



# Online Payments & HandPoint/PAX A920 Device

SAQ D Composite User Guide  
PCI v4.0

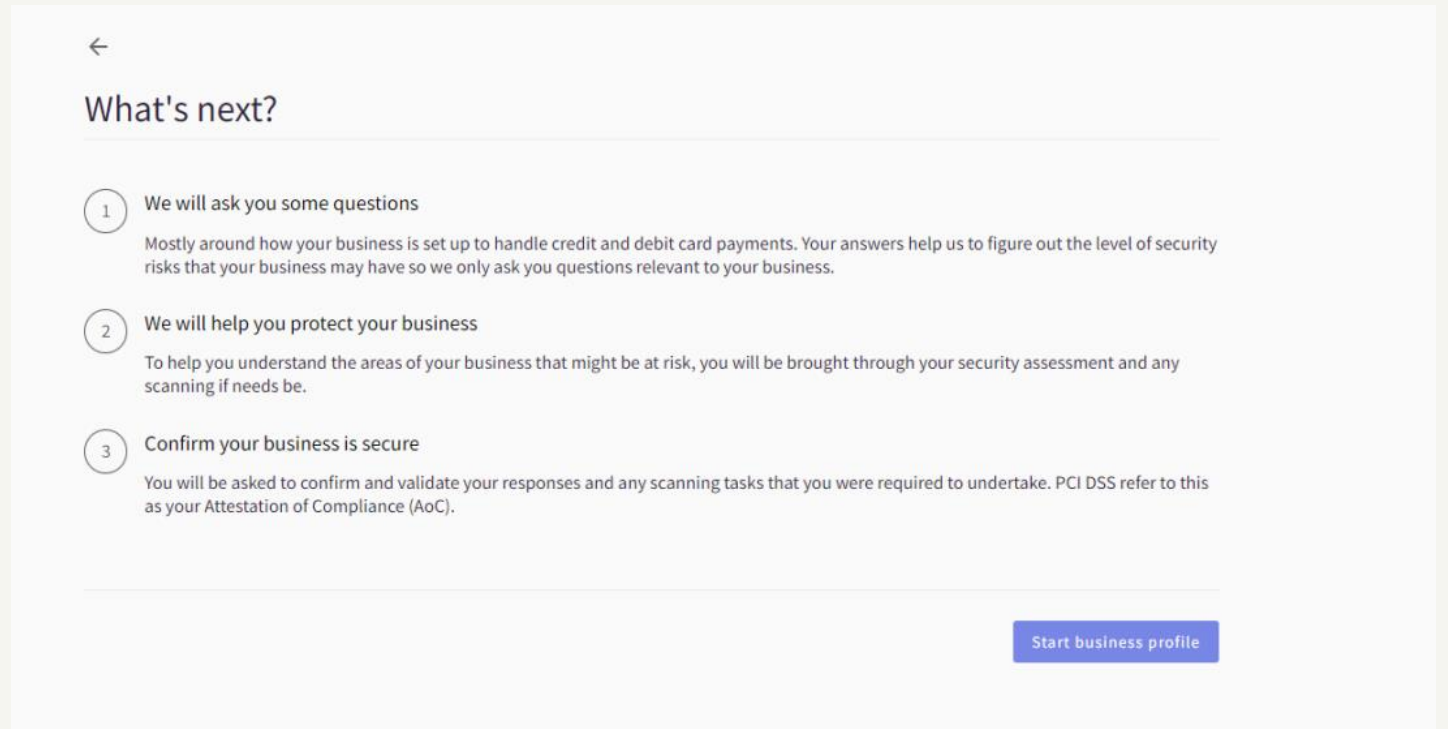
January 2024 – PCI v3.2.1

# 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

- 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.



