Pushpay Processing
PCI Self-Certification
Support Documentation

Disclaimer

This complimentary resource is provided as a reference document for Pushpay customers to use in their PCI-DSS Self Assessment questionnaire and attestations on compliance. This is **NOT** a PCI DSS document and it is only meant to help answer the questions within the PCI Self-Assessment Questionnaire. It is important to note that suggested answers are made under the assumption that Pushpay is **YOUR ONLY PROVIDER** in scope to PCI for the SAQ. Your organization is ultimately responsible for the answers provided in your assessment.

Overview

This document incorporates PCI DSS Version 4 and Self-Assessment Questionnaire (SAQ) changes which were made effective in 2024. Some of the screenshots within this document may not be perfectly aligned with the steps/questions shown in the AccessOne portal, if they have changed their layout. As a community resource, if you see a change and want to report it, please email **pci@pushpay.com** with the subject: "**PCI Doc Feedback**" with exactly where the change is and we'll try to update this document as quickly as possible for all customers.

Pushpay is a Level 1 PCI-DSS Service Provider with the highest possible level of compliance. Why do I still need to complete an assessment or be compliant?

- PCI Compliance is a requirement for any organization who accepts credit cards, directly or indirectly. Under PCI, organizations who accept credit cards as a form of payment (even donations) are considered "merchants" even if they are not selling anything.
- Customers who are only accepting donations online via Pushpay have the simplest self-certification process.
- Customers who manually process credit cards using a Kiosk solution will have some additional compliance requirements.

- Due to the complexity of their organizations, larger customers may also have additional requirements. Please reach out to your Customer Success Manager or Pushpay Support to request any additional information/documentation.

If you are unsure if you have further compliance requirements, or have any other questions or issues during the self-certification process, **please call the AccessOne PCI support team at 833-207-8338**.

New Merchants

After signing up with Pushpay, you will receive an email from **support@pciapply.com**, the company Pushpay uses to help you manage your PCI compliance. This tool greatly simplifies your compliance requirements. At its conclusion, you will receive a completed SAQ A document. It is a self-assessment that asserts your compliance with the applicable PCI requirements. You have a 60 day grace period to self-certify, after which time a non-compliance fee of $19.95 is issued each month until you complete the self-certification process. We encourage you to take the time to complete this. Depending on your familiarity with PCI, this process can take anywhere from 30 mins to 4 hours, if reading all the optional docs. The certification process can be worked on in stages.

Existing Merchants

As you approach the end of your anniversary you will receive an email alert that your PCI Compliance will expire soon with a link to the AccessOne portal. Log in using your existing Username and Password. After doing so you can update your **Merchant Information** and **Questionnaire**; both sections are required to be compliant. You can skip the **Merchant Information** steps unless you have changes to make.

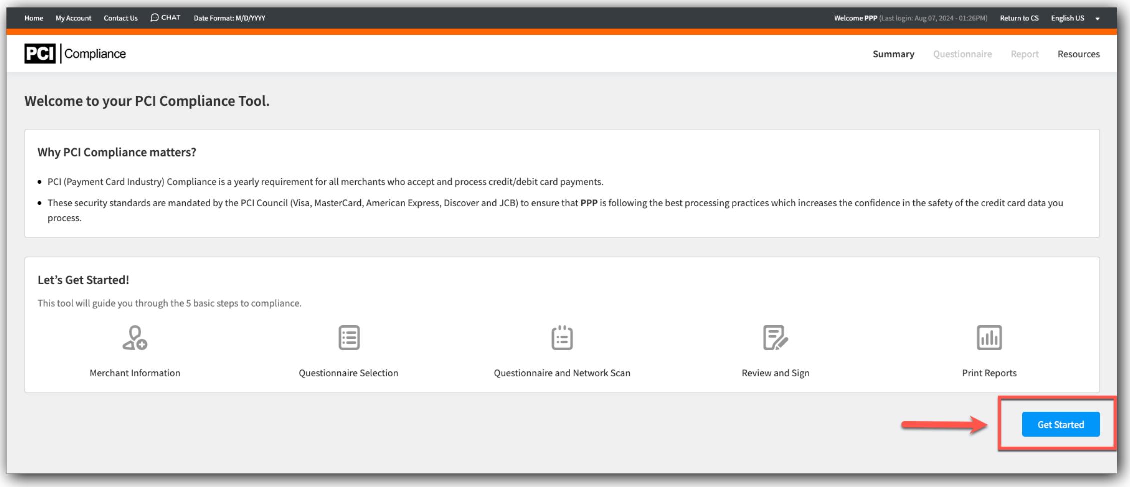
PCI SAQ Instructions

Finding the SAQ

Note: Historically, Pushpay partnered with Clover to assist clients with their PCI compliance, but this process is transitioning to AccessOne/Fiserv. If you have worked with Clover in the past, you may see communications from that team regarding the closing of your Clover logins and new invitations to the AccessOne portal. If you are new to the PCI SAQ, communications should come straight from AccessOne/Fiserv.

1. Open your email from AccessOne containing your PCI portal credentials and log in. If you have trouble getting registered or cannot find the email containing your credentials, please reach out to AccessOne's PCI Customer Service at **833-207-8338**.

2. Once logged into the portal, you should see a Welcome screen. Select **Get Started** (Or, if you've already started the process, and are returning, you can select **Continue**).



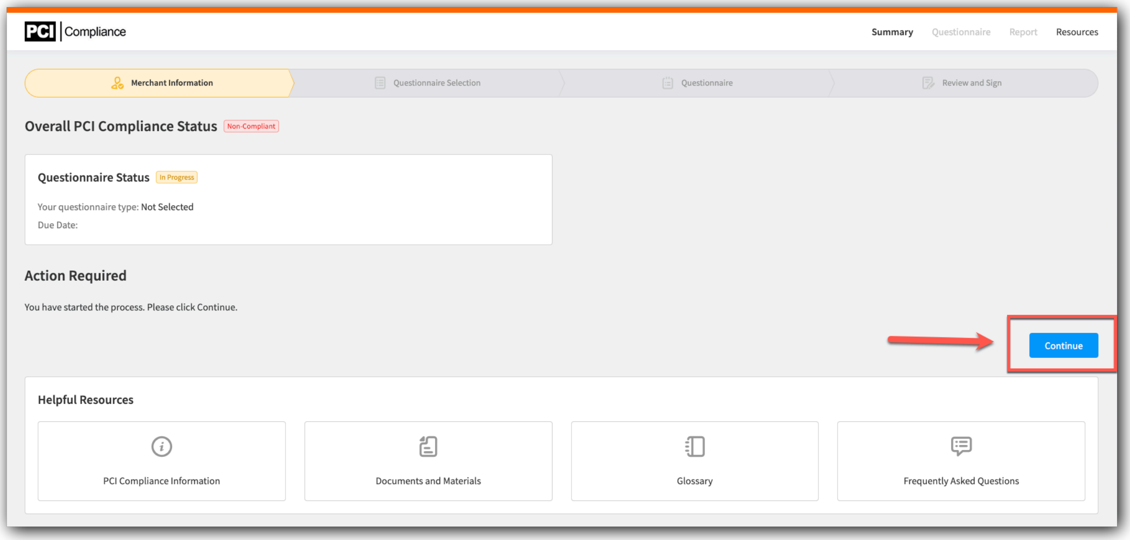
Welcome to your PCI Compliance Tool.

Why PCI Compliance matters?

- PCI (Payment Card Industry) Compliance is a yearly requirement for all merchants who accept and process credit/debit card payments.
- These security standards are mandated by the PCI Council (Visa, MasterCard, American Express, Discover and JCB) to ensure that PPP is following the best processing practices which increases the confidence in the safety of the credit card data you process.

Let's Get Started!

This tool will guide you through the 5 basic steps to compliance.



