Bookstore Manager

Technical Information Document

Filling Out Security Metrics SAQ C 3.2

Document Information:

Category	**Software**	**O/S**	**WinX**	**Last Modified**	**09/14/17**
Author	**JA**				

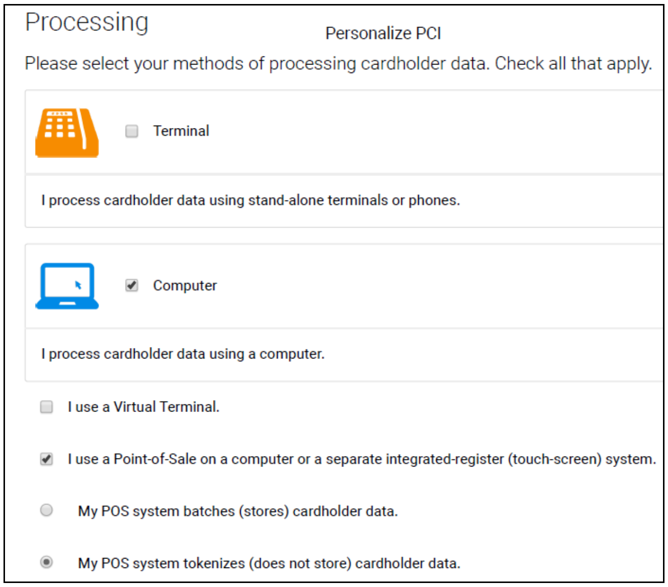
Document Summary

Explains how to fill out the Security Metrics SAQ C 3.2.

Document Contents

Filling Out the SAQ

The first time that you login to Security Metrics website, you will have to agree to their terms. The next window will ask you how you are processing card holder data. (See screenshot below).



Processing

Personalize PCI

Please select your methods of processing cardholder data. Check all that apply.

☐ Terminal

I process cardholder data using stand-alone terminals or phones.

☑ Computer

I process cardholder data using a computer.

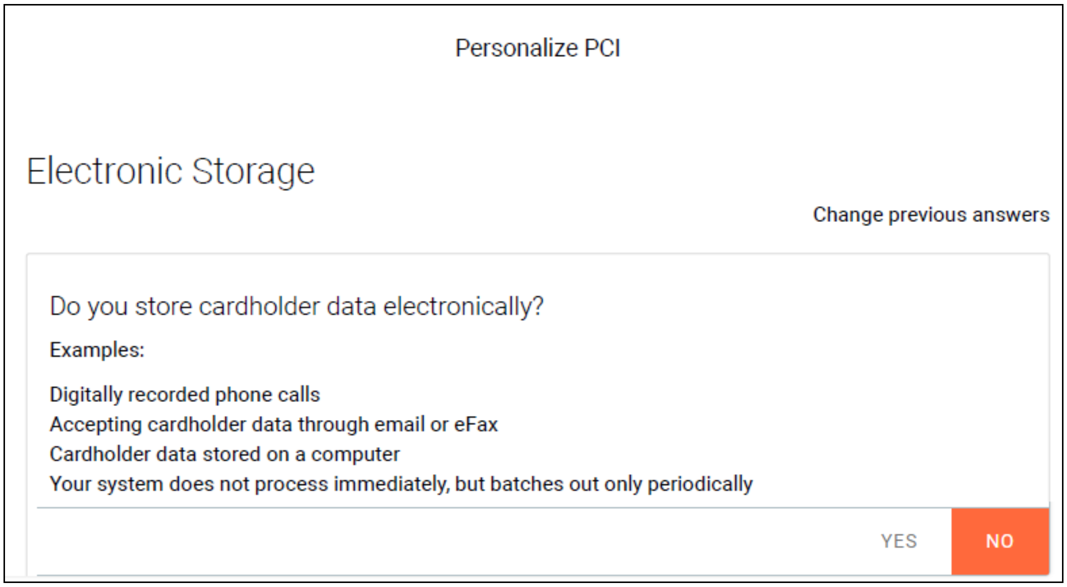
☐ I use a Virtual Terminal.

☑ I use a Point-of-Sale on a computer or a separate integrated-register (touch-screen) system.

○ My POS system batches (stores) cardholder data.

● My POS system tokenizes (does not store) cardholder data.

- Choose Computer
  - Check the box "I use a Point-of-Sale on a computer…"
    - Select "My POS system tokenizes (does not store data)…"
- (See below) The next question you will see is for Electronic Storage. Assuming that you are not storing cardholder data anywhere electronically, you should select NO.



Personalize PCI

Electronic Storage

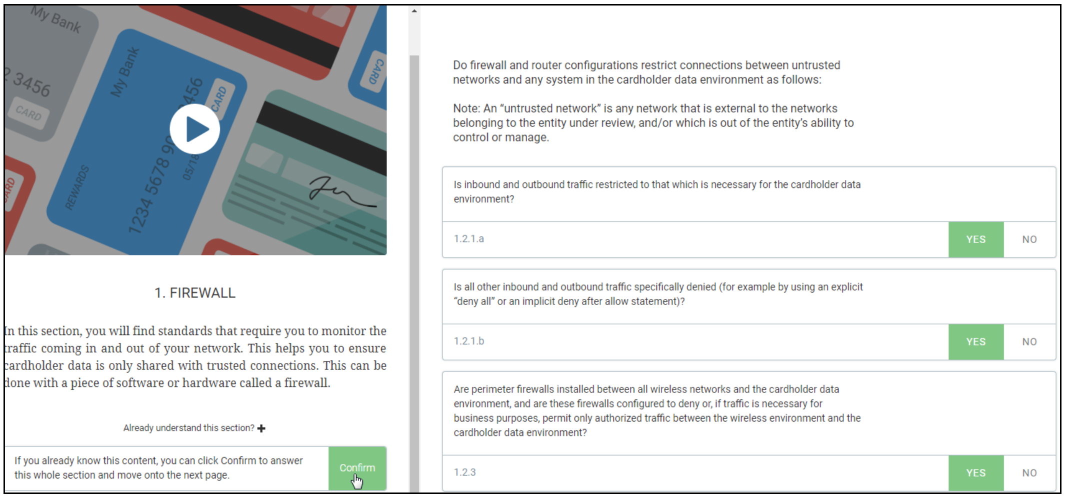
Do you store cardholder data electronically?

