

## Trustwave SAQ A “Wizard” Level Guidance

Rev 11/11/16

**SAQ A** is *only* applicable for merchants who accept credit cards online where customers enter their credit card info on a 3<sup>rd</sup> party payment gateway (Nelnet, Authorize.net, etc.) web page for processing. Merchant **never** receives, processes, transmits or stores full credit card data: 16-digit card number or 3 or 4 digit CVC number. Contact UM Treasury for assistance if this doesn't apply to your situation.

You should see one of the two screens below. If your *merchant account is new*, you should see the screen to the left. If you are *renewing the SAQ for this year*, you should see the screen to the right or Screen 3 (two pages below).

### Screen 1 – SAQ for a brand new merchant account

#### Registration

You will arrive at the Trustwave website from the Trustwave email invitation link. Registration is a one-time occurrence for the merchant account. Look for **red text** for UM Treasury guidance. **Red** outlined boxes require entry.

Enter data on the right side of screen and click “Continue>>.”

**These fields should be pre-filled**

**Complete these fields**

Company Name: \* Mcard  
Merchant ID: \* 123456789  
Country: \* United States of America  
ZIP/Postal Code: \* 48109

Authorized Contact  
Primary Contact:  This is for the actual PCI certification user, who will be the primary person contacting support.  
First Name:   
Last Name:   
Email:   
Phone Number:

**Continue >>**

### Screen 1 – Renewing the annual SAQ

After logging in, you'll see the “PCI Home” screen. Simply click “Start” to begin.

Trustwave TrustKeeper

PCI Manager | PCI Home | Merchant Profile | Documents | Trusted Commerce | User Management

no system notifications

**Click “Start”**

PCI Certification Status

PCI Self-Assessment  
Summary | History & Documents  
Recent: 2016-02-09 ✓

Trusted Commerce Seal  
Placing this seal on your website indicates that you are taking steps to secure credit card information.  
More Info

PCI Status  
Next Certification Deadline: 2017-02-09 ✓ **pass**

Certificate of Compliance  
Attestation of Compliance

**Screen 2 – SAQ for a brand new merchant account**

Create a log in. Note: If you have more than one merchant account, you'll need to create separate Trustwave logons (usernames) for each. It's highly recommended that you create answers for the "Security Questions" to assist if you cannot recall your logon created in the future.

Click "Register"

**Screen 2 – Renewing the annual SAQ**

You will either see the screen **below** or the one on the **next page** (Screen 3).

If you see the screen just below,

Do **NOT** select "Express Renewal."\*

Select "Start new Self-Assessment."

Then click "Next" to begin.

\*New PCI compliance requirements/questions are easily missed using "Express Renewal."

## Account Profile

Screen 3

The screenshot shows the Trustwave PCI Manager interface. At the top, there is a blue header with the Trustwave TrustKeeper logo, a PCI shield icon, and a messages icon. Below the header, the navigation menu includes "PCI Manager", "PCI Home", "Merchant Profile", "Scanning", "Security Policy", and "Traini". A notification bubble on the left says "notification history available". The main content area features a red warning message: "Only your customers should be processing credit cards on your website. Your staff *cannot* process credit cards through your website, by phone or in-person for this merchant account. Contact UM Treasury if so." Below this is a survey question: "1 How do you accept credit cards? Select all that apply." There are three selection cards: "Website" (with a checked checkbox and a hand cursor), "Mail/Telephone" (with a telephone icon), and "In Person" (with a card reader icon). A green "Next" button with a red arrow pointing to it is located to the right of the "In Person" card.

Screen 4

Trustwave®  
TrustKeeper™

PCI

messages

PCI Manager

PCI Home Merchant Profile Scan

notification history available

### Tell us about your business

1 How do you accept credit cards? Select all that apply. [Change Answer](#)

Website

**No credit card data should be collected/processed on your website. If so, contact UM Treasury.**

2 Where are credit card numbers collected?

Customers submit payments on my website (i.e. checkout/payment is part of my website).  
<http://www.>

My Website

Customers submit payments at a different web address (i.e. separate website for checkout/payment).

A Third-Party

Screen 5

Trustwave<sup>®</sup>  
TrustKeeper<sup>®</sup>

PCI

messages

**PCI Manager** PCI Home Merchant Profile Sc...

notification history available

## Tell us about your business

1 How do you accept credit cards? Select all that apply. [Change Answer](#)

Website

2 Where are credit card numbers collected? [Change Answer](#)

A Third-Party

**Continue >>**

Screen 6

The screenshot displays the PCI Manager interface. At the top, there is a blue header with the Trustwave TrustKeeper logo, a PCI shield icon, and a messages icon. Below the header is a navigation menu with links for PCI Home, Merchant Profile, Security Policy, Training, Documents, and Trusted Commerce. A notification bubble indicates 'no system notifications'. The main content area features a progress bar with four steps: 1 Overview, 2 Merchant Profile, 3 Business Environment, and 4 Questionnaire. The 'Next Steps' section for the '1 Overview' step is highlighted in green and contains the text 'No input required, just click "Next" below'. The '2 Merchant Profile' step lists 'Contact Info', 'Account Details', and 'Review Merchant IDs'. The '3 Business Environment' step lists 'Products and Payment Applications', 'Web Sites', 'Service Providers', and 'Network Vulnerability Scan Setup (if applicable)'. The '4 Questionnaire' step is described as the largest step and lists 'Choose Express Renewal, if qualified', 'Complete the PCI Self-Assessment Questionnaire, using the PCI Wizard or expert form', and 'Review and Submit your Self-Assessment'. A red arrow points to a green 'Next' button at the bottom right of the progress bar.