# 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](#)







- 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 D Composite 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, 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](#)

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

# SAQ P2PE 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](#)

- As you are using the Paysafe.JS system, you can please answer this question as '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

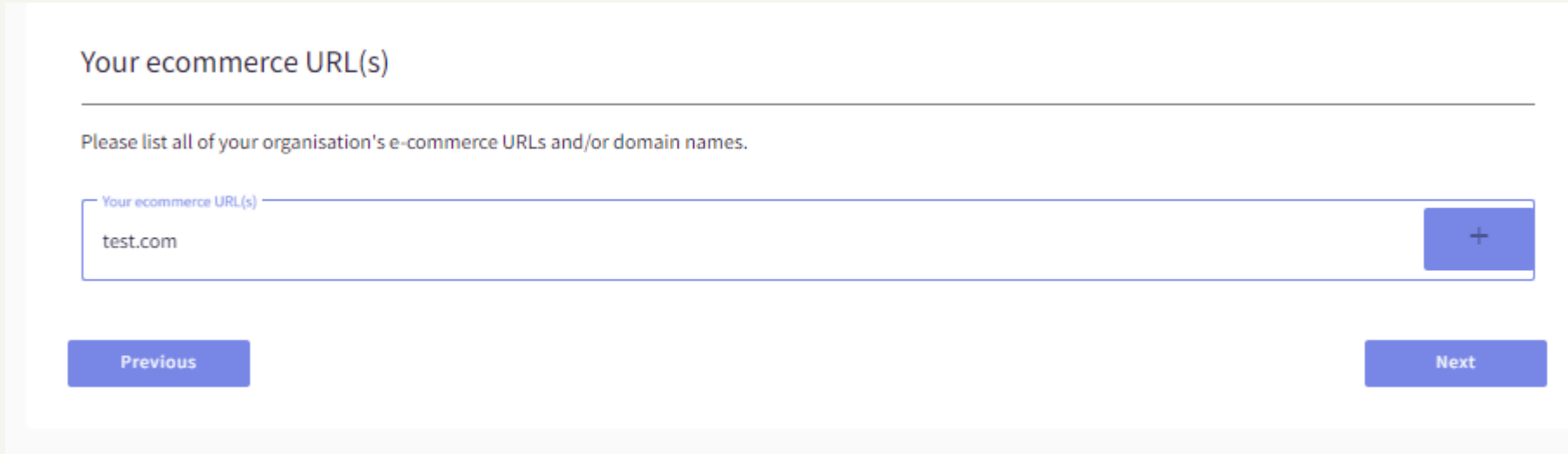
My customers make online payments to my business via a website accessed using a web browser

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

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

- As you are using the Paysafe.JS payment solution, please select the first question listed above and then select 'next'.

# SAQ D Composite User Guide



Your ecommerce URL(s)

---

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

Your ecommerce URL(s)

test.com

+

Previous

Next

The screenshot shows a web form titled "Your ecommerce URL(s)". Below the title is a horizontal line. Underneath is the instruction "Please list all of your organisation's e-commerce URLs and/or domain names." Below this is a text input field with the placeholder "Your ecommerce URL(s)" and the text "test.com" entered. To the right of the input field is a blue button with a white plus sign. 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 e-commerce store.
- Then select the '+' icon and select 'next' to proceed.
- Due to the PCI standard upgrade, you are now required to run a non-intrusive scan on your website domain. This will not affect the overall status of your compliance.

# 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](#)

- As you are using the Paysafe.JS solution – please select ‘yes’ to the above question to proceed.

# SAQ D Composite 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](#)

- As a service provider, Paysafe are required to be complaint for the payment services that are provided to you.
- Paysafe is validated as under Level 1 Service Provider – please select ‘yes’ to the above 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](#)

- Due to the PCI Standard change, quarterly scans of your website are now required for some merchants.
- As you are using the Paysafe API solution to process your payments, we are removing this requirement to streamline your journey.
- Due to this, you can answer the above question as 'no' and this will remove any scanning requirements.

# SAQ D Composite User Guide

- You are now being asked to input your payment gateway/processor.
- As you are using the Paysafe API solution - please search 'Paysafe' within the search box.
- Select the option as shown here and then select 'next'.

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](#)

- As Paysafe are validated under a Level 1 Service Provider – please select ‘yes’ to the above question.







# SAQ D Composite 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


[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](#)

- 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'.