Examples:

Digitally recorded phone calls
Accepting cardholder data through email or eFax
Cardholder data stored on a computer
Your system does not process immediately, but batches out only periodically

Section 1. FIREWALL

This section has a short video covering the different aspects of a Firewall. Assuming that you understand and agree with the video, you can click the "+" sign below the video to the right of "Already understand this section" and then click "Confirm". This will automatically set all answers to "YES" and take you to section 2.



1. FIREWALL

In this section, you will find standards that require you to monitor the raffic coming in and out of your network. This helps you to ensure ardholder data is only shared with trusted connections. This can be lone with a piece of software or hardware called a firewall.

Already understand this section? +

If you already know this content, you can click Confirm to answer this whole section and move onto the next page.

Do firewall and router configurations restrict connections between untrusted networks and any system in the cardholder data environment as follows:

Note: An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.

Is inbound and outbound traffic restricted to that which is necessary for the cardholder data environment?

1.2.1.a [✓ YES] NO

Is all other inbound and outbound traffic specifically denied (for example by using an explicit "deny all" or an implicit deny after allow statement)?

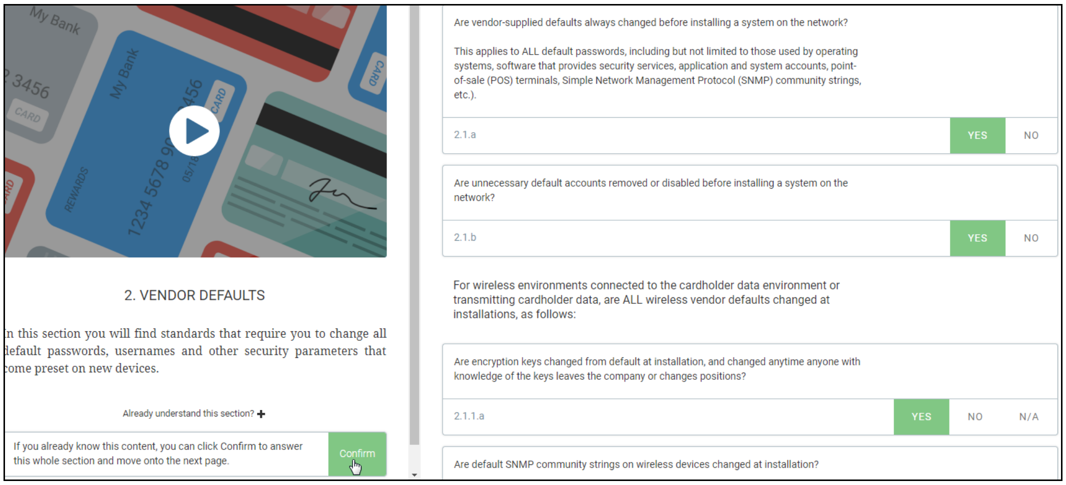
1.2.1.b [✓ YES] NO

Are perimeter firewalls installed between all wireless networks and the cardholder data environment, and are these firewalls configured to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment?

1.2.3 [✓ YES] NO

Section 2. VENDOR DEFAULTS

This section has a short video covering the different aspects of Vendor Defaults. Assuming that you understand and agree with the video, you can click the "+" sign below the video to the right of "Already understand this section" and then click "Confirm". This will automatically set all answers to "YES" and take you to section 3.



2. VENDOR DEFAULTS

n this section you will find standards that require you to change all lefault passwords, usernames and other security parameters that ome preset on new devices.

Already understand this section? +

If you already know this content, you can click Confirm to answer this whole section and move onto the next page.

Are vendor-supplied defaults always changed before installing a system on the network?

This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, Simple Network Management Protocol (SNMP) community strings, etc.).

2.1.a [✓ YES] NO

Are unnecessary default accounts removed or disabled before installing a system on the network?

2.1.b [✓ YES] NO

For wireless environments connected to the cardholder data environment or transmitting cardholder data, are ALL wireless vendor defaults changed at installations, as follows:

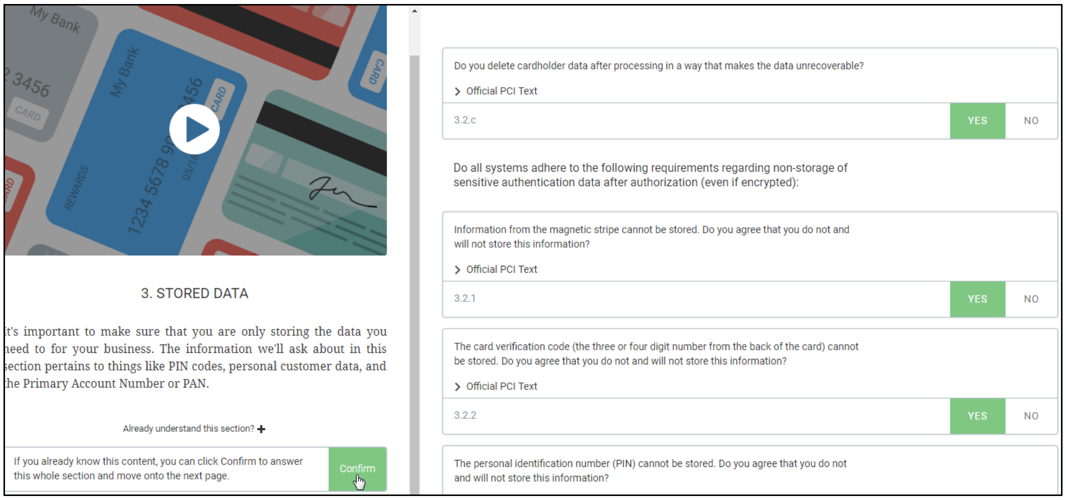
Are encryption keys changed from default at installation, and changed anytime anyone with knowledge of the keys leaves the company or changes positions?

2.1.1.a [✓ YES] NO N/A

Are default SNMP community strings on wireless devices changed at installation?