Trustwave® TrustKeeper™

PCI

messages

PCI Manager

PCI Home Merchant Profile Security Policy Training Documents Trusted Commerce

no system notifications

Start Over

1 Overview 2 Merchant Profile 3 Business Environment 4 Questionnaire

**Next Steps**

*No input required, just click "Next" below*

- Contact Info
- Account Details
- Review Merchant IDs

- Products and Payment Applications
- Web Sites
- Service Providers
- Network Vulnerability Scan Setup (if applicable)

This is the largest step, where you will:

- Choose Express Renewal, if qualified
- Complete the PCI Self-Assessment Questionnaire, using the PCI Wizard or expert form
- Review and Submit your Self-Assessment

Next

Screen 7

Trustwave TrustKeeper

PCI messages

PCI Manager

PCI Home Merchant Profile Scanning Security Policy Training Documents Trusted Commerce

notification history available

Start Over 1 Overview 2 Merchant Profile 3 Business Environment 4 Questionnaire

Account Details > Status Reporting

**General Info** Example of a test account below

Company: TO test acct A

Industry: \* Education/University Enter your data

Primary Contact: \* matt deseck[To test acct a]

Secondary Contact: Please Select...

Mailing Address: \* 3003 s state st

City: \* ann arbor

Country: \* United States of America

State: \* Michigan

ZIP/Postal Code: \* 48109

**Additional Info** Select no for both

**Service Providers** \*

Does your company have a relationship with one or more third-party service providers (e.g. gateways, web-hosting companies, airline booking agents, loyalty program agents, etc.)?

Yes  No

**Multiple Acquirers** \*

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

Yes  No

Previous Next

Screen 8

Trustwave TrustKeeper

PCI messages

PCI Manager

PCI Home Merchant Profile Scanning Security Policy Training Documents Trusted Commerce

notification history available

Start Over 1 Overview 2 Merchant Profile 3 Business Environment 4 Questionnaire

Account Details > Status Reporting

### PCI Assessment and Status Reporting

PCI Program: DEMO University of Michigan ?

Included in this Account:

Merchant ID	Primary
123456780	✓

No input required. Click "Next"

Previous Next

Screen 9

The screenshot shows the PCI Manager interface. At the top, there is a blue header with the Trustwave TrustKeeper logo, a PCI shield icon, and a messages icon. Below the header is a navigation bar with links for PCI Home, Merchant Profile, Scanning, Documents, and Trusted Co. A notification bubble indicates 'no system notifications'. A progress bar shows four steps: 1 Overview, 2 Merchant Profile, 3 Business Environment (current step), and 4 Questionnaire. The breadcrumb trail is 'Card Acceptance > Web Sites > Service Providers'. The main content area is titled 'Verify Your Card Acceptance Information' and contains the following information:

<b>In Person Purchases</b>	No
<b>Mail or Telephone Orders</b>	No
<b>Website Orders</b>	Yes
<b>Other Details</b>	Your web site redirects customers to a third-party (service provider) to take credit cards from customers and process payments. Your customers never enter credit card numbers on your own web site directly.

Below the information, there is a red text instruction: 'Simply click "Next"'. At the bottom right, there are three buttons: 'Previous', 'Change', and 'Next'. A red arrow points to the 'Next' button, which is highlighted in green.

Screen 10

Trustwave®  
TrustKeeper™

PCI

messages

**PCI Manager**    PCI Home    Merchant Profile    Scanning    Security Policy    Training    Documents    Trusted Commerce

notification history available

Start Over    1 Overview    2 Merchant Profile    **3 Business Environment**    4 Questionnaire

Card Acceptance > **Web Sites** > Service Providers

### Web Sites

List all web sites where customers can make purchases from your business.

Domain Name	Added By

**Add Web Site**    Add your website address.

Previous    **Next**

Screen 11

The screenshot displays the Trustwave TrustKeeper PCI Manager interface. The top navigation bar includes the TrustKeeper logo, a PCI shield icon, and a messages icon. Below this, the 'PCI Manager' title is followed by navigation tabs: PCI Home, Merchant Profile, Scanning, Security Policy, Training, Documents, and Trusted Commerce. A notification banner indicates 'notification history available'. A progress bar shows four steps: 1 Overview, 2 Merchant Profile, 3 Business Environment (current), and 4 Questionnaire. The main content area is titled 'Web Sites' and includes the instruction 'List all web sites where customers can make purchases from your business.' Below this is a table with columns 'Domain Name' and 'Added By'. A green 'Add Web Site' button is located below the table. A modal dialog is open in the foreground, titled 'Add Domain Name' with a red subtitle 'It can be your website's home page URL'. The dialog contains a text input field with the value 'example: www.treasury.umich.edu' and two buttons: 'Cancel' and 'Save'. A red arrow points to the 'Save' button.

Screen 12

Trustwave TrustKeeper

PCI Home Merchant Profile Scanning Security Policy Training Documents Trusted Commerce

notification history available

Start Over 1 Overview 2 Merchant Profile 3 Business Environment 4 Questionnaire

Card Acceptance > Web Sites > Service Providers

### Web Sites

List all web sites where customers can make purchases from your business.

Domain Name	Added By
www.treasury.umich.edu	To test acct a

If you have additional web sites, click "Add Web Site" to include them. Otherwise click "Next"

Add Web Site

Previous Next

Screen 13

Trustwave TrustKeeper

PCI messages

PCI Manager

PCI Home Merchant Profile Scanning Security Policy Training Documents Trusted Commerce

notification history available

Start Over 1 Overview 2 Merchant Profile 3 Business Environment 4 Questionnaire

Card Acceptance > Web Sites > Service Providers

### Service Providers

Identify any service providers you use either to host your web site or to handle the credit card processing from web site or mail/telephone orders.