Overall PCI Compliance Status Non-Compliant

Questionnaire Status In Progress

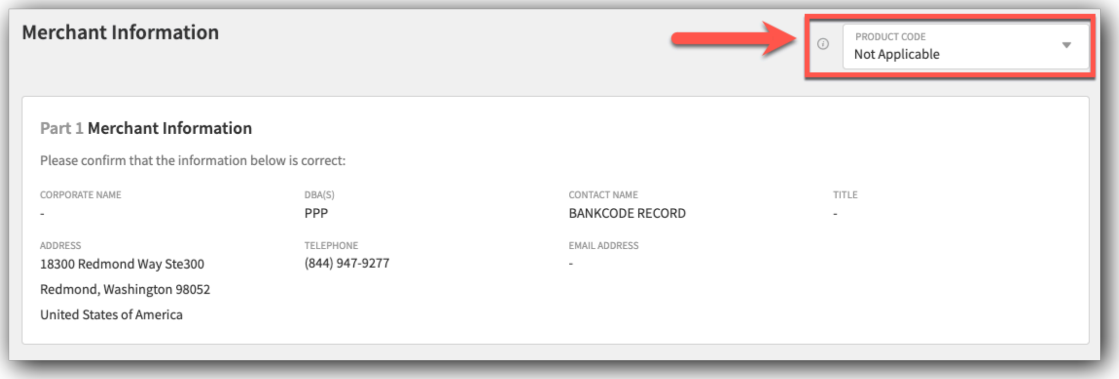
Your questionnaire type: Not Selected

Due Date:

Action Required

You have started the process. Please click Continue.

3. You will now see the option to enter Merchant Information, and answer questions regarding your payment channels and processing solutions. Leave the **Product Code** box as **Not Applicable**.



Merchant Information

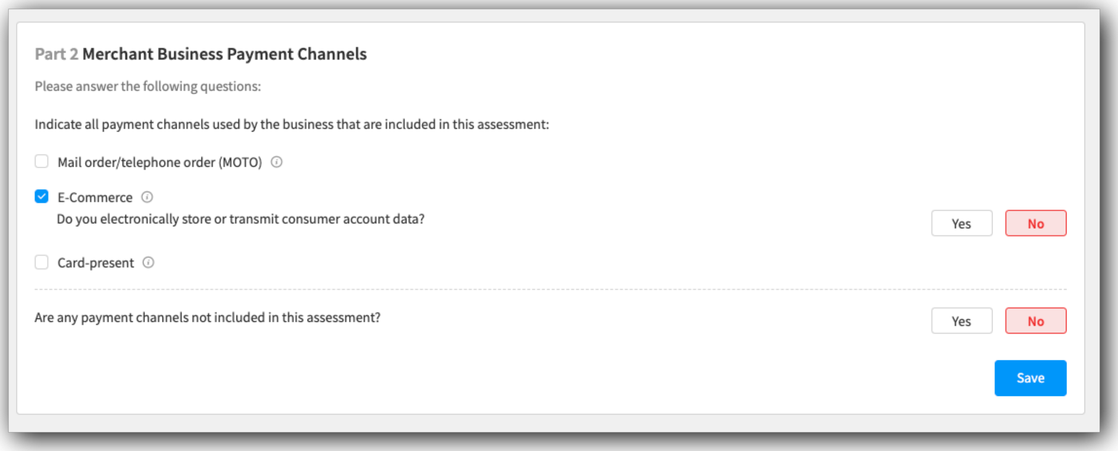
PRODUCT CODE
Not Applicable

Part 1 Merchant Information

Please confirm that the information below is correct:

CORPORATE NAME	DBA(S)	CONTACT NAME	TITLE
-	PPP	BANKCODE RECORD	-
ADDRESS	TELEPHONE	EMAIL ADDRESS	
18300 Redmond Way Ste300 Redmond, Washington 98052 United States of America	(844) 947-9277	-	

4. In **Merchant Business Payment Channels**, select **E-Commerce**



Part 2 Merchant Business Payment Channels

Please answer the following questions:

Indicate all payment channels used by the business that are included in this assessment:

□ Mail order/telephone order (MOTO)

☑ E-Commerce

Do you electronically store or transmit consumer account data? Yes [✓ No]

□ Card-present

Are any payment channels not included in this assessment? Yes [✓ No]

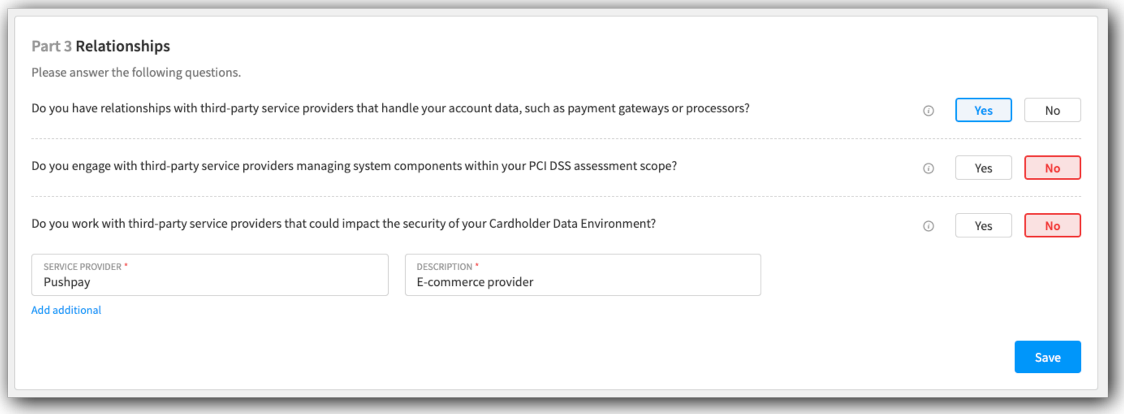
Save

5. For "*Do you electronically store or transmit consumer account data*", select **No**.

6. For "*Are any payment channels not included in this assessment*", select **No**.

7. In **Part 3 - Relationships**, For "*Do you have relationships with third-party service providers that handle your account data, such as payment gateways or processors*",

select **Yes.**



Part 3 **Relationships**

Please answer the following questions.

Do you have relationships with third-party service providers that handle your account data, such as payment gateways or processors? [✓ Yes] No

Do you engage with third-party service providers managing system components within your PCI DSS assessment scope? Yes [✓ No]

Do you work with third-party service providers that could impact the security of your Cardholder Data Environment? Yes [✓ No]

SERVICE PROVIDER * Pushpay

DESCRIPTION * E-commerce provider

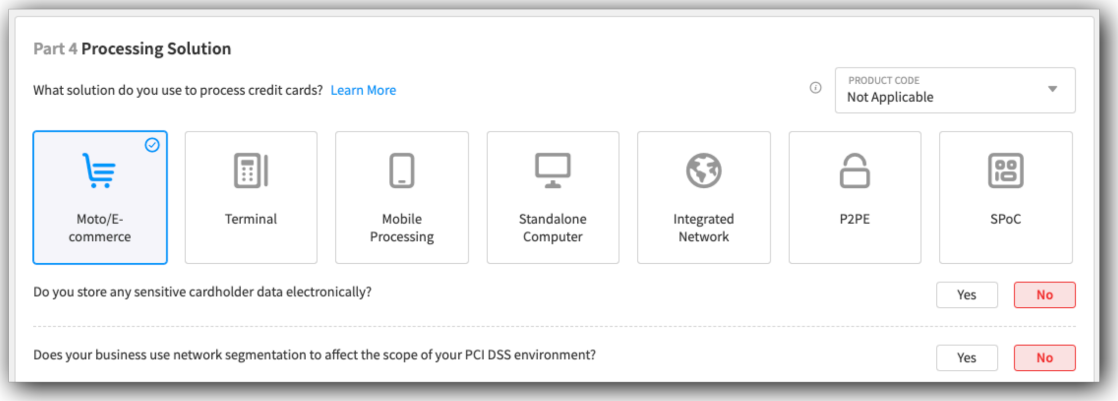
8. For "*Do you engage with third-party service providers managing system components within your PCI DSS assessment scope*", select **No**.

9. For "*Do you work with third-party service providers that could impact the security of your Cardholder Data Environment*", select **No**.