Section 3. STORED DATA

This section has a short video covering the different aspects of how data is stored. Assuming that you understand and agree with the video, you can click the “+” sign below the video to the right of “Already understand this section” and then click “Confirm”. This will automatically set all answers to “YES” and take you to section 4.



3. STORED DATA

t's important to make sure that you are only storing the data you need to for your business. The information we'll ask about in this section pertains to things like PIN codes, personal customer data, and the Primary Account Number or PAN.

Already understand this section? +

If you already know this content, you can click Confirm to answer this whole section and move onto the next page. Confirm

Do you delete cardholder data after processing in a way that makes the data unrecoverable?

> Official PCI Text

3.2.c YES NO

Do all systems adhere to the following requirements regarding non-storage of sensitive authentication data after authorization (even if encrypted):

Information from the magnetic stripe cannot be stored. Do you agree that you do not and will not store this information?

> Official PCI Text

3.2.1 YES NO

The card verification code (the three or four digit number from the back of the card) cannot be stored. Do you agree that you do not and will not store this information?

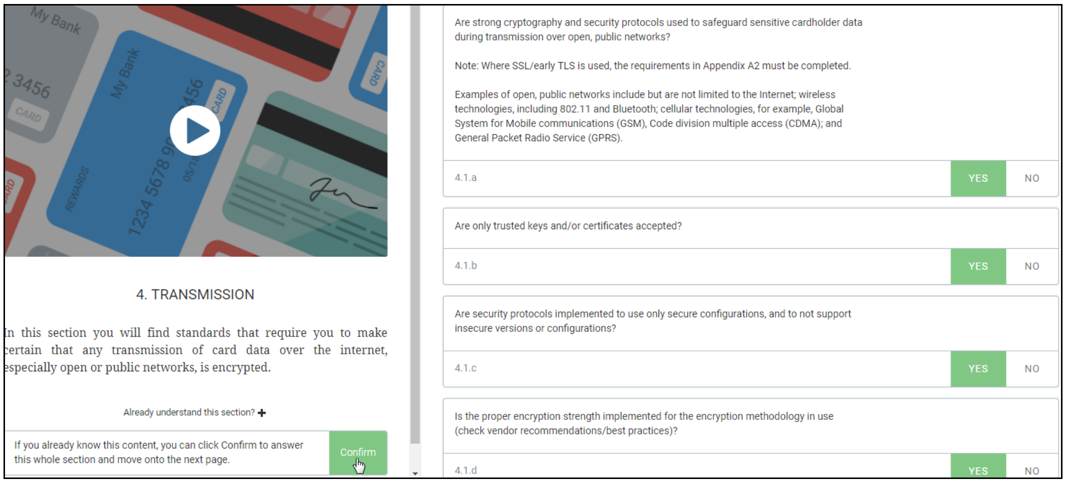
> Official PCI Text

3.2.2 YES NO

The personal identification number (PIN) cannot be stored. Do you agree that you do not and will not store this information?

Section 4. TRANSMISSION

This section has a short video covering the different aspects credit card transmission. Assuming that you understand and agree with the video, you can click the “+” sign below the video to the right of “Already understand this section” and then click “Confirm”. This will automatically set all answers to “YES” and take you to section 5.



4. TRANSMISSION

In this section you will find standards that require you to make certain that any transmission of card data over the internet, especially open or public networks, is encrypted.

Already understand this section? +

If you already know this content, you can click Confirm to answer this whole section and move onto the next page. Confirm

Are strong cryptography and security protocols used to safeguard sensitive cardholder data during transmission over open, public networks?

Note: Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.

Examples of open, public networks include but are not limited to the Internet; wireless technologies, including 802.11 and Bluetooth; cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access (CDMA); and General Packet Radio Service (GPRS).

4.1.a YES NO

Are only trusted keys and/or certificates accepted?

4.1.b YES NO

Are security protocols implemented to use only secure configurations, and to not support insecure versions or configurations?

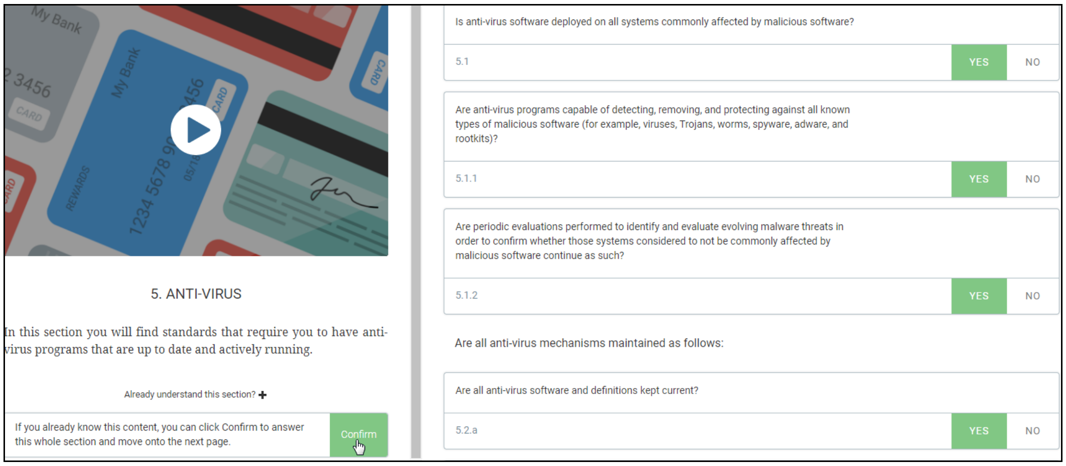
4.1.c YES NO

Is the proper encryption strength implemented for the encryption methodology in use (check vendor recommendations/best practices)?

4.1.d YES NO

Section 5. ANTI-VIRUS

This section has a short video covering the different aspects of an Anti-Virus. Assuming that you understand and agree with the video, you can click the “+” sign below the video to the right of “Already understand this section” and then click “Confirm”. This will automatically set all answers to “YES” and take you to section 6.



5. ANTI-VIRUS

In this section you will find standards that require you to have anti-virus programs that are up to date and actively running.

Already understand this section? +

If you already know this content, you can click Confirm to answer this whole section and move onto the next page.

Is anti-virus software deployed on all systems commonly affected by malicious software?