Service Provider	Services	Added By	Severity

You are not required to enter service providers at this time.

Add Service Provider  I don't use any service providers for my mail/telephone orders or to process my web site orders.

Previous Next

**SAQ Completion Selection** (If you see the following screen regarding *'Express Renewal,'* select *'Start a new Self-Assessment'*. Otherwise see next page.)

Screen 14

The screenshot displays the Trustwave PCI Manager interface. At the top, there is a blue header with the Trustwave TrustKeeper logo and a 'messages' icon. Below the header, a navigation bar includes 'PCI Manager' and several menu items: 'PCI Home', 'Merchant Profile', 'Documents', 'Trusted Commerce', and 'User Management'. A notification area shows 'no system notifications'. A progress bar indicates the current step is '4 Questionnaire'.

The main content area is titled 'Express Renewal Option > ...'. It features two radio button options:

- Express Renewal Recommended**  
Choose this option to reload your Self-Assessment Questionnaire from last year, to easily update what has changed for this year.
- Start new Self-Assessment**

The 'Express Renewal Recommended' option is crossed out with a large red 'X'. The 'Start new Self-Assessment' option is circled in red. To the right, a diagram titled 'Last Year's Assessment' shows a stack of documents with checkmarks, an arrow pointing to a 'PCI Compliant' badge, and another arrow pointing to a stack of documents. At the bottom right, there are 'Previous' and 'Next' buttons, with a red arrow pointing to the 'Next' button.

Screen 15

Click on the **Step-By-Step** button.

The screenshot shows the Trustwave PCI Manager interface. At the top, there is a blue header with the Trustwave TrustKeeper logo, a PCI shield icon, and a messages icon. Below the header is a navigation bar with links for PCI Home, Merchant Profile, Scanning, Security Policy, Training, Documents, and Trusted Commerce. A notification banner indicates that notification history is available. A progress bar shows four steps: 1 Overview, 2 Merchant Profile, 3 Business Environment, and 4 Questionnaire. The current step is 4 Questionnaire. Below the progress bar, there is a section titled "Wizard Option" with two radio button options. The first option, "Step-By-Step Recommended", is selected and includes a text box stating: "I'd like to simplify completing the certification process. Take me to the step-by-step PCI Wizard:". To the right of this option are three wizard icons labeled Step 1 (Name, Email), Step 2 (Scan Wizard, Start Scan), and Step 3 (PCI Wizard, SAQ). The second option, "Expert Level Form", is unselected and includes the text: "I understand the requirements of PCI DSS and I know which SAQ to complete. Skip the Wizard." To the right of this option is a preview of a "PCI DSS Questions" form with a yellow pencil icon. At the bottom right, there are "Previous" and "Next" buttons, with a red arrow pointing to the "Next" button.

## SAQ A version 3.2

Screen 16

**Tip:** Be sure to click on the gray circled “?” for helpful clarifications to each question.

The screenshot shows the Trustwave PCI Manager interface. At the top, there is a blue header with the Trustwave TrustKeeper logo, a PCI shield icon, and a messages icon. Below the header, there is a navigation bar with links for PCI Home, Merchant Profile, Scanning, Security Policy, and Training. A notification banner indicates that notification history is available. A progress bar shows four steps: 1 Overview, 2 Merchant Profile, 3 Business Environment, and 4 Questionnaire. The current step is 4 Questionnaire. Below the progress bar, there is a breadcrumb trail: Wizard Option > Card Data Storage & Processing > PCI Wizard > Self-Assessment Questionnaire Form.

The main content area is titled "Card Data Storage & Processing". It contains a section for "Credit Card Data Storage" with a question mark icon and a red warning: "Cannot accept, transmit or store full card # or CVC digits". The question is "Does your business store any sensitive credit card data electronically?". There are five radio button options: "Yes, my website stores credit card data.", "Yes, I store credit card data in a computer.", "Yes, I receive credit card data from a third-party in electronic format.", "Yes, I store credit card data in some other way.", and "None of the above - I never store credit card data." The "None of the above" option is selected with a green checkmark. A red arrow points to the "Next >>" button. To the right of the question, there is a red note: "Contact Treasury if you are able to answer 'Yes' to any of these questions." Below the "None of the above" option, there is a red note: "Standard answer".

Screen 17

The screenshot shows the Trustwave PCI Manager interface. At the top, there is a blue header with the Trustwave TrustKeeper logo, a PCI shield icon, and a messages icon. Below the header is a navigation bar with links for PCI Home, Merchant Profile, Scanning, Security Policy, and Training. A notification banner indicates that notification history is available. A progress bar shows four steps: Start Over, 1 Overview, 2 Merchant Profile, 3 Business Environment, and 4 Questionnaire. The current step is 4 Questionnaire, and the breadcrumb trail is Wizard Option > Card Data Storage & Processing > PCI Wizard > Self-Assessment Questionnaire Form.

### Card Data Storage & Processing

**Website Control**  **Click here for details**

Does your business have administrative control over any part of your website?

Yes **Select if you can modify/control any part of your website. Standard answer**

No - a third-party service provider handles ALL administration.  
**Select "No" if a vendor completely controls/modifies your website on your behalf.**

**Next >>**

The screenshot shows the Trustwave PCI Manager interface. At the top, there is a blue header with the Trustwave TrustKeeper logo, a PCI shield icon, and a messages icon. Below the header, the navigation menu includes "PCI Manager", "PCI Home", "Merchant Profile", "Scanning", "Security Policy", and "Training". A notification bubble indicates "notification history available". A progress bar shows four steps: "1 Overview", "2 Merchant Profile", "3 Business Environment", and "4 Questionnaire". The breadcrumb trail reads: "Wizard Option > Card Data Storage & Processing > PCI Wizard > Self-Assessment Questionnaire Form".

