meet the following minimum level of complexity:

- A minimum length of 12 characters (or IF the system does not support 12 characters, a minimum length of eight characters).
- Contain both numeric and alphabetic characters.

I have implemented a compensating control

N/A

No

Yes

SAQ D Composite User Guide

- Please answer 'N/A' to this question and write 'My organization uses the Amilia SmartRec e-commerce store to handle card payments, as well as a PAX A920 integrated terminal. We don't store data.' as the reason.

9.4.1.1

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

I have implemented a compensating control

N/A

No

Yes

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 A User Guide

The screenshot displays the SAQ A User Guide interface. At the top, there is a 'Show me:' dropdown menu set to 'Only unanswered questions' and a 'Show Help Text:' toggle with 'Yes' selected. Below this, the section title 'Build and Maintain a Secure Network and Systems' is shown. A light blue information box contains the text: '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"'. A 'Next' button is located at the bottom right of the main content area. On the right side, a 'Sections' panel lists seven items, each with a status icon: 'Build and Maintain a Secure Network and Systems' (checked), 'Protect Cardholder Data' (checked), 'Maintain a Vulnerability Management Program' (checked), 'Implement Strong Access Control Measures' (checked), 'Regularly Monitor and Test Networks' (checked), 'Maintain an Information Security Policy' (checked), and 'Confirm your compliance' (marked with a red X). The 'Confirm your compliance' item is highlighted with a red rectangular border.

- Once all questions are answered within this section – you can then confirm your compliance and complete one final item to become validated for the forthcoming year.
- **Please click the ‘Confirm your compliance’ section as shown above.**

SAQ A 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	

- Carefully 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 A User Guide

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

The screenshot displays a web interface for the SAQ A User Guide. It features a vertical list of five expandable sections, each with a checkmark icon and a dropdown arrow. The sections are: 'Type of business', 'Description of environment', 'Eligibility to complete SAQ B_IP', 'Acknowledgement of status and attestation', and 'Merchant Executive Officer'. Below these is the 'Attestation' section, which is currently expanded. It contains a green box with a checkmark icon and the text 'Information for Submission.' followed by a paragraph stating: '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.' At the bottom right of the 'Attestation' section, a blue button labeled 'Confirm your Attestation' is highlighted with a red rectangular box. A 'Previous' button is visible at the bottom left of the interface.

SAQ A User Guide

Once all stages are completed – you'll be redirected to this screen that shows your organization is now SAQ type D (A, P2PE) compliant for the forthcoming year.

If there is any outstanding issue throughout the year, the PCI portal will email you to notify you that action is required.