10. In the **Service Provider** field, enter **Pushpay**.

11. In the **Description** field, enter **E-Commerce provider.**

12. In **Part 4 - Processing Solution**, again leave the **Product Code** field as **Not Applicable**. Then select **Moto/E-commerce.**



Part 4 **Processing Solution**

What solution do you use to process credit cards? Learn More

PRODUCT CODE Not Applicable

[✓ Moto/E-commerce] Terminal Mobile Processing Standalone Computer Integrated Network P2PE SPoC

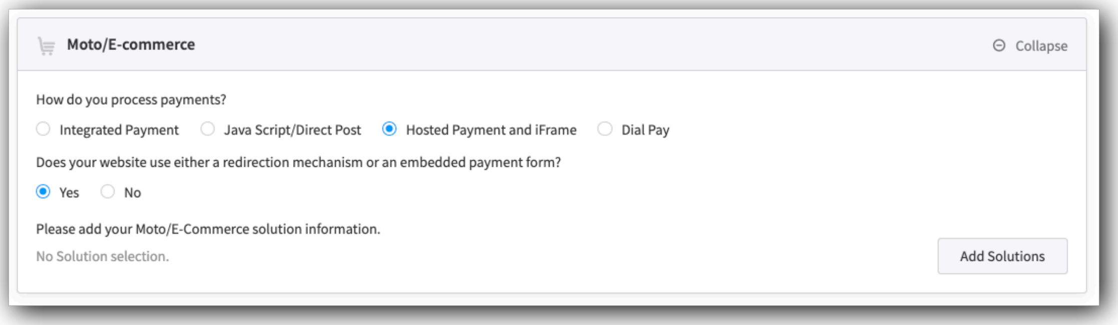
Do you store any sensitive cardholder data electronically? Yes [✓ No]

Does your business use network segmentation to affect the scope of your PCI DSS environment? Yes [✓ No]

13. For "*Do you store any sensitive cardholder data electronically*", select **No**.

14. For "*Does your business use network segmentation to affect the scope of your PCI DSS environment*", select **No**.

15. In the box that appears asking *"How do you process payments*", select **Hosted Payment and iFrame**.



How do you process payments?

○ Integrated Payment ○ Java Script/Direct Post ● Hosted Payment and iFrame ○ Dial Pay

Does your website use either a redirection mechanism or an embedded payment form?

● Yes ○ No

Please add your Moto/E-Commerce solution information.

No Solution selection.

16. The question "*Does your website use either a redirection mechanism or an embedded payment form"* should appear. Select **Yes**.

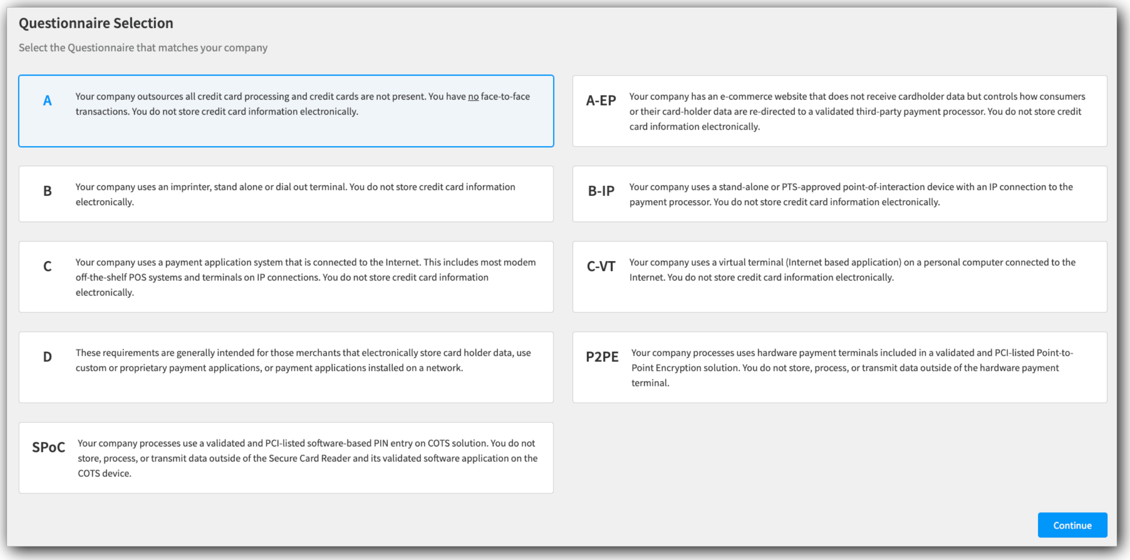
17. You will see an **Add Solutions** box appear. You can ignore this.

18. Check the box to confirm that you've **read and agree to the end-user license agreement.**

19. Choose **Select Questionnaire Manually**.

Note: If your organization has multiple Merchant IDs, you may see a popup message titled **Associated Merchant**. This will appear if the system recognizes that there are other Merchant IDs associated with the ID linked to your AccessOne profile. As noted in the message, select **Yes** if all Merchant IDs will share the same processing procedures and security policies. If this is not the case, select **No** (and each ID will need to have their compliance certified independently).

20. Select **Questionnaire A** then **Continue.**



Questionnaire Selection

Select the Questionnaire that matches your company

A Your company outsources all credit card processing and credit cards are not present. You have no face-to-face transactions. You do not store credit card information electronically.

A-EP Your company has an e-commerce website that does not receive cardholder data but controls how consumers or their card-holder data are re-directed to a validated third-party payment processor. You do not store credit card information electronically.

B Your company uses an imprinter, stand alone or dial out terminal. You do not store credit card information electronically.

B-IP Your company uses a stand-alone or PTS-approved point-of-interaction device with an IP connection to the payment processor. You do not store credit card information electronically.

C Your company uses a payment application system that is connected to the Internet. This includes most modem off-the-shelf POS systems and terminals on IP connections. You do not store credit card information electronically.

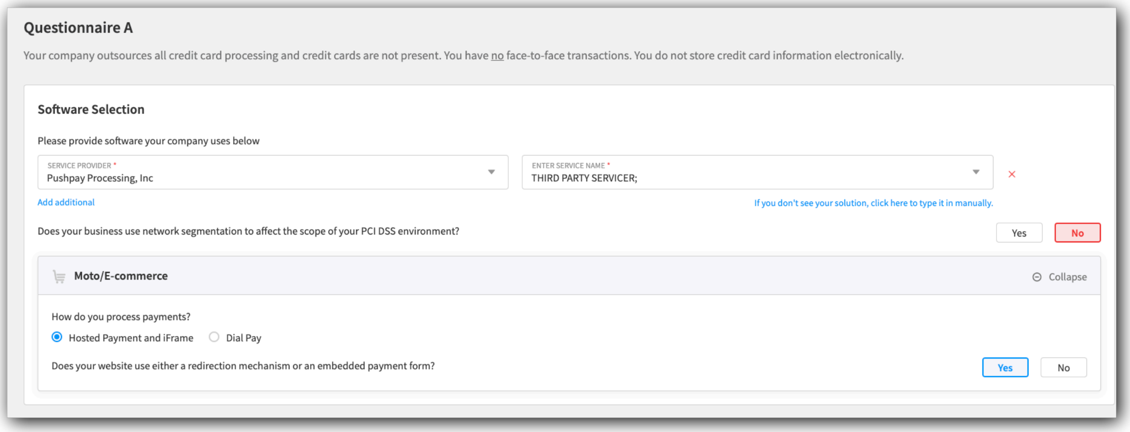
C-VT Your company uses a virtual terminal (Internet based application) on a personal computer connected to the Internet. You do not store credit card information electronically.

D These requirements are generally intended for those merchants that electronically store card holder data, use custom or proprietary payment applications, or payment applications installed on a network.

P2PE Your company processes uses hardware payment terminals included in a validated and PCI-listed Point-to-Point Encryption solution. You do not store, process, or transmit data outside of the hardware payment terminal.

SPoC Your company processes use a validated and PCI-listed software-based PIN entry on COTS solution. You do not store, process, or transmit data outside of the Secure Card Reader and its validated software application on the COTS device.

21. Under **Software selection**, select **Pushpay Processing, Inc** as your **Service Provider.**



Questionnaire A

Your company outsources all credit card processing and credit cards are not present. You have no face-to-face transactions. You do not store credit card information electronically.

Software Selection

Please provide software your company uses below

SERVICE PROVIDER * Pushpay Processing, Inc

ENTER SERVICE NAME * THIRD PARTY SERVICER;

Add additional
If you don't see your solution, click here to type it in manually.

Does your business use network segmentation to affect the scope of your PCI DSS environment? Yes [✓ No]

Moto/E-commerce

How do you process payments?