## Card Data Storage & Processing

### Payment Handling

When customers make purchases on your website, where is the credit card data submitted?

- Directly to a third-party; my website NEVER receives the credit card data. **Standard answer**
- My website receives the credit card data first then sends it on for processing.  
**Contact Treasury if you collect credit card data on your website**

Navigation buttons: << Previous, Next >> (with a red arrow pointing to the "Next >>" button)

Trustwave®  
TrustKeeper™

PCI

messages

**PCI Manager**    PCI Home    Merchant Profile    Scanning    Security Policy    Training

notification history available

Start Over ↻    1 Overview    2 Merchant Profile    3 Business Environment    **4 Questionnaire**

Wizard Option > **Card Data Storage & Processing** > PCI Wizard > Self-Assessment Questionnaire Form

## Card Data Storage & Processing

### Checkout Page

Do the web servers you administer have control over the payment page that is presented to your customers?

No - the payment page comes ENTIRELY from the third-party. **Standard answer**

Yes - some or all of the payment page is generated from my website

**Contact Treasury if "Yes" is applicable.**

<< Previous    **Next >>**

Screen 20

The screenshot displays the Trustwave PCI Manager interface. At the top, there is a blue header with the Trustwave TrustKeeper logo, a PCI shield icon, and a messages icon. Below the header, a navigation bar includes 'PCI Manager' and links for 'PCI Home', 'Merchant Profile', 'Scanning', 'Security Policy', and 'Training'. A notification bubble indicates 'notification history available'. A progress bar shows four steps: '1 Overview', '2 Merchant Profile', '3 Business Environment', and '4 Questionnaire', with '4 Questionnaire' being the active step. Below the progress bar, a breadcrumb trail reads: 'Wizard Option > Card Data Storage & Processing > PCI Wizard > Self-Assessment Questionnaire Form'. The main content area features a green checkmark icon and the heading 'Card Data Storage & Processing'. Below this, a red text message states 'No entry required. Click "continue"'. A circular icon with a green checkmark is followed by the text 'Section Completed!' and 'You have successfully completed this section and passed.'. At the bottom left, a red arrow points to a 'continue >>' button, which is being clicked by a mouse cursor.

Screen 21

Trustwave®  
TrustKeeper®

PCI

messages

**PCI Manager**   PCI Home   Merchant Profile   Scanning   Security Policy   Training   Documents   Trusted Commerce

notification history available

Start Over   1 Overview   2 Merchant Profile   3 Business Environment   **4 Questionnaire**

Wizard Option > Card Data Storage & Processing > **PCI Wizard** > Self-Assessment Questionnaire Form

**Physical Security**   **Begin**

**Security Policies**   **Begin**

Screen 22

The screenshot displays the Trustwave PCI Manager interface. At the top, there is a blue header with the Trustwave TrustKeeper logo, a PCI shield icon, and a messages icon. Below the header is a navigation bar with links for PCI Home, Merchant Profile, Scanning, Security Policy, Training, and Documentation. A notification bubble indicates that notification history is available. A progress bar shows four steps: 1 Overview, 2 Merchant Profile, 3 Business Environment, and 4 Questionnaire (the current step). The breadcrumb trail reads: Wizard Option > Card Data Storage & Processing > PCI Wizard > Self-Assessment Questionnaire Form.

The main content area is titled "Physical Security" and contains a question: "Paper Documents with Credit Card Data". An information icon (i) next to the question title has a red arrow pointing to it with the text "Click here for details". The question asks: "Does your business have or receive any paper documents containing full credit card numbers (see help for examples)?" There are two radio button options: "Yes" (with a note that "Yes" requires Treasurer's written exception) and "No" (with a note that "No" is the standard answer). The "No" option is selected. At the bottom of the question area are "Previous" and "Next" buttons, with a red arrow pointing to the "Next" button.

Below the question area is a section titled "Security Policies".

Screen 23

The screenshot displays the Trustwave TrustKeeper PCI Manager interface. At the top, there is a blue header with the TrustKeeper logo, a PCI shield icon, and a messages icon. Below the header is a navigation menu with options: PCI Manager, PCI Home, Merchant Profile, Scanning, Security Policy, Training, Documents, and Trusted Commerce. A notification bubble indicates 'notification history available'. A progress bar shows four steps: 1 Overview, 2 Merchant Profile, 3 Business Environment, and 4 Questionnaire (highlighted). Below the progress bar is a breadcrumb trail: Wizard Option > Card Data Storage & Processing > PCI Wizard > Self-Assessment Questionnaire Form.

The main content area features a light blue box with a green checkmark icon and the heading 'Physical Security'. Below this, it states 'No entry required. Click "continue"'. A circular icon with a green checkmark is followed by the text 'Section Completed! You have successfully completed this section and passed.' At the bottom left of this box, a red arrow points to a 'continue >>' button. A 'Close' button is located in the top right corner of the box.

Below the 'Physical Security' box is another light blue box with the heading 'Security Policies' and a 'Begin' button in the top right corner.

Screen 24

The screenshot shows the Trustwave TrustKeeper PCI Manager interface. At the top, there is a blue header with the Trustwave TrustKeeper logo, a PCI shield icon, and a messages icon. Below the header is a navigation menu with items: PCI Manager, PCI Home, Merchant Profile, Scanning, Security Policy, Training, Documents, and Trusted Commerce. A notification banner indicates "notification history available". A progress bar shows four steps: 1 Overview, 2 Merchant Profile, 3 Business Environment, and 4 Questionnaire (highlighted). Below the progress bar is a breadcrumb trail: Wizard Option > Card Data Storage & Processing > PCI Wizard > Self-Assessment Questionnaire Form.