5.1 YES NO

Are anti-virus programs capable of detecting, removing, and protecting against all known types of malicious software (for example, viruses, Trojans, worms, spyware, adware, and rootkits)?

5.1.1 YES NO

Are periodic evaluations performed to identify and evaluate evolving malware threats in order to confirm whether those systems considered to not be commonly affected by malicious software continue as such?

5.1.2 YES NO

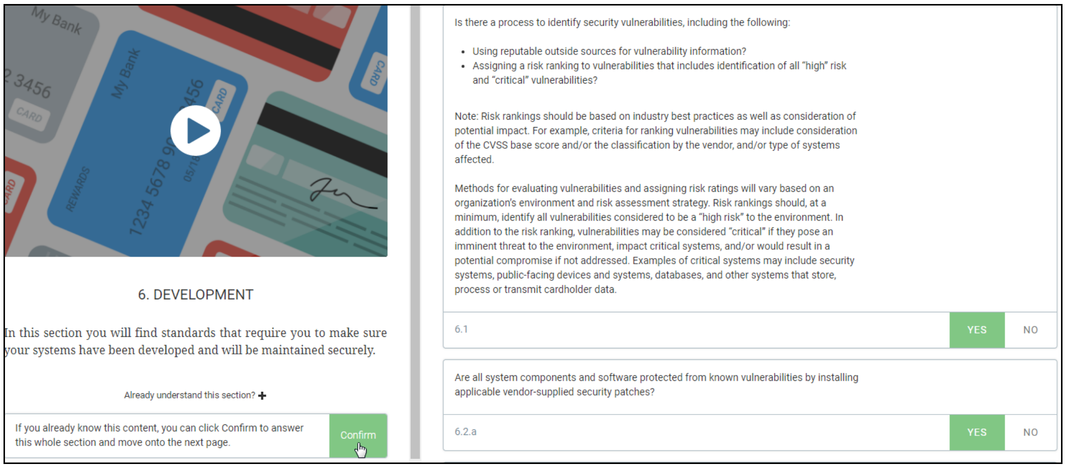
Are all anti-virus mechanisms maintained as follows:

Are all anti-virus software and definitions kept current?

5.2.a YES NO

Section 6. DEVELOPMENT

This section has a short video covering the different aspects of Development. Assuming that you understand and agree with the video, you can click the “+” sign below the video to the right of “Already understand this section” and then click “Confirm”. This will automatically set all answers to “YES” and take you to section 7.



6. DEVELOPMENT

In this section you will find standards that require you to make sure your systems have been developed and will be maintained securely.

Already understand this section? +

If you already know this content, you can click Confirm to answer this whole section and move onto the next page.

Is there a process to identify security vulnerabilities, including the following:

- Using reputable outside sources for vulnerability information?
- Assigning a risk ranking to vulnerabilities that includes identification of all “high” risk and “critical” vulnerabilities?

Note: Risk rankings should be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score and/or the classification by the vendor, and/or type of systems affected.

Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization’s environment and risk assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a “high risk” to the environment. In addition to the risk ranking, vulnerabilities may be considered “critical” if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process or transmit cardholder data.

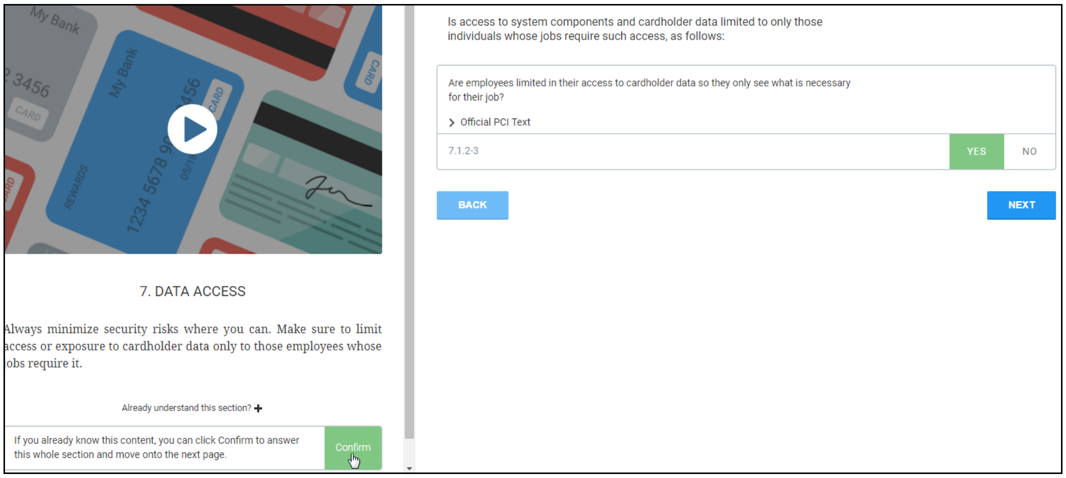
6.1 YES NO

Are all system components and software protected from known vulnerabilities by installing applicable vendor-supplied security patches?

6.2.a YES NO

Section 7. DATA ACCESS

This section has a short video covering the different aspects of how data is accessed. Assuming that you understand and agree with the video, you can click the "+" sign below the video to the right of "Already understand this section" and then click "Confirm". This will automatically set all answers to "YES" and take you to section 8.



7. DATA ACCESS

Always minimize security risks where you can. Make sure to limit access or exposure to cardholder data only to those employees whose jobs require it.

Already understand this section? +

If you already know this content, you can click Confirm to answer this whole section and move onto the next page.