● Hosted Payment and iFrame ○ Dial Pay

Does your website use either a redirection mechanism or an embedded payment form? [✓ Yes] No

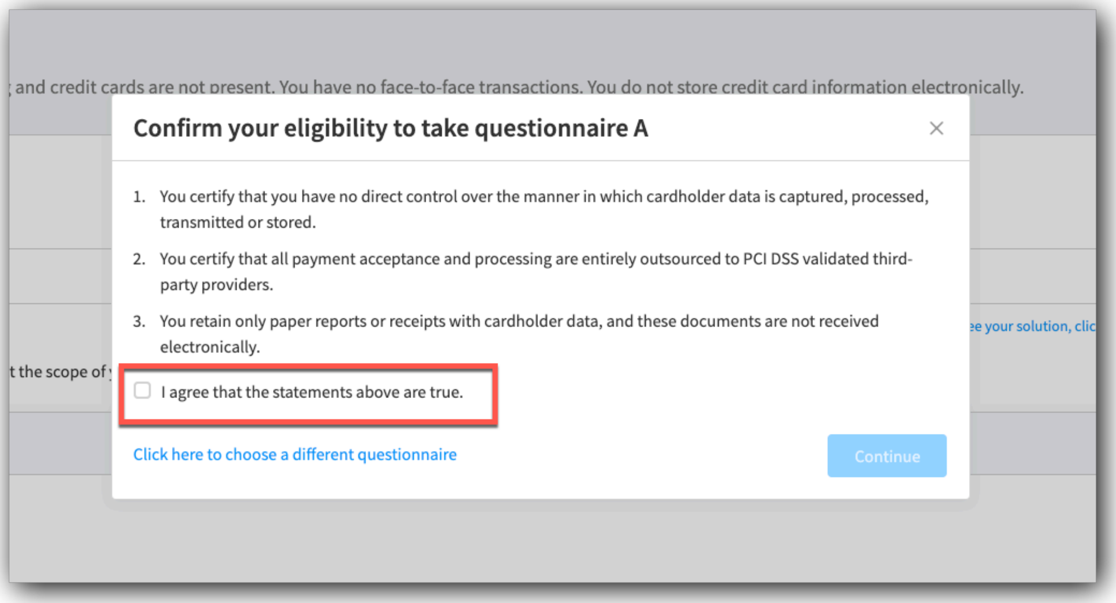
22. Select **Third Party Servicer** in the **Enter Service Name** field (it should be the only option)

23. As before, for *"Does your business use network segmentation to affect the scope of your PCI DSS environment"* select **No**.

24. As before, for *"How do you process payments"*, select **Hosted Payment and iFrame**.

25. As before, for *"Does your website use either a redirection mechanism or an embedded payment form"*, select **Yes**, then **Continue** below.

26. Confirm that you agree, then select **Continue** to confirm your eligibility to take Questionnaire A.



and credit cards are not present. You have no face-to-face transactions. You do not store credit card information electronically.

Confirm your eligibility to take questionnaire A

1. You certify that you have no direct control over the manner in which cardholder data is captured, processed, transmitted or stored.
2. You certify that all payment acceptance and processing are entirely outsourced to PCI DSS validated third-party providers.
3. You retain only paper reports or receipts with cardholder data, and these documents are not received electronically.

□ I agree that the statements above are true.

Questionnaire

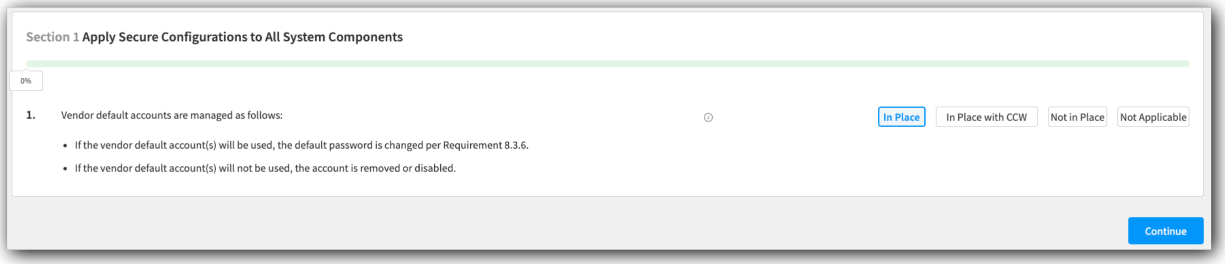
You will see a screen outlining the sections of Questionnaire A. Select **Start Questionnaire**.

Note: As mentioned above, It is important to note that suggested answers are made under the assumption that Pushpay is **YOUR ONLY PROVIDER** in scope to PCI for the Self-Assessment Questionnaire (SAQ). Your organization is ultimately responsible for the answers provided in your assessment.

In the sections below, when recommending you select '**In Place**', this guide assumes that you are compliant with the statements/processes listed. If you are unsure if you are compliant, or have any other questions while filling out your SAQ, please call the PCI support team at **833-207-8338**.

Section 1

This section refers to the web platform your website is hosted on. If you are compliant with these statements, select **In Place** for all options.



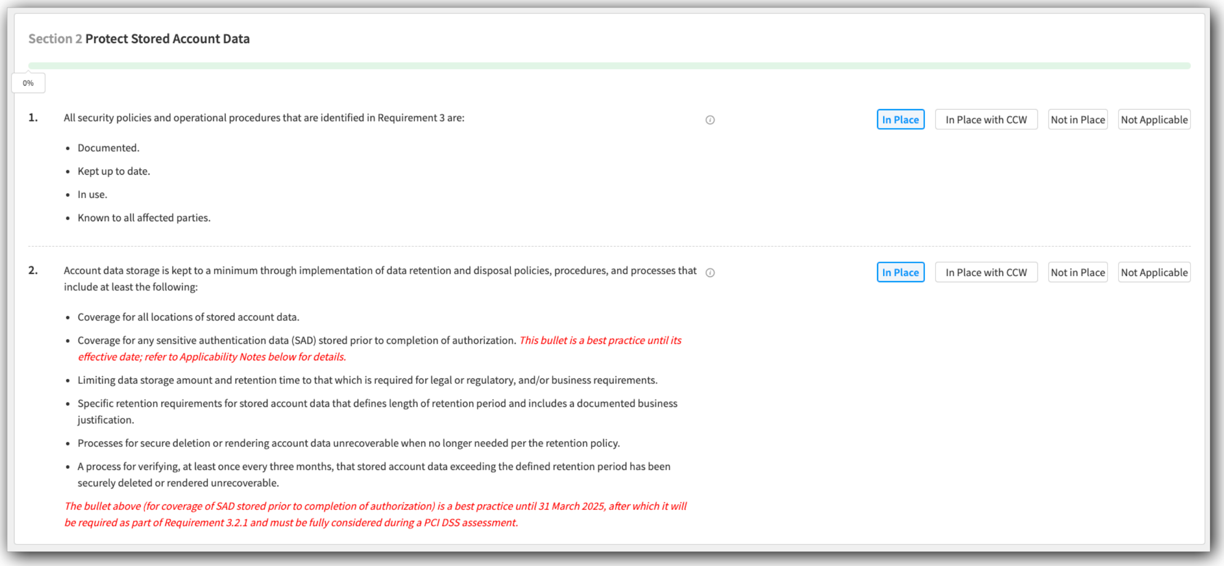
Section 1 Apply Secure Configurations to All System Components

1. Vendor default accounts are managed as follows:
   - If the vendor default account(s) will be used, the default password is changed per Requirement 8.3.6.
   - If the vendor default account(s) will not be used, the account is removed or disabled.

"In Place with CCW" means the control is in place with the aid of additional compensating controls. If this is selected, you will need to complete a Compensating Controls Worksheet (CCW) outside of this tool. Selecting "Not in Place" indicates that you are not compliant with a PCI requirement and may be subject to penalties. "Not Applicable" means that the described capabilities are not relevant to your use or handling of payment information. You will be required to supply a justification if you choose this option.

Section 2

This section applies to **paper** records that include cardholder account data (for example, receipts or printed reports). If you keep paper records you must have documented procedures for handling them. If you are compliant with these statements, select **In Place** for all options.



Section 2 Protect Stored Account Data

1. All security policies and operational procedures that are identified in Requirement 3 are:
   - Documented.
   - Kept up to date.
   - In use.
   - Known to all affected parties.

2. 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.