The main content area is titled "Physical Security" with a green checkmark icon and a "Review Q & A" button. Below this is a section titled "Security Policies" with a "Save & Close" button. The first policy is "Sharing Card Data with Third-Parties" with an information icon. A red arrow points to the information icon with the text "Click here for details". The question text is "Are there any third-party companies with whom you share any credit card data, or who could affect the security of the credit card data?". There are two radio button options: "Yes" and "No". The "No" option is selected, and a red arrow points to it with the text "Standard answer". At the bottom of the form, there are two buttons: "<< Previous" and "Next >>". A red arrow points to the "Next >>" button.

Screen 25

The screenshot shows the Trustwave TrustKeeper PCI Manager interface. At the top, there is a blue header with the TrustKeeper logo, a PCI shield icon, and a messages icon. Below the header, a navigation bar includes 'PCI Manager', 'PCI Home', 'Merchant Profile', 'Scanning', 'Documents', and 'Trusted Commerce'. A notification area shows 'no system notifications'. A progress bar indicates the current step is '4 Questionnaire', with previous steps being '1 Overview', '2 Merchant Profile', and '3 Business Environment'. A breadcrumb trail reads: 'Express Renewal Option > Wizard Option > Card Data Storage & Processing > PCI Wizard > Self-Assessment Questionnaire Form'. The main content area is titled 'Physical Security' and contains a section for 'Security Policies'. The first policy is 'Maintain Written Security Policies', which includes a question: 'Do you have written security policies and procedures that address the protection of paper with credit card numbers such as receipts and the physical security of your card processing device?'. The 'Yes' radio button is selected. A 'To Do List' on the right shows 'No tasks in your To Do List'. A 'Failure to comply with these policies may result in disciplinary action including termination.' warning is displayed. A red annotation states: 'All employees are bound by SPGs' and 'SPG 601.27 Info Security Policy' and 'SPG 601.7 Proper Use of Info Resources, Info Tech & Networks'. Another red annotation says: 'This should be in your internal controls written procedures.' A hand cursor is pointing at the 'Next >>' button.

**All employees are bound by SPGs**

**SPG 601.27 Info Security Policy**

**SPG 601.7 Proper Use of Info Resources, Info Tech & Networks**

**Failure to comply with these policies may result in disciplinary action including termination.**

**This should be in your internal controls written procedures.**

The screenshot shows the Trustwave TrustKeeper PCI Manager interface. At the top, there is a blue header with the TrustKeeper logo, a PCI shield icon, and a messages icon. Below the header is a navigation bar with links for PCI Home, Merchant Profile, Security Policy, Training, and Documents. A notification bubble indicates "no system notifications". A progress bar shows four steps: Start Over, 1 Overview, 2 Merchant Profile, 3 Business Environment, and 4 Questionnaire. The current step is "PCI Wizard" under "Self-Assessment Questionnaire Form".

The main content area is titled "Physical Security" with a green checkmark and a "Review Q & A" button. Below this is the "Security Policies" section with a "Save & Close" button. The question is "Define Security Responsibilities" with an information icon: "Does your security policy clearly define responsibilities regarding protecting credit card data for all employees and contractors?". There are two radio button options: "Yes" (selected) and "No". A red text note states: "This should be in your internal controls written procedures". At the bottom, there are "Previous" and "Next" navigation buttons, with a red arrow pointing to the "Next" button.

Screen 27

The screenshot displays the Trustwave PCI Manager interface. At the top, there is a blue header with the Trustwave TrustKeeper logo, a PCI shield icon, and a messages icon. Below the header is a navigation bar with links for PCI Home, Merchant Profile, Security Policy, Training, and Documents. A notification area shows "no system notifications". A progress bar indicates the current step is "4 Questionnaire", with previous steps being "1 Overview", "2 Merchant Profile", and "3 Business Environment". A breadcrumb trail shows the path: Wizard Option > Card Data Storage & Processing > PCI Wizard > Self-Assessment Questionnaire Form.

The main content area is titled "Physical Security" with a green checkmark icon and a "Review Q & A" button. Below this is a section titled "Security Policies" with a "Save & Close" button. The section contains a heading "Review Security Policies Annually" with an information icon. The question is: "Do you review and modify your policies at least once a year or any time you make a change to your business environment?". There are two radio button options: "Yes" (selected) and "No". A red text box on the right states: "Your internal controls written procedures and gap analysis should be reviewed and updated at least annually." At the bottom, there are two buttons: "<< Previous" and "Next >>". A red arrow points to the "Next >>" button, which is being clicked by a mouse cursor.

The screenshot shows the Trustwave TrustKeeper PCI Manager interface. At the top, there is a blue header with the TrustKeeper logo, a PCI shield icon, and a messages icon. Below the header, a navigation bar includes 'PCI Manager', 'PCI Home', 'Merchant Profile', 'Security Policy', 'Training', and 'Docume'. A notification area shows 'no system notifications'. A progress bar indicates the current step is '4 Questionnaire', with previous steps '1 Overview', '2 Merchant Profile', and '3 Business Environment'. The breadcrumb trail reads: 'Wizard Option > Card Data Storage & Processing > PCI Wizard > Self-Assessment Questionnaire Form'.

The main content area is divided into two sections:

- Physical Security** (marked with a green checkmark) with a 'Review Q & A' button.
- Security Policies** (marked with a yellow warning triangle) with a 'Save & Close' button.