Is access to system components and cardholder data limited to only those individuals whose jobs require such access, as follows:

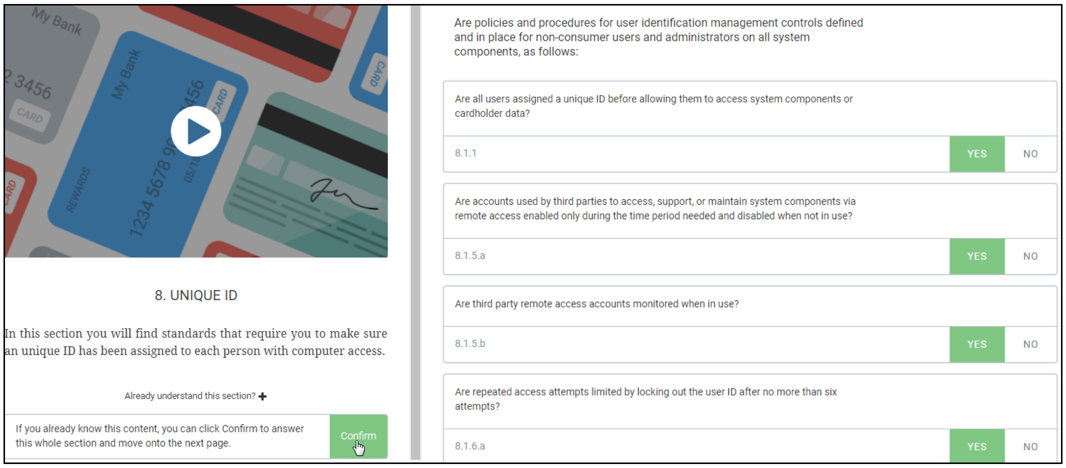
Are employees limited in their access to cardholder data so they only see what is necessary for their job?

> Official PCI Text

7.1.2-3

Section 8. UNIQUE ID

This section has a short video covering the different aspects of each user having a unique ID. Assuming that you understand and agree with the video, you can click the "+" sign below the video to the right of "Already understand this section" and then click "Confirm". This will automatically set all answers to "YES" and take you to section 9.



8. UNIQUE ID

In this section you will find standards that require you to make sure an unique ID has been assigned to each person with computer access.

Already understand this section? +

If you already know this content, you can click Confirm to answer this whole section and move onto the next page.

Are policies and procedures for user identification management controls defined and in place for non-consumer users and administrators on all system components, as follows:

Are all users assigned a unique ID before allowing them to access system components or cardholder data?

8.1.1

Are accounts used by third parties to access, support, or maintain system components via remote access enabled only during the time period needed and disabled when not in use?

8.1.5.a

Are third party remote access accounts monitored when in use?

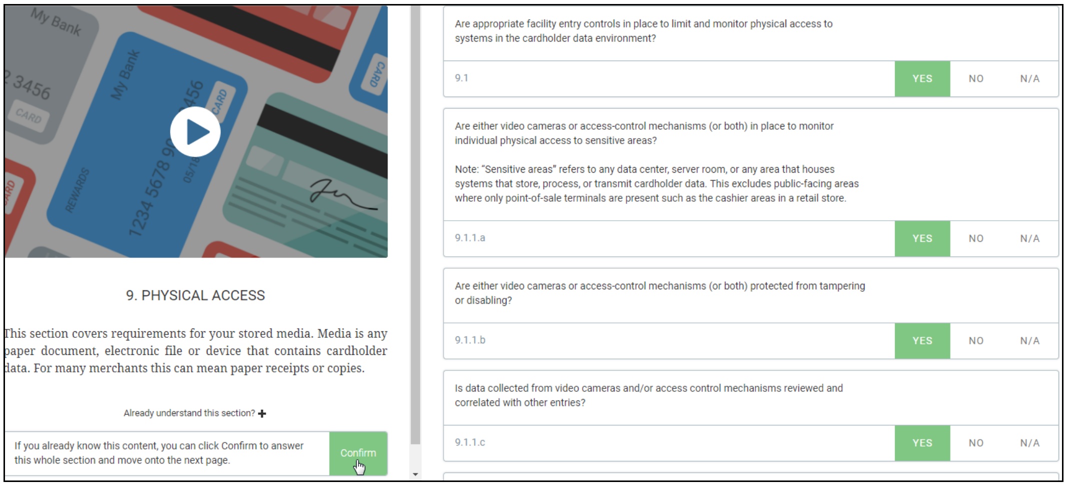
8.1.5.b

Are repeated access attempts limited by locking out the user ID after no more than six attempts?

8.1.6.a

Section 9. PHYSICAL ACCESS

This section has a short video covering the different aspects of physical access to the PC. Assuming that you understand and agree with the video, you can click the "+" sign below the video to the right of "Already understand this section" and then click "Confirm". This will automatically set all answers to "YES" and take you to section 10.



9. PHYSICAL ACCESS

This section covers requirements for your stored media. Media is any paper document, electronic file or device that contains cardholder data. For many merchants this can mean paper receipts or copies.

Already understand this section? +

If you already know this content, you can click Confirm to answer this whole section and move onto the next page.

Confirm

Are appropriate facility entry controls in place to limit and monitor physical access to systems in the cardholder data environment?

9.1 YES NO N/A

Are either video cameras or access-control mechanisms (or both) in place to monitor individual physical access to sensitive areas?

Note: "Sensitive areas" refers to any data center, server room, or any area that houses systems that store, process, or transmit cardholder data. This excludes public-facing areas where only point-of-sale terminals are present such as the cashier areas in a retail store.

9.1.1.a YES NO N/A

Are either video cameras or access-control mechanisms (or both) protected from tampering or disabling?

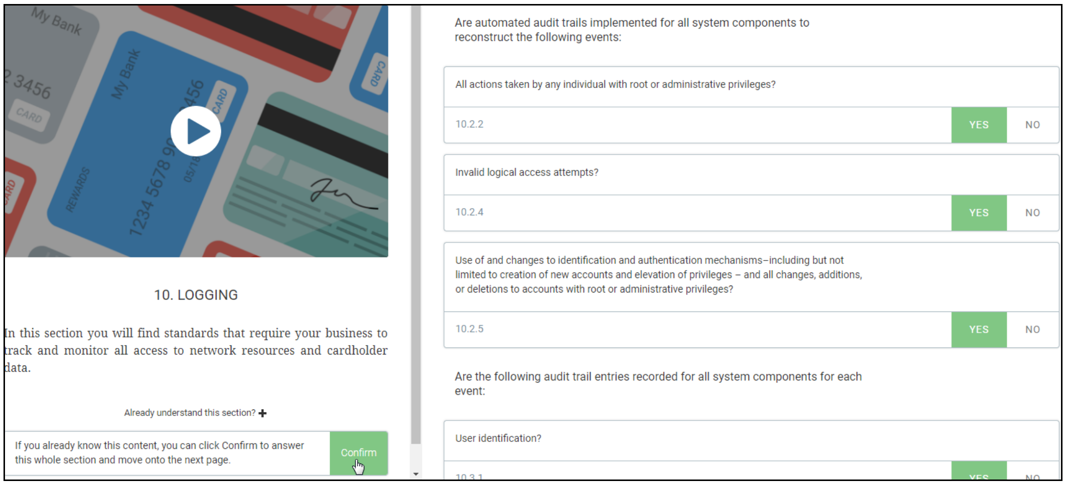
9.1.1.b YES NO N/A

Is data collected from video cameras and/or access control mechanisms reviewed and correlated with other entries?