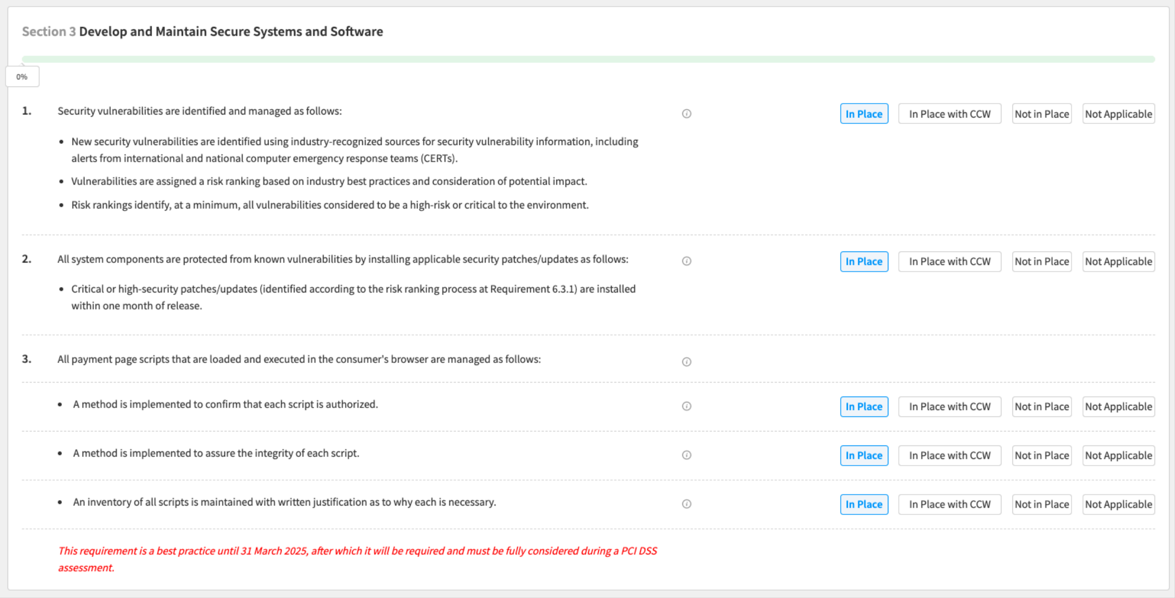
   The bullet above (for coverage of SAD stored prior to completion of authorization) is a best practice until 31 March 2025, after which it will be required as part of Requirement 3.2.1 and must be fully considered during a PCI DSS assessment.

OR

If you do not keep paper records, select **Not Applicable**, and enter “**We do not maintain paper records with account data**” in the text fields provided.

Section 3

This section applies to webservers that host the pages on your website that provide the address (the URL) of Pushpay’s payment page. We recommend that you verify these procedures with your website administrator and/or hosting provider.
If you are compliant with these statements, select **In Place** for all options.



Section 3 **Develop and Maintain Secure Systems and Software**

0%

1. Security vulnerabilities are identified and managed as follows:

- New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs).
- Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact.
- Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment.

[✓ In Place] In Place with CCW Not in Place Not Applicable

2. All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows:

- Critical or high-security patches/updates (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release.

[✓ In Place] In Place with CCW Not in Place Not Applicable

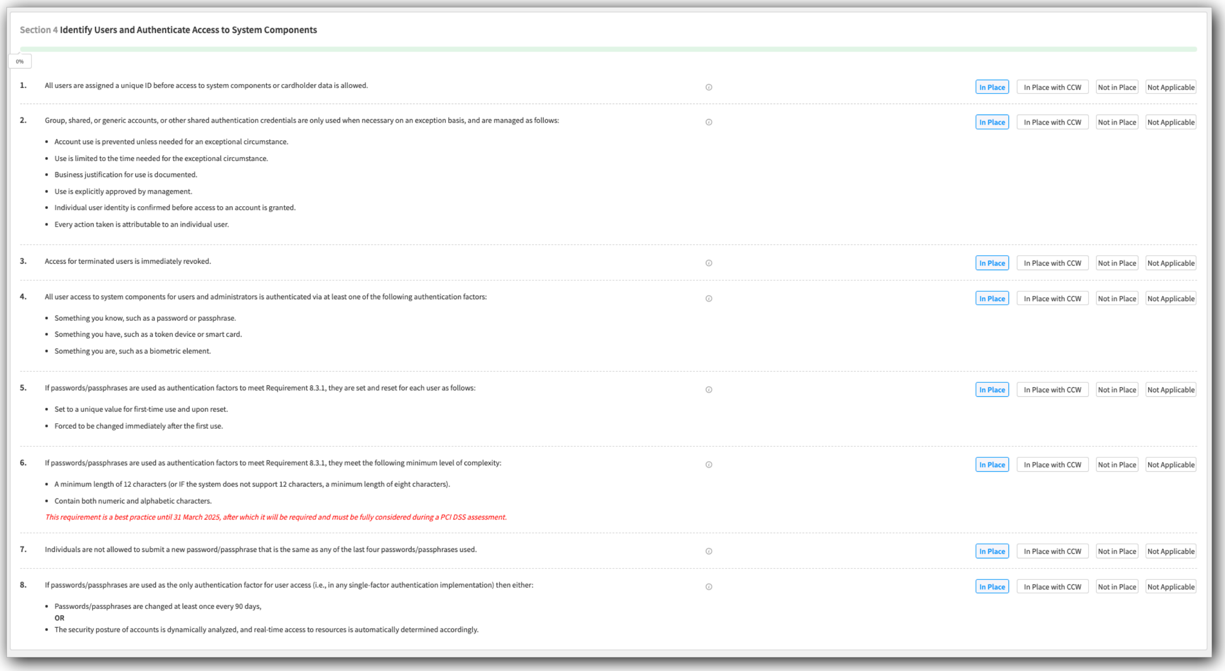
3. All payment page scripts that are loaded and executed in the consumer's browser are managed as follows:

- A method is implemented to confirm that each script is authorized. [✓ In Place] In Place with CCW Not in Place Not Applicable
- A method is implemented to assure the integrity of each script. [✓ In Place] In Place with CCW Not in Place Not Applicable
- An inventory of all scripts is maintained with written justification as to why each is necessary. [✓ In Place] In Place with CCW Not in Place Not Applicable

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

Section 4

Once again this section applies to webservers that host the pages on your website that provide the address (the URL) of Pushpay’s payment page. We recommend that you verify these procedures with your website administrator and/or hosting provider.
If you are compliant with these statements, select **In Place** for all options.



Section 4 **Identify Users and Authenticate Access to System Components**

1. All users are assigned a unique ID before access to system components or cardholder data is allowed.

2. Group, shared, or generic accounts, or other shared authentication credentials are only used when necessary on an exception basis, and are managed as follows:
   - Account use is prevented unless needed for an exceptional circumstance.
   - Use is limited to the time needed for the exceptional circumstance.
   - Business justification for use is documented.
   - Use is explicitly approved by management.
   - Individual user identity is confirmed before access to an account is granted.
   - Every action taken is attributable to an individual user.

3. Access for terminated users is immediately revoked.

4. All user access to system components for users and administrators is authenticated via at least one of the following authentication factors:
   - Something you know, such as a password or passphrase.
   - Something you have, such as a token device or smart card.
   - Something you are, such as a biometric element.

5. If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they are set and reset for each user as follows:
   - Set to a unique value for first-time use and upon reset.
   - Forced to be changed immediately after the first use.

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.

   This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

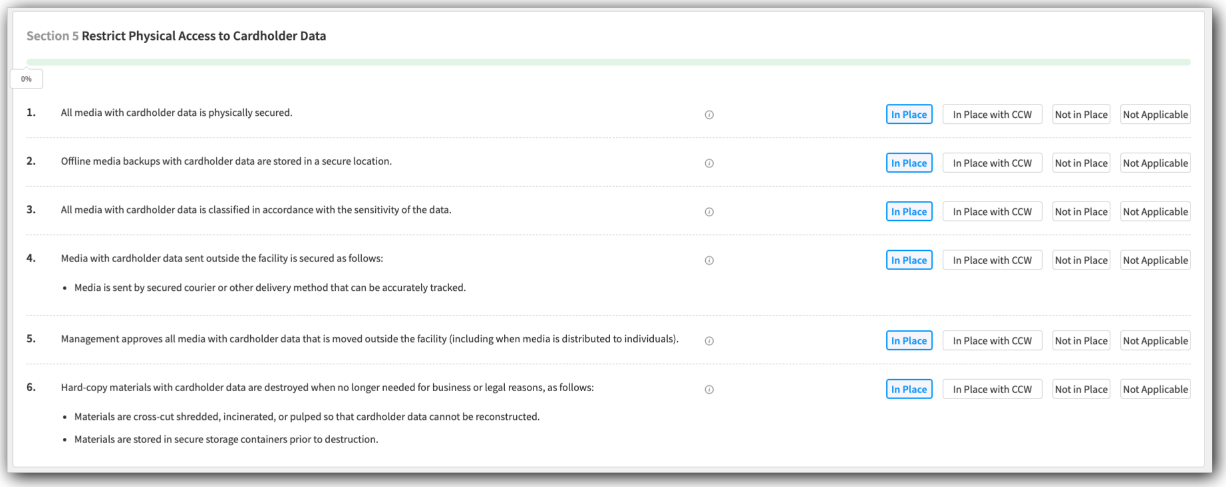
7. Individuals are not allowed to submit a new password/passphrase that is the same as any of the last four passwords/passphrases used.