Under 'Security Policies', the 'Computer and Device Usage' section is highlighted with a red arrow pointing to an information icon. A red arrow also points to the text 'Click here for details' above the information icon. The text below reads: 'Do your written policies and procedures cover the use of technology as follows (check all that apply):'

- Require explicit approval by authorized parties to use the technologies
- Maintain a list of all such devices and personnel with access
- Specify locations the technology can be used and a description of acceptable business usage
- None of the above

Red text on the right side of the list states: 'Covered by SPG 601.07'. Below the list, a blue note reads: 'NOTE: for most merchants, these are not applicable. However, N/A is not an option and selecting "None of the above" will cause the SAQ to fail. Please check the 3 boxes as shown.' At the bottom of the section, there are 'Previous' and 'Next' buttons, with a red arrow pointing to the 'Next' button.

Screen 29

The screenshot shows the Trustwave PCI Manager interface. At the top, there is a blue header with the Trustwave TrustKeeper logo, a PCI shield icon, and a messages icon. Below the header is a navigation bar with links for PCI Home, Merchant Profile, Security Policy, Training, and Documents. A notification bubble indicates "no system notifications". A progress bar shows four steps: 1 Overview, 2 Merchant Profile, 3 Business Environment, and 4 Questionnaire (highlighted in green). Below the progress bar is a breadcrumb trail: Wizard Option > Card Data Storage & Processing > PCI Wizard > Self-Assessment Questionnaire Form.

The main content area is titled "Physical Security" with a green checkmark icon and a "Review Q & A" button. Below this is a section titled "Security Policies" with a "Save & Close" button. The first policy is "Maintain an Incident Response Plan" with an information icon. The question asks: "In the event of a compromise to customer credit card numbers or to your card processing device, do you have a formal plan on how to respond, including notification of the appropriate law enforcement agency, your merchant bank, and the various card associations?". There are two radio buttons: "Yes" (selected) and "No". A red text box contains the instruction: "As a merchant your initial responsibility is to contact Treasury 763-1299 immediately. If necessary, Treasury will provide additional instructions." At the bottom, there are two buttons: "<< Previous" and "Next >>". A red arrow points to the "Next >>" button, which is being clicked by a mouse cursor.

Screen 30

Trustwave TrustKeeper

PCI Manager

PCI Home Merchant Profile Scanning Security Policy Training Documents Trusted Commerce

notification history available

Start Over 1 Overview 2 Merchant Profile 3 Business Environment 4 Questionnaire

Wizard Option > Card Data Storage & Processing > PCI Wizard > Self-Assessment Questionnaire Form

**Congratulations! PCI Wizard successfully completed.**  
[Click here to complete the submission process](#)

Physical Security Review Q & A

Security Policies Close

**Section Completed!**  
You have successfully completed this section and passed.  
continue >>

**No entry required. Click "Next"**

**Almost Finished! You have successfully completed the PCI Wizard.**  
Click the "Next" button below to review the PCI Certification form and complete the submission process.  
Click "Cancel" to remain on this page.

Cancel Next

Screen 31

There are 8 new PCI version 3.2 questions Trustwave hasn't integrated into the questionnaire, so follow along to now answer them.

Trustwave TrustKeeper

PCI

messages

umtre

PCI Manager

PCI Home Merchant Profile Scanning Documents Trusted Commerce User Management

no system notifications

Contact Support

Start Over

1 Overview 2 Merchant Profile 3 Business Environment 4 Questionnaire

Express Renewal Option > Wizard Option > Card Data Storage & Processing > PCI Wizard > Self-Assessment Questionnaire Form

PCI SAQ A 3.2

Please answer any remaining questions to complete the PCI process.

### Eligibility

Merchant certifies eligibility to complete this shortened version of the Self-Assessment Questionnaire because, for this payment channel:

- Merchant accepts only card-not-present (e-commerce or mail/telephone-order) transactions);  
**NOTE:** The blue answer is recommended based on your profile.
- All processing of cardholder data is entirely outsourced to PCI DSS validated third-party service providers;  
**NOTE:** The answer in blue is based on your responses to a wizard question: Card Data Storage & Processing
- Merchant does not electronically store, process, or transmit any cardholder data on merchant systems or premises, but relies entirely on a third party(s) to handle all these functions;  
**NOTE:** The answer in blue is based on your responses to a wizard question: Card Data Storage & Processing
- Merchant has confirmed that all third party(s) handling storage, processing, and/or transmission of cardholder data are PCI DSS compliant; and
- Merchant retains only paper reports or receipts with cardholder data electronically.  
**NOTE:** The answer in blue is based on your responses to a wizard question: Card Data Storage & Processing
- Additionally, for e-commerce channels:  
The entirety of all payment pages delivered to the consumer's browser originates directly from a third-party PCI DSS validated service provider(s).  
**NOTE:** The answer in blue is based on your responses to a wizard question: Card Data Storage & Processing

Save for later

<< Previous Section Next Section >>

### Sections Completed

- Eligibility
- System Settings
- Account Security
- Physical Access Controls
- Security Policies and Procedures

Acknowledge & Submit

Be sure to continual verify that your vendor is PCI compliant.  
Contact the Treasurer's Office if the vendor becomes noncompliant.

Screen 32

Click the two **Yes** buttons and then click the **'Next Section'** button at the bottom.

- Please be sure all staff do not use vendor supplied logons.
- There should not be any shared logons.
- If someone leaves, ensure that person's logon is disabled as soon as possible.

[Express Renewal Option](#) > [Wizard Option](#) > [Card Data Storage & Processing](#) > [PCI Wizard](#) > **Self-Assessment Q**

**PCI SAQ A 3.2**

Please answer any remaining questions to complete the PCI process.