# 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](#)

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

# 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](#) [Next](#)

- Please answer this question as 'yes'.

# SAQ D Composite User Guide

Your Point-to-Point Encryption system

---

Please select your P2PE solution from the list

  
 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.

# 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 ✕

- 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


Previous Next

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

# 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](#)

- Due to the security of your payment device, nobody should be allowed to remotely access it.
- Due to this, please answer this question as 'no'.

# 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](#)

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

# SAQ D Composite 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

[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 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.

[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 31<sup>st</sup> 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](#)

- As you are validating your compliance via the online portal, you can answer the above question as 'no'.

# 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](#)

- As you are validating your compliance via the online portal, you can answer the above question as 'no'.

# 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

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

# 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

- 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 D Composite 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 web servers, 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

Previous Next

# SAQ D Composite 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.

The screenshot displays a user interface for the SAQ D Composite. It features a central panel with a red shield icon containing a white 'X', indicating non-compliance. Below this icon, the text reads: "You're not compliant" and "Please complete your remaining compliance tasks". To the right of this panel, a section titled "YOUR NEXT STEP" contains the text: "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.", and "Your security assessment is a key part of your PCI DSS compliance reporting." A blue button labeled "Begin step" is positioned below this text. On the far right, there is a vertical image showing a hand holding a credit card over a laptop keyboard. Below the main panel, a section titled "Here are your available compliance tools" contains two widgets. The first widget, "Your business profile", shows a calendar icon with a green checkmark, indicating it is "Complete" for "SAQ type P2PE", and has "More info" and "Manage" buttons. The second widget, "Complete security assessment", shows a document icon with a red 'X', indicating "4 Unanswered questions" and "0 Remediation tasks", and also has "More info" and "Manage" buttons.



# SAQ D Composite User Guide

The screenshot displays the SAQ D Composite 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. The main content area is titled 'Protect Account Data' and includes 'Requirement 3: Protect Stored Account Data'. Below this, there are two paragraphs of text: 'Processes and mechanisms for protecting stored account data are defined and understood' and 'Storage of account data is kept to a minimum.' A 'Question group 3.2.1' section is visible at the bottom, containing a blue help button labeled 'Help answering this requirement'. On the right side, there is a 'Sections' sidebar with a list of items: 'Build and Maintain a Secure Network and Systems' (checked), 'Protect Account Data' (checked and highlighted with a blue background), 'Maintain a Vulnerability Management Program' (checked), 'Implement Strong Access Control Measures' (checked), 'Maintain an Information Security Policy' (checked), and 'Confirm your compliance' (unchecked and red).

- You will see within the 'sections' area shown above you will have one question relating to 'protecting account data' and one question relating to 'implement 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.
- 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.

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.
- 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.

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 D Composite 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.

I have implemented a compensating control

**i** 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 D Composite User Guide

SAQ D Composite User Guide interface showing a section titled "Build and Maintain a Secure Network and Systems". The interface includes a "Show me:" dropdown menu set to "Only unanswered questions" and a "Show Help Text:" toggle set to "Yes". A message states: "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 visible. The "Sections" list on the right includes: "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", and "Confirm your compliance" (highlighted in a red box).