8. If passwords/passphrases are used as the only authentication factor for user access (i.e., in any single-factor authentication implementation) then either:
   - Passwords/passphrases are changed at least once every 90 days,
     OR
   - The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly.

Section 5

This section applies to **paper** records that include cardholder account data (for example, receipts or printed reports). You should answer based on how you handle **giving slips/envelopes**.

If you handle paper records securely as described here, select **In Place** for all options.



Section 5 **Restrict Physical Access to Cardholder Data**

1. All media with cardholder data is physically secured.

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

3. All media with cardholder data is classified in accordance with the sensitivity of the data.

4. Media with cardholder data sent outside the facility is secured as follows:
   - Media is sent by secured courier or other delivery method that can be accurately tracked.

5. Management approves all media with cardholder data that is moved outside the facility (including when media is distributed to individuals).

6. Hard-copy materials with cardholder data are destroyed when no longer needed for business or legal reasons, as follows:
   - Materials are cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed.
   - Materials are stored in secure storage containers prior to destruction.

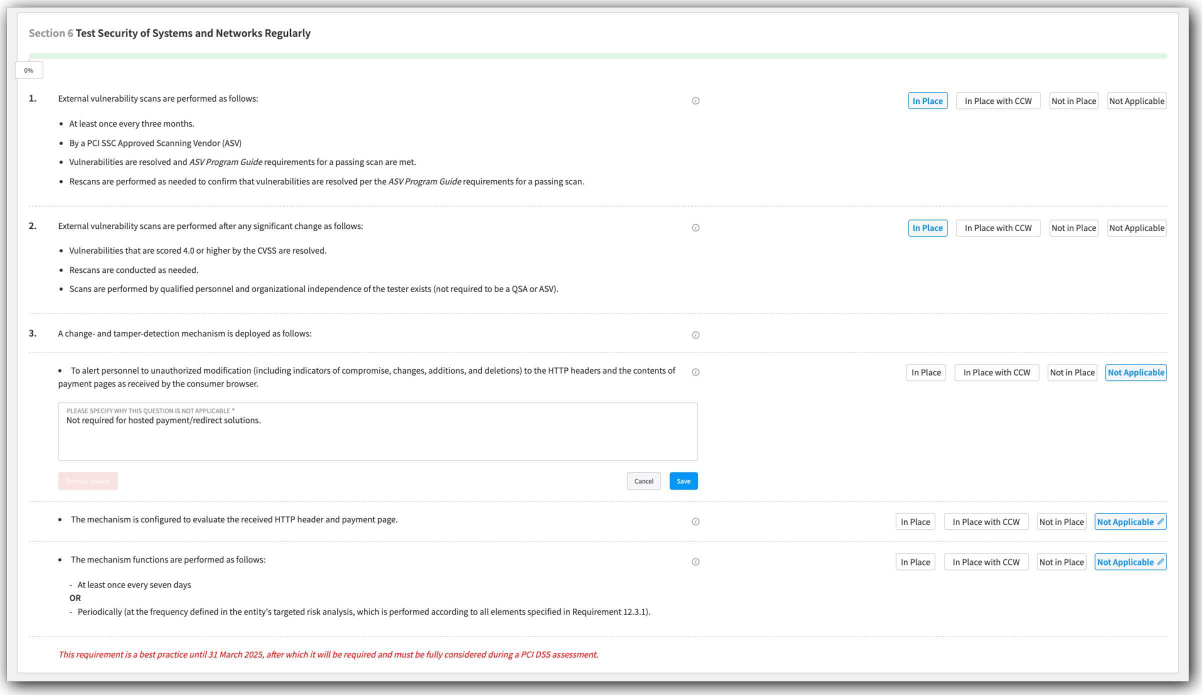
OR

If you do not keep paper records as described here, select **Not Applicable**, and enter "**We do not maintain paper records with account data; we do not have offline media backups**" in the text fields provided.

Section 6

This section applies to webservers that host the pages on your website that provide the address (the URL) of Pushpay's payment page. The portal will assist with setting up the required vulnerability scans in the final step.

1. For number 1, select **In Place.**
2. For number 2, select **In Place.**
3. For number 3, select **Not Applicable** for all 3 bullets.
    a. You should be presented with a text field to specify why the question is not applicable. In all 3 fields, enter **"Not required for hosted payment/redirect solutions."**



Section 6 **Test Security of Systems and Networks Regularly**

0%

1. External vulnerability scans are performed as follows:

- At least once every three months.
- By a PCI SSC Approved Scanning Vendor (ASV)
- Vulnerabilities are resolved and *ASV Program Guide* requirements for a passing scan are met.
- Rescans are performed as needed to confirm that vulnerabilities are resolved per the *ASV Program Guide* requirements for a passing scan.

[✓ In Place] In Place with CCW Not in Place Not Applicable

2. External vulnerability scans are performed after any significant change as follows:

- Vulnerabilities that are scored 4.0 or higher by the CVSS are resolved.
- Rescans are conducted as needed.
- Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV).

[✓ In Place] In Place with CCW Not in Place Not Applicable

3. A change- and tamper-detection mechanism is deployed as follows:

- To alert personnel to unauthorized modification (including indicators of compromise, changes, additions, and deletions) to the HTTP headers and the contents of payment pages as received by the consumer browser.

In Place In Place with CCW Not in Place [✓ Not Applicable]

PLEASE SPECIFY WHY THIS QUESTION IS NOT APPLICABLE *
Not required for hosted payment/redirect solutions.

- The mechanism is configured to evaluate the received HTTP header and payment page.

In Place In Place with CCW Not in Place [✓ Not Applicable]

- The mechanism functions are performed as follows:

  - At least once every seven days

  OR

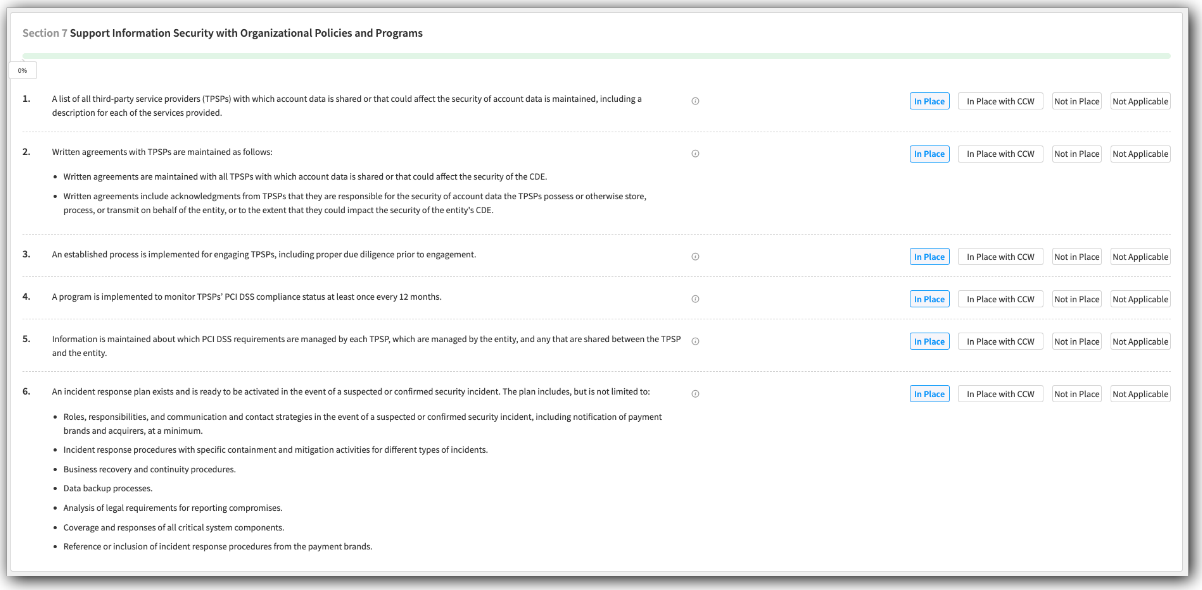
  - Periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1).