### System Settings

Unanswered  All

No.	Question	Yes	No	N/A
2.1 (a)	Are vendor-supplied defaults always changed before installing a system on the network? <i>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, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.).</i>	<b>Yes</b>	No	N/A
2.1 (b)	Are unnecessary default accounts removed or disabled before installing a system on the network?	<b>Yes</b>	No	N/A

[Save for later](#) [<< Previous Section](#) [Next Section >>](#)

Screen 33

If you adhere to the five questions below, click the **Yes** buttons and then click the **'Acknowledge & Submit'** button. The next screen should be screen 31 in the Trustwave SAQ A Wizard Level Guidance PDF.

 **You have completed the PCI SAQ A 3.2**  
Please click **Acknowledge and Submit** to complete the form.

 **Account Security** **You should be able to answer 'Yes' to all.**

No. Question  Unanswered  All

**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:**

8.1.1	Are all users assigned a unique ID before allowing them to access system components or cardholder data?	<input checked="" type="button" value="Yes"/>	<input type="button" value="No"/>	<input type="button" value="N/A"/>
8.1.3	Is access for any terminated users immediately deactivated or removed?	<input checked="" type="button" value="Yes"/>	<input type="button" value="No"/>	<input type="button" value="N/A"/>
8.2	In addition to assigning a unique ID, is one or more of the following methods employed to authenticate all users? <ul style="list-style-type: none"><li>Something you know, such as a password or passphrase</li><li>Something you have, such as a token device or smart card</li><li>Something you are, such as a biometric</li></ul>	<input checked="" type="button" value="Yes"/>	<input type="button" value="No"/>	<input type="button" value="N/A"/>
8.2.3 (a)	Are user password parameters configured to require passwords/passphrases meet the following? <ul style="list-style-type: none"><li>A minimum password length of at least seven characters</li><li>Contain both numeric and alphabetic characters</li></ul> Alternatively, the passwords/passphrases must have complexity and strength at least equivalent to the parameters specified above.	<input checked="" type="button" value="Yes"/>	<input type="button" value="No"/>	<input type="button" value="N/A"/>
8.5	Are group, shared, or generic accounts, passwords, or other authentication methods prohibited as follows: <ul style="list-style-type: none"><li>Generic user IDs and accounts are disabled or removed;</li><li>Shared user IDs for system administration activities and other critical functions do not exist; and</li><li>Shared and generic user IDs are not used to administer any system components?</li></ul>	<input checked="" type="button" value="Yes"/>	<input type="button" value="No"/>	<input type="button" value="N/A"/>

**Sections Completed**

- Eligibility
- System Settings
- Account Security**
- Physical Access Controls
- Security Policies and Procedures

**Acknowledge & Submit** 

**Save for later** **<< Previous Section** **Next Section >>**

**After answering the 5 questions, click the 'Acknowledge & Submit' button**

Screen 34

1 Overview > 2 Merchant Profile > 3 Business Environment > **4 Questionnaire** >

Wizard Option > Wizard Option > Card Data Storage & Processing > PCI Wizard > **Self-Assessment Questionnaire Form**

### Confirmation of Compliant Status

**Verify Statements:**

- PCI DSS Self-Assessment Questionnaire A, 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 read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times. ([https://www.pcisecuritystandards.org/security\\_standards/documents.php](https://www.pcisecuritystandards.org/security_standards/documents.php))
- If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.
- No evidence of full track data[1], CAV2, CVC2, CID, or CVV2 data[2], or PIN data[3] storage after transaction authorization was found on ANY system reviewed during this assessment.
  1. Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full track data after transaction authorization. The only elements of track data that may be retained are primary account number (PAN), expiration date, and cardholder name.
  2. The three- or four-digit value printed by the signature panel or on the face of a payment card used to verify card-not-present transactions.
  3. Personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.

**Remember that this questionnaire is completed annually but the merchant contact is responsible for ensuring PCI compliance is adhered to at all times!**

### Merchant Acknowledgement

Merchant Company: Univ of Michigan Event

Sign:  I am hereby signing and intend to authenticate this document.