- 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 D Composite User Guide

**Confirm your compliance**  
Please review the form below and ensure all sections are correct and complete

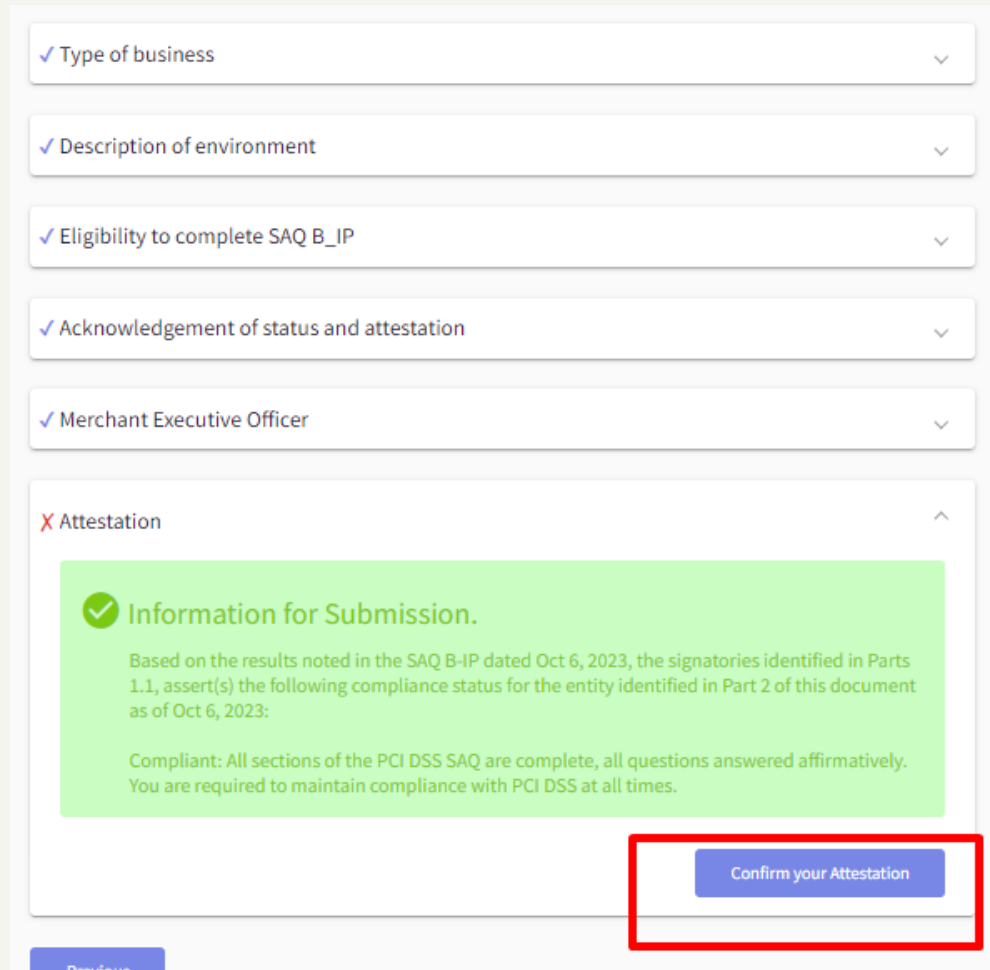
✓ Your organization information details ^

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 D Composite User Guide

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



The screenshot displays a series of dropdown menus for the SAQ D Composite form. The first five dropdowns are expanded, showing a checkmark and the text: '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 collapsed. The 'Attestation' section header is marked with a red 'X' and an upward arrow. The content of the 'Attestation' section is displayed in a green box with a checkmark icon and the heading 'Information for Submission.' The text reads: '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.' A blue button labeled 'Confirm your Attestation' is located at the bottom right of the 'Attestation' section and is highlighted with a red rectangular border. A 'Previous' button is partially visible at the bottom left of the form.

# SAQ D Composite 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 D Composite User Guide

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

The screenshot displays a series of dropdown menus for the SAQ D Composite form. The dropdowns 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 features a green box with a checkmark icon and the text: '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.' A blue button labeled 'Confirm your Attestation' is located at the bottom right of the Attestation section and is highlighted with a red rectangular border. A 'Previous' button is partially visible at the bottom left.

# SAQ D Composite 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.

The screenshot displays a user interface for SAQ D Composite. At the top left, a blue shield icon with a green checkmark is shown above the text "You're compliant", "Valid until 27 March 2025", and a "DOWNLOAD AOC" button. To the right, a large white box contains the text "YOU ARE NOW COMPLIANT" and "Congratulations, you're all done." next to a blue coffee cup icon with steam. Below this, the text "Here are your available compliance tools" is displayed. Two tool cards are shown: "Your business profile" (Complete, SAQ type P2PE) with "More info" and "Manage" buttons, and "Complete security assessment" (Last attested Mar 27, 2024, 12:32:16 PM) with "More Info" and "Manage" buttons.