9.1.1.c YES NO N/A

Section 10. LOGGING

This section has a short video covering the different aspects of logging. Assuming that you understand and agree with the video, you can click the "+" sign below the video to the right of "Already understand this section" and then click "Confirm". This will automatically set all answers to "YES" and take you to section 11.



10. LOGGING

In this section you will find standards that require your business to track and monitor all access to network resources and cardholder data.

Already understand this section? +

If you already know this content, you can click Confirm to answer this whole section and move onto the next page.

Confirm

Are automated audit trails implemented for all system components to reconstruct the following events:

All actions taken by any individual with root or administrative privileges?

10.2.2 YES NO

Invalid logical access attempts?

10.2.4 YES NO

Use of and changes to identification and authentication mechanisms–including but not limited to creation of new accounts and elevation of privileges – and all changes, additions, or deletions to accounts with root or administrative privileges?

10.2.5 YES NO

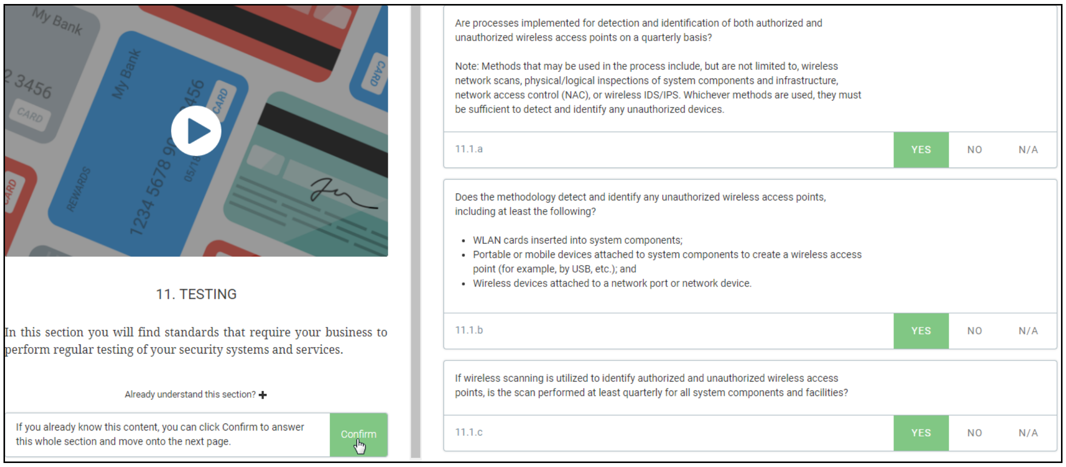
Are the following audit trail entries recorded for all system components for each event:

User identification?

10.3.1 YES NO

Section 11. TESTING

This section has a short video covering the different aspects of Testing. Assuming that you understand and agree with the video, you can click the "+" sign below the video to the right of "Already understand this section" and then click "Confirm". This will automatically set all answers to "YES" and take you to section 12.



11. TESTING

In this section you will find standards that require your business to perform regular testing of your security systems and services.

Already understand this section? +

If you already know this content, you can click Confirm to answer this whole section and move onto the next page.

Are processes implemented for detection and identification of both authorized and unauthorized wireless access points on a quarterly basis?

Note: Methods that may be used in the process include, but are not limited to, wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS. Whichever methods are used, they must be sufficient to detect and identify any unauthorized devices.

11.1.a [✓ YES] NO N/A

Does the methodology detect and identify any unauthorized wireless access points, including at least the following?

- WLAN cards inserted into system components;
- Portable or mobile devices attached to system components to create a wireless access point (for example, by USB, etc.); and
- Wireless devices attached to a network port or network device.

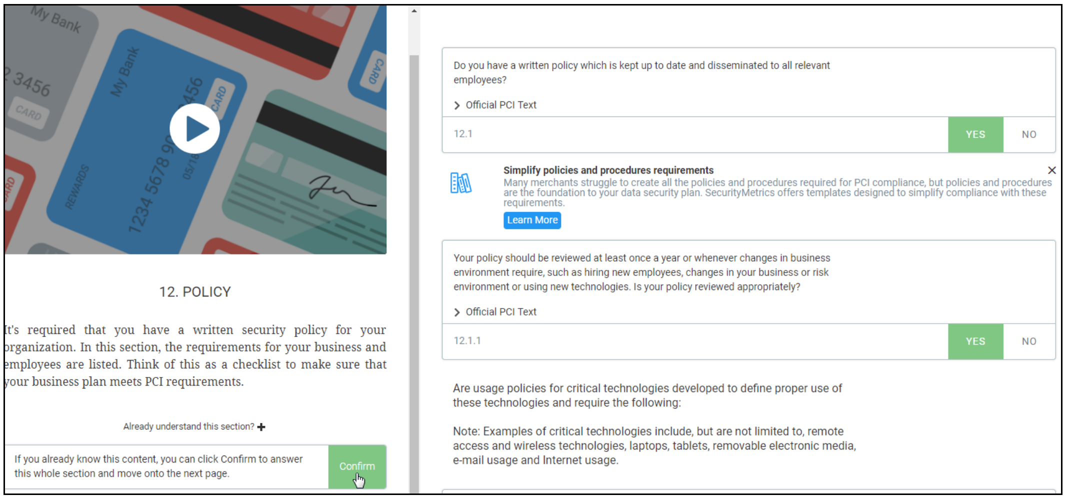
11.1.b [✓ YES] NO N/A

If wireless scanning is utilized to identify authorized and unauthorized wireless access points, is the scan performed at least quarterly for all system components and facilities?