Title: Merchant Contact Title

Merchant Executive Officer: Merch Contact Name

Today's Date: 11/11/16

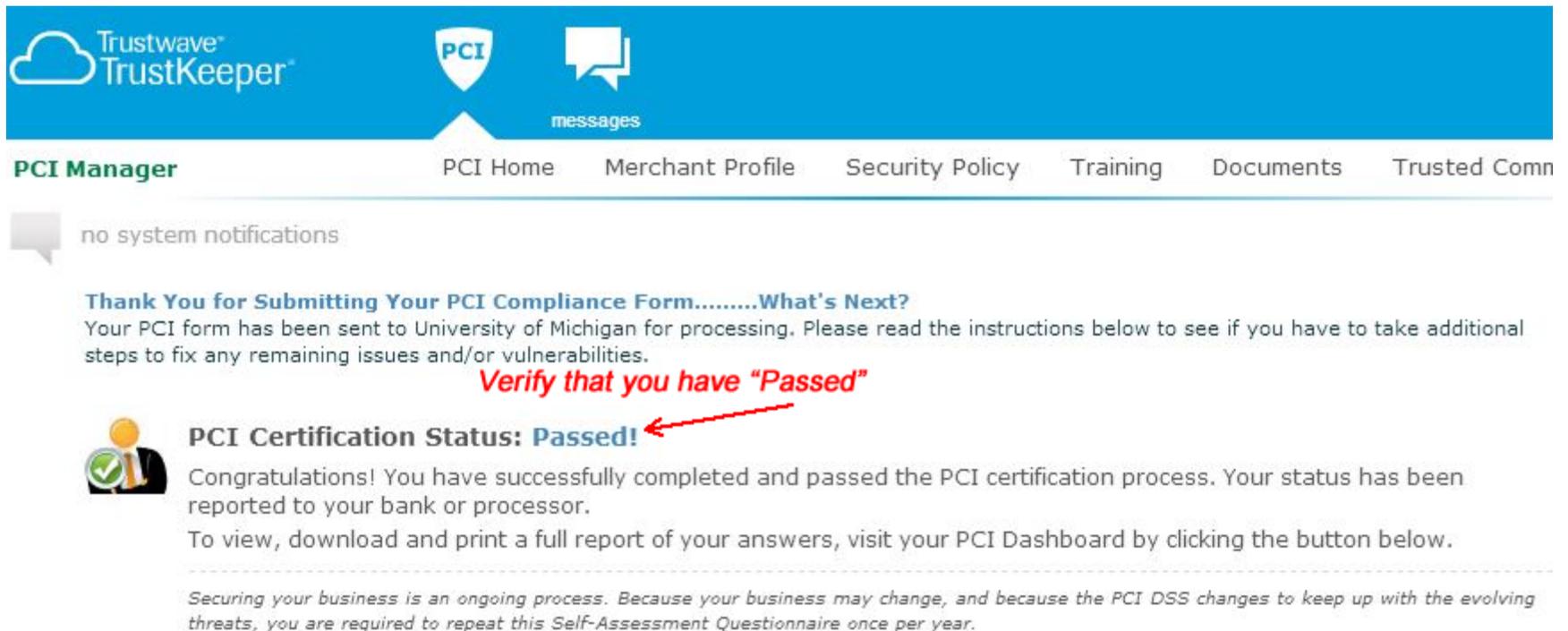
**Copies of this SAQ will be available to the Department Budget Administrator, Treasurer's Office, Internal Controls and University Audit.**

<< Cancel Submit

## SAQ Completion

Screen 35

If you did not pass, the screen should indicate which question(s) were incorrect. If you simply answered incorrectly, go back and change your answer. If you answered incorrectly due to how you process credit cards, you will need to change your method(s) prior to correcting your answer.



The screenshot shows the PCI Manager interface. At the top, there is a blue header with the Trustwave TrustKeeper logo on the left, a PCI shield icon in the center, and a messages icon on the right. Below the header is a navigation bar with links for PCI Home, Merchant Profile, Security Policy, Training, Documents, and Trusted Comm. A notification area shows 'no system notifications'. The main content area features a blue heading: 'Thank You for Submitting Your PCI Compliance Form.....What's Next?'. Below this, a message states: 'Your PCI form has been sent to University of Michigan for processing. Please read the instructions below to see if you have to take additional steps to fix any remaining issues and/or vulnerabilities.' A red arrow points to the text 'Verify that you have "Passed"'. Below this, a green checkmark icon is next to the text 'PCI Certification Status: Passed!'. A red arrow points from the 'Passed!' text to the 'Verify that you have "Passed"' text. Below the status, a message says: 'Congratulations! You have successfully completed and passed the PCI certification process. Your status has been reported to your bank or processor. To view, download and print a full report of your answers, visit your PCI Dashboard by clicking the button below.' At the bottom, a red arrow points to a button labeled 'Visit your PCI Dashboard'.

Trustwave®  
TrustKeeper®

PCI

messages

**PCI Manager**    PCI Home    Merchant Profile    Security Policy    Training    Documents    Trusted Comm

no system notifications

**Thank You for Submitting Your PCI Compliance Form.....What's Next?**  
Your PCI form has been sent to University of Michigan for processing. Please read the instructions below to see if you have to take additional steps to fix any remaining issues and/or vulnerabilities.

*Verify that you have "Passed"*

**PCI Certification Status: Passed!**

Congratulations! You have successfully completed and passed the PCI certification process. Your status has been reported to your bank or processor.  
To view, download and print a full report of your answers, visit your PCI Dashboard by clicking the button below.

*Securing your business is an ongoing process. Because your business may change, and because the PCI DSS changes to keep up with the evolving threats, you are required to repeat this Self-Assessment Questionnaire once per year.*

**Visit your PCI Dashboard**

Screen 36

The screenshot shows the Trustwave TrustKeeper PCI Manager interface. At the top, there's a navigation bar with 'PCI Home', 'Merchant Profile', 'Security Policy', 'Training', 'Documents', and 'Trusted Commerce'. Below this, a notification says 'notification history available' and a 'Contact Support' button is visible. The main section is titled 'PCI Certification Status'. Under 'PCI Self-Assessment', there are tabs for 'Summary' and 'History & Documents'. A table lists the assessment: 'PCI SAQ A 3.2' completed on '2014-11-24' with a green checkmark. A red box highlights the 'SAQ.pdf' link, with a red arrow pointing to it from the text 'Step 2 Click here to save a copy of your completed SAQ.'. To the right, a 'Start' button is present, with a red arrow pointing to it from the text 'Step 3 Click here to save a copy of your completion certification.'. Below the table, the 'PCI Status' is shown as 'pass' with a green checkmark. A 'Next Certification Deadline' of '2015-11-24' is also displayed. On the right side, a sidebar contains 'Trusted Commerce Seal', 'Certificate of Compliance' (with a 'Click Here' link), and 'Attestation of Compliance'. At the bottom right, a large blue message reads 'CONGRATS! You're done with the annual SAQ.'

Remember the PCI compliance SAQ is done annually but *being PCI compliance is done 24/7 365 days.*

Contact UM Treasury [merchantservices@umich.edu](mailto:merchantservices@umich.edu) with any questions.