In Place In Place with CCW Not in Place [✓ Not Applicable]

This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

Section 7

'Third Party Service Provider (TPSP)' in this section refers to Pushpay. If you are compliant with these statements, select **In Place** for all options. We can supply our latest PCI Attestation of Compliance on request.



Section 7 Support Information Security with Organizational Policies and Programs

1. A list of all third-party service providers (TPSPs) with which account data is shared or that could affect the security of account data is maintained, including a description for each of the services provided.

2. Written agreements with TPSPs are maintained as follows:
   - Written agreements are maintained with all TPSPs with which account data is shared or that could affect the security of the CDE.
   - Written agreements include acknowledgments from TPSPs that they are responsible for the security of account data the TPSPs possess or otherwise store, process, or transmit on behalf of the entity, or to the extent that they could impact the security of the entity's CDE.

3. An established process is implemented for engaging TPSPs, including proper due diligence prior to engagement.

4. A program is implemented to monitor TPSPs' PCI DSS compliance status at least once every 12 months.

5. Information is maintained about which PCI DSS requirements are managed by each TPSP, which are managed by the entity, and any that are shared between the TPSP and the entity.

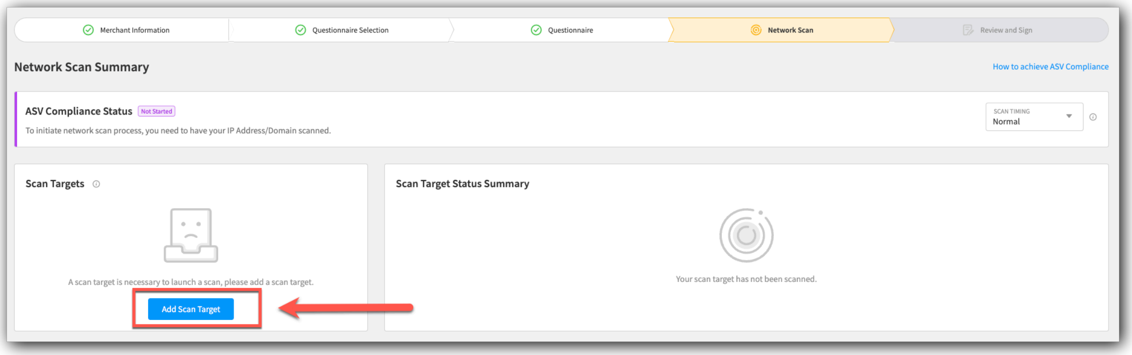
6. An incident response plan exists and is ready to be activated in the event of a suspected or confirmed security incident. The plan includes, but is not limited to:
   - Roles, responsibilities, and communication and contact strategies in the event of a suspected or confirmed security incident, including notification of payment brands and acquirers, at a minimum.
   - Incident response procedures with specific containment and mitigation activities for different types of incidents.
   - Business recovery and continuity procedures.
   - Data backup processes.
   - Analysis of legal requirements for reporting compromises.
   - Coverage and responses of all critical system components.
   - Reference or inclusion of incident response procedures from the payment brands.

Section 8

With PCI DSS version 4, organizations must now conduct quarterly scans using an Approved Scanning Vendor (ASV) for any page on their site that redirects to Pushpay. While Pushpay aggressively scans its applications for vulnerabilities, websites that connect to Pushpay can still be vulnerable to attacks. For this reason, the PCI requires that you scan your website(s), too. Even if your web hosting provider performs vulnerability scans, Pushpay strongly recommends following the steps indicated below. Your provider may not use an ASV, their provided report may include other websites supported by your provider, or there might be delays in receiving the reports. See the **SAQ A** section of the following PCI help document, for more information on the updated requirements for PCI DSS version 4, **visit here:** https://blog.pcisecuritystandards.org/pci-dss-v4-whats-new-with-self-assessment-questionnaires

You may need to work with your web hosting provider to enable these scans and resolve any findings.

1. Select **Add Scan Target**



Network Scan Summary

ASV Compliance Status

To initiate network scan process, you need to have your IP Address/Domain scanned.

SCAN TIMING: Normal

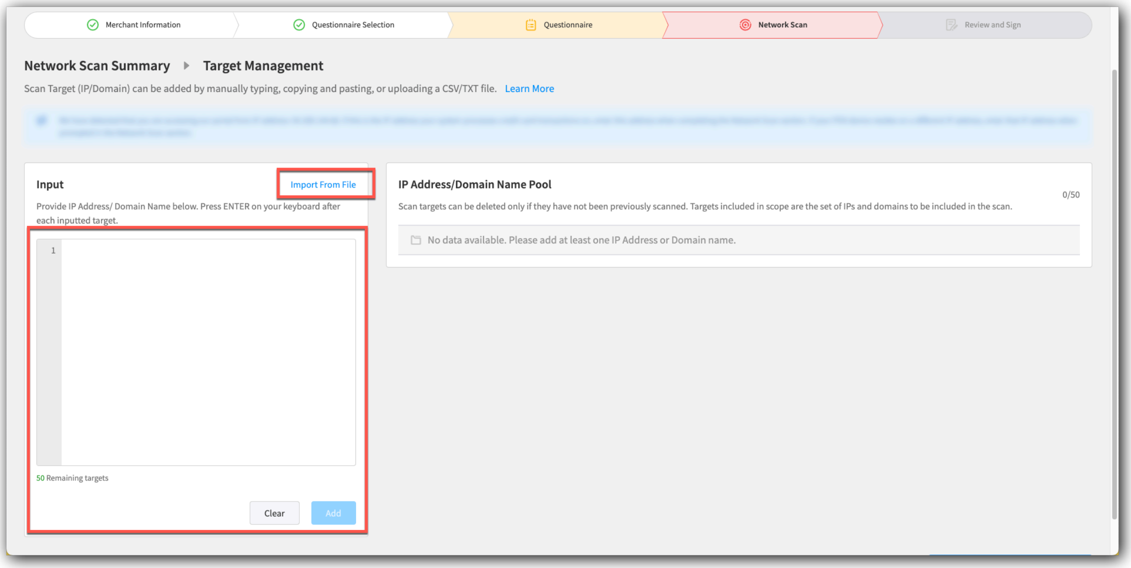
Scan Targets

A scan target is necessary to launch a scan, please add a scan target.

Scan Target Status Summary

Your scan target has not been scanned.

2. Identify all areas of your site in which you have a ‘Give Now’ (or similar) button that sends users to Pushpay to pay or give. Add each of these ‘targets’ (domain or IP) into the **IP Address/Domain Name Pool** either by **1)** typing them into the **Input** field manually, or **2)** selecting **Import from File** to import a CSV or TXT file containing your targets.



Network Scan Summary ▸ Target Management

Scan Target (IP/Domain) can be added by manually typing, copying and pasting, or uploading a CSV/TXT file.

[redacted]

Input

Provide IP Address/ Domain Name below. Press ENTER on your keyboard after each inputted target.