11.1.c [✓ YES] NO N/A

Section 12. POLICY

This section has a short video covering the different aspects of policies. Assuming that you understand and agree with the video, you can click the "+" sign below the video to the right of "Already understand this section" and then click "Confirm". This will automatically set all answers to "YES" and take you to the How do you accept cards? section.



12. POLICY

It's required that you have a written security policy for your organization. In this section, the requirements for your business and employees are listed. Think of this as a checklist to make sure that your business plan meets PCI requirements.

Already understand this section? +

If you already know this content, you can click Confirm to answer this whole section and move onto the next page.

Do you have a written policy which is kept up to date and disseminated to all relevant employees?

> Official PCI Text

12.1 [✓ YES] NO

Simplify policies and procedures requirements
Many merchants struggle to create all the policies and procedures required for PCI compliance, but policies and procedures are the foundation to your data security plan. SecurityMetrics offers templates designed to simplify compliance with these requirements.

Your policy should be reviewed at least once a year or whenever changes in business environment require, such as hiring new employees, changes in your business or risk environment or using new technologies. Is your policy reviewed appropriately?

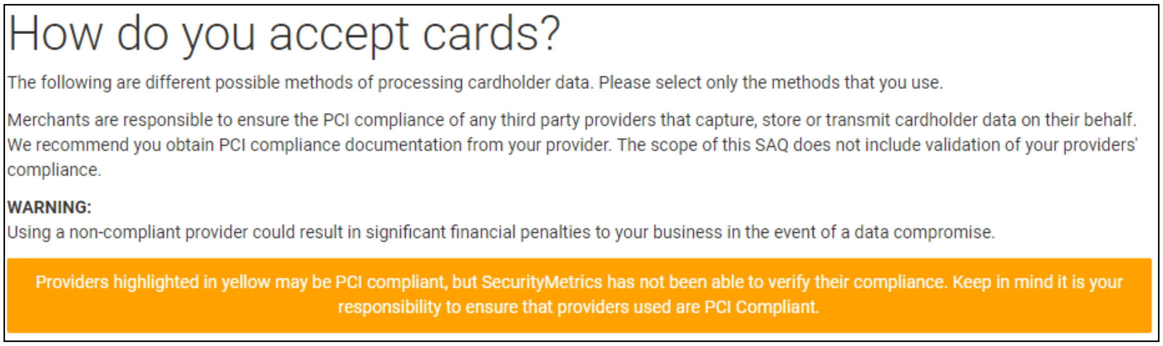
> Official PCI Text

12.1.1 [✓ YES] NO

Are usage policies for critical technologies developed to define proper use of these technologies and require the following:

Note: Examples of critical technologies include, but are not limited to, remote access and wireless technologies, laptops, tablets, removable electronic media, e-mail usage and Internet usage.

How do you accept cards?



How do you accept cards?

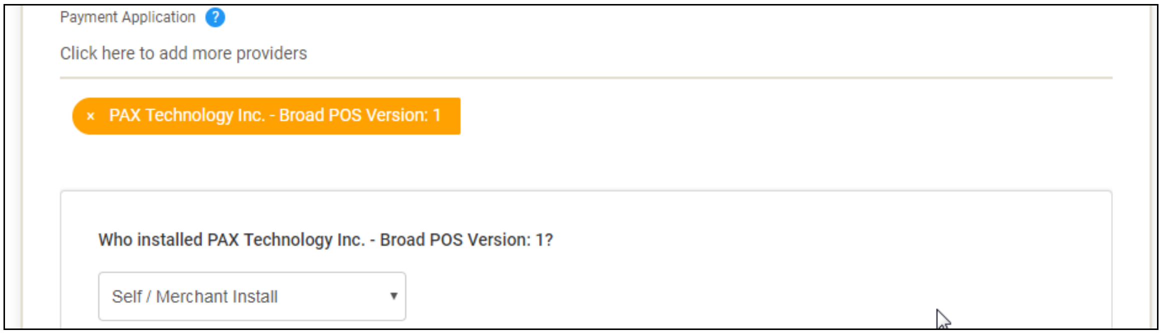
The following are different possible methods of processing cardholder data. Please select only the methods that you use.

Merchants are responsible to ensure the PCI compliance of any third party providers that capture, store or transmit cardholder data on their behalf. We recommend you obtain PCI compliance documentation from your provider. The scope of this SAQ does not include validation of your providers' compliance.

WARNING:
Using a non-compliant provider could result in significant financial penalties to your business in the event of a data compromise.

Providers highlighted in yellow may be PCI compliant, but SecurityMetrics has not been able to verify their compliance. Keep in mind it is your responsibility to ensure that providers used are PCI Compliant.

On the last page, you ONLY have to fill out the last 4 options. **Leave the Payment Gateway, Web Host, Shopping Cart, Co-Location, and Point-of-Sale-Terminal fields blank**!



Payment Application ?

Click here to add more providers

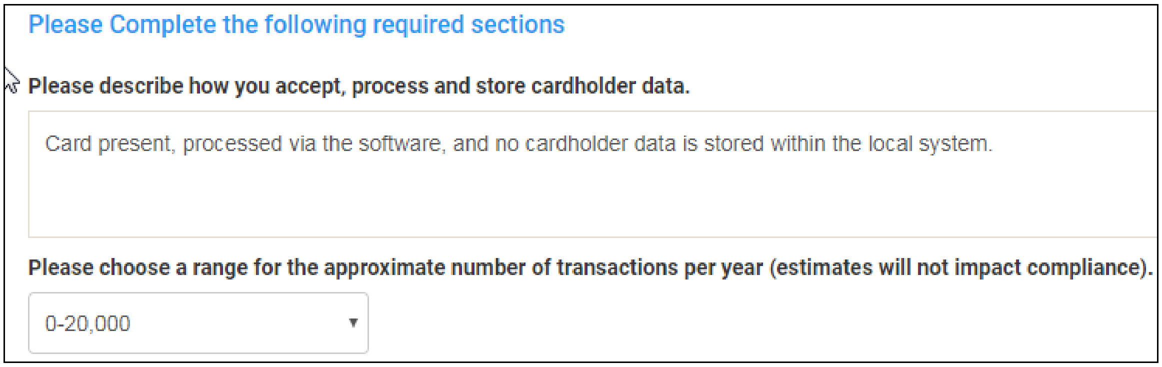
× PAX Technology Inc. - Broad POS Version: 1

Who installed PAX Technology Inc. - Broad POS Version: 1?

Self / Merchant Install ▾

- "Payment Application" should be set to "PAX Technology Inc. - Broad POS Version: 1" (As you type PAX, it should bring up PAX for selecting.)
- "Who installed PAX Technology Inc. - Broad POS Version: 1" should be set to "Self / Merchant Install"

You will have to fill out the last 2 questions.



Please Complete the following required sections

Please describe how you accept, process and store cardholder data.

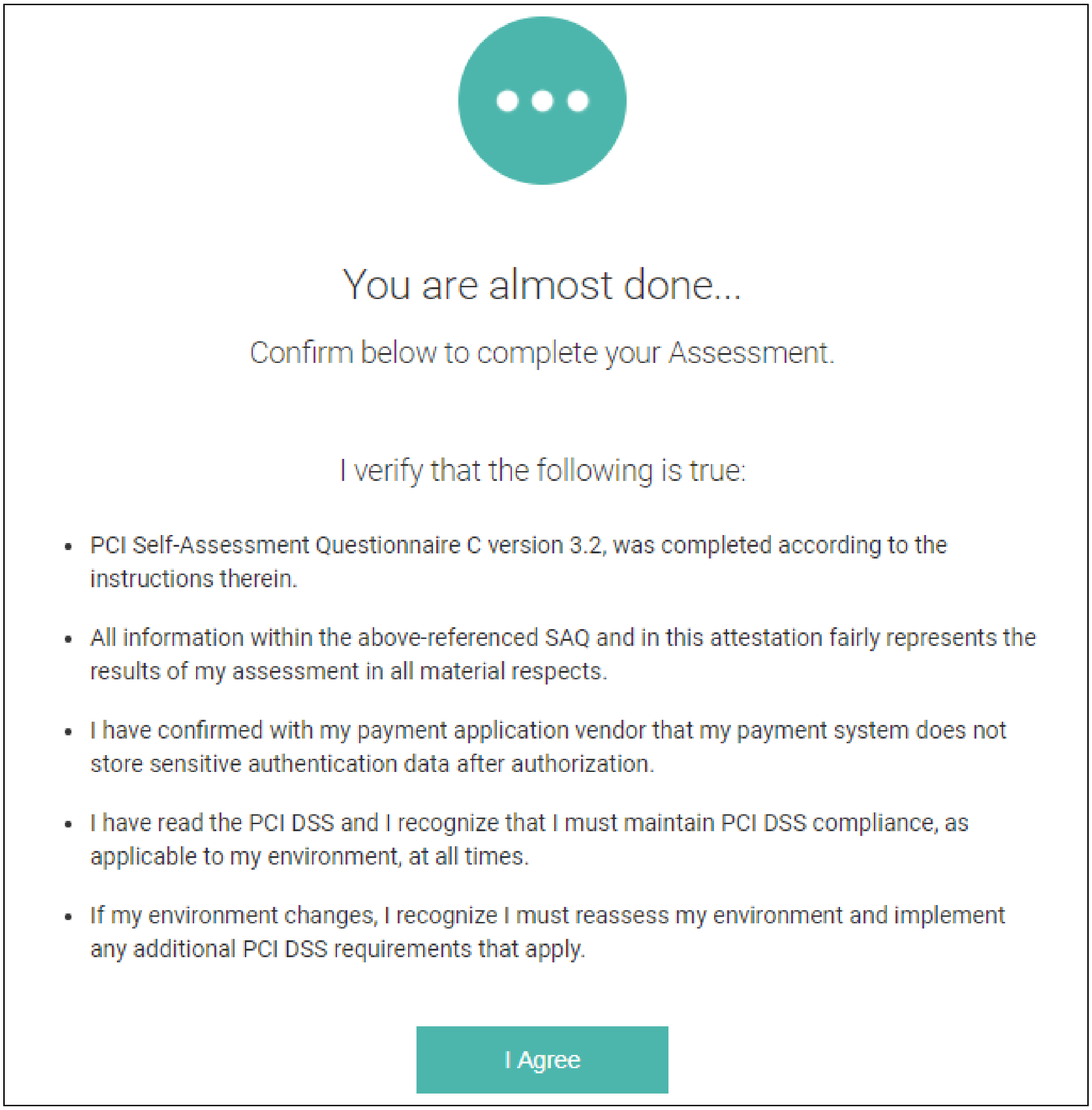
Card present, processed via the software, and no cardholder data is stored within the local system.

Please choose a range for the approximate number of transactions per year (estimates will not impact compliance).

0-20,000 ▾

- Explain how you accept, process, and store cardholder data.
- Select the # of transactions per year.
- Click the Next button to proceed to the Assessment acknowledgement page.

Assessment Acknowledgement



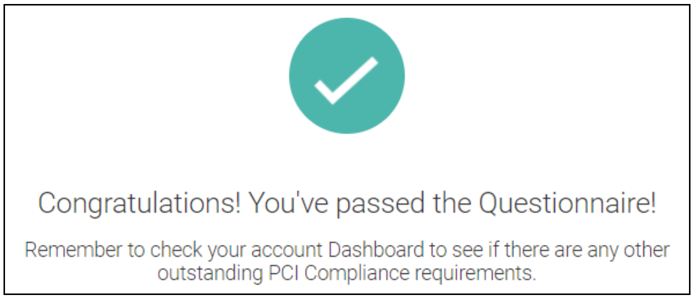
You are almost done...

Confirm below to complete your Assessment.

I verify that the following is true:

- PCI Self-Assessment Questionnaire C version 3.2, was completed according to the instructions therein.
- All information within the above-referenced SAQ and in this attestation fairly represents the results of my assessment in all material respects.
- I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
- I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
- If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.

Click “I Agree” and you will have completed your SAQ!



Congratulations! You've passed the Questionnaire!

Remember to check your account Dashboard to see if there are any other outstanding PCI Compliance requirements.