50 Remaining targets

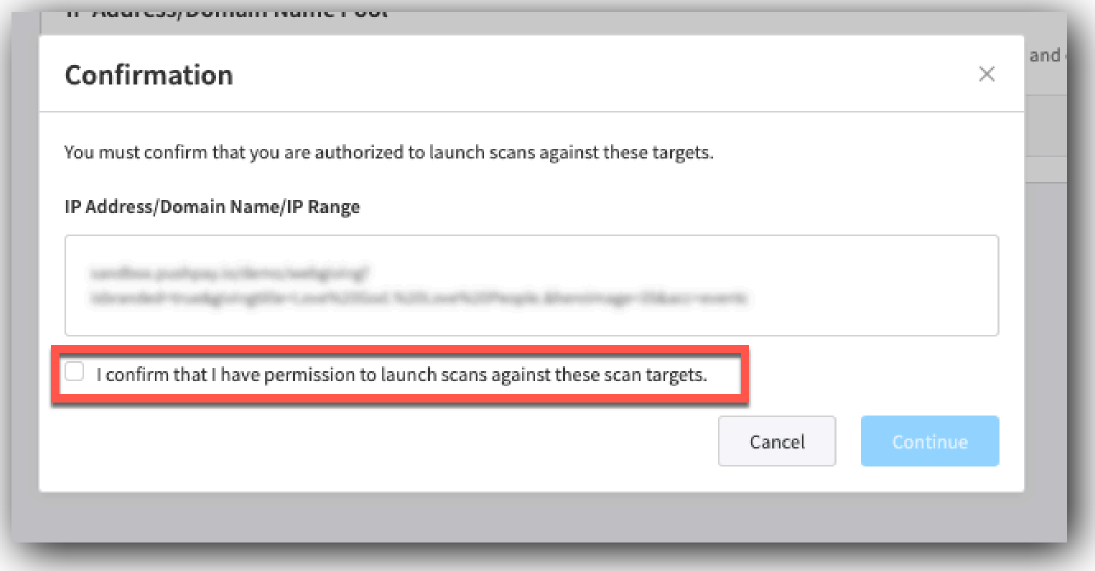
IP Address/Domain Name Pool

0/50

Scan targets can be deleted only if they have not been previously scanned. Targets included in scope are the set of IPs and domains to be included in the scan.

No data available. Please add at least one IP Address or Domain name.

3. After entering a target, click **Add**, and you'll see a confirmation box appear. Confirm that you have permission to scan the target(s) you've added and select **Continue**.



Confirmation

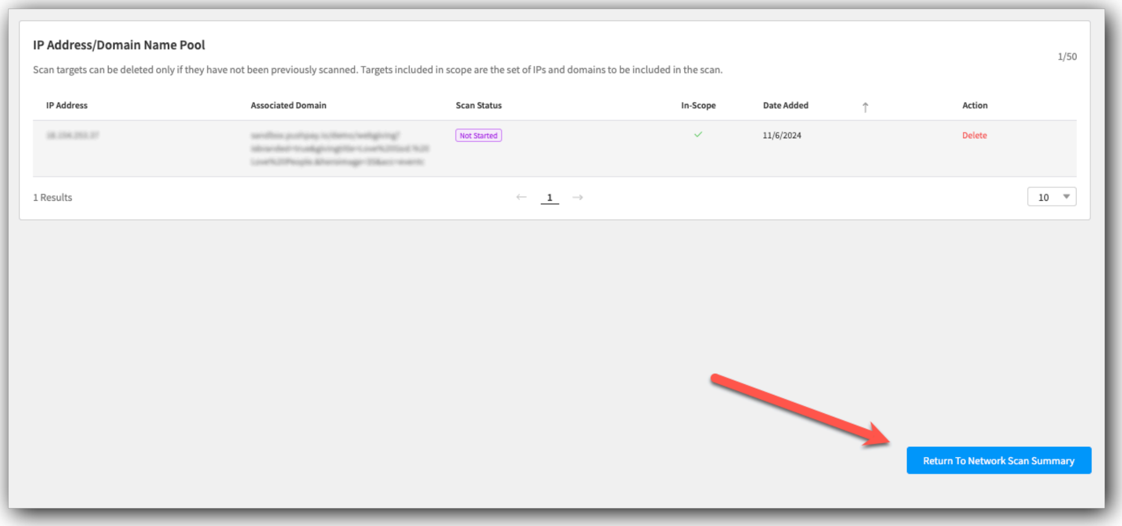
You must confirm that you are authorized to launch scans against these targets.

IP Address/Domain Name/IP Range

[redacted]

□ I confirm that I have permission to launch scans against these scan targets.

4. Once you've added all desired targets and see them added to the **IP Address/Domain Name Pool** on the right, click on **Return to Network Scan Summary** in the bottom-right corner.



IP Address/Domain Name Pool

1/50

Scan targets can be deleted only if they have not been previously scanned. Targets included in scope are the set of IPs and domains to be included in the scan.

IP Address	Associated Domain	Scan Status	In-Scope	Date Added ↑	Action
[redacted]	[redacted]	Not Started	✓	11/6/2024	Delete

1 Results

5. When you're ready to begin your scan, select **Launch Scan**.

If any targets fail the scan, take the suggested actions and work with your IT team and/or hosting provider to resolve them.

Once all chosen targets have a passing scan, you can submit your **ASV Compliance Request**. The ASV team will then review your request.

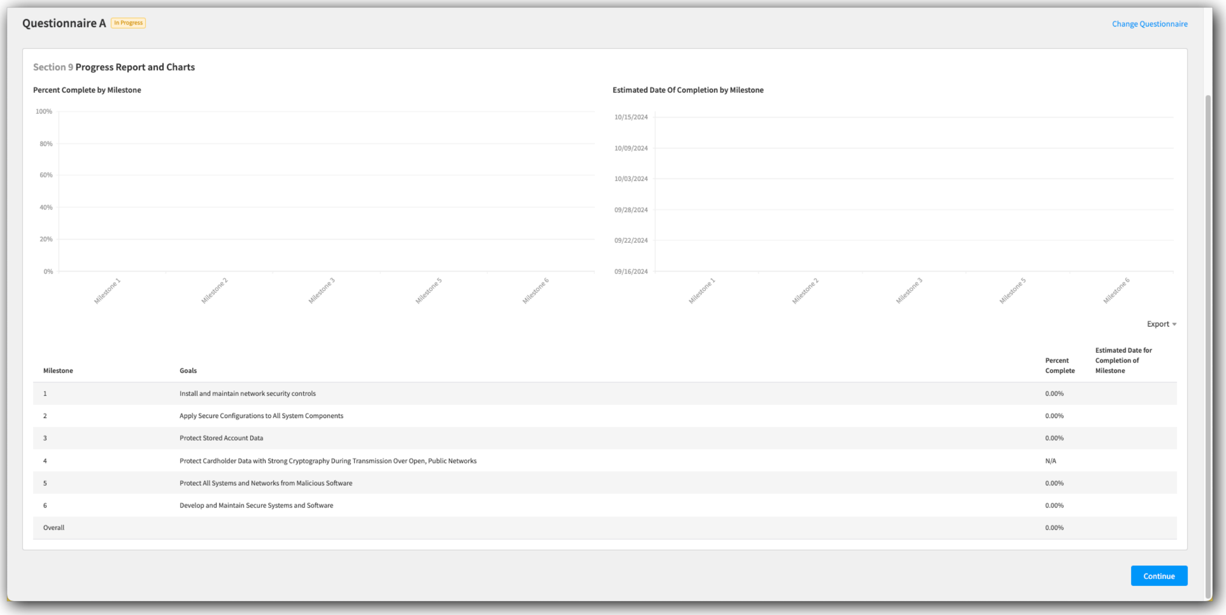
Note: The review process may take 1-2 business days.

It is imperative that you submit a report showing that all chosen targets have a passing scan to maintain your PCI DSS compliance paperwork.

Note: If any questions arise while completing your scan, please reach out to AccessOne's PCI Customer Service team at **833-207-8338**).

Section 9

The final section of the Questionnaire displays a report of milestones to complete. Any outstanding tasks that need to be completed before compliance can be finalized, will be noted here.



Milestone	Goals	Percent Complete	Estimated Date for Completion of Milestone
1	Install and maintain network security controls	0.00%	
2	Apply Secure Configurations to All System Components	0.00%	
3	Protect Stored Account Data	0.00%	
4	Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks	N/A	
5	Protect All Systems and Networks from Malicious Software	0.00%	
6	Develop and Maintain Secure Systems and Software	0.00%	
Overall		0.00%	

Note on Updating your Merchant Information

As we all grow in the space of payment processing, you may find yourself expanding your services, ex: usage of Pushpay for Kiosk, assisting your donors with face to face giving experiences, or taking paper forms with credit card information. If in the future you decide to add these types of new services, you will need to update your Merchant Information, and then your SAQ.

Note: If you have any questions when logging in or updating this information, please reach out to AccessOne's PCI Customer Service team at **833-207-8338**).